

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: C. Douglas Yeager
U.S. Patent No.: 8,548,924
Issue Date: October 1, 2013
Appl. Serial No.: 13/403,141
Filing Date: February 23, 2012
Title: SELF-AUTHORIZING TOKEN

DECLARATION OF DR. PATRICK TRAYNOR

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable under Section 1001 of Title 18 of the United States Code.

Date: 18 September 2026

By: 
Patrick G. Traynor

TABLE OF CONTENTS

I.	ASSIGNMENT.....	20
II.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	20
III.	MATERIALS CONSIDERED.....	24
IV.	OVERVIEW OF CONCLUSIONS FORMED	27
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	28
VI.	LEGAL STANDARDS	29
	A. Anticipation.....	30
	B. Obviousness	30
VII.	INTERPRETATIONS OF THE '924 PATENT CLAIMS AT ISSUE.....	34
VIII.	THE '924 PATENT	35
	A. Overview of the '924 Patent	35
	B. Prosecution History.....	37
IX.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '924 PATENT CLAIMS UNPATENTABLE.....	38
	A. GROUND 1A – Huomo-Smets Renders Obvious Claims 1-71 and 76-87 38	
	1. Huomo	38
	2. Smets	42
	3. Huomo-Smets Combination.....	46
	(a) Huomo and Smets are Analogous Art to the '924 Patent	46
	(b) A POSITA would have been Motivated to Combine Huomo and Smets.....	46
	(c) A POSITA would have Reasonably Expected Success when Combining Huomo and Smets	51
	4. Analysis	52
	(a) Claims 60, 79.....	55
	(b) Claims 65, 83.....	74
	(c) Claims 77, 86.....	77
	(d) Claims 1, 10, 22, 31, 40, 52.....	78
	(e) Claims 2, 11, 23, 32, 41, 53, 61, 80.....	86
	(f) Claims 3, 12, 24, 33, 42, 54, 62.....	87

(g) Claims 4, 13, 25, 34, 43, 55, 63, 81.....	88
(h) Claims 5, 26, 35.....	90
(i) Claims 6, 16, 27, 36, 46, 56, 64, 82.....	91
(j) Claims 7, 17, 28, 37, 47, 57, 66, 84.....	91
(k) Claims 8, 19, 29, 38, 49, 58.....	92
(l) Claims 9, 18, 21, 30, 39, 48, 51, 59, 67, 78, 85, 87	93
(m) Claims 14, 44.....	94
(n) Claims 15, 45.....	95
(o) Claims 20, 50.....	96
(p) Claim [76].....	96
(q) Claims 68-69	96
(r) Claim 70	96
(s) Claim 71	97
(t) Claim 76	98
B. GROUND 1B – Huomo-Smets-Kisliakov Renders Obvious Claims 1-71, 76-87	98
1. Kisliakov	98
2. Huomo-Smets-Kisliakov Combination.....	101
3. Analysis	104
(a) Claims 1, 10, 22, 31, 40, 52, 60, 79.....	104
(b) Claims 2, 11, 23, 32, 41, 53, 61, 80.....	104
C. GROUND 2A – Ryan-Abbott Renders Obvious Claims 1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, and 84-86	105
1. Ryan.....	105
2. Abbott.....	110
3. Ryan-Abbott Combination	112
(a) Ryan and Abbott are Analogous Art to the '924 Patent	112
(b) A POSITA would have been Motivated to Combine Ryan and Abbott	113
(c) A POSITA would have Reasonably Expected Success	116
4. Analysis	117
(a) Claims 60, 79.....	117

(b) Claims 77, 86.....	131
(c) Claims 1, 22, 31, 52.....	131
(d) Claims 2, 23, 32, 53, 61, 80.....	134
(e) Claims 4, 25, 34, 55, 63, 81.....	135
(f) Claims 6, 27, 36, 56, 64, 82.....	135
(g) Claims 7, 28, 37, 57, 66, 84.....	135
(h) Claims 8, 29, 38, 58.....	136
(i) Claims 67, 85.....	137
(j) Claims 68, 69.....	138
(k) Claim 70	139
(l) Claim 71	139
(m) Claim 72	139
(n) Claim 73	140
(o) Claim 74	140
(p) Claim 75	141
(q) Claim 76	141
D. GROUND 2B – Ryan-Abbott-Peart Renders Obvious Claims 3, 5, 9-13, 16-19, 21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, and 87	
141	
1. Peart.....	141
2. Ryan-Abbott-Peart Combination.....	142
(a) Peart is Analogous Art to the '924 Patent.....	142
(b) A POSITA would have been Motivated to Combine Ryan-Abbott-Peart	142
(c) A POSITA would have Reasonably Expected Success	147
3. Analysis	147
(a) Claims 10, 40.....	147
(b) Claims 3, 12, 24, 33, 42, 54, 62.....	149
(c) Claims 5, 26, 35.....	150
(d) Claims 9, 18, 21, 30, 39, 48, 51, 59, 78, 87	150
(e) Claims 11 and 41	151
(f) Claims 13 and 43	151

(g)	Claims 16, 46.....	151
(h)	Claims 17, 47.....	151
(i)	Claims 19, 49.....	151
E.	GROUND 2C – Ryan-Abbott-Smets Renders Obvious Claims 65, and 83	152
1.	Ryan-Abbott-Smets Combination.....	152
2.	Analysis	156
(a)	Claims 65, 83.....	156
F.	GROUND 2D – Ryan-Abbott-Peart-Smets Renders Obvious Claims 15, 20, 45, 50.....	157
1.	Analysis	158
(a)	Claims 15, 20, 45, 50.....	158
G.	GROUND 2E/2F – Ryan-Abbott-Smets-Kisliakov Renders Obvious Claims 2, 23, 32, 53, 61, 80 / Ryan-Abbott-Peart-Smets-Kisliakov Renders Obvious Claims 11, 41	158
1.	Ryan-Abbott-Smets-Kisliakov (Ground 2E) / Ryan-Abbott-Peart-Smets-Kisliakov (Ground 2F) Combinations	158
2.	Analysis	160
(a)	Claims 2, 11, 23, 32, 41, 53, 61, 80.....	160
X.	CONCLUSION.....	160

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1.pre]	A token comprising:
[1.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[1.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[1.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and
[1.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.
Claim 2	
[2]	The token of claim 1 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 3	
[3]	The token of claim 1 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 4	
[4]	The token of claim 1 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.

Claim 5	
[5]	The token of claim 1 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.
Claim 6	
[6]	The token of claim 1 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 7	
[7]	The token of claim 1 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 8	
[8.1]	The token of claim 1 wherein: the secure element comprises an executable application; and
[8.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 9	
[9.1]	The token of claim 1 wherein: the secure element comprises a payment card application;
[9.2]	the secure element interrogator is configured to interrogate the payment card application; and
[9.3]	the transaction information comprises card-present data.
Claim 10	
[10.pre]	A token comprising:
[10.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[10.2]	a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;
[10.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of

	transaction data communications only between the secure element and the secure element interrogator; and
[10.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.
Claim 11	
[11]	The token of claim 10 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 12	
[12]	The token of claim 10 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 13	
[13]	The token of claim 10 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.
Claim 14	
[14]	The token of claim 10 wherein the communications controller creates a random unpredictable number and sends it to the secure element.
Claim 15	
[15]	The token of claim 10 wherein the transaction information comprises a dynamic card verification code.
Claim 16	
[16]	The token of claim 10 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 17	
[17]	The token of claim 10 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

Claim 18	
[18]	The token of claim 10 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 19	
[19.1]	The token of claim 10 wherein: the payment card application comprises an executable payment card application; and
[19.2]	the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.
Claim 20	
[20]	The token of claim 19 wherein the executable payment card application includes an application level protocol for authentication of the secure element.
Claim 21	
[21]	The token of claim 10 wherein the transaction information comprises card-present data.
Claim 22	
[22.pre]	A token comprising:
[22.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[22.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[22.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and
[22.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information to the computer terminal through the communications connector.
Claim 23	

[23]	The token of claim 22 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 24	
[24]	The token of claim 22 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 25	
[25]	The token of claim 22 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.
Claim 26	
[26]	The token of claim 22 wherein the secure element comprises a payment card application and the transaction information comprises track data.
Claim 27	
[27]	The token of claim 22 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 28	
[28]	The token of claim 22 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 29	
[29.1]	The token of claim 22 wherein: the secure element comprises an executable application; and
[29.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 30	
[30.1]	The token of claim 22 wherein: the secure element comprises a payment card application;

[30.2]	the secure element interrogator is configured to interrogate the payment card application; and
[30.3]	the transaction information comprises card-present data.
Claim 31	
[31.pre]	A token comprising:
[31.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[31.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[31.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator; and
[31.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.
Claim 32	
[32]	The token of claim 31 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 33	
[33]	The token of claim 31 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 34	
[34]	The token of claim 31 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 35	
[35]	The token of claim 31 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.

Claim 36	
[36]	The token of claim 31 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 37	
[37]	The token of claim 31 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 38	
[38.1]	The token of claim 31 wherein: the secure element comprises an executable application; and
[38.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 39	
[39.1]	The token of claim 31 wherein: the secure element comprises a payment card application;
[39.2]	the secure element interrogator is configured to interrogate the payment card application; and
[39.3]	the transaction information comprises card-present data.
Claim 40	
[40.pre]	A token comprising:
[40.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[40.2]	a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;
[40.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator; and
[40.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

Claim 41	
[41]	The token of claim 40 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 42	
[42]	The token of claim 40 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 43	
[43]	The token of claim 40 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 44	
[44]	The token of claim 40 wherein the communications controller creates a random unpredictable number and sends it to the secure element.
Claim 45	
[45]	The token of claim 40 wherein the transaction information comprises a dynamic card verification code.
Claim 46	
[46]	The token of claim 40 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 47	
[47]	The token of claim 40 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 48	
[48]	The token of claim 40 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 49	

[49.1]	The token of claim 40 wherein: the payment card application comprises an executable payment card application; and
[49.2]	the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.
Claim 50	
[50]	The token of claim 49 wherein the executable payment card application includes an application level protocol for authentication of the secure element.
Claim 51	
[51]	The token of claim 40 wherein the transaction information comprises card-present data.
Claim 52	
[52.pre]	A token comprising:
[52.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[52.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[52.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communications only between the secure element and the secure element interrogator; and
[52.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information to the computer terminal through the communications connector.
Claim 53	
[53]	The token of claim 52 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 54	
[54]	The token of claim 52 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

Claim 55	
[55]	The token of claim 52 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 56	
[56]	The token of claim 52 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 57	
[57]	The token of claim 52 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 58	
[58.1]	The token of claim 52 wherein: the secure element comprises an executable application; and
[58.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 59	
[59.1]	The token of claim 52 wherein: the secure element comprises a payment card application;
[59.2]	the secure element interrogator is configured to interrogate the payment card application; and
[59.3]	the transaction information comprises card-present data.
Claim 60	
[60.pre]	A token for transmitting a communications data package to a host device, the token comprising:
[60.1]	a mounting structure;
[60.2]	a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;
[60.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one

	transaction data communication between the secure element and the secure element interrogator and to generate the communications data package based on the transaction information; and
[60.4]	a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.
Claim 61	
[61]	The token of claim 60 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.
Claim 62	
[62]	The token of claim 60 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 63	
[63]	The token of claim 60 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element occurs only within libraries or memory space residing on the mounting structure.
Claim 64	
[64]	The token of claim 60 wherein all communications to and from the secure element consist of communications from and to a secure element reader.
Claim 65	
[65]	The token of claim 60 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.
Claim 66	
[66]	The token of claim 60 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

Claim 67	
[67]	The token of claim 60 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 68	
[68]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller.
Claim 69	
[69]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller and the host device has the physical form of a mobile phone or a PDA.
Claim 70	
[70]	The token of claim 60 wherein the mounting structure comprises a substrate.
Claim 71	
[71]	The token of claim 60 wherein the mounting structure comprises a packaging case.
Claim 72	
[72]	The token of claim 60 wherein the token has the physical form of a payment card.
Claim 73	
[73]	The token of claim 60 wherein the token has the physical form of a fob.
Claim 74	
[74]	The token of claim 60 wherein the token has the physical form of a cartridge.
Claim 75	
[75]	The token of claim 60 wherein the token has the physical form of a dongle.

Claim 76	
[76]	The token of claim 60 wherein the token has the physical form of a secure digital (SD) chip.
Claim 77	
[77]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device is configured to transmit the data communications package over a wireless network.
Claim 78	
[78.1]	The token of claim 60 wherein: the secure element comprises a payment card application;
[78.2]	the secure element interrogator is configured to interrogate the payment card application; and
[78.3]	the transaction information comprises card-present data.
Claim 79	
[79.pre]	A cellular network device comprising:
[79.1]	a mounting structure;
[79.2]	a secure element affixed to the mounting structure, the secure element including a data file containing transaction information; and
[79.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate a communications data package based on the transaction information.
Claim 80	
[80]	The token of claim 79 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.
Claim 81	
[81]	The token of claim 79 wherein the secure element interrogator exchanges the at least one transaction data communication with the

	secure element only within libraries or memory space residing on the mounting structure.
Claim 82	
[82]	The token of claim 79 wherein all communications to and from the secure element consist of communications from and to a secure element reader.
Claim 83	
[83]	The token of claim 79 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.
Claim 84	
[84]	The token of claim 79 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 85	
[85]	The token of claim 79 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 86	
[86]	The cellular network device of claim 79 further comprising a communications controller affixed to the mounting structure and configured for receiving the communications data package for transmission by the cellular network device over a wireless network.
Claim 87	
[87.1]	The cellular network device of claim 79 wherein: the secure element comprises a payment card application;
[87.2]	the secure element interrogator is configured to interrogate the payment card application; and
[87.3]	the communications data package comprises card-present data.

I. ASSIGNMENT

1. I have been retained on behalf of Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) to offer technical opinions related to U.S. Patent No. 8,548,924 (“the ’924 Patent”) (EX1001). I understand that Petitioners are requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) to institute an *inter partes* review (“IPR”) proceeding of the ’924 Patent.

2. I have been asked to provide my independent analysis of the ’924 patent based on the prior art publications cited in this declaration.

3. I am not and never have been, an employee of Apple or Samsung. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’924 Patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’924 Patent.

II. QUALIFICATIONS AND BACKGROUND INFORMATION

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. My qualifications are summarized here and explained in more detail

in my curriculum vitae, which is attached as Appendix A to this declaration. My curriculum vitae, included with this declaration, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

6. I earned a B.S. in Computer Science from the University of Richmond in 2002 and an M.S. and Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2004 and 2008, respectively. My dissertation, entitled “Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks,” focused on security problems that arise in cellular infrastructure when gateways to the broader Internet were created.

7. I am currently a Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. I was hired under the “Rise to Preeminence” Hiring Campaign and serve as the Associate Chair for Research in my Department. I also hold the endowed position of the John and Mary Lou Dasburg Preeminent Chair in Engineering.

8. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from 2008 to March 2014 at the Georgia Institute of Technology. I have supervised many Ph.D, M.S, and undergraduate students during the course of my career.

9. My area of expertise is security, especially as it applies to mobile systems and networks, including cellular networks. As such, I regularly teach students taking my courses and participating in my research group to program and evaluate software and architectures for mobile and cellular systems. I have taught courses on the topics of network and systems security, cellular networks, and mobile systems at both Georgia Tech and the University of Florida. I also advised and instructed the Information Assurance Officer Training Program for the United States Army Signal Corps in the Spring of 2010.

10. I have received numerous awards for research and teaching, including being named a Kavli Fellow (2017), a Fellow of the Center for Financial Inclusion (2016), and a Research Fellow of the Alfred P. Sloan Foundation (2014). I also won the Lockheed Inspirational Young Faculty Award (2012), was awarded a National Science Foundation (NSF) CAREER Award (2010), and received the Center for Enhancement of Teaching and Learning at Georgia Tech's "Thanks for Being a Great Teacher" Award (2009, 2012, 2013).

11. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results are highly cited, and I have received multiple "Best Paper" Awards. I have also written a book entitled "Security for Telecommunications Networks", which is used in wireless and cellular security courses at a number of top universities.

12. I am a Senior Member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). I am also a member of the USENIX Advanced Computing Systems Association.

13. I serve as an Associate Editor for IEEE Security and Privacy Magazine, have been the Program Chair for eight conferences and workshops, and have served as a member of the Program Committee for over 50 different conferences and workshops. I am also currently the Security Subcommittee Chair for the ACM US Technology Policy Committee (USACM).

14. I was a co-Founder and Research Fellow for a private start-up, Pindrop Security, from 2012 to 2014. Pindrop provides anti-fraud and authentication solutions for Caller-ID spoofing attacks in enterprise call centers by creating and matching acoustic fingerprints. Pindrop Security currently employs over 200 people, and their technology is based off of my research (US Patent 9,037,113 B2).

15. I was a co-Founder and Chief Executive of a private start-up, CryptoDrop. CryptoDrop developed a ransomware detection and recovery tool to provide state of the art protection to home, small business, and enterprise users. This technology was also based off of my research (US Patent 10,685,114 B2).

16. I was also a co-Founder and Chief Executive of a private start-up, Skim Reaper. Skim Reaper developed tools to detect credit card skimming devices,

and worked with a range of banks, international law enforcement, regulators, and retailers. This technology was also based off of my research (US Patent 10,496,914 B2).

17. I am a named inventor on ten US patents. These patents detail methods for determining the origin and path taken by phone calls as they traverse various networks, cryptographically authenticating phone calls, providing a secure means of indoor localization using mobile/wireless devices, detecting credit card skimmers, identifying cloned credit cards, and blocking ransomware from encrypting data.

III. MATERIALS CONSIDERED

18. In writing this declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of secure communication systems/networks; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:

19. I have reviewed the '924 Patent (EX1001), and relevant excerpts of the prosecution history (EX1002) of the '924 Patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

EX1004	U.S. Patent No. 8,538,332 to Huomo et al. (“Huomo”)
EX1005	U.S. Patent Appl. Pub. No. 2006/0022033 to Smets et al. (“Smets”)
EX1006	U.S. Patent No. 7,213,766 to Ryan et al. (“Ryan”)
EX1007	U.S. Patent No. 7,103,575 to Linehan (“Linehan”)
EX1008	U.S. Patent No. 8,001,054 to Peart et al. (“Peart”)
EX1009	International Pub. No. WO2001096990A2 to Abbott et al. (“Abbott”)
EX1010	U.S. Patent Appl. Pub. No. US2003/0212896A1 to Kisliakov (“Kisliakov”)
EX1012	ISO/IEC 7816-4 Second edition (2005). Available at https://www.freecalypso.org/pub/GSM/ISO7816/ISO_7816-4_2005.pdf
EX1013	U.S. Patent Appl. Pub. No. 2009/0119516 to Tanabiki et al. (“Tanabiki”)
EX1014	U.S. Patent Appl. Pub. No. 2004/0139021 to Reed et al. (“Reed”)
EX1015	U.S. Patent Appl. Pub. No. 2008/0073426 to Koh et al. (“Koh”)
EX1016	ISO/IEC 14443-4 First edition (2001). Available at: http://www.emutag.com/iso/14443-4.pdf

EX1017	U.S. Patent Appl. Pub. No. 2005/0212690 to Nishikawa ("Nishikawa")
EX1018	U.S. Patent Appl. Pub. No. 2006/0255160 to Winkler ("Winkler")

20. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '924 Patent at the time of the earliest possible priority date of the '924 Patent, and I have done so during my review of these materials. I have been informed by Counsel to use the date of January 25, 2007 as the Priority Date.

21. I have no financial interest in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

22. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '924 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '924 Patent and the prior art discussed below.

IV. OVERVIEW OF CONCLUSIONS FORMED

23. This declaration explains the conclusions that I have formed based on my analysis of all of the considered materials and my personal experience. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art references listed above, I believe that:

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-71, 76-87 of the '924 Patent are rendered obvious by Huomo in view of Smets (Ground 1A).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-71, 76-87 of the '924 Patent are rendered obvious by Huomo in view of Smets and Kisliakov (Ground 1B).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, 84-86 of the '924 Patent are rendered obvious by Ryan in view of Abbott (Ground 2A).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 3, 5, 9-13, 16-19,

21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, 87 of the '924

Patent are rendered obvious by Ryan in view of Abbott and Peart

(Ground 2B).

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 65, 83 of the '924 Patent are rendered obvious by Ryan in view of Abbott and Smets (Ground 2C).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 15, 20, 45, 50 of the '924 Patent are rendered obvious by Ryan in view of Abbott, Peart, and Smets (Ground 2D).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 2, 11, 23, 32, 41, 53, 61, 80 of the '924 Patent are rendered obvious by Ryan in view of Abbott, Smets, and Kisliakov (Ground 2E) and Ryan in view of Abbott, Peart, Smets, and Kisliakov (Ground 2F).

24. In support of these conclusions, I provide more detailed comments regarding the obviousness of claims 1-87 ("the Challenged Claims") of the '924 Patent in my analysis below.

V. LEVEL OF ORDINARY SKILL IN THE ART

25. In my opinion, one of ordinary skill in the art relating to, and at the time of, the Priority Date would have been someone with (1) at least a bachelor's degree in computer science, computer engineering, or a related field, and (2) at least two years of industry experience including researching or developing software related to secure communication systems/networks ("POSITA"). Additional education could substitute for professional experience, and professional experience for education.

26. My analysis and conclusions set forth in this declaration are based on the perspective of a POSITA. Further, all positions in this declaration are from the vantage point of a POSITA as of January 25, 2007.

27. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

VI. LEGAL STANDARDS

28. I have been informed by Counsel and understand that documents and materials that qualify as prior art can render a patent claim unpatentable as being anticipated or obvious.

29. I am informed by Counsel and understand that all prior art references are to be looked at from the viewpoint of a person of ordinary skill in the art at the time of the invention, and that this viewpoint prevents one from using his or her own insight or hindsight in deciding whether a claim is anticipated or rendered obvious.

A. Anticipation

30. I understand that patents or printed publications that qualify as prior art can be used to invalidate a patent claim as anticipated or as obvious.

31. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

32. I understand that a prior art reference “anticipates” an asserted claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present).

B. Obviousness

33. I understand that even if a patent is not anticipated, it is still invalid if

the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA.

34. I have been informed by Counsel and understand that a claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.

35. I am informed by Counsel and understand that when a patented invention is a combination of known elements, a court determines whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

36. I am informed by Counsel and understand that a patent claim composed of several limitations is not proved obvious merely by demonstrating

that each of its limitations was independently known in the prior art. I am informed by Counsel and understand that identifying a reason those elements would be combined can be important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. I am informed by Counsel and understand that it is improper to use hindsight in an obviousness analysis, and that a patent's claims should not be used as a "roadmap."

37. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others.

38. I have been informed by Counsel and understand that an obviousness evaluation can be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that

market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

39. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

40. I have been informed by Counsel and understand that practical and common sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I have been informed by Counsel and understand that a person of ordinary skill looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. I have been informed by Counsel and understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

41. I have been informed by Counsel and understand that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill at the time of invention, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of

invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

42. I have been informed by Counsel and understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

43. In sum, my understanding is that prior art teachings are properly combined where one of ordinary skill having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

44. I have been informed by Counsel and understand that in an *inter partes* review, “the petitioner shall have the burden of proving a proposition of unpatentability,” including a proposition of obviousness, “by a preponderance of the evidence.” 35 U.S.C. §316(e).

VII. INTERPRETATIONS OF THE '924 PATENT CLAIMS AT ISSUE

45. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as

understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '924 patent was filed Feb. 23, 2012, and claims priority to January 25, 2007, which I refer to as the "Critical Date" in this proceeding. Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the '924 Patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

46. I have applied Petitioner Apple's district court constructions (reproduced below) to the Challenged Claims within this declaration:

Claim Term	Construction
"transaction information" (All claims)	information used to process a transaction that includes at least bank account information specific to a card holder

VIII. THE '924 PATENT

A. Overview of the '924 Patent

47. The '924 Patent relates to "the field of devices configured to authorize

transactions using secure element microchips,” such as “tokens that contain secure element microchips and are configured to authorize financial transactions over the internet.” EX1001, 1:24-28. A “token” is described as any of several form factors — “fobs, cartridges, or dongles, or form factors that resemble removable digital memory media such as secure digital (SD) chips” — and “[e]ach token has a mounting structure such as substrate (for card devices) or a packaging case (for fobs, cartridges, and dongles or SD chips).” EX1001, 4:15-21.

48. The '924 Patent acknowledges that in prior payment technologies “a microchip referred to as a ‘Secure Element’ (SE) is embedded into the payment card, the payment fob, or another other device that may be used for making payments,” and that “[i]n order to extract information from the SE, an interrogator, also referred to herein as a ‘reader’, is required to interact electrically with the SE.” EX1001, 1:32-38. I note the '924 patent further acknowledges that such readers “typically follow[] standards set forth by the International Organization for Standardization (ISO),” EX1001, 1:38-39, and frames the asserted need as “devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions,” EX1001, 1:47-50.

49. The '924 Patent recites that “[b]ecause readers are not typically part of most PCs, it is very beneficial to place the reader functionality on the card

device and translate information from the SE into a data stream format such as a USB (Universal Serial Bus) that PCs are generally capable of processing.”

EX1001, 4:54-58. It describes “incorporating a reader on a card device or within a cellular network adapter to extract and deliver banking track data that were generally not previously possible because of the inability to extract information from the SE or from a magnetic stripe at a computer terminal without a reader.” EX1001, 5:27-32.

B. Prosecution History of the '924 Patent

50. The '924 Patent issued on October 1, 2013 from U.S. Patent Application No. 13/403,141 (“the '141 application”), filed on February 23, 2012, and which claims priority to a series of applications. See EX1001, cover page (21)-(22), (45), (60) (“Provisional application No. 60/897,110, filed on Jan. 25, 2007, provisional application No. 60/932,704, filed on Jun. 1, 2007.”), (63) (“Continuation of application No. 12/019.318, filed on Jan. 24, 2008, now Pat. No. 8,151,345.”).

51. The '141 application was filed with 31 claims, which were rejected based on Ryan (US7,213,766; EX1006), Gold (US2005/0231467), and Somers (US2007/0262138). EX1002, 53-58, 205-215. In response to the rejection, the applicant argued that the prior art “fails to disclose or suggest a secure element and an interrogator affixed to the same mounting structure.” EX1002, 258. For several

dependent claims, the applicant relied on Brian Charles Murray's Declaration for ISO 7816-4 features not recited in the independent claims. EX1002, 259-260. The applicant further added new claims 32-87, including new independent claim 46 that "provides a useful token" and new independent claim 64 that "provides a cellular network device." EX1002, 262-266. In a Notice of Allowability, the examiner's statement of reasons for allowance recited the "prior arts of record and further search does not teach/suggest... 'a secure element affixed to the mounting structure...; a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element...'" EX1002, 334.

52. As demonstrated by the analysis in each of the Grounds below, however, the claims never should have been allowed in their current form. *Infra*, §**Error! Reference source not found.** Critically, Ryan of record, as well as other pertinent prior art never presented to the Examiner during examination, disclose what the Examiner mistakenly believed to be missing from the prior art.

IX. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '924 PATENT CLAIMS UNPATENTABLE

A. GROUND 1A – Huomo-Smets Renders Obvious Claims 1-71 and 76-87

1. Huomo

53. Huomo describes an NFC (Near Field Communication) enabled communication device having a "secure element 30" that stores transaction data,

transaction applications, and encryption algorithm and keys, a “controller 20” that receives data from the secure element 30 through an interface that is “in compliance with ISO 7816,” and an “NFC communicator 15” for transmission of the transaction data to another (recipient) device (e.g., PDA, laptop) via an NFC link. EX1004, Abstract (“A communications device has a NFC communicator (15)... The device also has at least one secure element (30; 31) separate from the nearfield RF communicator (15) to provide secure data storage for transaction data representing or relating to a transaction. A controller controls operation of the NFC communicator, reads transaction data from the at least one secure element [and] communicate[s] the read transaction data to a near field RF communicator in near field range as proof of the transaction to enable an action related to the transaction to be carried out.”), 2:35-67, 3:20-40, 5:24-40, 6:23-41, 7:19-67, FIGS. 1 (reproduced below), 2, 10.

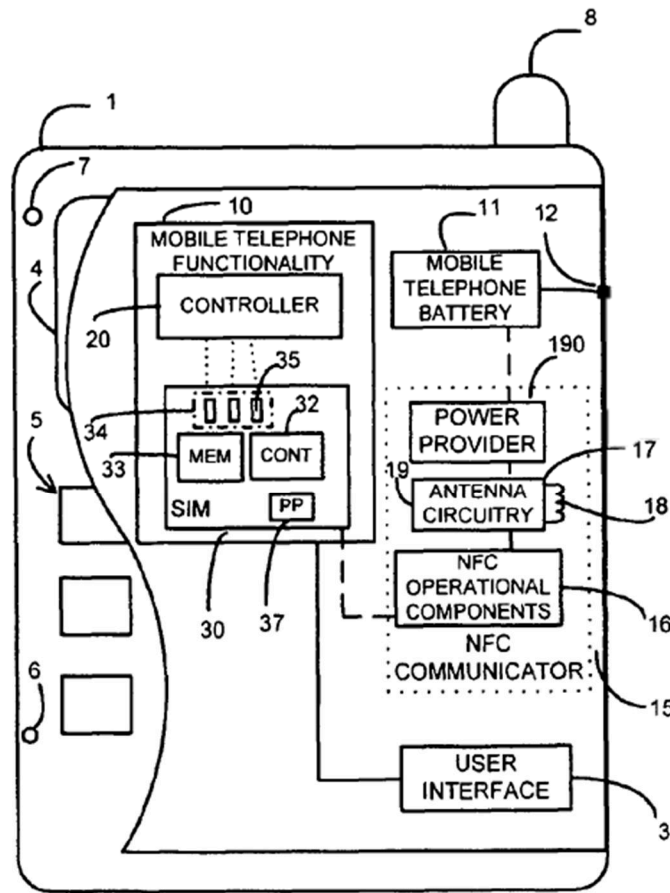


FIG. 1

EX1004, FIG. 1

54. As illustrated in FIG. 1, “secure element 30,” “controller 20,” and “NFC communicator 15” are each provided on the same mounting structure of “device 1,” e.g., implemented as “an integrated circuit or collection of integrated circuits” on “a PCB board.” EX1004, 5:22-23, 7:31-38, 24:4-17, FIGS. 1-2.

55. Uomo's secure element 30 (e.g., "SIM," "USIM") having "memory store 33" is "programmed with or programmable with an operating system and one or more applications platforms applications so as to be capable of encrypting

transaction data and storing encrypted transaction data.” EX1004, Abstract (“The device also has at least one secure element (30; 31) separate from the nearfield RF communicator (15) to provide secure data storage for transaction data representing or relating to a transaction. A controller controls operation of the NFC communicator, reads transaction data from the at least one secure element.”), 7:19-67 (“in FIGS. 1 and 2, the secure elements 30...are programmed with or programmable with an operating system and one or more applications platforms applications so as to be capable of encrypting transaction data and storing encrypted transaction data (for example ticket data, access data, purchase data) in accordance with that applications platform...memory store 333...secure element 30 is provided by the SIM...or USIM”), 3:58-67, 7:65-8:41 (“The secure element may however be any appropriate storage element having processing capability to enable the secure element 30 or 31 to communicate (receive and send) secure data (that is encrypted data) and to store data in a secure encrypted manner to inhibit reading of or tampering with the secure data by an unauthorised device or person or unauthorised functionality. The secure element may also be able to communicate and store unencrypted data, such as data that is freely publicly available or user data that the user does not consider to be private data...any other form of secure element that is capable of storing data in a secure manner and communicating that secure data...”), 10:35-12:57 (details of “memory 33”). Application areas of

Huomo include “the financial transaction area which involves payment for products such as goods and services.” EX1004, 1:56-60.

2. Smets

56. Like Huomo and the '924 Patent, Smets describes transaction systems in which secure transaction data is stored in a secure element and communicated through a reader to a host to enable transactions. EX1005, Abstract, [0002], [0005], [0009]-[0010], [0025]-[0026]. In more detail, Smets describes formatting and communicating “proximity card transaction data” stored on “a payment card 1” (e.g., “PayPass Card” that is “consistent with the ISO 14443 Standard”) to “a reader terminal 2” then to a host, by embedding such transaction data within standardized magnetic stripe track formats (e.g., “Track 1,” “Track 2,” and “Track 3” data), “for processing magnetic stripe card transactions” consistent with ISO 7811. *See e.g.*, EX1005, Abstract, [0004]-[0008], [0013], [0025], [0026], [0037]-[0039], FIG. 5 (reproduced below). Through such formatting, proximity payment card implementations are made “compatible with existing standardized magnetic stripe payment card transaction processes.” EX1005, [0011]-[0012]; EX1012, §§5-6.

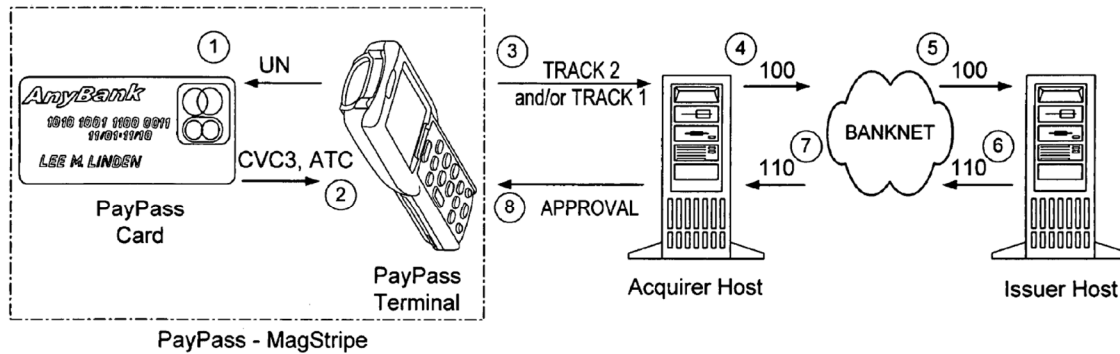


FIG. 5

EX1005, FIG. 5

57. Smets describes application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication for improved security, through “generation of a dynamic authentication value or number (CVC3)” from “an unpredictable number (UN),” and optionally “the card’s application transaction counter (ATC),” using “a secret encryption key” stored on the payment card, such that the value of the CVC3 “changes with each transaction” and “the unauthorized person cannot use that CVC3 number...for the next or any other transactions.” EX1005, [0010] (“A security solution, which may be utilized in PayPass, is based on generation of a dynamic authentication value or number (CVC3). The dynamic authentication value changes with each transaction. Thus, in the event an unauthorized person obtains the CVC3 number for a particular transaction, the unauthorized person cannot use that CVC3 number as the authentication value for the next or any other transactions.”), [0014], [0024]-[0025] (“The PayPass implementation provides a

‘Pay Pass-Mag Stripe’ application, which can process transactions based on proximity cards and magnetic stripe cards. (See FIG. 5). The PayPass-Mag Stripe application is an extension of the currently available magnetic-stripe applications for debit and credit payments.”), [0026], (“With reference to FIG. 5, in a proximity payment card transaction between an interacting payment card (e.g., PayPass card 1) and a reader terminal 2, as part of the security procedure, terminal 2 generates and transmits to the payment card an unpredictable number (UN). In response, payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal. Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number. Alternatively, payment card 1 may be personalized at the card issuer option to compute the CVC3 number based on a portion of the UN and on the card’s application transaction counter (ATC). In such cases, payment card 1 transmits both the computed CVC3 number and the ATC to the terminal 2...For the subject proximity payment card transaction, terminal 2 packages or formats.

58. The computed dynamic CVC3, optionally along with the transaction counter (ATC) and/or the unpredictable number (UN), is integrated in Track data (e.g., a discretionary data field of Track 2) using an issuer-specific bitmap as a placing index, then communicated to the host for authorization of the transaction. EX1005, EX1005, Abstract (“The proximity payment card transaction data such

[as] dynamic authentication codes are placed in unused space in the same standard formatted data structures. The availability of unused space varies with card issuer or vendor. An issuer-specific bitmap provides an index to the available space in discretionary data fields in magnetic stripe tracks. The bitmap also is stored in the card's discretionary data field.”), [0014] (“The proximity payment card transaction data is placed in unused portions of discretionary data fields (e.g., Track 2 discretionary data field).”), [0026] (“terminal 2 packages or formats the ATC, UN, and the CVC3 number in a discretionary data field according to these rules.

Terminal may then communicate the discretionary data field under magnetic stripe card conventions to an acquirer host 4 and/or issuer host 5 for authorization of the transaction. Terminal 2 may, for example, send the discretionary data field as part of Track 2 in Data Element 35 (DE35) of a standardized message 100 to the issuer for authorization or approval (8, 110).”), [0029]-[0031] (“Each bit in the bitmap refers to a position in the discretionary data field... for Track 2 discretionary data field (‘Track 2 Data’)... resulting in a bitmap of 16 bits or 2 bytes. For Track 1 discretionary data field (‘Track 1 Data’)... resulting in a bitmap of length 6 bytes or 48 bits...Specific bitmaps used in PayPass applications may indicate specific positions in Track 2 Data for placing UN and ATC. Another bitmap, Position CVC3 (PCVC) may be used to indicate specific positions in Track 2 Data for placing the CVC3 number.”), [0035], [0037]-[0038].

3. Huomo-Smets Combination

(a) Huomo and Smets are Analogous Art to the '924 Patent

59. Huomo and Smets are analogous art to the '924 Patent, which is generally directed to “the field of devices configured to authorize transactions using secure element microchips.” EX1001, 1:24-28; cl. 1 (“A token”); *supra*, §IX.A.1-2 (Huomo and Smets). Huomo and Smets are also reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50 (“What are needed therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.”), 4:52-67, 5:5-11, 5:12-26, 5:27-36, 5:37-55, 5:61-6:3 (encrypting track data “in order to securely transport the data packet over a public network”), 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27; *supra*, §IX.A.1-2 (Huomo and Smets).

(b) A POSITA would have been Motivated to Combine Huomo and Smets

60. Huomo already provides an NFC communication platform for transmitting transaction data stored in a secure element, e.g., a proximity payment card compatible with ISO/IEC 14443. *Supra*, §IX.A.1; *see e.g.*, EX1004, Title, Abstract, 3:44-55 (“a secure element, for example a SIM card, USIM card, WIM card, SWIM card, SD card, SMC card or other form of secure element, is operable

to transfer data from its memory or data store to an external near field RF communicator through an NFC communicator....in accordance with or compatible with ISO/IEC 14443”), FIGS. 1-2. Smets provides a known technique to structure proximity transaction data stored in a payment card, including a dynamic authentication code (e.g., CVC3), so that its implementation is compatible with existing magnetic stripe infrastructure and processes, e.g., compatible with both ISO/IEC 14443 for contactless proximity payment card transactions and ISO 7811 for magnetic stripe card transactions. *Supra*, §IX.A.2; *see e.g.*, EX1005, Abstract, [0010] (“MasterCard PayPass™ ISO/IEC 14443 Implementation Specification (‘PayPass’) for implementation of electronic payment systems based on proximity payment cards”), [0011]-[0014], [0025] (“The PayPass implementation is consistent with the ISO 14443 Standard and the ISO 7811”), [0026].

61. A POSITA would have been motivated to incorporate Smets’s teaching of backward-compatible data formatting for integrating proximity payment data, including the dynamic authentication code (e.g., CVC3), into Huomo’s proximity (e.g., NFC based) payment card system. EX1005, [0011]-[0013]. Multiple considerations would have led a POSITA to implement this combination.

62. **First**, a POSITA would have incorporated Smets’s backward-compatible formatting of proximity transaction data including a dynamic CVC3

into Huomo's proximity transaction system, because this would promote the ability of the combination's contactless transactions (both following the same ISO 14443 standard) to be processed using existing magnetic stripe infrastructure of the legacy payment networks, which is a major commercial advantage and a common goal expressed in both Huomo and Smets. *See e.g.*, EX1004, Title, Abstract, 2:18-19 (desire for "flexibility and backwards compatibility with existing systems and devices"), 3:44-55; EX1005, Abstract, [0010]-[0011] ("Any electronic payment system based on the new card technologies is likely to gain acceptance by users only if the new system is backwards compatible with legacy infrastructure (e.g., terminals, card readers, and back office operations), which was designed for processing magnetic stripe cards. Thus, it may be advantageous to provide payment cards that can function with both magnetic stripe card systems and proximity payment card systems. In such cards, it may be preferable to transmit the dynamic authentication value (CVC3) and other proximity card function specific data to the issuer or other validating party in a format which does not disturb the data fields or information required by ISO 7811 for magnetic stripe card transactions."), [0025].

63. **Second**, a POSITA would have incorporated Smets's teaching into Huomo's system, because it would provide enhanced security through dynamic authentication. Huomo already supports encrypted storage, where the secure

element stores encryption “keys” and “encryption software or an encryption algorithm to ensure secure storage of data relating to a transaction such as, for example, a financial transaction or transactions.” EX1004, 3:59-62 (“‘secure element’ means any element which is capable of being used and is ‘trusted’ to hold secure encrypted information and/or data, although not all of the data held by the secure element need be encrypted”), 5:26-52, 7:19-31, 8:25-41, 11:28-35. Huomo also strongly emphasizes that the secure transaction data in the secure element is kept isolated and not visible (or not required to be understood) by the host or NFC communicator. EX1004, 1:64-2:24 (“the secure data is made secure (for example a manner of encryption) is not known to and is not relevant to the NFC communicator... the NFC communicator does not need to be a secure or trusted device, only the secure element and the device that decrypts communicated secure data need to be trusted devices...the NFC communicator communicates the secured data to a near field RF communicator without any knowledge of these features of the secure element.”). Smets’s use of dynamic authentication value (e.g., CVC3) (along with the UN and transaction counter) adds dynamic authentication specific to each transaction and protection against fraud and replay attacks. EX1005, [0010], [0014], [0026].

64. **Third**, a POSITA would have been motivated to incorporate Smets’s teaching into Huomo’s system for the common goal of improved interoperability

across vendors and systems. EX1004, 2:16-19 (desire for “interoperability to maintain a consistent and viable user experience...flexibility and backwards compatibility with existing systems and devices”); EX1005, [0011]. Smets identifies that vendors and issuers do not use magnetic-stripe discretionary fields consistently, which breaks interoperability. EX1005, [0011] (“Unfortunately, usage of the discretionary data fields by vendors and issuers is not consistent. For example, the static authentication values (e.g., CVC2) used by vendors may be either a 3 digit or a 4 digit number. Thus, the space available in the discretionary data fields for placing the CVC3 number may vary from card to card according to vendor encoding of the discretionary data fields. This varying availability of discretionary data space makes it difficult to standardize use of the space for storing proximity card function related data (e.g., CVC3).”). Smets provides a solution to this problem by using a vendor/issuer-specific bitmap that explicitly signals where data should be placed. EX1005, [0014] (“An issuer or vendor-specific bitmap identifies available unused space in the discretionary data fields in the cards. Dynamic authentication codes, unidentified numbers, automatic transaction counter and/or other proximity card transaction parameters are placed in the discretionary data fields in available free space, which is identified by the bitmap.”). This allows each issuer to define how much space is available and exactly where data may go without changing terminals or networks, while “[c]ard

behavior is independent of vendor usage of the discretionary data fields.” EX1005, [0015], [0026], [0033] (“on-card processes are always the same, independent of the values of the bitmaps.”).

65. Additionally, a POSITA would have found it obvious that the Huomo-Smets combination uses the same type of ISO 7816-4 commands and responses (APDUs) for a plurality of transaction data communications between the secure element (e.g., payment card) and the reader in a single interrogation session to acquire Track data for transactions, as Huomo’s secure element and reader interface is explicitly “in compliance with ISO 7816,” and Smets provides the details of command-layer command-response pairs defined by ISO 7816-4. *Supra*, §IX.A.1-2; EX1004, 7:51-52; EX1005, [0036]-[0039], FIG. 6.

(c) A POSITA would have Reasonably Expected Success when Combining Huomo and Smets

66. The combination amounts to use of a known technique (e.g., Smets’s teaching of proximity data structure) in a known system (e.g., Huomo) to yield predictable results. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through routine software updates. Smets specifies how to structure proximity transaction data stored in a payment card, including a dynamic authentication code (e.g., CVC3). Huomo’s secure element and reader interface is

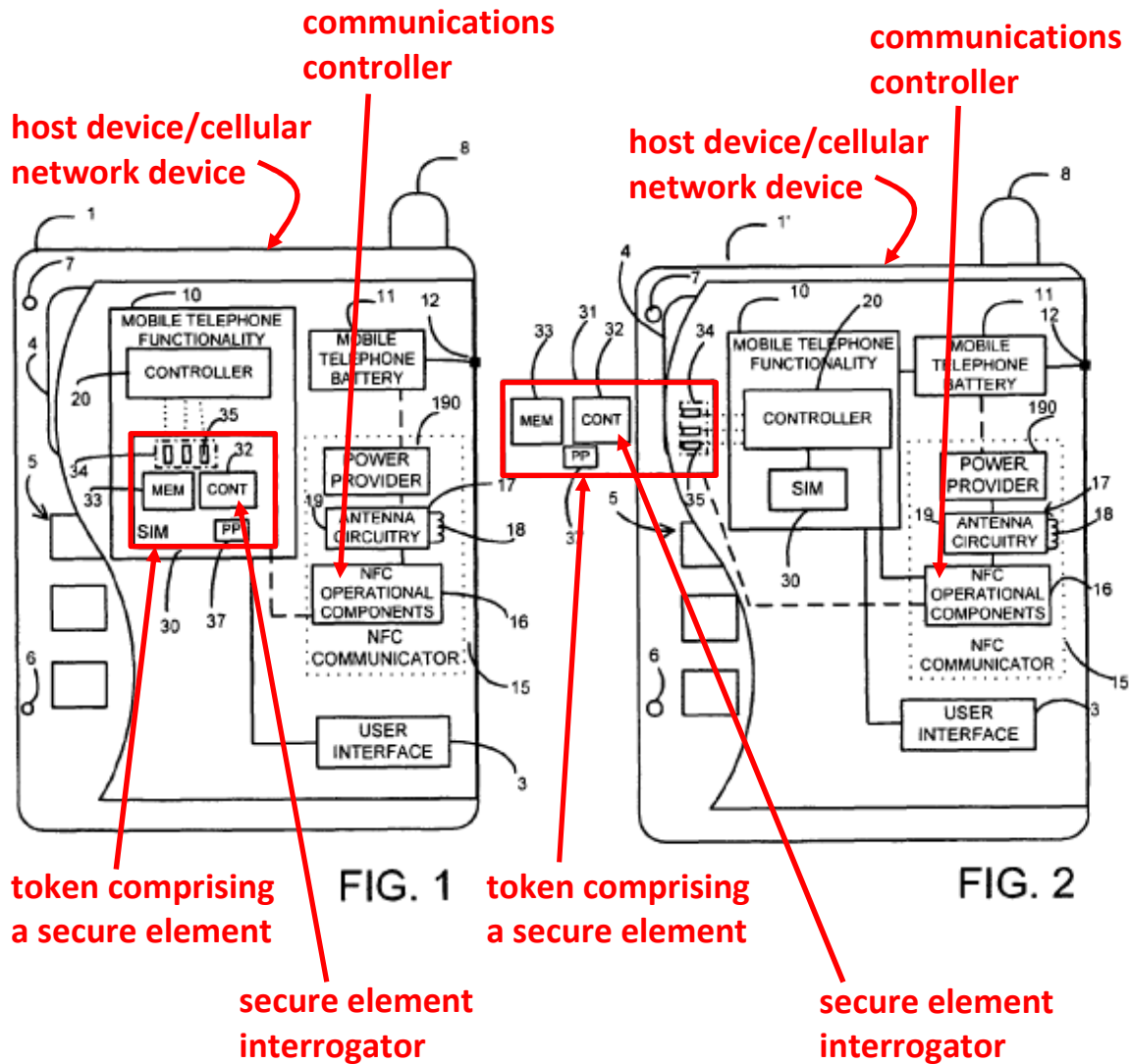
explicitly “in compliance with ISO 7816,” and Smets provides the details of command-layer command-response pairs defined by ISO 7816-4. EX1004, 7:51-52; EX1005, [0036]-[0039], FIG. 6.

4. Analysis

67. Huomo-Smets renders obvious the claims in multiple manners. The following analysis presents two mappings, each of which render the claims obvious.

a) First Mapping

68. Huomo’s “secure element” (SE) included in “a SIM card, SD card or other secure memory storage” is a ***token***. EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66; EX1001, 4:8-21 (“smart token” and “‘token’ is used to encompass all of these form factors.”). Huomo’s SE card (***token***) is within “a larger device or host system, for example a mobile telephone, PDA, lap-top or other electrical device” (***host device/cellular network device***). EX1004, 3:56-62. Huomo’s SE cards 30/31 (***token***) each have a ***secure element interrogator*** including “a controller (CONT) 32... which controls the functionality of the secure element in accordance with its operating systems and the installed applications platform or platforms.” EX1004, 7:31-46. The NFC communicator controller (e.g., NFC operational components 16 including controller 40) is the ***communications controller***. EX1004, 24:50-60, 15:17-19.

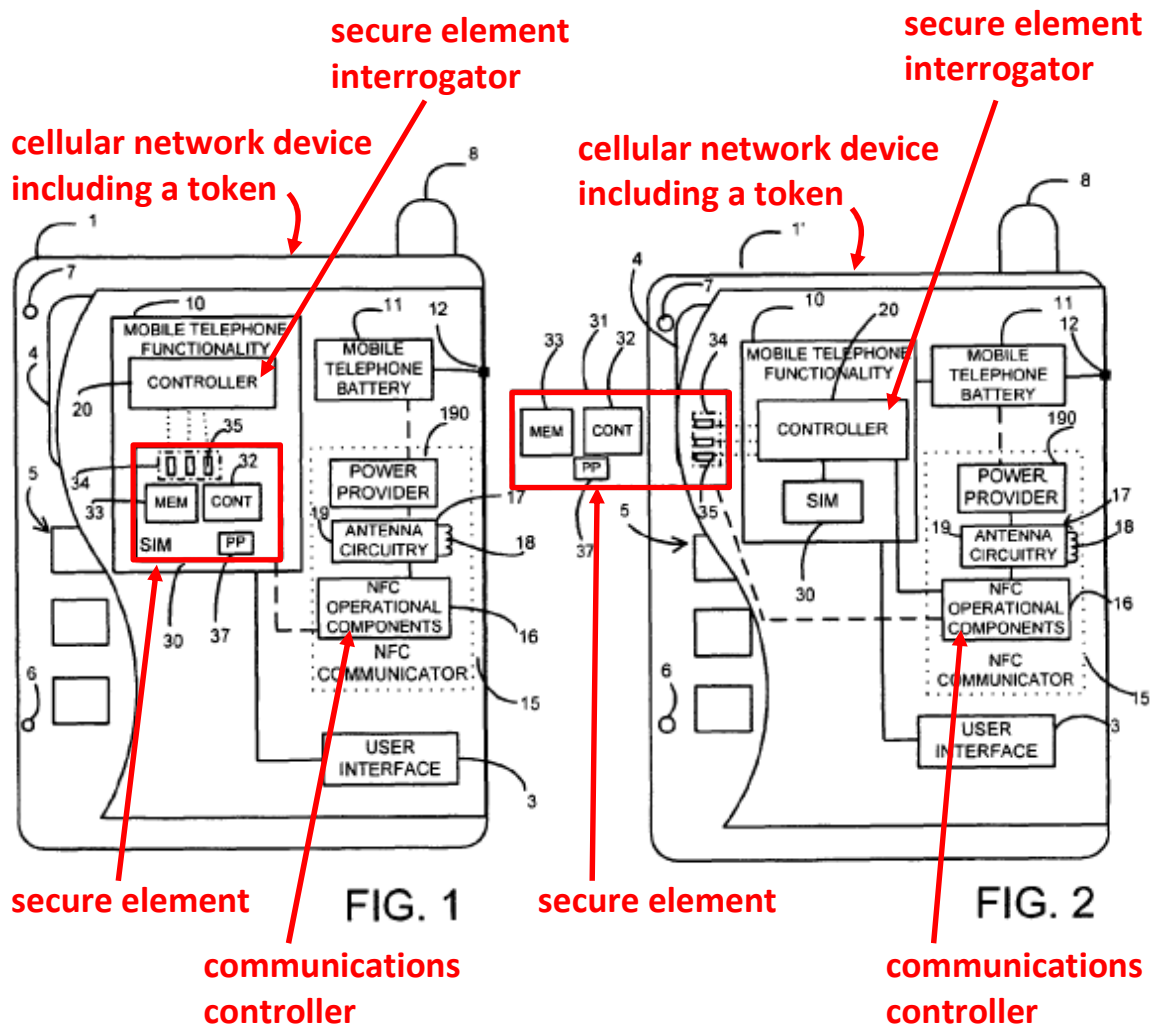


EX1004, FIGS. 1, 2

a) Second Mapping

69. Huomo's devices 1/1' are each a *cellular network device* that includes a *token* with a SE 30/31. EX1004, 5:24-6:22, FIGS. 1, 2. Huomo's *token* includes the *secure element* 30/31 coupled to "a controller 20" (*secure element interrogator*) of the device 1/1' (*cellular network device*) to "enable

communication of data between the controller and the secure element 30,” and the controller 20 is coupled to operational components 16 and controller 40 of NFC communicator 15 (*communications controller*) to “enable communication of data between the controller 20 and the NFC communicator 15.” EX1004, 6:23-28, FIGS. 1-2. The NFC communicator that supplies secure data from the SE 30/31 to a near field RF communicator (*host device*). EX1004, 1:64-3:55, 5:24-6:41, 10:19-34, 14:35-42, 15:13-16, FIGS. 1-2, 13.



EX1004, FIGS. 1, 2

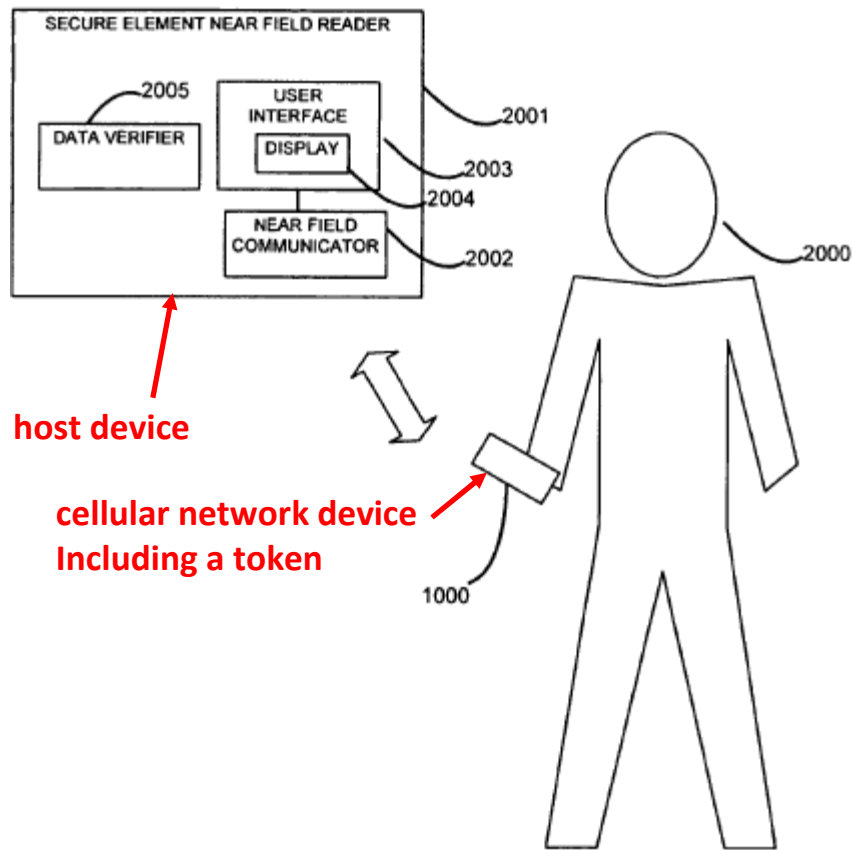


FIG. 13

EX1004, FIG. 13

(a) Claims 60, 79

[60.pre] A token for transmitting a communications data package to a host device, the token comprising:

[79.pre] A cellular network device comprising:

70. To the extent limiting, Huomo-Smets renders it obvious according to two predictable mappings.

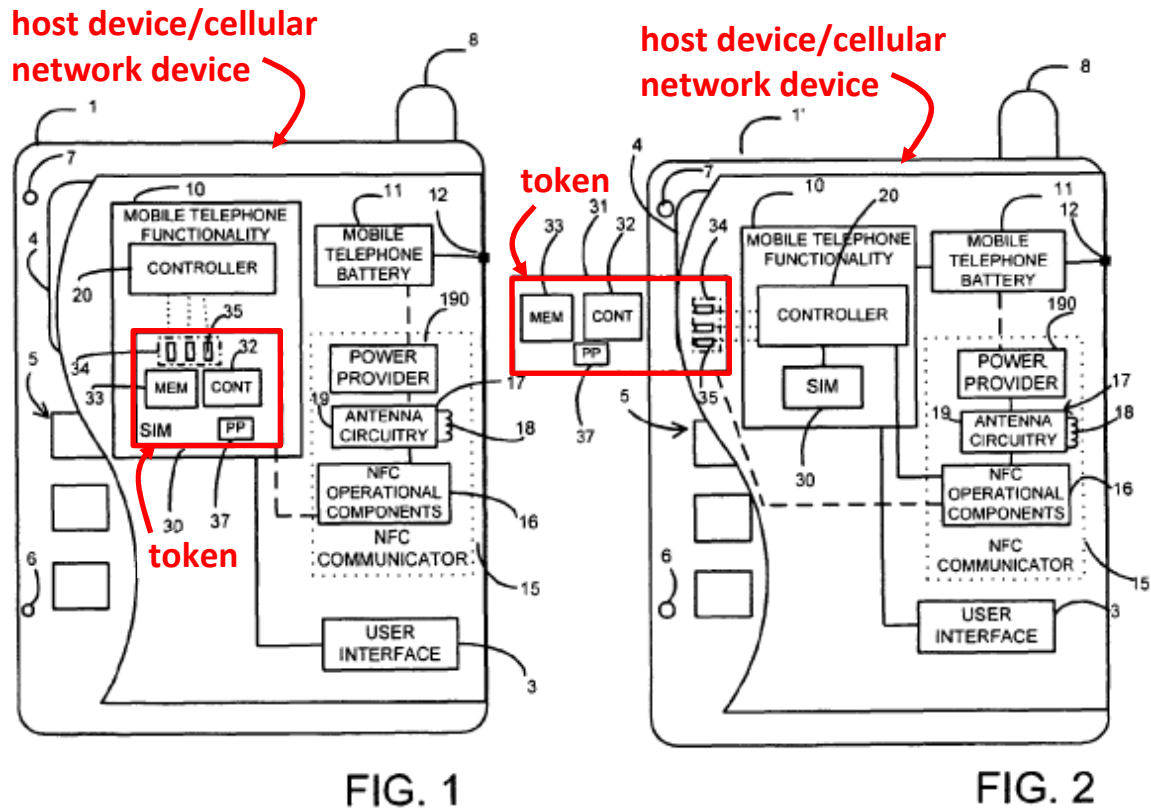
a) First Mapping

71. Huomo describes “a secure element” (SE) included in “a SIM card, SD card or other secure memory storage” (*token*). EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66; EX1001, 4:8-21 (“smart token” and “‘token’ is used to encompass all of these form factors.”). Huomo describes its SE card (*token*) within “a larger device or host system, for example a mobile telephone, PDA, laptop or other electrical device” (*host device/cellular network device*). EX1004, 3:56-62. In Huomo, “a mobile telephone or PDA” (*host device/cellular network device*) “is operable to receive data from the secure element” card (*token*). EX1004, 3:20-40. The ’924 Patent uses *host device* broadly, describing as the computer terminal that receives information from a card device or the cellular network device that receives it from a cellular network adapter — Huomo’s device 1/1’ addresses this element directly. EX1001, EX1001, 5:1-4 (“the term ‘host device’ is used to refer to either (a) the computer terminal that receives the information from a card device or (b) the cellular network device that receives the information from the cellular network adapter.”), 4:36-40 (“Such mobile phones and PDAs are referred to herein as cellular network devices. The term ‘cellular network adapter’ is used herein to describe a system that includes in a secure element (SE) microchip for use in a cellular network device.”); 12:54-55 (“the card device, which is the client device, exchanges information with the USB host device.”); 17:62-64 (“communication from the base band device or host PC to the

card device.”).

72. Huomo’s FIGS. 1 and 2 show devices 1/1’ (*host device/cellular network device*) that are “mobile telephones (cellular telephones or ‘cell phones’).” EX1004, 6:35-54, 25:35-36. Each device 1/1’ (*host device/cellular network device*) comprises a SE card (SIM 30/SD card 31) (*token*) for “secure storage of data relating to a transaction.” EX1004, 5:24-40, 7:65-8:24, 15:62-16:17, 20:42-44. The SE card (*token*) is coupled to a controller 20 of the device 1/1’ (*host device/cellular network device*) through a “coupling interface 34 comprising one or more coupling elements 35” “to enable communication of data between the controller and the secure element” card (*token*) “in compliance with ISO 7816.” EX1004, 6:23-28, 7:47-52, 8:5-34, 20:48-54, 21:11-14. Based on Huomo’s explicit disclosure of an ISO 7816 interface between the SE card and the controller 20, a POSITA would have recognized, and found obvious from Huomo’s description, that the SE card and the controller 20 exchange data using an APDU (Application Protocol Data Unit) (*communications data package*) defined in ISO 7816 (e.g., ISO 7816-4). *See*, EX1013, [0006] (“the IC card and an external system (reader) exchange data using an APDU (Application Protocol Data Unit) defined in ISO/IEC 7816-4.”); EX1014, [0016] (“The client 102 communicates with the smart card 104 using application protocol data units (APDUs)”), [0030] (“a file system using the ISO 7816-4 standard”); EX1015, [0034] (“the APDU

stands for Application Protocol Data Unit that is a communication unit between a reader and a card. The structure of an APDU is defined by the ISO 7816 standards.”)).



EX1004, FIGS. 1, 2

b) Second Mapping

73. Huomo’s devices 1/1’ (*cellular network device*) each includes a **token** with a SE 30/31. EX1004, 5:24-6:22, FIGS. 1, 2.

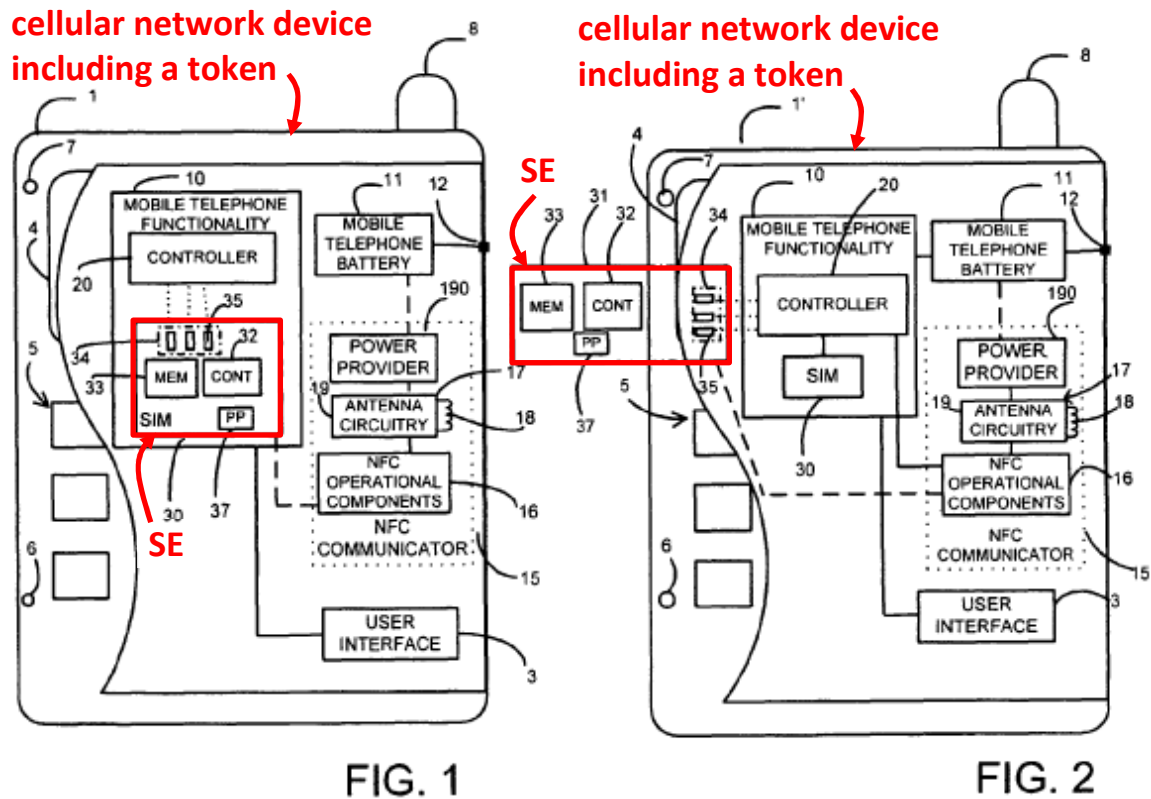


FIG. 1

FIG. 2

EX1004, FIGS. 1, 2

74. The **token** of Huomo's device 1/1' (**cellular network device**) also includes an NFC communicator that supplies secure data from the SE 30/31 to a near field RF communicator (**host device**) via NFC communication protocols in accordance with ISO/IEC 14443. EX1004, 1:64-3:55, 5:24-6:41, 10:19-34, 14:35-42, 15:13-16 ("device 1000 is similar to the devices 1 and 1'") FIGS. 1-2, 13; *supra*, §IX.A.1. A POSITA would have known that the ISO/IEC 14443 protocol transfers APDUs as defined in ISO 7816-4. EX1016, 6. Based on Huomo's explicit disclosure of the NFC communicator transmitting data to another RF communicator using an ISO/IEC 14443 protocol, a POSITA would have

recognized, and found it obvious from Huomo's description, that the NFC communicator of the *token* of device 1/1' (*cellular network device*) transmits the data using APDUs (*communications data package*) defined in ISO 7816-4 to the RF communicator (*host device*).

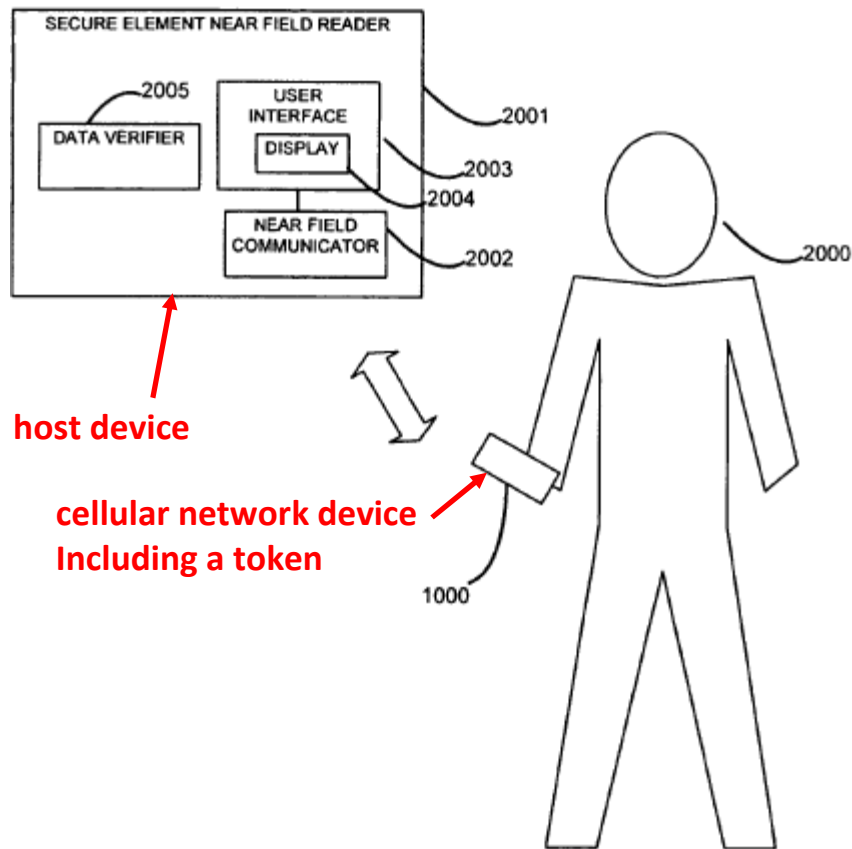


FIG. 13

EX1004, FIG. 13

[60.1]/[79.1] a mounting structure;

75. Huomo-Smets provides these elements.

a) First Mapping

76. Huomo describes that the SE is in the form of “a SIM card, SD card or other secure memory storage” (*token*). EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66. The SE cards 30/31 “each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit” (IC). EX1004, 7:19-46. A POSITA would have recognized, and found obvious from Huomo’s description, that the SIM card includes an IC chip mounted on a substrate (*mounting structure*). EX1017, [0013], [0145], FIG. 1. A POSITA would have also recognized, and found obvious, from Huomo’s description, that a SD card includes chips mounted to a printed circuit board and integrated in a plastic cover (*mounting structure*). EX1018, [0002]. Based on Huomo’s express disclosure of the SE in the form of a SIM card or SD card, a POSITA would have understood and found it obvious that the device 1/1’ (*cellular network device*) includes the SE card (*token*) that includes a substrate or a printed circuit board in a plastic cover (*mounting structure*).

b) Second Mapping

77. Huomo describes that its device 1/1’ (*cellular network device*) “may be provided wholly or partially as an integrated circuit or collection of integrated circuits.” EX1004, 5:21-23, 7:31-38. Huomo’s “NFC communicator” (e.g., “NFC communicator 15” of FIG. 3) “may be implemented as an integrated circuit connected to any peripherals and an antenna,” e.g., “implemented on a PCB

board.” EX1004, 24:4-17. A POSITA would have found it obvious from Huomo’s description that the ICs in Huomo’s *token* are affixed to a *mounting structure* such as a PCB board (*substrate* of Claim [70]) in the device’s housing (*a packaging case* of claim 71), advantageously effectuating Huomo’s stated objectives and implementation.

[60.2]/[79.2] a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;

78. Huomo-Smets provides these elements. Huomo uses the term “secure element” to describe an “element which is capable of being used to hold secure encrypted information and/or data.” EX1004, 25:41-44. Huomo describes that each device 1/1’ each comprises a SE in the form of a card (SIM 30/SD card 31) that provides “secure storage of data relating to a transaction.” EX1004, 2:25-46, 3:63-4:24, 5:24-40, 7:65-8:24, 15:62-16:17, 20:42-44. The SE cards 30/31 “each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit” (IC). EX1004, 7:19-46. Huomo’s memory store 33 of the secure element provides “transaction data storage” for “transaction data” including “payment data” for “a financial product such as a credit or debit card” (*transaction information*). EX1004, 10:35-11:7, 2:44-46, 3:63-4:15, 25:51-62. The credit/debit card number is linked to an issuing bank and a bank account, is used to route messages to the issuing bank, and therefore is bank account information.

EX1007, 15:40-46. A POSITA would have found it obvious that the SE for storing transaction data comprises *a data file containing transaction information* in its memory store 33 based on Smets's teachings. EX1004, 7:19-67, 10:35-12:57 (describing "memory store 33 in greater detail"), FIGS. 1-2. For example, Smets discloses "file control information" and that "data... are included in record 1 of the file," confirming that the SE stores information in data files in the combined system. EX1005, [0037].

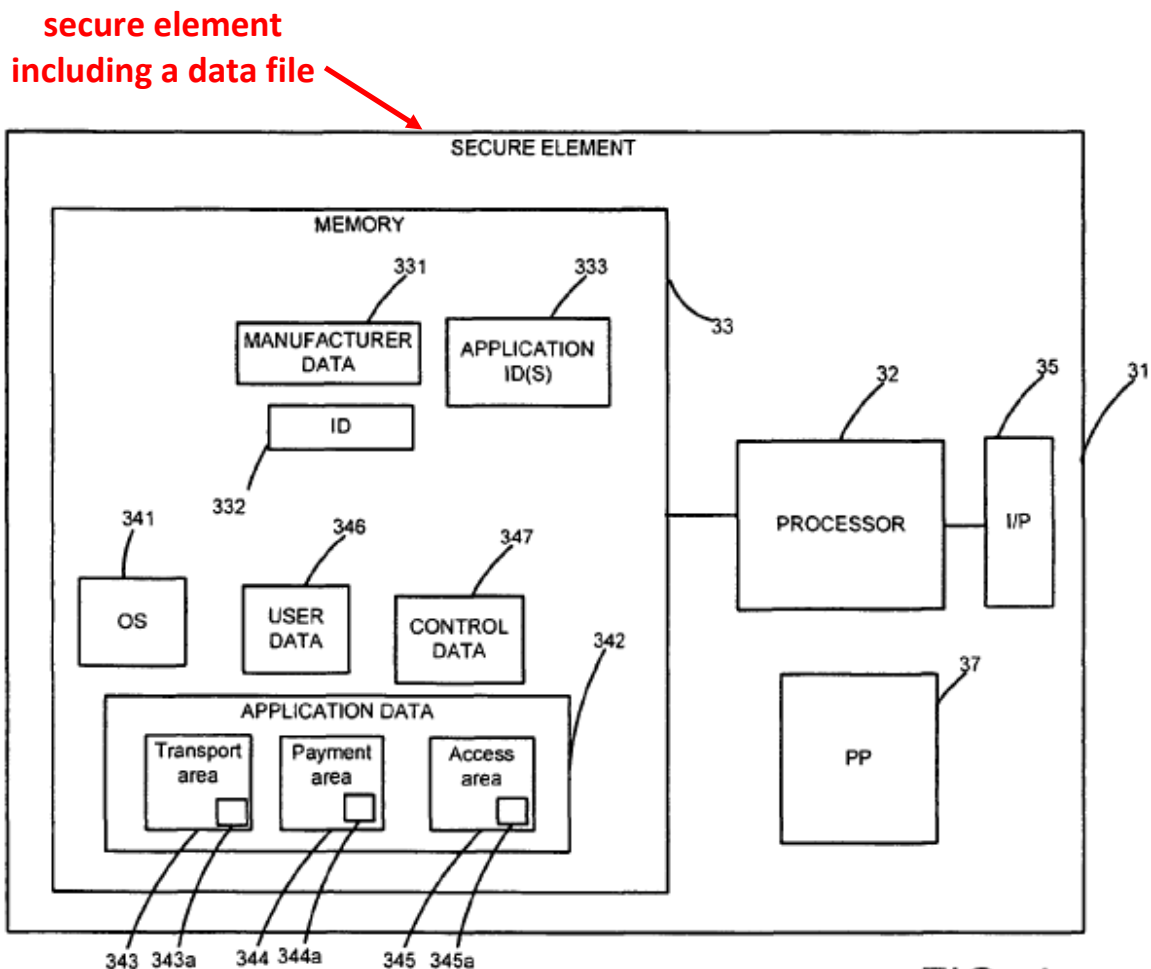


FIG. 4

EX1004, FIG. 4

a) First Mapping

79. For the first mapping, a POSITA would have understood and found it obvious, based on Huomo's description, that the controller 32 and memory store 33 of the SE card 30/31 are affixed to the substrate or printed circuit board in the plastic cover (*mounting structure*). EX1004, 7:19-46 (The SE cards 30/31 (*token*) "each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit" (IC)); *see also*, EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66; EX1017, [0013], [0145], FIG. 1; EX1018, [0002].

b) Second Mapping

80. For the second mapping, Huomo describes "secure element 30" (e.g., "SIM") of device 1 is an "integrated circuit." EX1004, Abstract, 5:24-52 ("a secure element (30 in FIG. 1...) carrying encryption software or an encryption algorithm to ensure secure storage of data relating to a transaction such as, for example, a financial transaction or transactions such as a purchase of a product such as a service 30 and/or or goods and/or information pertaining to or identifying the purchased service or product, for example ticket, permit, pass or access data...The secure element 30...is configured to be programmed or is already programmed with an operating system and one or more applications platforms to enable the secure element to load a corresponding application to enable a transaction to be effected such as at least one of payment for products such as

goods and/ or services and purchase or acquisition of ticket data, permit data, pass data or access data which requires communication of secure data. To this end the secure element is capable of encrypting and possibly also decrypting data. This may be achieved using, for example, a public-private key encryption system, with a private key or keys being securely held by the secure element.”), 7:19-67 (“in FIGS. 1 and 2, the secure elements 30...are programmed with or programmable with an operating system and one or more applications platforms applications so as to be capable of encrypting transaction data and storing encrypted transaction data (for example ticket data, access data, purchase data) in accordance with that applications platform...the secure elements 30 and 31 each have a controller (CONT) 32...and a data or memory store (MEM) 33, generally both provided by an integrated circuit...the secure element 30 is provided by the SIM (Subscriber Identity Module) or USIM (Universal Subscriber Identity Module)”); *supra*, §IX.A.1. As discussed in [60.1], a POSITA would have found it obvious from Huomo’s description that the ICs in Huomo’s token are affixed to the **mounting structure** such as a PCB board in the device’s housing, advantageously effectuating Huomo’s stated objectives and implementation.

[60.3]/[79.3] a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate [the/a] communications data package based on the transaction

information; and

81. Huomo-Smets provides these elements.

a) First Mapping

82. Huomo's SE cards 30/31 (***token***) each have a ***secure element interrogator*** including "a controller (CONT) 32... which controls the functionality of the secure element in accordance with its operating systems and the installed applications platform or platforms." EX1004, 7:31-46. The controller 32 (***secure element interrogator***) and memory store 33 of the SE card 30/31 are affixed to the substrate or printed circuit board in the plastic cover (***mounting structure***).

EX1017, [0013], [0145], FIG. 1; EX1018, [0002]; *see also, supra*, [60.1] (citing EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66).

83. Huomo's controller 32 (***secure element interrogator***) "controls the functionality of the secure element" including "decrypting encrypted data" stored in the memory store and "transfer of data from a memory store of the secure element," which would involve ***interrogating the secure element*** (memory store 33 of secure element 30). EX1004, 7:19-52, 8:25-42, 2:47-49, 5:41-61, 24:55-60 ("processor of the secure element will control transmission of data from the secure element").

84. I note that the fact that controller 32 is provided within Huomo's secure element 30 is consistent with the '924 Patent, which recites that the

interrogator “may be physically incorporated into the secure element” and that in a “‘Reader On Card’ (ROC) device the interrogator and SE are integrated together on the same medium, device or circuit.” EX1001, 7:43-8:3.

85. As discussed above in [60.2], the Huomo-Smets combination teaches that the secure element, through its memory store 33, stores transaction/payment data for each financial product (credit/debit card number) in one or more data files and therefore teaches that the controller 32 (*secure element interrogator*) *acquires the transaction information* (including credit/debit card number) *from the secure element data file* to transfer the data from the memory store 33. *Id.* For this example, as discussed above in [60.pre], the SE card controller 32 sends the transaction data to the host device controller (e.g. Huomo’s controller 20) by generating an APDU (Application Protocol Data Unit) (*generating the communications data package*) defined in ISO 7816-4 *based on the transaction information* (including credit/debit card number).

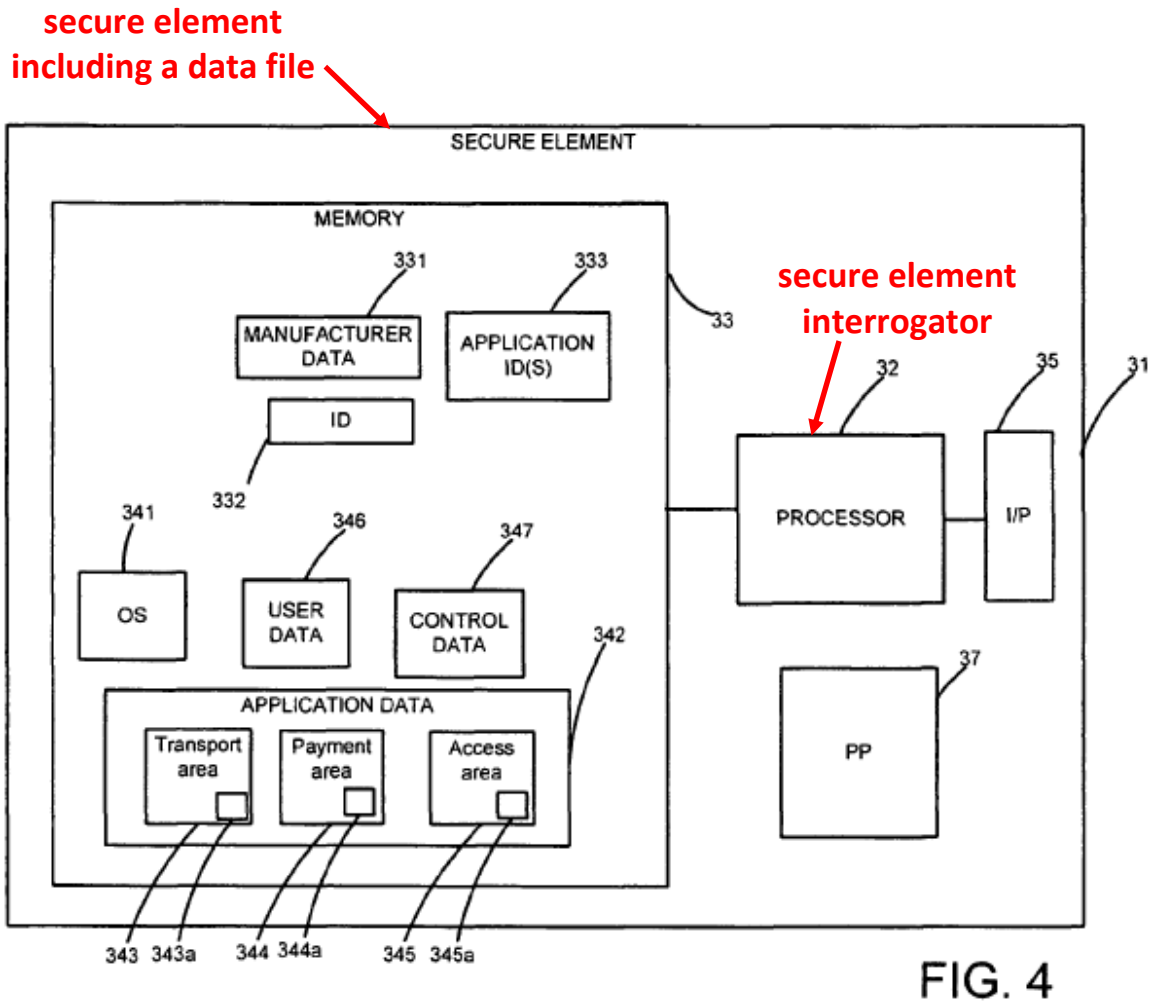


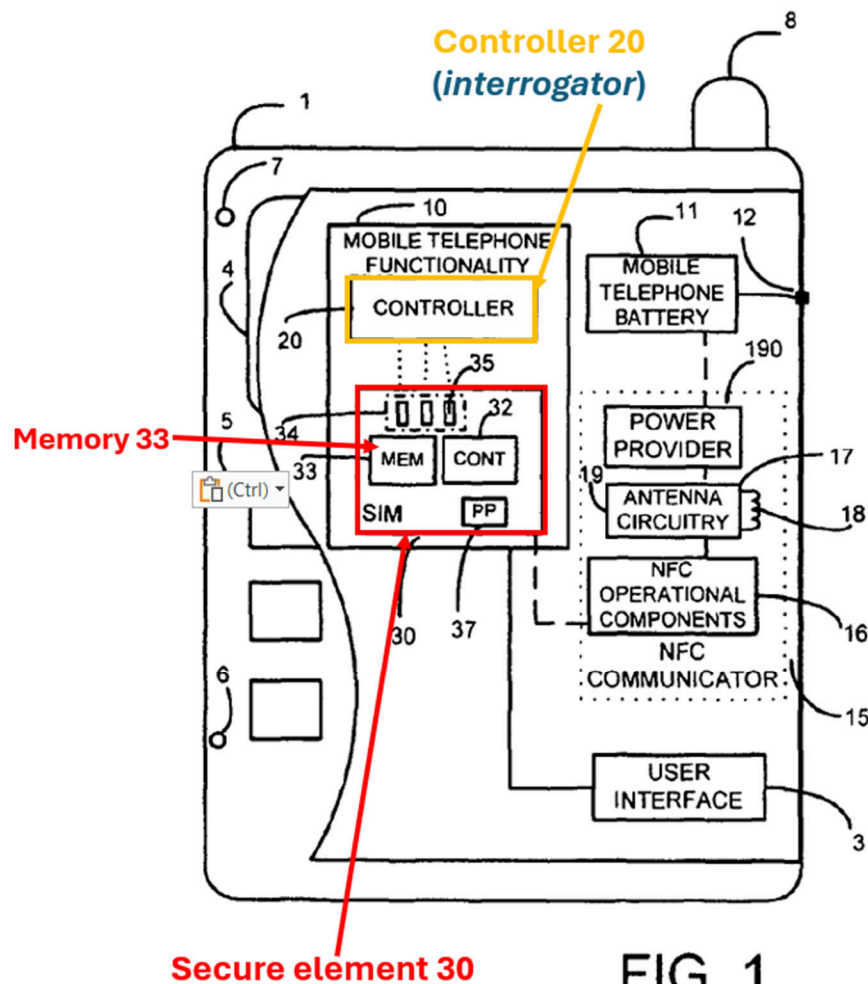
FIG. 4

EX1004, FIG. 4

b) Second Mapping

86. According to the second mapping, Huomo's **token** includes the secure element 30/31 coupled to "a controller 20" (**secure element interrogator**) of the device 1/1' (**cellular network device**) to "enable communication of data between the controller and the secure element 30," and the controller 20 is coupled to the NFC communicator 15 to "enable communication of data between the controller 20 and the NFC communicator 15." EX1004, 6:23-28, FIGS. 1-2. Given that the

device “may be provided wholly or partially as an integrated circuit or collection of integrated circuits,” a POSITA would have found it obvious from Huomo’s description that the “controller 20” is also provided as integrated circuit(s), e.g., on a PCB board of the device housing (*affixed to the mounting structure*). EX1004, 5:22-23, 7:31-38, 24:4-17; *supra*, §IX.A.4, Element [60.1].



EX1004, FIG. 1

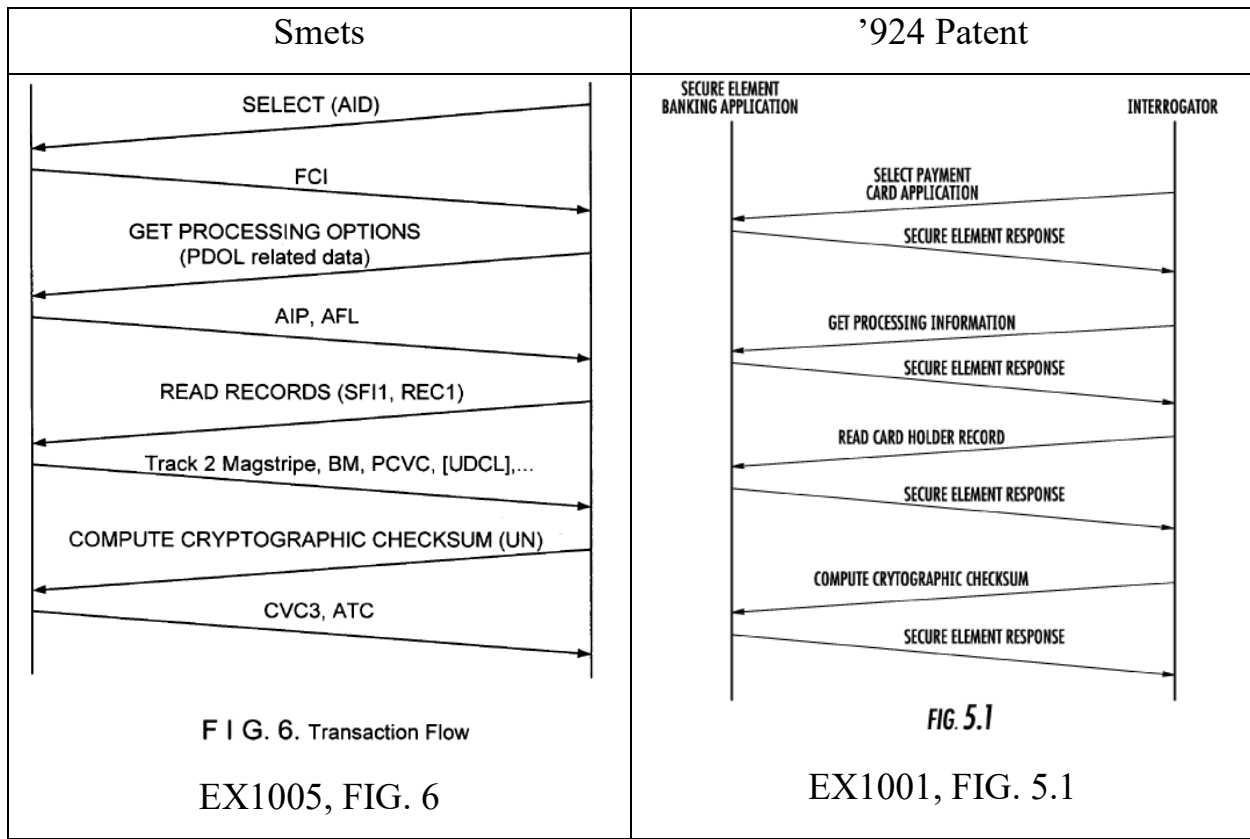
87. The controller 20 (*secure element interrogator*) “communicate[s] data with the secure element” through an interface that is “in compliance with ISO

7816.” EX1004, 5:52-56, 6:23-28, 7:47-52, 10:10-14; *supra*, §IX.A.1. A POSITA would have found it obvious that the controller 20 is ***configured to interrogate the secure element*** using the communication capability to communicate data with the secure element. *Id.*

88. As discussed above in [60.2], the Huomo-Smets combination teaches that the secure element, through its memory store 33, stores transaction/payment data for each financial product (credit/debit card number) in one or more data files and therefore teaches that the controller 20 (***secure element interrogator***) ***acquires the transaction information*** (including bank account information, e.g., credit/debit card number) ***from the secure element data file*** to acquire the data from the memory store 33. *Id.* For this example, the controller 20 generates an APDU (Application Protocol Data Unit) (***generates the communications data package***) defined in ISO 7816-4 ***based on the transaction information*** (including credit/debit card number) and sends the APDU to the NFC communicator of device 1/1', which then transmits the APDU to the RF communicator (***host device***).

89. For both the first and second mappings, in the Huomo-Smets combination, as discussed above, the secure element and the interrogator ***exchange transaction data communications*** in a single interrogation session to acquire the transaction/payment data including bank account information, e.g., credit/debit

card number (*transaction information*), in accordance with Huomo and Smets. *Supra*, §IX.A.3; EX1004, 7:19-52; EX1005, [0036]-[0039], FIG. 6 (below). Smets's FIG. 6 illustrates "the interactions and communications between a proximity payment card and a terminal during the conduct of an electronic transaction" (*exchange of transaction data communications*). EX1005, [0022], [0036]-[0037]. In Smets, the terminal is a reader/interrogator. EX1005, [0008] ("reader/terminal"), [0026] ("reader terminal"). A POSITA would have found it obvious to implement the *exchange of transaction data communications* between the secure element and the interrogator (either controller 32 or controller 20) based on Smets's teachings. *Supra*, §IX.A.3. Smets's description of the exchange of transaction data communications aligns with the '924 Patent's description of the "interaction and data exchange between the interrogator chip and... the SE" as shown in the '924 Patent's FIG. 5.1 (below). EX1001, 12:7-10.



[60.4] a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.

90. Huomo-Smets provides these elements.

a) First Mapping

91. For the first mapping, Huomo describes an NFC communicator can be “combined with a removable secure element” and the secure element provides a data store for the NFC communicator. EX1004, 25:63-26:7. A POSITA would have understood and found it obvious based on Huomo’s description that the controller 32, memory store 33, coupling interface 34 comprising one or more coupling elements 35, and NFC communicator of the SE card 30/31 are affixed to

the substrate or printed circuit board in the plastic cover (*mounting structure*).

EX1017, [0013], [0145], FIG. 1; EX1018, [0002]. Huomo discloses that “where the NFC communicator has a direct link to the secure element, then relevant data may be transferred directly from the secure element to the NFC communicator,” and “there may be no direct link between any host processor and the secure element and... the NFC communicator controller... will control transmission of data from the secure element” such that “communication between the secure element... and the mobile telephone functionality 10 is via the NFC communicator.” EX1004, 24:50-60, 15:17-19. For this example, the NFC communicator controller (e.g., NFC operational components 16 including controller 40) (*communications controller*) receives the APDU (*communications data package*) from the secure element controller (*interrogator*) and transmits the APDU (*communications data package*) to the host device controller 20 through the coupling elements 35.

b) Second Mapping

92. For the second mapping, the *communications controller* (e.g., operational components 16 and controller 40 of NFC communicator 15) of the *token* provided by the integrated circuit(s) affixed to a PCB board in the device housing (*affixed to the mounting structure*) receives the APDU (*communications data package*) from controller 20 (*secure element interrogator*) and transmits the

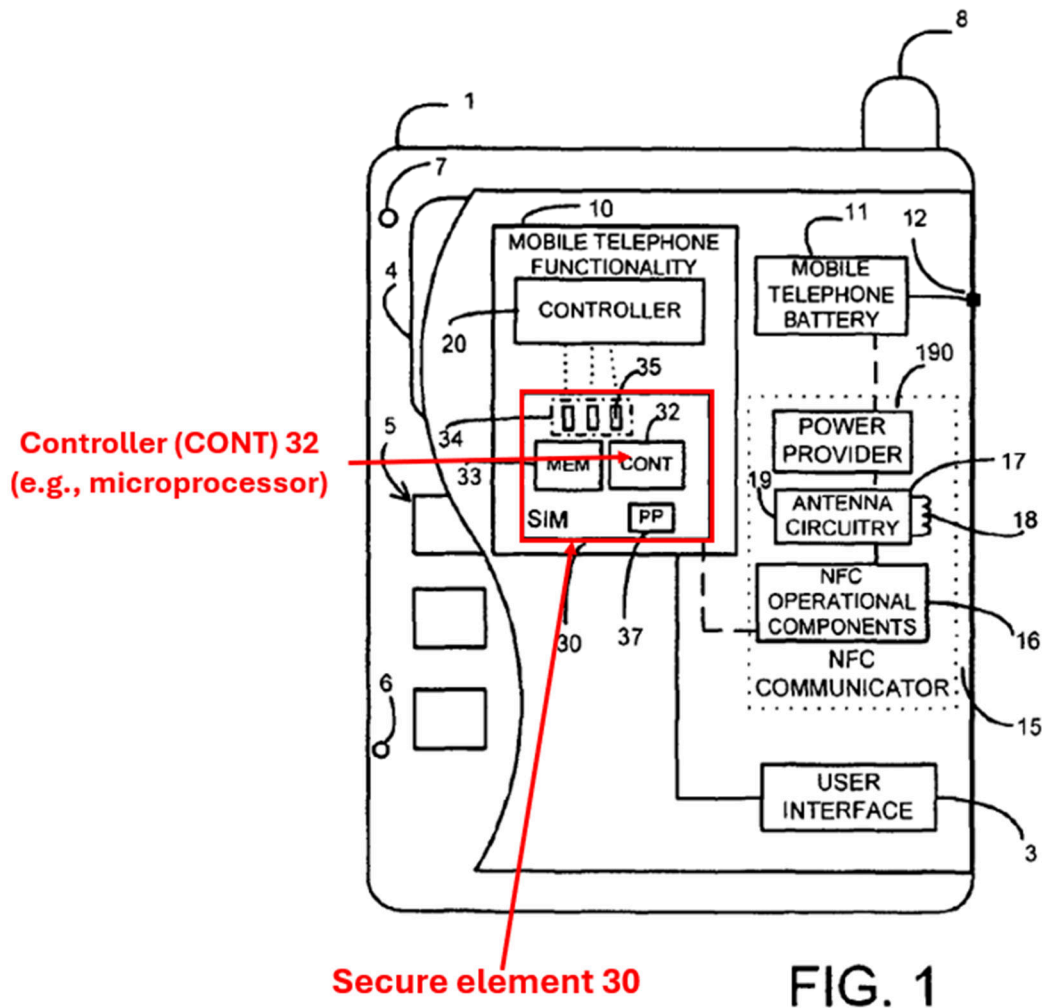
APDU (*communications data package*) to “an external near field RF communicator” (*host device*) through the NFC connection. *Supra*, §IX.A.1, 4, Elements [60.1]-[60.3]; EX1004, Abstract, (“An embodiment provides a device having a secure element to enable transfer of data from a memory store of the secure element directly or indirectly to an NFC communicator wherein such NFC communicator: is operable to communicate with an external near field RF communicator...wherein in operation as a result of communication with the other or external near field RF communicator, data from the secure element is transmitted to the other or external near field RF communicator”), 3:20-40 (“transmission of data by the NFC communicator to another or external near field RF communicator”), 5:22-40 (“an NFC communicator 15 to communicate data stored by the secure element 30 or 31 to another near field RF communicator”), 6:23-41 (“in FIGS.1 and 2, the secure element is coupled to a controller 20 of the device 1 to enable communication of data between the controller and the secure element 30 or 31 and the controller 20 is coupled to the NFC communicator 15 to enable communication of data between the controller 20 and the NFC communicator 15.”), 13:50-55, 20:11-12, 23:42-45, 24:4-17 (“the NFC communicator...may be implemented as an integrated circuit...on a PCB board”), 25:11-16, 25:35-40, FIGS. 1-2, claims 11-12.

(b) Claims 65, 83

[65]/[83] The token of claim 60/79 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.

93. Huomo-Smets provides these claims. Under both mappings, and as I discussed above, the Huomo-Smets combination structures its transaction data stored in the secure element 30, including a dynamic authentication code (e.g., CVC3) (*dynamic card verification code*) computed from the *unpredictable number* (UN), in accordance with Smets, for compatibility with existing magnetic stripe infrastructure and enhanced security through dynamic authentication. *Supra*, §§IX.A.2-4; EX1005, [0010], [0014], [0024]-[0026], [0037]-[0039], FIG. 5.

Huomo's secure element 30/31 has its own "controller (CONT) 32 (which may be a microprocessor, microcontroller or state machine, for example) which controls the functionality of the secure element in accordance with its operating systems and the installed applications platform or platforms...provided by an integrated circuit." EX1004, 7:31-38, FIG. 1 (below).



EX1004, FIG. 1 (annotated)

94. In the combined system, the “controller (CONT) 32” (*microprocessor*) of the secure element 30/31 uses application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication to calculate the dynamic CVC3 (*dynamic card verification code*), from the UN and optionally “the card’s application transaction counter (ATC),” using a secret encryption key stored on the secure element, in accordance with Smets. *Supra*, §IX.A.2-3; EX1005, [0010] (“A security solution, which may be utilized in PayPass, is based on

generation of a dynamic authentication value or number (CVC3). The dynamic authentication value changes with each transaction.”), [0014], [0024]-[0025] (“The PayPass implementation provides a ‘Pay Pass-Mag Stripe’ application, which can process transactions based on proximity cards and magnetic stripe cards. (See FIG. 5). The PayPass-Mag Stripe application is an extension of the currently available magnetic-stripe applications for debit and credit payments.”), [0026] (“payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal. Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number. Alternatively, payment card 1 may be personalized at the card issuer option to compute the CVC3 number based on a portion of the UN and on the card’s application transaction counter (ATC).”), [0037]-[0039].

(c) Claims 77, 86

[77] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device is configured to transmit the data communications package over a wireless network.

[86] The cellular network device of claim 79 further comprising a communications controller affixed to the mounting structure and configured for receiving the communications data package for transmission by the cellular network device over a wireless network.

95. Huomo-Smets provides these claims. As discussed above, the combination’s device 1/1’ in one example is a mobile telephone (cellular telephone or cell phone) (***cellular network device***) configured to “communicate secure data,

via the mobile telecommunications network” or the NFC connection (*transmit the data communications package over a wireless network*). EX1004, 6:35-41 (“In the examples shown in FIGS. 1 and 2 the devices 1 and 1’ are mobile telephones (cellular telephones or ‘cell phones’), although the device may be any suitable portable (user-carryable) user device having mobile communications such as a for example a portable computing device, for example a PDA or laptop having mobile communications facilities”), 15:25-35 (“devices...communicate secure data, via the mobile telecommunications network”), FIGS. 1-2; *supra*, §IX.A.4, Elements [60.pre], [60.4]. For Claim 86, the *communications controller* — operational components 16 and controller 40 of NFC communicator 15, provided by integrated circuit(s) on the mounting structure — receives the communications data package from the interrogator for that transmission. *Supra*, Elements [60.1], [60.4].

(d) Claims 1, 10, 22, 31, 40, 52

[1.pre]/[10.pre]/[22.pre]/[31.pre]/[40.pre]/[52.pre] A token comprising:

96. Huomo-Smets provides these elements. *Supra*, [60.pre].

[1.1]/[10.1]/[22.1]/[31.1]/[40.1]/[52.1] a mounting structure having a communication connector configured to connect to a computer terminal;

97. Huomo-Smets provides these elements. *Supra*, [60.1].

a) First Mapping

98. Huomo’s SE card (*token*) connects to a controller 20 of the device 1/1’, which may be a laptop, (*computer terminal*) through a “coupling interface 34

comprising one or more coupling elements 35 which may be electrical contact elements” (*communication connector*) “to enable communication of data between the controller and the secure element” card (*token*) “in compliance with ISO 7816.” EX1004, 3:33-40, 6:23-41, 7:47-52, 8:5-34, 20:48-54, 21:11-14. Based on Huomo’s express disclosure of the SE in the form of a SIM card or SD card, a POSITA would have understood and found it obvious that the SE card (*token*) includes a substrate or a printed circuit board in a plastic cover (*mounting structure*) with contact terminals (*communication connector*) to connect to the device 1/1’ (*computer terminal*).

b) Second Mapping

99. Huomo’s NFC communicator “communicate[s] data stored by the secure element 30 [of sending device 1/1’]... to another near field RF communicator” of “another device” (recipient device) through a near field radio frequency (“RF”) connection/link (*communication connector*). *Supra*, §IX.A.1; EX1004, Abstract, 2:3-7 (“the NFC communicator [of the sending device] is operable to supply the secure data via NFC communication to a near field RF communicator which may either have the functionality to decrypt the secure data or more likely will supply the secure data to another device which has that capability”), 2:47-67 (“communicate with an external near field RF communicator”), 3:20-26, 5:24-40 (“an NFC communicator 15 to communicate

data stored by the secure element 30 or 31 to another near field RF communicator...by modulating the H (magnetic) field of an RF signal.”), 6:23-28, FIGS. 1-2. In one example shown in FIG. 13, Huomo describes “a secure element near field reader 2001 incorporating a near field RF communicator 2002... and associated with a user interface 2003 having a display 2004 to display information and instructions to the user. The controller of the near field RF communicator may be a secure controller configured to decrypt and verify ticket data received from a user's device. A POSITA would have understood that the near field reader 2001 is *a computer terminal*.

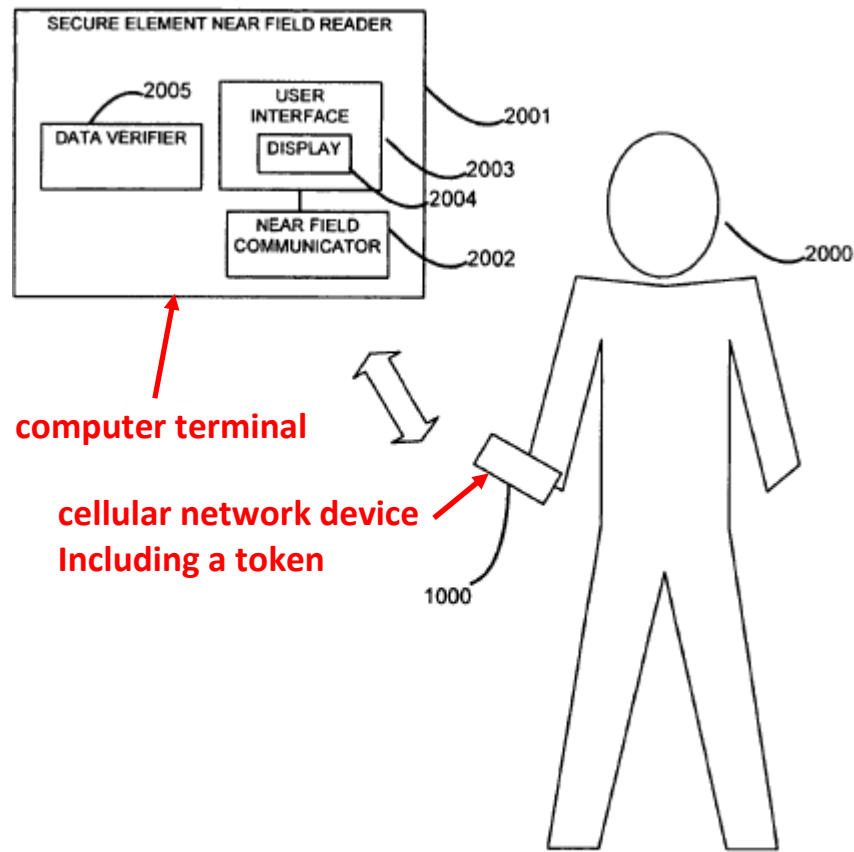


FIG. 13

EX1004, FIG. 13

[1.2]/[10.2]/[22.2]/[31.2]/[40.2]/[52.2] a secure element affixed to the mounting structure, the secure element comprising a data file,

100. Huomo-Smets provides these elements. *Supra*, [60.2].

[10.2]/[40.2] ... the secure element comprising a payment card application...

101. Huomo-Smets provides these elements. *Supra*, §IX.A.4, Element [1.2]. The SE 30/31 “is configured to be programmed or is already programmed with an operating system and one or more applications platforms to enable the secure element to load a corresponding application to enable a transaction to be

effected such as at least one of payment” (*payment card application*) for products and/or services. EX1004, 5:41-6:22. Huomo explains that “[t]he types of transactions that can be handled by the device 1 or 1’are determined by the applications platform or platforms loaded onto the secure element 30 or 31.” *Id.*; *see also id.*; 11:28-52 (“Generally the applications platform(s) will be stored in area(s) of memory for which the operating system encrypts data for security and from which the operating system only allows secure, encrypted (for example public private key encryption using a private key or keys or secure algorithm securely stored by the secure element) data communication. The user data area may have secure data and insecure data storage areas...As an example the application platform layer 302 may provide at least one of a: 1) a banking applications platform defining payment protocols in accordance with banking standards and procedures (including credit card requirements, EMV specifications and the like)...”), 16:18-33 (“the user may wish to use the device as a credit card and may request that VISA (Registered Trade Mark) or MasterCard (Registered Trade Mark) or some other similar credit card company activates or loads a credit card applications platform (for example an EMV platform) onto the secure element.”); EX1005, [0025] (“The standardization method and format may be incorporated in suitable electronic payment system applications so that the system can process both proximity payment card transactions and magnetic stripe card

transactions... The PayPass-Mag Stripe application is an extension of the currently available magnetic-stripe applications for debit and credit payments...It will be understood that the selection of the PayPass implementation for purposes of illustration is only exemplary, and that the principles of the present invention can be more generally applied to electronic payment devices and systems that operate under other common industry or proprietary standards.”), [0036]-[0037].

[1.3]/[10.3]/[22.3]/[31.3]/[40.3]/[52.3] a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging [a plurality of/at least one] transaction data communication(s) only between the secure element and the secure element interrogator; and

102. Huomo-Smets provides these elements. *Supra*, [60.3]. The exchange between the secure element and the secure element interrogator takes place within the SE between memory store 33 and controller 32. EX1004, 7:19-52; *see also* 6:23-28; 7:47-52. A POSITA would have understood and found obvious from Huomo’s description that the transaction data communications acquiring the transaction/payment data including the credit/debit card number (***transaction information***) to pass only between those two components alone, especially as Huomo describes no other participant on that link. EX1004, 6:23-28, 7:47-52, FIG. 1.

[1.4]/[10.4]/[22.4]/[31.4]/[40.4]/[52.4] a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information [as a single data

communication/as track data] to the computer terminal through the communications connector.

103. Huomo-Smets provides these elements. *Supra*, [60.4].

a) First Mapping

104. Huomo's NFC communicator controller (*communications controller*) receives the APDU (*data*) from the secure element controller (*interrogator*) and transmits the APDU with the transaction/payment data including the credit/debit card number (*transaction information*) to the device 1/1' (*computer terminal*) controller through the coupling elements 35 (*communication connector*).

b) Second Mapping

105. Huomo's "NFC communicator 15" (*communications controller*) receives the APDU (*data*) from controller 20 (*secure element interrogator*) and transmits the APDU with the transaction/payment data including a credit/debit card number (*transaction information*) to "an external near field RF communicator" (*computer terminal*) through the NFC connection (*communications connector*). *Supra*, §§IX.A.1, 4, Elements [60.1]-[60.3]; EX1004, Abstract ("An embodiment provides a device having a secure element to enable transfer of data from a memory store of the secure element directly or indirectly to an NFC communicator wherein such NFC communicator: is operable to communicate with an external near field RF communicator...wherein in operation as a result of communication with the other or external near field RF communicator, data from the secure

element is transmitted to the other or external near field RF communicator”), 3:20-40 (“transmission of data by the NFC communicator to another or external near field RF communicator”), 5:22-40 (“an NFC communicator 15 to communicate data stored by the secure element 30 or 31 to another near field RF communicator”), 6:23-41 (“in FIGS.1 and 2, the secure element is coupled to a controller 20 of the device 1 to enable communication of data between the controller and the secure element 30 or 31 and the controller 20 is coupled to the NFC communicator 15 to enable communication of data between the controller 20 and the NFC communicator 15.”), 13:50-55, 20:11-12, 23:42-45, 24:4-17 (“the NFC communicator...may be implemented as an integrated circuit...on a PCB board”), 25:11-16, 25:35-40, FIGS. 1-2, claims 11-12.

106. For both mappings, because the exchange of transaction data communications between secure element and the *interrogator* for acquiring transaction information from the secure element during a single interrogation session occur only between the secure element and the interrogator, it would have been obvious that the output transaction information transmitted by the communications controller to the computer terminal is *a single data communication*. *Supra*, §IX.A.4, Element [1.3]. Even if Huomo alone did not make this obvious, the Huomo-Smets combination makes it explicit, where at the end of an interrogation to acquire transaction information, the transaction

information is transmitted to the computer terminal as **Track data** via “a standardized message” (*a single data communication*). *Supra*, §IX.A.2-4, Element [1.3]; EX1005, Abstract, [0014], [0026] (“terminal 2 packages or formats the ATC, UN, and the CVC3 number in a discretionary data field according to these rules. Terminal may then communicate the discretionary data field under magnetic stripe card conventions to an acquirer host 4 and/or issuer host 5 for authorization of the transaction. Terminal 2 may, for example, send the discretionary data field as part of Track 2 in Data Element 35 (DE35) of a standardized message 100 to the issuer for authorization or approval (8, 110).”), [0029]-[0031], [0035], [0036]-[0039], FIG. 6.

(e) **Claims 2, 11, 23, 32, 41, 53, 61, 80**

[2]/[11]/[23]/[32]/[41]/[53] The token of claim 1/10/22/31/40/52 wherein the plurality of/at least one transaction data communication(s) comprises communications formatted according to ISO 7816-4.

[61]/[80] The token of claim 60/79 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.

107. Huomo-Smets provides these claims. As discussed above, the Huomo-Smets combination provides ISO 7816-4 command-layer commands and responses (APDUs), e.g., “GET PROCESSING OPTIONS,” “READ RECORD,” “COMPUTE CRYPTOGRAPHIC CHECKSUM,” for a plurality of transaction data communications between the secure element and the secure element

interrogator in a single interrogation session to acquire Track data for transactions.

Supra, §IX.A.1-4, Element [1.3]; EX1004, 7:51-52; EX1005, [0036]-[0039], FIG.

6.

(f) Claims 3, 12, 24, 33, 42, 54, 62

[3]/[12]/[24]/[33]/[42]/[54]/[62] The token of claim 1/10/22/31/40/52/60 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

108. Huomo-Smets provides these claims. For example, Huomo's secure element 30/31 already stores an *encryption algorithm* and an *encryption key* (e.g., "a private key or keys" of a "a public-private key encryption system") to encrypt transaction data. *Supra*, §IX.A.1; EX1004, 3:58-62 ("As used herein 'secure element' means any element which is capable of being used and is 'trusted' to hold secure encrypted information and/or data, although not all of the data held by the secure element need be encrypted."), 5:26-52 ('a secure element (30 in FIG. 1 and 31 in FIG. 2) carrying encryption software or an encryption algorithm to ensure secure storage of data relating to a transaction...the secure element is capable of encrypting and possibly also decrypting data. This may be achieved using, for example, a public-private key encryption system, with a private key or keys being securely held by the secure element."), 7:19-65 ("The encryption system may be a public-private key encryption system in which case the secure element will hold a private key or keys. Alternatively the encryption system may be based on a secure

algorithm in which case the secure element will hold the secure algorithm.”), 8:25-34, 11:28-34 (“Generally the applications platform(s) will be stored in area(s) of memory for which the operating system encrypts data for security and from which the operating system only allows secure, encrypted (for example public private key encryption using a private key or keys or secure algorithm securely stored by the secure element) data communication.”), 15:33-36 (“transaction data...encrypted, for example by public/private key”), 23:67-24:3 (“A secure element may use any appropriate encryption algorithm to secure data, provided of course that this can be decrypted by the eventual legitimate reader.”)..

109. As discussed for the Huomo-Smets combination, the secure element uses the stored encryption key to calculate a dynamic CVC3, using the unpredictable number (UN) and an “application transaction counter (ATC)” (*transaction counter*) also stored on the secure element, in accordance with Smets. *Supra*, §IX.A.2-3; EX1005, [0026] (“Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number. Alternatively, payment card 1 may be personalized at the card issuer option to compute the CVC3 number based on a portion of the UN and on the card’s application transaction counter (ATC).”); *see also id.*, [0014], claims 3 and 10 (“an automatic transaction counter (ATC)”).

(g) Claims 4, 13, 25, 34, 43, 55, 63, 81

[4]/[13]/[25]/[34]/[43]/[55]/[63]/[81] The token of claim 1/10/22/31/40/52/60/79 wherein the secure element interrogator exchanges the plurality of/at least one transaction data communication(s) with the secure element only within libraries or memory space residing on the mounting structure.

110. Huomo-Smets provides these claims. *Supra*, §IX.A.3-4, Element [60.3]; EX1004, 6:23-28, 7:51-52; EX1005, [0036]-[0039], FIG. 6 (below). Under both mappings, that exchange occurs only between the combination's ***secure element*** and ***interrogator***, over their coupling interface, and only within libraries or memory space (e.g., “memory 33”) ***residing on the mounting structure*** — both components are integrated circuit(s) on the same substrate or PCB, so no transaction data communication leaves the mounting structure. EX1004, Abstract, 2:35-37, 2:47-67 (“transfer of data from a memory store of the secure element”), 3:44-55, 5:22-23, 6:23-28 (“the secure element is coupled to a controller 20 of the device 1 to enable communication of data between the controller and the secure element 30”), 7:31-52 (“The secure element 30 or 31 also has a coupling interface 34 comprising one or more coupling elements 35 which may be electrical contact elements but could be wireless or contactless coupling elements, for example capacitive, inductive or electromagnetic coupling elements. The coupling elements may, for example, be in compliance with ISO 7816.”), 24:4-17, FIG. 1 (below); EX1005, [0036]-[0039], FIG. 6.

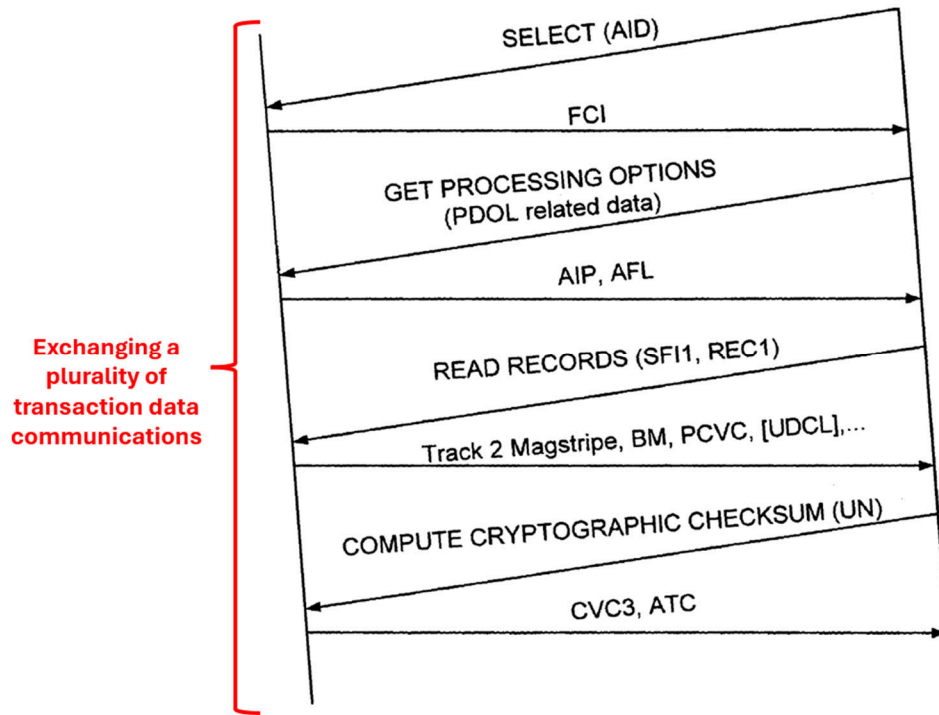


FIG. 6. Transaction Flow

EX1005, FIG. 6 (annotated)

(h) Claims 5, 26, 35

[5]/[35] The token of claim 1/31 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.

[26] The token of claim 22 wherein the secure element comprises a payment card application and the transaction information comprises track data.

111. Huomo-Smets provides these claims. *Supra*, §IX.A.4, Element [10.2] (regarding *payment card application*); EX1004, 5:41-6:22, 11:28-52, 16:18-33; EX1005, [0025], [0036]-[0037].

112. As discussed above, the combined system embeds transaction data retrieved from the secure element within standardized magnetic stripe track

formats (e.g., Track 1, Track 2, and Track 3 data) (*single data communication ... comprises track data*) before transmitting to the host (*computer terminal*), for processing magnetic stripe card transactions. *Supra*, §IX.A.2-3; EX1005, Abstract, [0004]-[0008], [0011]-[0013], [0025]-[0026], [0037]-[0039], FIG. 5 (reproduced below).

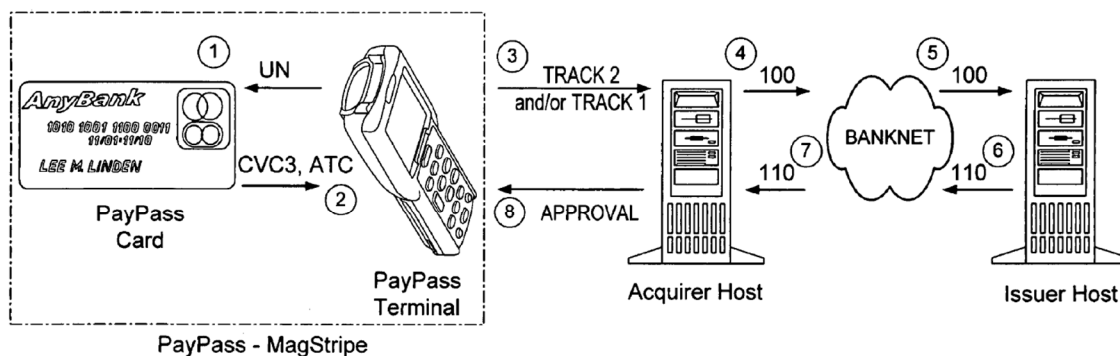


FIG. 5

EX1005, FIG. 5

(i) Claims 6, 16, 27, 36, 46, 56, 64, 82

[6]/[16]/[27]/[36]/[46]/[56]/[64]/[82] The token of claim 1/10/22/31/40/52/60/79 wherein [all] communications to and from the secure element consist of communications from and to a secure element reader.

113. Huomo-Smets provides these claims. *Supra*, §IX.A.4, Element [60.3] (the secure element interrogator reading transaction information from the secure element 30 corresponds to *a secure element reader*).

(j) Claims 7, 17, 28, 37, 47, 57, 66, 84

[7]/[17]/[28]/[37]/[47]/[57]/[66]/[84] The token of claim 1/10/22/31/40/52/60/79 further comprising an antenna that transmits data to and

from the secure element, wherein the secure element is interrogated by an external reader.

114. Huomo-Smets provides these claims. For example, a Huomo describes NFC communicator 15 comprises “a coupler 17 comprising an inductor or coil in the form of an antenna 18 and antenna circuitry 19” (*antenna*) that inductively couples to the antenna of another near field RF communicator to transmit and receive data. EX1004, 6:55-7:3, 8:50-53, 24:4-6, FIGS. 1-2. Huomo further describes a “load modulation” mode in which the NFC communicator responds to commands “sent to an NFC communicator from, for example, an RFID reader” (*interrogated by an external reader*), and a “secure element near field reader 1007 capable of reading by near field communication transaction data from the secure element” of devices 1000-1002. EX1004, 13:50-15:2, 15:5-50 (describing FIG. 10).

(k) Claims 8, 19, 29, 38, 49, 58

[8.1]/[29.1]/[38.1]/[58.1] The token of claim 1/22/31/52 wherein: the secure element comprises an executable application; and [19.1]/[49.1] The token of claim 10/40 wherein: the payment card application comprises an executable payment card application; and

115. Huomo-Smets provides these elements. For example, Huomo’s banking applications and payment applications stored in the secure element are executable payment card applications (or applets). *Supra*, §IX.A.4, Claim [5]; EX1004, 5:41-6:22, 11:28-52, 16:18-33. Huomo explains that the data stored by

memory store 33 “will generally include data such as program data comprising commands and instructions of the applications platform(s) and operating system and content data such as data used by the program data, transaction data and user data.” EX1004, 10:46-51; *see also id.*, 13:522 (“the operating system may be provided as a JAVA applet...The applications platforms may be provided in any of the ways available for provision of the operating system. As an example, an applications platform may be provided as a JAVA (Registered Trade Mark of Sun Microsystems)-enabled applet where a JAVA based or compatible operating system is used.), 16:64-65 (“the service provider loads the applications platform onto the device using an appropriate JAVA-enabled applet, MIDlet or other software program as discussed above”), claim 25.

[8.2]/[19.2]/[29.2]/[38.2]/[49.2]/[58.2] the secure element interrogator is configured to interrogate the executable [payment card] application to acquire the transaction information from the data file.

116. Huomo-Smets provides these elements. *Supra*, §IX.A.4, Element [1.3] and Claim [5].

(I) Claims 9, 18, 21, 30, 39, 48, 51, 59, 67, 78, 85, 87

[9.1]/[30.1]/[39.1]/[59.1]/[78.1]/[87.1] The token of claim 1/22/31/52/60/79 wherein: the secure element comprises a payment card application;
[18.1]/[48.1]/[67.1]/[85.1] The token of claim 10/31/60/79 wherein: the secure element comprises a plurality of payment card applications from different card associations and

117. Huomo-Smets provides these elements. *Supra*, §IX.A.4, Claim [5].

For [18.1], [48.1], [67.1], and [85.1], in the combined system, Huomo's secure element is "programmed with an operating system and one or more applications platforms," and "[t]he types of transactions that can be handled by the device 1 or 1'are determined by the applications platform or platforms loaded onto the secure element 30 or 31." EX1004, 5:41-6:22. A POSITA would have found it obvious to beneficially load payment applications of different card associations on that secure element, so a single token could serve a cardholder's several cards, furthering Huomo's express objectives. EX1005, [0025].

[9.2]/[30.2]/[39.2]/[59.2]/[78.2]/[87.2] the secure element interrogator is configured to interrogate the payment card application; and [18.2]/[48.2]/[67.2]/[85.2] the secure element interrogator interrogates one of the payment card applications.

118. Huomo-Smets provides these elements. *Supra*, §IX.A.4, Claim [5].

[9.3]/[21]/[30.3]/[39.3]/[51]/[59.3]/[78.3] the transaction information comprises card-present data. [87.3] the communications data package comprises card-present data.

119. Huomo-Smets provides these elements. *Supra*, §IX.A.4, Claim [5] (track data provides *card-present data*); EX1001, 5:12-36.

(m) Claims 14, 44

120. Huomo-Smets provides these claims. As discussed above, Smets describes its reader terminal providing "an unpredictable number (UN)" to the payment card (secure element), which then "computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal."

EX1005, [0026], [0028], [0037]. A POSITA would have found it obvious in view of Huomo and Smets, that components or computing systems in the transaction stream, other than the reader, beneficially perform the same function of generating the unpredictable number and transmitting to the secure element, effectuating the stated functionality and objectives. For example, in the Huomo-Smets combination, a POSITA would have found it obvious that the NFC communicator 15 (*communications controller*) beneficially creates the UN and sends the UN to the secure element 30. EX1008, 5:35-41 (“RFID reader 104 sends a UN to transaction device 102 at, for example, the start of a payment transaction. Transaction device 102 encrypts the UN together with other information (a transaction counter and a user identifier) using a secret key and sends the transaction to RFID reader 104.”), 7:22-30 (“The unpredictable number is generated and/or regenerated by any one of the computing systems in the transaction stream. For example, the unpredictable number is generated by computing systems at the account issuer 112, acquirer 110, the receiver, or merchant system 132 locations.”)).

(n) Claims 15, 45

[15]/[45] The token of claim 10/40 wherein the transaction information comprises a dynamic card verification code.

121. Huomo-Smets provides these claims. *Supra*, Claim 65.

(o) Claims 20, 50

[20]/[50] The token of claim 19/49 wherein the executable payment card application includes an application level protocol for authentication of the secure element.

122. Huomo-Smets provides these claims. *Supra*, §IX.A.4, Claim [65] (the combination’s “‘PayPass-MagStripe’ application” providing *an application level protocol* for dynamic authentication of the secure element).

(p) Claim [76]

[76] The token of claim 60 wherein the token has the physical form of a secure digital (SD) chip.

123. Huomo-Smets provides Claim 76. *Supra*, Element [60.pre].

(q) Claims 68-69

[68] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller.

[69] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller and the host device has the physical form of a mobile phone or a PDA.

124. Huomo-Smets provides these claims. *Supra*, §IX.A.4, Elements [60.pre], [79.pre] (“cellular network device,” “mobile phone”); *supra*, Element [60.2] (“secure element”), [60.3] (“interrogator”), [60.4] (“communications controller”);

(r) Claim 70

[70] The token of claim 60 wherein the mounting structure comprises a

substrate.

125. Huomo-Smets provides claim 70.

a) First Mapping

126. A POSITA would have recognized, and found obvious from Huomo's description, that the SIM card includes an IC chip mounted on a substrate (***mounting structure comprises a substrate***). Supra, §IX.A.4, Element [60.1; *see also* EX1017, [0013], [0145], FIG. 1.

b) Second Mapping

127. A POSITA would have found it obvious from Huomo's description that the ICs in Huomo's ***token*** are affixed to a ***mounting structure*** such as a PCB board (***substrate***).

(s) Claim 71

[71] The token of claim 60 wherein the mounting structure comprises a packaging case.

128. Huomo-Smets provides claim 71.

a) First Mapping

129. A POSITA would have also recognized, and found obvious, from Huomo's description, that a SD card includes chips mounted to a printed circuit board and integrated in a plastic cover (***mounting structure comprises a packaging case***). Supra, §IX.A.4, Element [60.1]; EX1018, [0002].

b) Second Mapping

130. A POSITA would have found it obvious from Huomo's description that the ICs in Huomo's *token* are affixed to a *mounting structure* such as a PCB board in the device's housing (*a packaging case*).

(t) Claim 76

[76] The token of claim 60 wherein the token has the physical form of a secure digital (SD) chip.

131. Huomo-Smets provides claim 76. *Supra*, Element [60.pre] (first mapping).

B. GROUND 1B – Huomo-Smets-Kisliakov Renders Obvious Claims 1-71, 76-87

1. Kisliakov

132. Like Huomo, Smets, and the '924 Patent, Kisliakov describes systems in which secure data is stored in a secure element (e.g., smart card) and communicated through a reader to a host, e.g., to enable transactions such as payments. EX1010, Abstract, [0002]-[0003] ("smart cards...for storing data (e.g., a personal identification number) associated with the card...including a storage means... The data stored in the storage means is generally read by some form of terminal device, which includes a magnetic read head, for example."), [0086] ("the smart card 100B includes a microprocessor 259 having an integrally formed central processing unit (CPU) 275 and storage means 276"), [0095] ("the reader 300 includes a transmitter...for transmitting information...causes information...to be

transmitted to a remote console...for use in controlling some functions, such as a banking application”), [0101] (“the reader 300 is hard wired to a personal computer system 700 via a communications cable 603. Alternatively, instead of www.anz.com,” “retriev[ing] on-line music associated with the Blues Guitar Masters Internet site” through “an application associated with the Blues Guitar Masters Internet page commences,”), [0264] (“a personal identification number (PIN) and other data may be kept secure...providing some protection against discovery and copying of the data stored on the card 100B”), [0219] (“message[s] sent from the reader 300 to the computer 100 or set-top box 601”), [0234].

133. Kisliakov expressly describes (1) the “International Standards Organisation (ISO)/International Electrotechnical Commission (IEC) 7816-4 Standards,” which “describe a file system designed for smart cards, together with commands that can be used to interface with the file system,” and (2) communications (commands and responses) between the secure element (e.g., smart card or CPU card 100B) and the secure element reader (e.g., reader 300) as using “Application Protocol Data Unit (APDU)” format, “as described in the ‘ISO/IEC 7816-4 Standards.’ EX1010, [0001] (“smart card for use with a reader device... (CPU) smart card”), [0006] (“The ‘International Standards Organisation (ISO)/ International Electrotechnical Commission (IEC) 7816-4 Standards’ describe a file system designed for smart cards, together with commands that can

be used to interface with the file system.”), [0086] (“the smart card 100B”), [0268] (“The CPU card 100B preferably communicates with the reader 300 using the ‘T=0’ protocol as defined in the ‘International Standards Organisation (ISO)/International Electrotechnical Commission (IEC) 7816-3: 1997 Standards, Part 3: Electronic Signals and Transmission Protocol’, [hereinafter referred to as the ‘ISO 7816-3 standards’]. However, any other suitable bidirectional protocol (e.g. T=1), can be used for communications between the CPU card 100B and the reader 300. As will be described in detail below, the reader 300 issues different commands to the CPU card 100B depending on a user interface element 154 selected by the user. All commands issued to the CPU card 100B by the reader 300 are in an ‘Application Protocol Data Unit (APDU)’ format as described in the ‘ISO/IEC 7816-4 Standards, Part 4: Electronic Signals and Transmission Protocol’ [hereinafter referred to as the ‘ISO 7816-4 standards’].”); *see also id.*, [0272]-[0286] (describing transactional user input processing, carried over ISO 7816-4), [0338]-[0349] (describing transaction authentication using ISO 7816-4 commands, e.g., “GET CHALLENGE,” “EXTERNAL AUTHENTICATE,” “PROCESS COORD”), [0323]-[0335] (ISO 7816-4 file access commands used during secure operations, “SELECT FILE,” “READ BINARY,” “WRITE BINARY,” “UPDATE BINARY,” “ERASE BINARY”), [0343] (explicitly links PROCESS COORD APDUs to transaction authorization), [0354] (“The commands and classes referred

to herein are configured in accordance with the ISO 7816-4 standard.”), [0241]-[0245] (a payment transaction that necessarily relies on the above ISO 7816-4 APDU exchanges).

2. Huomo-Smets-Kisliakov Combination

a) Kisliakov is Analogous Art to the '924 Patent

134. Kisliakov is analogous art to the '924 Patent. EX1001, 1:24-29; cl. 1 (“A token”); *supra*, §IX.B.1 (Kisliakov);. In addition to being in the same field of endeavor, Kisliakov is reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50 (“What are needed therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.”), 4:52-67, 5:5-11, 5:12-26, 5:27-36, 5:37-55, 5:61-6:3 (encrypting track data “in order to securely transport the data packet over a public network”), 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27.

b) A POSITA would have been Motivated to Combine Huomo-Smets-Kisliakov

135. Smets already describes ISO 7816-4 type commands and responses (Application Protocol Data Units, or APDUs), e.g., “GET PROCESSING OPTIONS,” “READ RECORD,” for transaction data communications between the payment card (or secure element) and the reader in a single interrogation session, without expressly using the term “ISO 7816-4” or “APDU.” *Supra*, §IX.A.2;

EX1005, [0036]-[0039], FIG. 6. Kisliakov provides an example of conventional commands and responses expressed in the APDU format “as described in the ‘ISO/IEC 7816-4 Standards.’” EX1010, [0268]. This is also consistent with Huomo’s secure element and reader (controller 20) interface that is “in compliance with ISO 7816.” EX1004, 7:51-52, FIG. 1.

136. Multiple predictable benefits would have motivated a POSITA to implement Huomo-Smets system as an ISO 7816-4 file system and data communication between the interrogator (e.g., controller 32 or controller 20) and the secure element (e.g., its memory 33) as ISO 7816-4 file system commands, in accordance with Kisliakov.

137. **First**, a POSITA would have combined Huomo-Smets and Kisliakov to promote reliable and robust operation, and interoperability, by using messaging in conformance with a published standard. EX1004, 7:47-52 (“in compliance with ISO 7816”); *see also* 6:23-28, 8:5-34, 20:48-54, 21:11-14, 9:55-59, 11:52-55, 12:13-15, 14:38-62, 18:54-56; EX1010, [0323], [0414].

138. **Second**, a POSITA would have been motivated to implement Kisliakov’s suggestions in the Huomo-Smets system to promote file handling and control. For example, implementing messaging according to 7816-4 would have promoted a defined addressing scheme for the secure element’s storage such that distinct categories of cardholder data occupy separate files that the interrogator

(e.g., controller 32 or controller 20) can select individually. EX1010, [0351], [0414]. Kisliakov describes a SELECT FILE command carrying a “two-byte file identifier,” such that “[i]f the two-byte file identifier as shown in Table 31 points to a valid file, then that file becomes an active file.” EX1010, [0324]. The reader then reads that file alone, because Kisliakov’s read binary process is “executed to read data from a currently selected elementary file stored in the storage means 276.” EX1010, [0414]. A POSITA would have recognized that this facilitates a given transaction retrieve only the data that transaction needs. Where information such as “the user’s home address” and “the user’s credit card number” are in “separate files in the memory 276 of the card 110B,” selecting one beneficially leaves the other unread. EX1010, [0351].

*c) A POSITA would have Reasonably Expected Success when
Combining Huomo-Smets and Kisliakov*

139. The combination amounts to use of a known technique (ISO 7816-4 messaging in accordance with Kisliakov) in a known system (e.g., Huomo’s system that uses ISO 7816 compliant messaging) to yield predictable results. *KSR*, 550 U.S. at 417. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through conventional software updates, and Huomo describes communication over an ISO 7816 compliant interface, Huomo’s controller 32 controls “transfer of

data from a memory store of the secure element,” and Kisliakov’s card is a CPU card whose processor likewise executes file-system commands against the “storage means” it manages. EX1004, 7:47-56; EX1010, [0268].

3. Analysis

(a) Claims 1, 10, 22, 31, 40, 52, 60, 79

140. Even if Huomo-Smets did not render obvious interrogat[ing] the secure element to acquire [the] transaction information from the data file by exchanging at least one (or a plurality of) transaction data communication[s] [only] between the secure element and the secure element interrogator, Huomo-Smets-Kisliakov does. Supra, §§IX.B.1-2. In the combination, the interrogator (controller 32 (first mapping), controller 20 (second mapping)) acquires that transaction information by interrogating its memory, and exchanges ISO 7816-4 APDUs—e.g., SELECT FILE and READ BINARY commands and their responses—with the secure element’s memory store 33 (and with nothing else). EX1010, [0268], [0323], [0326], [0414]; EX1001, 11:33-37 (such commands “interrogate the secure element and execute file system functions according to ISO 7816-4”).

(b) Claims 2, 11, 23, 32, 41, 53, 61, 80

141. Claims [2], [11], [23], [32], [41], [53], [61] recite *plurality of transaction data communications comprises communications formatted*

according to ISO 7816-4. Even if the Huomo-Smets combination did not render obvious *ISO 7816-4* type of commands and responses (APDUs) (*plurality of transaction data communications*) between the secure element and the secure element interrogator (e.g., controller 32 (first mapping), controller 20 (second mapping)), the Huomo-Smets-Kisliakov combination renders obvious such features through express disclosure. *Supra*, §§IX.B.1-2.

Remaining Challenged Claims

142. The remaining limitations of Claims 1-71 and 76-87 are met as shown in Ground 1A. *Supra*, §IX.A.4.

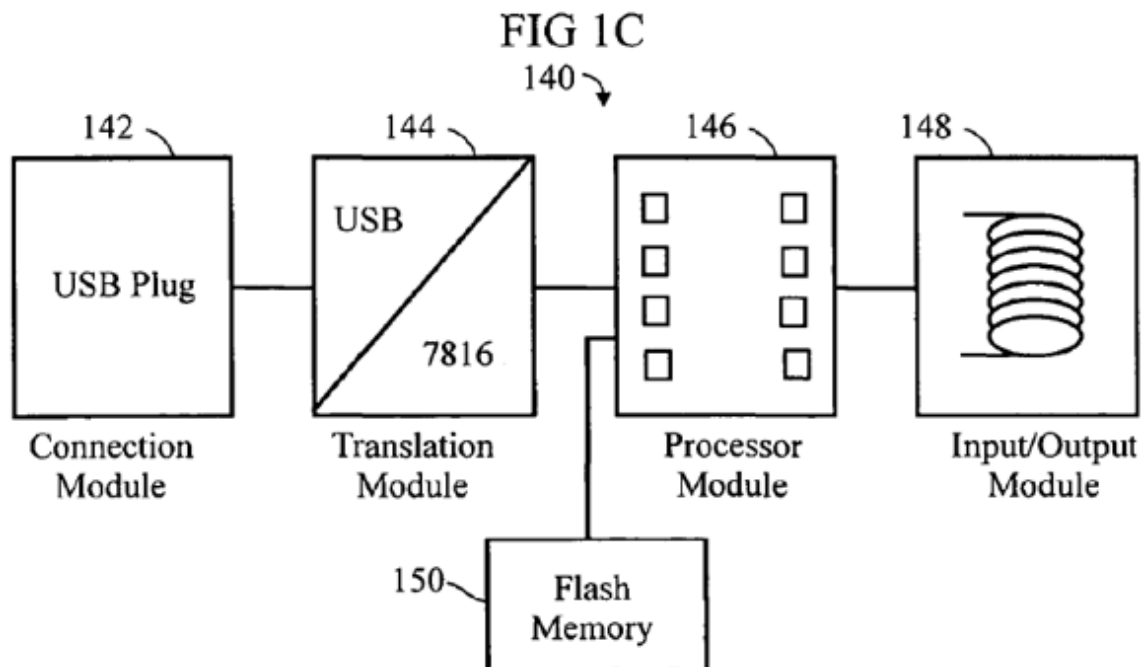
C. GROUND 2A – Ryan-Abbott Renders Obvious Claims 1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, and 84-86

1. Ryan

143. Ryan describes a “compact personal token apparatus” (e.g., “smart fob”) that bridges the “virtual world of the Internet” and “real world transactions.” *See e.g.*, EX1006, Title, Abstract, 2:7-9 (“secure identification, electronic payment transaction and authentication are completed”), 1:45 (“Internet transactions”), 2:31-40, 3:18-23 (“using USB tokens for...user authentication (storing digital signatures, certificates, key sets, finger-based biometric templates, usernames and passwords), digital content and transaction security as well as enterprise and Internet security”), 5:13-30 (“Each electronic certificate includes transaction data

and identification data...”), 12:58-67 (“real world transactions”), 15:52-55, 29:20-22 (“The device (smart fob, USB key fob) can function as a Smart Card for online-banking. This embodiment could include a SIM card.”).

144. Figure 1C illustrates Ryan’s modular architecture, comprising four modules—connection module 142 (e.g., USB plug), translation module 144, processor module 146, and input/output (I/O) module 148—provided on the same mounting structure of token 140. EX1006, 17:35-18:54, FIG. 1A; *see also id.*, 19:24-40, FIG. 1C (the same architecture is extended with flash memory 150, in a “Secure Digital (SD) card format, and including SIM card,” which stores application data and transaction values).



EX1006, FIG. 1C

145. Ryan’s “connection module 102” interfaces with a host (PC or other

device), for example, “the connection module can be a USB plug, for plugging directly into a personal computer (PC),” while “[o]ther possibilities for connecting (communicating) with the personal computer are FireWire, IR, Bluetooth, standard serial port, WLAN, etc., basically any suitable interface between an external memory/processing apparatus and a personal computer.” EX1006, 17:47-57.

146. The “processor module 106” (e.g., “a smartcard processor”) controls device operation and can be a dual interface (DI) smart-card-type chip capable of interacting with both contact (ISO 7816) and contactless (ISO 14443/15693) interfaces. EX1006, 2:18-60 (“The dual interface (DI) smart cards typically have an 8, 16 or 32 bit microprocessor controller”), 4:34-47 (“a smartcard processor having a smartcard processor-compliant interface of communicating according to a smartcard input and output protocol”), 13:58-61 (“The processor module may comprise a dual interface (DI) chip.”), 18:12-38 (“ISO 7816 is a smart card contact interface...The processor module 106 is for controlling operation of the compact personal token apparatus (‘device’) of the present invention and is preferably capable of operating as a dual-interface (DI) chip. For example, Mifare ProX, Infineon 66 series, etc. The dual interface chip is available from various vendors (e.g., Philips, Infineon, ST Microelectronic), and is capable of interfacing from ISO 7816 (contact interface) to either or both of ISO 14443 and 15693 (contactless interfaces).”).

147. The “processor module 106” (e.g., dual interface processor) stores transaction data internally or via associated flash/EEPROM (FIG. 1C) and communicates with “translation module 104” through “ISO 7816 compliant messages.” EX1006, 3:18-23 (“storing digital signatures, certificates, key sets, finger-based biometric templates, usernames and passwords”), 5:13-30 (“Each electronic certificate includes transaction data and identification data...”), 14:28-37 (“ISO 7816 compliant messages...a dual interface processor having an ISO 7816 compliant interface communicating through the interface module with the host processing device.”), 15:11-25 (“The apparatus may further comprise a processor module; and additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module; wherein the additional memory can be used for user authentication and to run applications.”), 19:24-40 (“In this embodiment 140, a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications. The memory management for the device may be handled by a crypto controller operating system with an 8 bit address bus in the dual interface (DI) chip. The flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card. (A crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.)”), 28:30-37 (“a flash memory or

EEPROM device powered and addressed by the dual interface controller chip. The additional memory can be used for user authentication (storing digital signatures, certificates, key sets, finger-based biometric templates, usernames and passwords) and to run applications.”), FIG. 1C.

148. “Translation module 104” (or “interface translator chip (104)”) bridges the host interface (e.g., USB) and the processor module, performing bidirectional message translation from “standard-compliant contact based interface messages to ISO 7816 compliant messages” (ISO 7816 signaling) and from “ISO 7816 compliant messages to standard-compliant contact based interface messages.” EX1006, 4:34-47 (“the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.”), 18:12-29 (“The translation module 104 is for going (moving signals) from USB (the exemplary interface with the computer) to a smart card interface format, such as ISO 7816, and vice-versa. The translation module may comprise a Philips TDA8030 USB/7816. (ISO 7816 is a smart card contact interface.)”), 27:19-20. Ryan explains that the translation function may be implemented as a dedicated microcontroller, “[a] micro-controller such as an 8 bit micro-controller (ST7 FSCR1E4MI) can be used as an interface translator chip (104) between the USB connection 102 and the processor module 106. (The

processor could be mounted in a SIM module.)” EX1006, 18:18-22. Ryan further explains, “[t]he translation module may be incorporated in the processor module [so] that the device can go directly from USB to wireless without being limited by smart card software architecture limitations.” EX1006, 13:58-67.

2. Abbott

149. Like Ryan, Abbott describes a USB-compliant personal key architecture (e.g., “compact personal token (300)”) in which a translation module (e.g., “translation module 318”) resides within an interface processor positioned between a host computer and a secure smartcard processor (e.g., “smartcard processor 320”). *See e.g.*, EX1009, Title, Abstract, 9:12-10:15, claim 1 (“A compact personal token (300)...”), FIG. 3.

150. Messages originating at the host are packaged using USB conventions and transmitted to the personal key/token (300) and, upon arrival, the translation module 318 performs “unpackaging...to recover the smartcard reader command” and then translates that command into “a smartcard command within the personal key...[which is] provided to the smartcard processor [320].” EX1009, 4:9-18, 10:17-11:7, FIGS. 3, 4B. Conversely, responses generated by the smartcard processor 320 are returned to the interface processor, translated into reader-level responses if needed, and then transmitted back to the host after being “packaged by the translation module 318” using USB framing, including the addition of USB

headers and related metadata prior to transmission. EX1009, 10:17-11:11 (“In one embodiment, messages and commands that are sent to the personal key 300 packaged as: USB command= USB header+ USB cdata (wherein USB cdata is the smartcard compliant command) and messages and responses from the personal key 300 are packaged as: USB response =USB header+ USB rdata (wherein USB rdata is the smartcard compliant response)...messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318 and unpackaged by the communication module 312 [on the host computer] before being provided to the operating system [of the host computer].”), Table II (“the translation module 318 adds a USB header to create a USB response”).

151. This bidirectional translation pipeline enables the smartcard processor 320 to operate as if it were connected to a conventional smartcard reader, while still communicating over a USB interface (326). EX1009, 11:12-13 (“the SREM 316 emulates the presence of a smartcard reader for the smartcard processor 320”), claim 2 (“the interface processor (314) emulates a smartcard reader to the smartcard processor (320)”). The packaging step ensures that smartcard-level transaction responses (e.g., command results, ATR responses, or protocol exchanges) are properly formatted for transport over the USB interface, while preserving the semantics of the underlying smartcard communication. EX1009, 10:17-11:11, 14:1-15 (“After the personal key 300 is activated, it sends a message

indicating as such to the host computer 102...a response that is compatible with the smartcard application 110, namely, an ATR message... after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320... The smartcard provides a response consistent with the ISO standards to the emulation module 316.”).

3. Ryan-Abbott Combination

(a) Ryan and Abbott are Analogous Art to the '924 Patent

152. Ryan and Abbott are analogous art to the '924 Patent, both because they are within the same field of endeavor (EX1001, 1:24-28; cl. 1 (“A token”); *supra*, §IX.C.1-2) and reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50 (“What are needed therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.”), 4:52-67, 5:5-11, 5:12-26, 5:27-36, 5:37-55, 5:61-6:3 (encrypting track data “in order to securely transport the data packet over a public network”), 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27; *infra*, IX.C.3; EX1009, 1:16-18 (“an inexpensive USB-compliant personal key that is compatible with existing smartcard processors, drivers, and instruction sets”), 2:9-11 (“These challenges include...ensuring the security of e-mail and other electronic communications, as

well as Internet commerce.”); *see also, supra*, §III.B (application of Ryan by Examiner).

(b) A POSITA would have been Motivated to Combine Ryan and Abbott

153. Ryan already defines its translation module 104 as a protocol translation boundary between the host interface (e.g., USB) and the smartcard domain (e.g., ISO 7816), and it may be implemented as a microcontroller performing interface translation between USB and the processor module. *Supra*, §IX.C.1; EX1006, 14:31-35, 18:12-22. This bidirectional conversion role already includes parsing and constructing messages at both interfaces. Abbott provides an example of a translation module that performs a closely aligned function and makes express the known technique of including packaging and unpackaging of messages with USB framing (adding/removing USB header and metadata to/from smartcard response / command messages). *Supra*, §IX.C.1. Abbott explains that “messages transmitted by the smartcard processor 320...are packaged by the translation module 318” before transmission to the host. EX1009, 10:17-11:11, FIGS. 3, 4B, Table II. A POSITA would have naturally been motivated to look to Abbott for implementation details for a packaged single-message transmission. In the Ryan-Abbott combination, Ryan’s translation module 104 is enhanced with Abbott’s suggestions of message packaging functionality of translation module

318.

154. Multiple considerations would have led a POSITA to implement this combination.

155. **First**, a POSITA would have been motivated to implement this combination for clean separation between transport protocol (USB) and application protocol (ISO 7816 smart-card messaging). Abbott's explicit message packaging ensures that each layer is clearly delimited. EX1006, 17:35-18:38; FIGS. 1A, 1C; EX1009, 9:12-11:16. This reduces ambiguity in message parsing on the host side and enables compatibility with existing middleware or drivers that expect USB-framed payloads, which is particularly important for transaction-oriented data exchanged with secure elements.

156. **Second**, a POSITA would have been motivated to implement the Ryan-Abbott combination for enhanced robustness or fault tolerance (the system works reliably even when things go wrong). Incorporating Abbott's message packaging functionality into Ryan's translation module promotes message headers for error detection, improved synchronization and safer multi-message handling, such that messages do not get mixed up, errors are easier to detect, and communication stays consistent. EX1006, 13:58-67, 18:12-29, 27:19-20; EX1009, 4:9-18, 10:17-11:13, FIGS. 3, 4B, Table II. A POSITA would have recognized the benefit of such error detection if a transmission were interrupted, for example.

157. **Third**, a POSITA would have been motivated to use Abbott's message packaging suggestions in Ryan for improved host-side interoperability. For example, incorporating Abbott's structured message format promotes compatibility with various host drivers and middleware through supporting standardized communication framing (e.g., USB). EX1006, Abstract (desire for capability of "exchanging information with other devices having compatible interfaces"), 14:28-37, 18:12-38; EX1009, 1:16-18 ("compatible with existing smartcard processors, drivers, and instruction sets"), 3:17-23 (desire to use with "legacy personal identification devices...mak[ing] maximum use of existing smartcard protocols, software and devices wherever possible...retain[ing] at least a limited compatibility with existing devices designed to interact with smartcards"), 4:9-18, 10:17-11:13.

158. I note that, in addition, a POSITA would have found it obvious to use Abbott's SREM (smartcard reader emulation module) functionality in Ryan's processor module 106/146 to explicitly emulate reader behavior as a functional enhancement. I note that Abbott explains that the interface processor 314 "implement[s] a translation module [318] for interpreting USB-compliant messages into smartcard processor-compliant messages," EX1009, 4:3-8, and that the translation module 318 "operates in conjunction with" the SREM 316, which "implements functions that emulate those of a smartcard reader," EX1009, 10:8-

16. A POSITA would have found it obvious to locate both the reader-emulation and message-packaging functions in Ryan's processor module 106/146, especially in view of Abbott's description of a single interface processor performing both, and because Ryan itself explains that "the processor module (e.g., 106 or 126) could include (incorporate) the translation module (e.g., 104 or 124) within the processor module itself, thus enabling an even more cost effective solution, enabling using a single chip approach." EX1006, 19:15-24; EX1007, 4:3-8, 10:8-

16. Abbott explains that the SREM "provides all instructions and commands to the smartcard processor 320 and receives messages and responses ... according to the [smartcard] protocol." EX1009, 10:10-16. Ryan's translation module 104 already performs bidirectional movement and conversion of signals between USB and smart-card formats, and may be implemented as a programmable microcontroller and even be integrated into the processor module. *Supra*, §IX.C.1; EX1006, 18:12-22; EX1009, 1:16-18 ("compatible with existing smartcard processors, drivers, and instruction sets"). Additional recognized benefits include, decoupling of host interfaces from processor constraints and stronger modular separation and control over secure communications, promoting interoperability and transaction reliability. EX1006, 19:31-40; EX1009, 10:17-11:11.

(c) A POSITA would have Reasonably Expected Success

159. A POSITA would have reasonably expected success in implementing

this combination, as Ryan already performs bidirectional conversion between USB messages and smart-card messages, adding a structured packaging layer (USB headers/metadata) is largely an extension of its existing translation function rather than a fundamental architectural change. Moreover, Ryan explicitly contemplates the translation module may be implemented as a programmable microcontroller or even integrated into the processor module), which further supports the feasibility of adding packet-formatting logic such as USB encapsulation, in accordance with Abbott.

160. A POSITA would have expected reasonable likelihood of success in availing Ryan's processor module of Abbott's SREM (smartcard reader emulation module) functionality into to explicitly emulate reader behavior as a functional enhancement, particularly because Ryan already describes the processor module as a dual-interface chip that "manages the memory allocation and file access" of the token's on-board memory. EX1006, 2:21-25, 18:30-38. Incorporating features like SREM functionality into the processor module are largely a software/firmware extension, and no structural redesign is required. *Id.*

4. Analysis

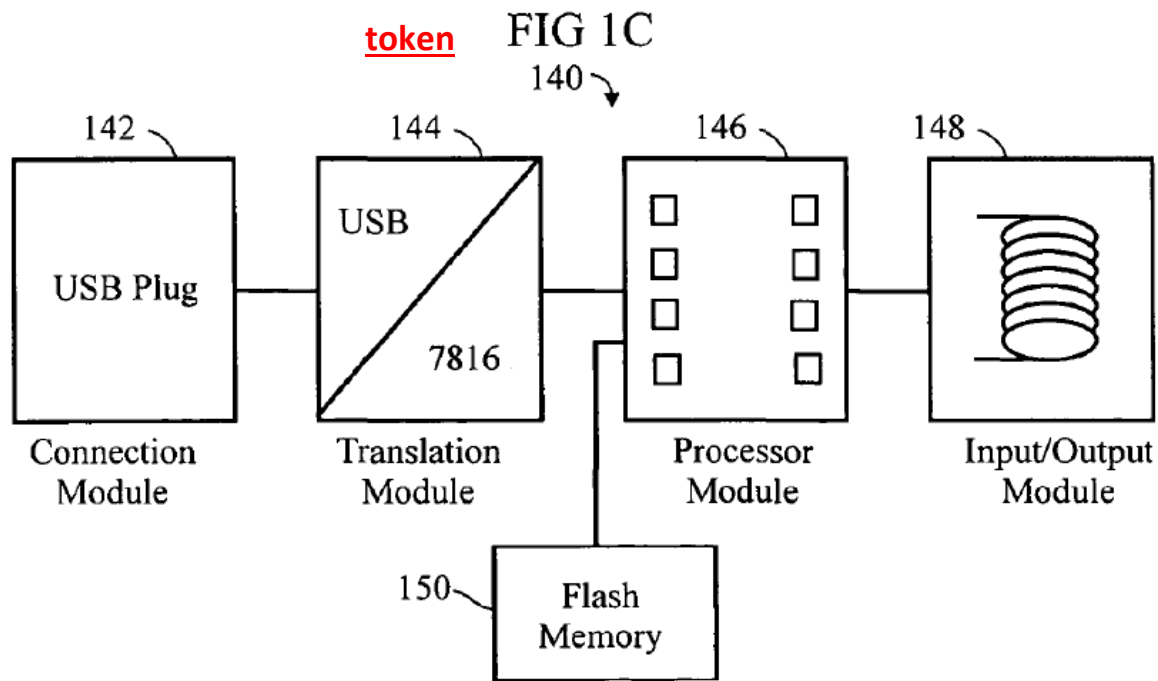
161. Similar to Ground 1A, elements and claims are addressed in groups.

(a) Claims 60, 79

[60.pre] A token for transmitting a communications data package to a host

device, the token comprising:

162. Even if the preamble is treated as a limitation, Ryan-Abbott provides Element [60.pre]. As I discussed above, Ryan describes a “compact personal token apparatus” (e.g., “smart fob”) that bridges the “virtual world of the Internet” and “real world transactions.” *See e.g.*, EX1006, Title, Abstract, 2:7-9, 1:45, 2:31-40, 3:18-23, 5:13-30, 12:58-67, 13:32-38 (“The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob. In some implementations it will take the general form factor required of the standard compliant interface such as SD and Mini SD cards, Multi Media Cards (MMC), PCMCIA Cards, etc. The compact personal token apparatus generally comprises a wireless interface.”), 15:52-55, 29:20-22 (“The device (smart fob, USB key fob) can function as a Smart Card for online-banking. This embodiment could include a SIM card.”); *cf.* EX1001, 1:54-56, 4:8-21; *supra*, §IX.C.1. For example, token 140 of Figure 1C includes four modules— connection module 142 (e.g., USB plug), translation module 144, processor module 146, and input/output (I/O) module 148—arranged in a pipeline and provided on the same mounting structure of token 140. EX1006, Abstract (“compact personal token apparatus (100,120,140,200,220, 300,320,500)”), 17:35-18:54, 19:24-40, FIG. 1C (reproduced below).



EX1006, FIG. 1C

163. Ryan's token connects to a host device. Ryan states that the apparatus "may further comprise a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader." EX1006, 15:29-33. Ryan also describes "a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system." EX1006, 14:28-30. Ryan explains that information "received through the RFID-interface can be stored in the memory of the personal token and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual

world and the real world.” EX1006, 15:4-8.

164. In the Ryan-Abbott combination, the transaction information acquired from the processor module is transmitted to the host as a single packaged message (*a communications data package*), in accordance with Abbott’s suggestions. See §IX.C.3, *supra*; EX1009, 10:17-11:11 (“messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318”), FIGS. 3, 4B, Table I.

[79.pre] A cellular network device comprising:

165. Ryan-Abbott provides Element [79.pre] to the extent it is limiting. For example, Ryan describes “cell phone,” such as “smart cellular phones,” used as “transaction device, data storage device using SD or MMC cards for that,” communicating via various wireless technology (e.g., TDMA, CDMA, GSM digital cellular system) over Internet or “mobile phone networks” (*cellular network device*). EX1006, 6:12-20, 10:3-6 (“A PDA is a handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone”), 11:20-24 (“TDMA Short for ‘Time Division Multiple Access’, a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA is used

by the GSM digital cellular system.”), 12:45-48 (“wireless Technology that allows a user to communicate and/or connect to the Internet or mobile phone networks without physical wires. Wi-Fi, Bluetooth®, CDMA and GSM are all examples of wireless technology.”).

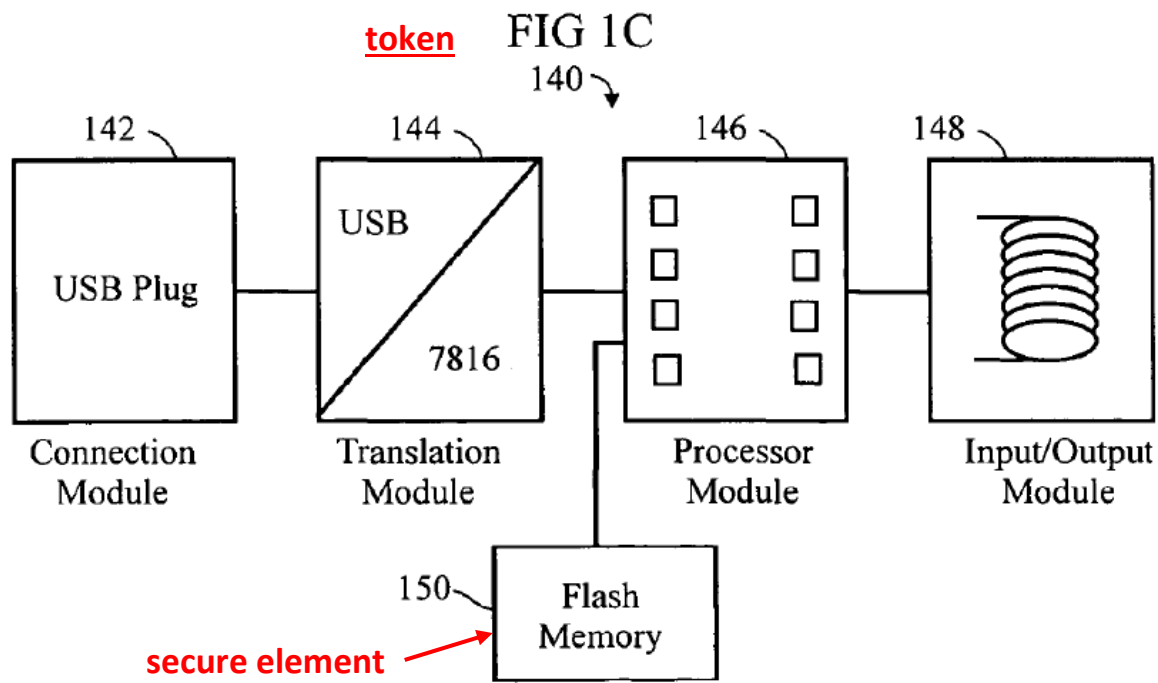
166. Ryan makes clear that “the compact personal token apparatus (or equivalent) may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA), when the personal token device communicates contactlessly in the real world. It does not necessarily have to be removed from the host device.” EX1006, 13:39-44.

[60.1]/[79.1] a mounting structure;

167. Ryan-Abbott provides Elements [60.1], [79.1]. For example, Ryan explains that the token device’s major components are “mounted on a circuit board (PCB...)” (***mounting structure***) and “within a housing” (***mounting structure***)). EX1006, 4:34-47 (“The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system”), 17:35-57, 15:29-33 (“a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device”), FIG. 1A.

[60.2]/[79.2] a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;

168. Ryan-Abbott provides Elements [60.2], [79.2]. For example, in Ryan's token includes flash memory 150. In the FIG. 1C embodiment, "a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications." EX1006, 19:31-36; *see also* EX1006, 4:34-47, FIGS. 1A, 1C. Ryan describes the "flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card." EX1006, 19:36-38. Ryan describes that a "flash memory chip" is "managed by a 32 bit micro-controller." EX1006, 3:9-13. Based on Ryan's explicit disclosure of a flash memory chip with its own micro-controller, a POSITA would have found it obvious that the flash memory 150 includes and is managed by a micro-controller, providing a *secure element*.



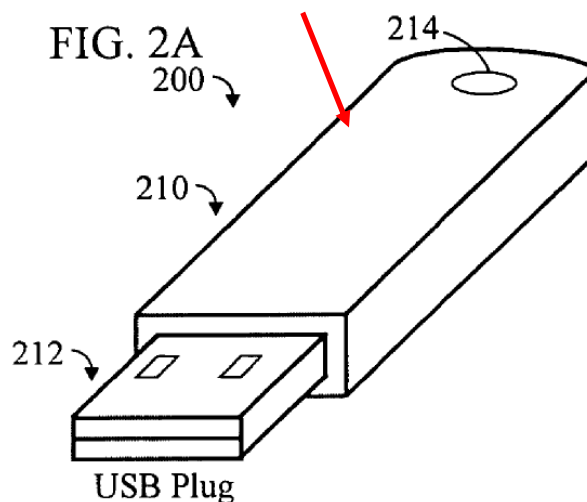
EX1006, FIG. 1C

169. Ryan's token is "embodied in the form of a 'smart fob' apparatus... comprising a main body portion 210 housing the electronics (cf. 104,106, 108) and a USB plug 212 (cf. 102) extending from an end of the body portion 210."

EX1006, 19:45-52. Ryan's flash memory 150 as a SD/SIM card (*secure element*) is *affixed to the mounting structure* by, e.g., a secure mechanical engagement holding the secure element on the PCB and within the housing (*mounting structure* per [60.1]) of the main body portion 210 of the token. A POSITA would have further found obvious that the flash memory is beneficially affixed to the mounting structure with the processor module for packaging efficiency and physical connection based on Ryan's express description that the memory is powered and addressed by the processor module. EX1006, 15:21-24; 19:31-40. Ryan describes that memory residing on the token's mounting structure together with the processor module that addresses it. Ryan explains that the token's "major components, mounted on a circuit board (PCB, not shown) and within a housing (not shown)" include "a processor module 106," and describes the FIG. 1C embodiment 140 as "based on the embodiment 100 of FIG. 1A." EX1006, 17:35-41, 19:24-30, FIGS. 1A, 1C. Ryan describes that "[t]he flash memory could be integrated into the dual interface (DI) chip itself." EX1006, claim 1, 29:35-36. A POSITA would have understood from these descriptions that the memory holding

the token's stored credentials would beneficially sit on the same circuit board, within the same housing, as the processor module that powers it and addresses it over "an 8 bit address bus," and in any event resides within the token's housing (*mounting structure*), which the '924 Patent describes as "a packaging case (for fobs, cartridges, and dongles or SD chips)." EX1006, 15:21-24, 17:35-41, 19:31-36; EX1001, 4:15-21.

**token with mounting structure on/within which
secure element is affixed**



EX1006, FIG. 2A

170. Ryan describes the transaction information stored in that memory, including that "credit card details can be encrypted and stored in the smart fob." EX1006, 24:24-26. Ryan discloses that the processor module 106/146 and the output module 148 "is sufficient for conducting real world, contactless transactions, in the manner of a smart card." EX1006, 20:7-10. For example, the

“smart fob can be used as a payment device for retail purchase” and “personalised like a conventional credit/debit card for electronic payment.” EX1006, 24:9-18, 31:5-7 (“store a credit card and/or debit card on the fob to pay for the purchase.”), 31:39-40. The credit/debit card number is linked to an issuing bank and a bank account, is used to route messages to the issuing bank, and therefore is bank account information. EX1007, 15:40-46. A POSITA would have understood, and found obvious from Ryan’s teachings, that credentials and stored value of this kind reside in one or more data files of the token’s on-board non-volatile memory, in furtherance of Ryan’s express objectives.

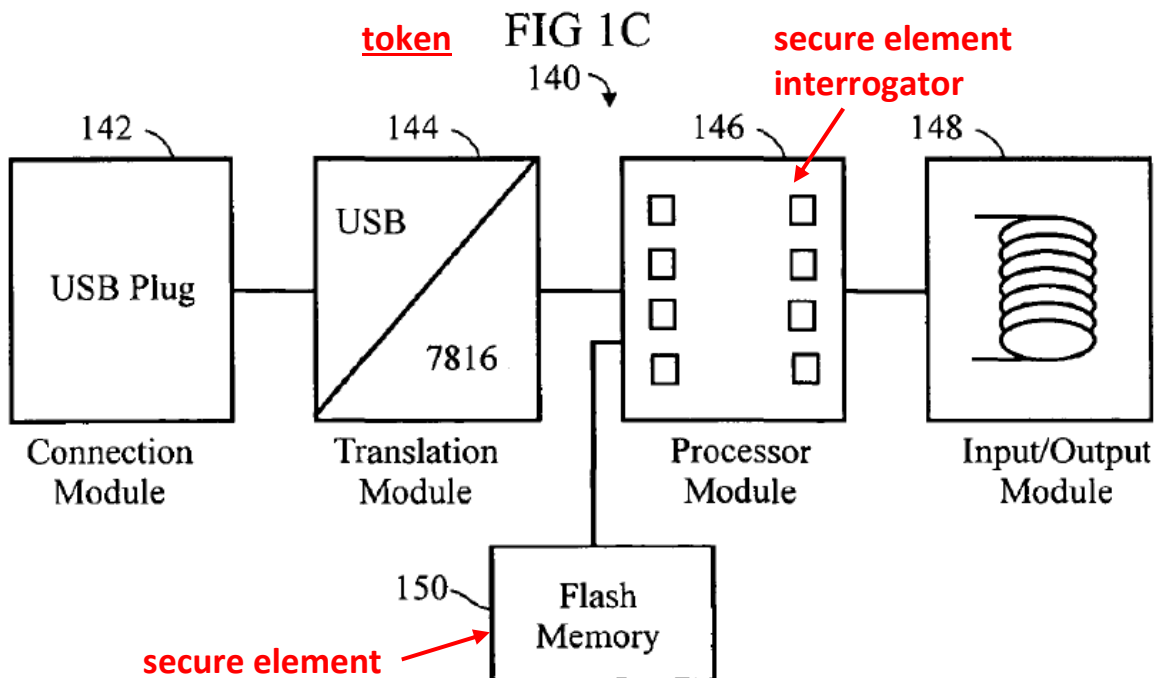
171. Ryan repeatedly describes loading, storing, decrementing, and using stored value on the token device (e.g., “smart fob,” “a SIM card, “SD card”) itself, which resides in one or more data files (*a data file*) of the on-card non-volatile memory, e.g., a flash memory 150 (*secure element*). EX1006, claim 1, 4:21 (“a smartcard chip, for securely storing information”), 19:31-40, 24:24-26, 21:23-60, 23:10-14, 28:30-37, 30:52-57.

172. Ryan describes “tamper-resistant” techniques, and that the data on the chip is encrypted and decrypted, further highlighting the module is a “secure element.” Ryan’s token can include a “tamper-resistance area... for performing various of the e-commerce and other applications.” EX1006, 32:54-63.

[60.3]/[79.3] a secure element interrogator affixed to the mounting structure and

configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate [the/a] communications data package based on the transaction information

173. Ryan-Abbott provides Element [60.3]/[79.3]. Ryan's processor module 106/146 provides a *secure element interrogator*. EX1006, 18:30-38, 19:24-40, FIGS. 1A, 1C. The processor module 106/146 is mounted on the circuit board of the token housing (*affixed to the mounting structure*). EX1006, 17:35-41, FIGS. 1A, 1C.



EX1006, FIG. 1C

174. Ryan describes the processor module 106/146 addressing the flash memory 150. EX1006, 15:21-25 ("flash memory and EEPROM device powered

and addressed by the processor module.”). Ryan further explains that “[t]he memory management for the device may be handled by a crypto controller operating system with an 8 bit address bus in the dual interface (DI) chip,” and that “[a] crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.” EX1006, 19:31-40.

175. Ryan describes the transaction information the processor module reads out from the secure element. Ryan indicates that “credit card details can be encrypted and stored in the smart fob,” (EX1006, 24:24-26), and that the memory can be used to run applications, EX1006, 28:30-37. A POSITA would have understood that the processor module decrypting the stored credit card details (*transaction information*) for a transaction interrogates and obtains those details out of the memory holding them, especially in view of Ryan’s description that the crypto controller operating system is “capable of encrypting and decrypting data to be stored in internal or external memory” (*configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator*). EX1006, 19:31-40, 24:24-26.

176. Ryan describes the processor module generating the outbound message. Ryan explains that the processor module is for “preparing messages to be sent by the contactless and/or wireless interfaces and interpreting messages

received via the interface(s),” EX1006, 15:40-43, and claims that “the processor module prepares messages to be sent by the contactless and wireless interfaces,” EX1006, cl. 43. In the Ryan-Abbott combination, the processor module 106/146 packages the transaction information it reads from the memory into a single message (*communications data package based on the transaction information*) before that information passes outward, in accordance with Abbott’s suggestions. *Supra*, §IX.C.3; EX1009, 10:8-16, FIGS. 3, 4B, Table II.

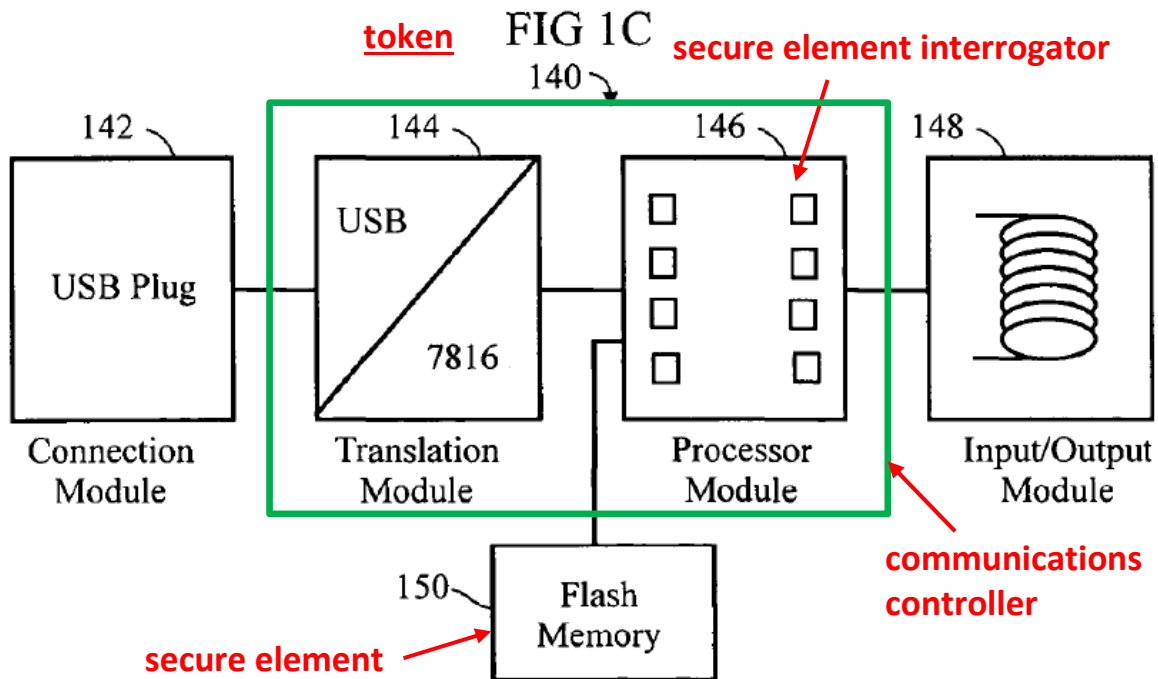
177. In describing the processor module addressing the memory, Ryan renders obvious the use of a device that is capable of such interrogation, and configuration of that device as distinct of the structures that are subject of its interrogation (*secure element interrogator*). As such, Ryan additionally renders obvious [60.2] and [60.3] in this manner, even if the processor module and memory together are considered to provide the secure element.

[60.4] a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.

178. Ryan-Abbott provides Element [60.4]. Ryan describes Ryan’s processor module 106/146 provides the *secure element interrogator* described in [60.3], and that chip, together with the coupled translation module 104/144, which is also mounted on the “circuit board” of the token housing (*affixed to the mounting structure*), performs the *communications controller* capabilities.

EX1006, 4:34-47 (“the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages”), 17:35-41, 18:12-22 (“A micro-controller such as an 8 bit micro-controller (ST7 FSCR1E4MI) can be used as an interface translator chip (104) between the USB connection 102 and the processor module 106. (The processor could be mounted in a SIM module.).”), FIGS. 1A, 1C. Ryan explains that “[t]he translation module 104 is for going (moving signals) from USB (the exemplary interface with the computer) to a smart card interface format, such as ISO 7816, and vice-versa.” EX1006, 18:12-15; *see also* 14:31-35 (“translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and provid[es] the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages.”); EX1001, 7:43-61 (“the communications controller may be physically incorporated into the reader or may be physically incorporated into the secure element or the communications controller may be a physically separate electronic element. In some embodiments the capabilities defined herein for the communications controller may physically be performed in the chip that is primarily the SE and/or the interrogator, or the capabilities of the interrogator may physically be performed in the chip that is primarily the SE and/or the communications controller, or the capabilities of the

SE may be physically performed in the chip that is primarily the communications controller and/or the interrogator, or the capabilities of the interrogator and the SE and the communications controller may all be performed in a single chip. In any case, the capabilities of the communications controller, the SE and the interrogator are still considered to be performed by the ‘communications controller,’ the ‘SE’ and the ‘interrogator’ respectfully.”).



179. The combination’s translation module 104/144 in the *communications controller* receives the packaged message (*communications data package*) from the processor module 106/146 (*secure element interrogator*) and transmits it to the host computer (*host device*) through the connection module

102/142. *Supra*, §IX.C.3-4, Elements [60.pre], [60.3]; EX1006, 15:29-33, 17:47-57, FIGS. 1A, 1C; EX1009, 10:17-11:11, FIGS. 3, 4B, Table II.

180. The translation module's USB framing carries the same package outward. Abbott describes that "the translation module 318 adds a USB header to create a USB response," which encapsulates the smartcard response for transport (e.g., without altering it). EX1009, 10:17-11:11, Table II. A POSITA would have understood the message the communications controller transmits to be the same communications data package the interrogator generated, especially in view of Abbott's description of the header as added to the response the smartcard processor produced. EX1009, 10:17-11:11, Table II.

(b) Claims 77, 86

[77] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device is configured to transmit the data communications package over a wireless network.

[86] The cellular network device of claim 79 further comprising a communications controller affixed to the mounting structure and configured for receiving the communications data package for transmission by the cellular network device over a wireless network.

181. Ryan-Abbott provides Claims 77 and 86. *Supra*, §IX.C.4, Elements [60.4], [79.pre].

(c) Claims 1, 22, 31, 52

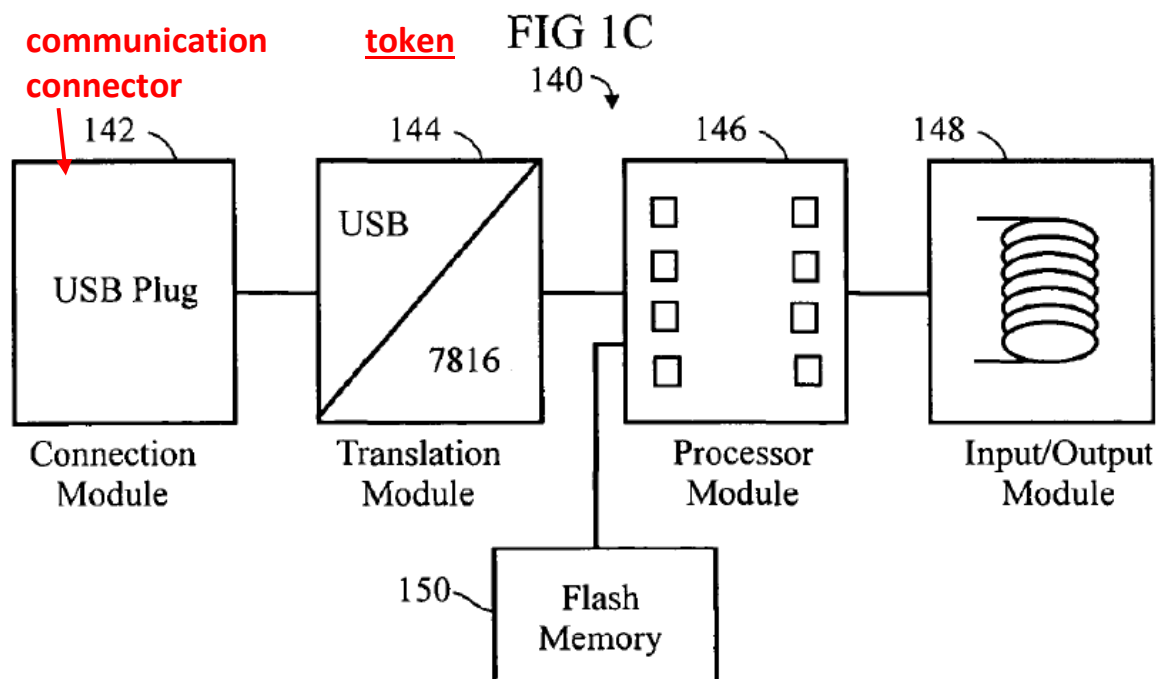
[1.pre]/[22.pre]/[31.pre]/[52.pre] A token comprising:

182. Ryan-Abbott provides [1.pre]/[22.pre]/[31.pre]/[52.pre]. *Supra*,

§IX.C.4, [60.pre].

[1.1]/[22.1]/[31.1]/[52.1] a mounting structure having a communication connector configured to connect to a computer terminal;

183. Ryan-Abbott provides [1.1]/[22.1]/[31.1]/[52.1]. *Supra*, §IX.C.4, [60.1]. The token device has a “connection module 142” (e.g., “a USB plug”) (***communication connector***) “for plugging directly into a personal computer (PC)” (***computer terminal***). EX1006, 4:34-47, 17:35-57, 15:29-33, FIG. 1C (reproduced below).



EX1006, FIG. 1C

[1.2]/[22.2]/[31.2]/[52.2] a secure element affixed to the mounting structure, the secure element comprising a data file,

184. Ryan-Abbott provides [1.2]/[22.2]/[31.2]/[52.2]. *Supra*, §IX.C.4, [60.2].

[1.3]/[22.3]/[31.3]/[52.3] a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging [a plurality of/at least one] transaction data communication(s) only between the secure element and the secure element interrogator; and

185. Ryan-Abbott provides [1.3]/[22.3]/[31.3]/[52.3]. *Supra*, §IX.C.4, [60.3]. The data communications exchange runs between the processor module and the flash memory 150 it addresses, with no other component in between.

EX1006, 15:21-25, 19:31-40, FIGS. 1A, 1C. A POSITA would have understood that the exchange occurs “only between” the secure element and the secure element interrogator, which takes place on that internal address bus alone, especially because Ryan describes the flash memory 150 as “powered and addressed by the processor module” and describes no other participant on that link. EX1006, 15:21-25.

[1.4]/[22.4]/[31.4]/[52.4] a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information [as a single data communication] to the computer terminal through the communications connector.

186. Ryan-Abbott provides [1.4]/[22.4]/[31.4]/[52.4]. *Supra*, §IX.C.4, [60.4]. The combination’s translation module 104/144 in the *communications controller* receives the packaged message from the processor module 106/146 (*secure element interrogator*) and transmits it to the host computer (*computer terminal*) through the connection module 102/142 (*communications connector*) as

a *single data communication*. *Supra*, §IX.C.3-4, Elements [60.pre], [60.3];

EX1006, 15:29-33, 17:47-57, FIGS. 1A, 1C; EX1009, 10:17-11:11, FIGS. 3, 4B,

Table II.

(d) Claims 2, 23, 32, 53, 61, 80

[2]/[23]/[32]/[53] The token of claim 1/22/31/52 wherein the plurality of/at least one transaction data communication(s) comprises communications formatted according to ISO 7816-4.

[61]/[80] The token of claim 60/79 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.

187. Ryan-Abbott provides these claims. Ryan describes the processor module that addresses that memory as equipped for ISO 7816 contact operation. EX1006, 18:30-38, 13:58-61; *see also*, 2:18-60, 4:34-47, 18:12-38. A POSITA would have found obvious from Ryan's description, that the processor module 106/146 and that memory exchange the transaction data communications using APDUs defined in ISO 7816-4 (*communications formatted according to ISO 7816-4*), and — for Claims 2, 23, 61, and 80, which recite a plurality of transaction data communications — that acquiring the transaction information from the secure element's data file comprises more than a single command-and-response pair, especially where the file holding that information is selected before its contents are read. EX1006, 15:21-25, 19:31-40, 24:24-26, 28:30-37; EX1013, [0006]; EX1014, [0016], [0030]; EX1015, [0034]).

(e) Claims 4, 25, 34, 55, 63, 81

[4]/[25]/[34]/[55]/[63]/[81] The token of claim 1/10/22/31/40/52/60/79 wherein the secure element interrogator exchanges the plurality of/at least one transaction data communication(s) with the secure element only within libraries or memory space residing on the mounting structure.

188. Ryan-Abbott provides these claims. Ryan's processor module 106/146 and the flash memory 150 it addresses are mounted on the circuit board of the token housing (***mounting structure***). EX1006, 17:35-41, FIGS. 1A, 1C; *supra*, [60.2]. The exchange of transaction data communications occurs only between the memory and interrogator, through their coupling interface, all residing on the same device housing, e.g., by integrated circuit(s) on a PCB board in the device (***mounting structure***).

(f) Claims 6, 27, 36, 56, 64, 82

[6]/[27]/[36]/[56]/[64]/[82] The token of claim 1/22/31/52/60/79 wherein [all] communications to and from the secure element consist of communications from and to a secure element reader.

189. Ryan-Abbott provides these claims. *Supra*, §IX.C.4, Element [60.3] (the secure element interrogator reading transaction information from the secure element corresponds to ***a secure element reader***).

(g) Claims 7, 28, 37, 57, 66, 84

[7]/[28]/[37]/[57]/[66]/[84] The token of claim 1/22/31/52/60/79 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

190. Ryan-Abbott provides these claims. Ryan describes the output

module comprising “an RF antenna,” the smart card processor “communicating through an RFID-contactless interface and connected to an inductive antenna,” and “an antenna coil in the device that enables the contactless part of a separate contactless smart card to communicate with contactless readers.” EX1006, 18:39-40, 19:4-5, 19:61-20:2, 14:28-39, 29:23-26, 32:43-47. Ryan further describes the data held in that memory reaching the contactless path, explaining that “information exchanged and stored can be accessed in the real world application via its contactless interface.” EX1006, 17:6-26. A POSITA would have understood that an external contactless reader exchanging that stored data through the token’s antenna and dual-interface chip thereby *interrogat[es] the secure element* holding it. EX1006, 17:6-26, 18:30-38.

191.

(h) Claims 8, 29, 38, 58

[8.1]/[29.1]/[38.1]/[58.1] The token of claim 1/22/31/52 wherein: the secure element comprises an executable application; and

192. Ryan-Abbott provides [8.1]/[29.1]/[38.1]/[58.1]. Ryan describes its memory (*secure element*) is used “for user authentication . . . and to run applications,” such as “e-payment and similar applications” (*executable application*), and describes the flash memory as included for “running applications.” EX1006, 14:66-15:2, 28:30-37; *see also id.*, 2:61-64, 11:20-24

(“The non-hardware part of a computer, handheld (e.g., PDA) or smartphone (‘smart’ cellular telephone) consisting of instructions used to operate these devices. Includes applications that are added to, or included on, the device, as well as the operating system built into a device.”), 15:21-25 (“The apparatus may further comprise a processor module; and additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module; wherein the additional memory can be used for user authentication and to run applications.”), 19:31-40, 24:12-13 (“The smart fob can be personalised like a conventional credit/debit card for electronic payment”), 24:25-26 (“credit card details can be encrypted and stored in the smart fob”), 28:1-7, FIGS. 1-3.

[8.2]/[29.2]/[38.2]/[58.2] the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

193. Ryan-Abbott provides [8.2]/[29.2]/[38.2]/[58.2]. *Supra*, §IX.C.4, Element [1.3].

(i) Claims 67, 85

[67.1]/[85.1] The token of claim 60/79 wherein: the secure element comprises a plurality of payment card applications from different card associations and

194. Ryan-Abbott provides [67.1]/[85.1]. *Supra*, §IX.C.4, Claim [8]. A POSITA would have found it obvious, in view of Ryan’s express description above, to beneficially load payment applications of different card associations on

that secure element, so a single token serves a cardholder's several cards, for example, furthering Ryan's express objectives.

[67.2]/[85.2] the secure element interrogator interrogates one of the payment card applications.

195. Ryan-Abbott provides [67.2]/[85.2]. *Supra*, §IX.C.4, Element [1.3], Claim [8].

(j) Claims 68, 69

[68] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller.

[69] The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller and the host device has the physical form of a mobile phone or a PDA.

196. Ryan-Abbott provides Claims 68 and 69. As discussed above, Ryan's token comprises the *secure element*, the *secure element interrogator*, and the *communications controller*, and its connection module connects the token to a "host device such as PC, PDA, smart cellular phone or similar device" (*host device comprises a cellular network device*). *Supra*, §IX.C.4, Elements [79.pre], [60.2]-[60.4]; EX1006, 15:29-33. Ryan further explains that the token "may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA)" such that the cell phone or PDA houses all three components and the host device is *a mobile phone or a PDA* (Claim 69). EX1006, 13:39-44.

(k) Claim 70

[70] The token of claim 60 wherein the mounting structure comprises a substrate.

197. Ryan-Abbott provides Claim 70. Ryan explains that the token device (100)'s major components are “mounted on a circuit board (PCB...)” (*mounting structure comprises a substrate*) and “within a housing” (*mounting structure comprises a packaging case*). EX1006, 4:34-47, 17:35-57, 15:29-33, FIG. 1A.

(l) Claim 71

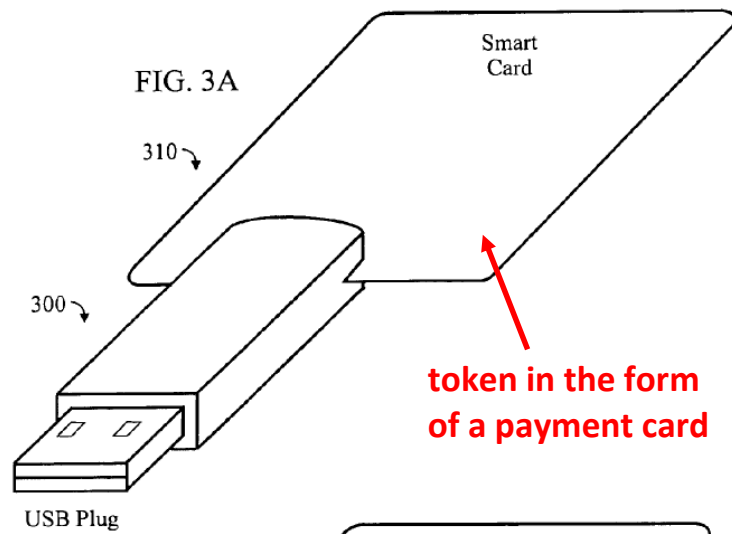
[71] The token of claim 60 wherein the mounting structure comprises a packaging case.

198. Ryan-Abbott provides Claim 71. Ryan explains that the token device (100)'s major components are “mounted on a circuit board (PCB...)” and “within a housing” (*mounting structure comprises a packaging case*). EX1006, 4:34-47, 17:35-57, 15:29-33, FIG. 1A.

(m) Claim 72

[72] The token of claim 60 wherein the token has the physical form of a payment card.

199. Ryan-Abbott provides claim 72. Ryan discloses that the token includes a smart card 310. EX1006, 20:11-18.



EX1006, FIG. 3A

(n) Claim 73

[73] The token of claim 60 wherein the token has the physical form of a fob.

200. Ryan-Abbott provides claim 73. Ryan discloses that the “compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob.” EX1006, 12:63-65, 13:32-34, 13:67-14:1, 15:52-54, 16:16-18, 17:6-10, 19:45-47, 19:61-63.

(o) Claim 74

[74] The token of claim 60 wherein the token has the physical form of a cartridge.

201. Ryan-Abbott provides Claim 74. Ryan discloses that the token can take a variety of suitable forms, including separable fobs and cards (e.g., PCMCIA card), thereby rendering obvious [74]. EX1006, 19:61-67, 13:34-37, 20:2-3, EX1001, 3:29-37.

(p) Claim 75

[75] The token of claim 60 wherein the token has the physical form of a dongle.

202. Ryan-Abbott provides Claim 75. Ryan-Abbott provides claim 75.

Ryan discloses that the “device (smart fob, USB key fob) can function as a dongle for software license authentication.” EX1006, 29:15-16.

(q) Claim 76

[76] The token of claim 60 wherein the token has the physical form of a secure digital (SD) chip.

203. Ryan-Abbott provides claim 76. Ryan discloses that the token “can be embodied in a format (form factor) such as that of an SD (secure digital) card which can be plugged into any device having an appropriate interface for inserting an SD card, such as a laptop, palmtop, cell phone, digital camera, personal digital assistant (PDA), MP3 player, or the like.” EX1006, 16:4-10, 13:34-37.

D. GROUND 2B – Ryan-Abbott-Peart Renders Obvious Claims 3, 5, 9-13, 16-19, 21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, and 87

1. Peart

204. Peart discloses a system and method for securing transaction information using a seeded cryptographic algorithm (e.g., a “standard triple Data Encryption Standard (DES) operation”) in which variable data is hashed to derive a seed and an “unpredictable number (UN)” is generated and used by a transaction device (102) in encrypting and authenticating transaction data. EX1008, Title, Abstract, 1:34-38, 2:63-3:15, 5:3-34, 6:24-61, FIGS. 2-3 & 5.

205. The “unpredictable number” is integrated into the encrypted transaction information (“a cryptogram”), sent in an authorization message and later validated by a verifying entity (e.g., “an ‘acquirer’ or account issuer”), which confirms that the unpredictable number and cryptogram correspond to expected values, thereby establishing transaction authenticity. EX1008, Abstract, 2:21-30, 5:4-54, 6:7-7:30, 8:21-35, 9:19-10:2, FIG. 1, 3, 4. Peart’s seeded cryptographic algorithm for securing transaction information is described in technology-agnostic terms and expressly applied to “any environment wherein security of a transaction is required.” EX1008, Title, Abstract, 5:4-54, 7:22-30, 8:21-35, FIG. 1.

2. Ryan-Abbott-Peart Combination

(a) Peart is Analogous Art to the ’924 Patent

206. Peart is analogous art to the ’924 Patent, both because it is within the same field of endeavor (EX1001, 1:24-28; *supra*, §IX.D.1; EX1008, 5:35-54, cl. 1), and because Peart is reasonably pertinent to the problems the ’924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50; EX1008 5:1-34.

(b) A POSITA would have been Motivated to Combine Ryan-Abbott-Peart

207. Ryan already describes secure transaction environments employing cryptographic protection of transaction data including “secret cryptographic keys,” “cryptography” applications, and a “crypto controller...capable of encrypting and decrypting data to be stored in internal or external memory” on its smart token.

See e.g., EX1006, 1:29-30 (“The [smart card] processor uses a limited instruction set for applications such as cryptography.”), 1:45 (desire for “improved security of Internet transactions”), 2:3-9 (“secure identification, electronic payment transaction and authentication”), 2:66-67 (“The main focus of the smart card industry has been on secure card applications”), 10:35-12:39 (“SD Short for ‘Secure Digital’... SDIO Short for ‘Secure Digital Input/Output’... SIM Short for ‘Secure Identity Module’... SAM Short for ‘Secure Application Module’... SSL Short for ‘Secure Sockets Layer’...secure data transmission... [USB tokens] can generate secret cryptographic keys (Public & Private Key Infrastructure) and store private data (digital certificates, digital signatures, biometric identifiers, passwords, system settings etc)...remotely and securely access a corporate network via the Internet... stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system”), 19:24-40, 22:24-41 (“The smart fob can operate as a security device... conduct a business transaction in a secure fashion, without the fear of anyone spying or manipulating the data... the cryptographic and application software can be updated online anytime”), 24:24-26 (“Personal data, frequent flyer miles as well as credit card details can be encrypted and stored in the smart fob.”), 24:60-61 (“there is a need in the market for a teen payment product that allows secure payments online”), 32:23-31 (“Some of this digital content could be encrypted for limited time use or

conditional access. Optionally, all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be counterfeited or altered in any way.”).

208. Peart addresses the same problem through a seeded cryptographic algorithm producing an “unpredictable number” from “variable data” such as “a counter” and “the time of the transaction,” beneficial for “any environment wherein security of a transaction is required.” *Supra*, §IX.D.1; EX1008, Abstract, 2:21-3:15, 7:22-30.

209. A POSITA would have found it obvious to use Peart’s suggestions in the Ryan-Abbott system, for enhanced secure transaction data transmission, consistent with the express desires of both Ryan and Abbott. EX1006, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 22:24-41, 24:60-61; *see also* EX1009, 2:9-11 (“These challenges include...ensuring the security of e-mail and other electronic communications, as well as Internet commerce.”), 5:1-13 (“Supporting secure online banking, benefits administration, account management; Supporting secure workflow and supply chain integration (form signing)...Encrypting files...Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)...Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)”), 8:11-14 (“These separate communication paths 220 and 224 allow the

user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 130 to eavesdrop or intercede.”).

210. In Ryan-Abbott-Peart, the transaction information is encrypted at the secure element (per Peart), such that the output is encrypted data. *Supra*, §§IX.C.1, IX.D.1. Multiple considerations would have led a POSITA to implement this combination.

211. **First**, a POSITA would have been motivated to incorporate Peart’s cryptographic algorithm into Ryan-Abbott, because this would provide a self-contained cryptographic mechanism suitable for protecting transaction data before it leaves a secure processing environment. *Supra*, §IX.D.1; EX1006, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 22:24-41, 24:60-61. Peart’s algorithm would be executed within Ryan-Abbott’s processor module (secure element) before any transaction information is exposed to external interfaces. *Id.* A POSITA would have done so to avail the system of the benefit of decoupling user-interface interaction from transaction security. Even if transaction initiation or form population occurs through less trusted host-side mechanisms, the transaction data itself can be cryptographically protected at the secure element using Peart’s seeded cryptographic algorithm. This advances Ryan’s objective of a secure transaction model and mitigates risks in exposing transaction flows to general-purpose host

environments. *Id.*

212. **Second**, a POSITA would have been motivated to incorporate Peart into Ryan-Abbott for transaction uniqueness and protection against replay attacks. As Peart's unpredictable number is derived from transaction-specific variable data (e.g., "a transaction counter" or "time of the transaction") and processed through encryption, such incorporation in the Ryan-Abbott-Peart combination would support replay-attack protection independent of the external communication channel. EX1008, Abstract ("The seed value is computed by subjecting variable data to a Secure Hashing Algorithm...the seed value as a counter value"), 2:66-67, 5:35-41 ("Transaction device 102 encrypts the UN together with other information (a transaction counter and a user identifier) using a secret key and sends the transaction to RFID reader 104"), 6:29-40 ("The variable data includes...a counter value provided by RFID reader 104 or RFID transaction device 102, the time of the transaction...and the number of milliseconds since the RFID reader 104 has processed the most recent transaction"), FIG. 3.

213. **Third**, a POSITA would have been motivated to incorporate Peart's algorithm into Ryan-Abbott, because the use of a seed derived from variable data and a repeatable cryptographic process (per Peart) promotes a verifying/authorizing entity (e.g., "an 'acquirer' or account issuer") to reproduce or validate expected outputs, providing robust validation independent of the client

environment. *See e.g.*, EX1008, Abstract, 2:21-30, 4:3-7, 5:1-54 (“reader...sends the encrypted data (called a cryptogram) and a copy of the UN to account issuer 112...wherein account issuer 112 stores the UN (Step 406), checks that the cryptogram is valid, decrypts the cryptogram (Step 408) and checks that the cryptogram contains an encrypted form of the UN sent by RFID reader 104 (Step 410). If the values are all valid, the transaction is known to have been generated by a transaction device issued by issuer 112 and that it has not been tampered with.”), FIG. 4.

(c) A POSITA would have Reasonably Expected Success

214. Availing Ryan-Abbott of Peart’s suggestions would have been technically straightforward to a POSITA. Ryan describes cryptographic computation and secure storage, while Peart specifies a concrete method for generating transaction-specific cryptographic values derived from variable data such as counters and other transaction parameters. Peart’s use of standard primitives, e.g., secure hashing and “a data encryption standard operation” aligns with Ryan’s smart-card-class processor environment. EX1006, 4:15-22; EX1008, Abstract. Peart’s teachings can be executed within Ryan-Abbott before any transaction information is exposed to external interface.

3. Analysis

(a) Claims 10, 40

[10.pre]/[40.pre] A token comprising:

215. Ryan-Abbott-Peart provides [10.pre]/[40.pre]. *Supra*, §IX.C.4, Element [1.pre].

[10.1]/[40.1] a mounting structure having a communication connector configured to connect to a computer terminal;

216. Ryan-Abbott-Peart provides [10.1]/[40.1]. *Supra*, §IX.C.4, Element [1.1].

[10.2]/[40.2] a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;

217. Ryan-Abbott-Peart provides [10.2]/[40.2]. *Supra*, §IX.C.4, Element [1.2], Claim [8].

[10.3]/[40.3] a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of/at least one transaction data communication(s) only between the secure element and the secure element interrogator, and

218. Ryan-Abbott-Peart provides [10.3]/[40.3]. *Supra*, §IX.C.4, Element [1.3].

[10.4]/[40.4] a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

219. Ryan-Abbott-Peart provides these elements. As I discussed above in §IX.C.4, Element [1.4], Ryan-Abbott provides a communications controller affixed to the mounting structure and configured to receive the data from the secure

element interrogator and to transmit the transaction information to the computer terminal through the communications connector. Ryan-Abbott-Peart further provides transmitting the transaction information as track data. Peart discloses that information from a transaction device (***token***) to an external reader (***computer terminal***) “is transmitted in magnetic stripe or multi-track magnetic stripe format” (***track data***). EX1008, 8:54-9:18. A POSITA would have been motivated to implement Peart’s suggestion in Ryan-Abbott because “of the proliferation of devices using magnetic stripe format” and to further promote information transferred from the communications controller to the computer terminal “in a format recognizable by a merchant system or account issuer.” EX1008, 8:54-62.

(b) Claims 3, 12, 24, 33, 42, 54, 62

[3]/[12]/[24]/[33]/[42]/[54]/[62] The token of claim 1/10/22/31/40/52/60 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

220. Ryan-Abbott-Peart provides these claims. Ryan discloses “secret cryptographic keys,” “cryptography” applications, and a “crypto controller...capable of encrypting and decrypting data to be stored in internal or external memory” on its smart token. *See e.g.*, EX1006, 1:29-30, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 19:24-40, 22:24-41, 24:24-26, 24:60-61, 32:23-31. Peart discloses that the transaction device (***token***) “encrypts the UN together with other information (a transaction counter and a user identifier) using a secret key” and

“the secret key is loaded onto transaction device 102 by issuer 112 when transaction device 102 is created using standard industry secure methods for key management.” In the combined system, the encryption algorithm and the transaction counter are stored at least temporarily in the secure element, such that the token encrypts the information including the transaction counter using the secret key. *Supra*, §IX.D.2 EX1006, 1:29-30, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 19:24-40, 22:24-41, 24:24-26, 24:60-61, 32:23-31; EX1008, 5:35-54.

(c) Claims 5, 26, 35

[5]/[35] The token of claim 1/31 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.

[26] The token of claim 22 wherein the secure element comprises a payment card application and the transaction information comprises track data.

221. Ryan-Abbott-Peart provides these claims. *Supra*, §IX.C.4, Claim [8] (regarding *payment card application*); *supra*, §IX.D.3, Element [10.4] (regarding *track data*).

(d) Claims 9, 18, 21, 30, 39, 48, 51, 59, 78, 87

[9.1]/[30.1]/[39.1]/[59.1]/[78.1]/[87.1] The token of claim 1/22/31/52/60/79 wherein: the secure element comprises a payment card application;

[18.1]/[48.1] The token of claim 10/40 wherein the secure element comprises a plurality of payment card applications from different card associations and

222. Ryan-Abbott-Peart provides these elements. *Supra*, §IX.C.4, Claim [8], *supra*, [67.1] (plurality of payment card applications from different card

associations).

[9.2]/[30.2]/[39.2]/[59.2]/[78.2]/[87.2] the secure element interrogator is configured to interrogate the payment card application; and [18.2]/[48.2] the secure element interrogator interrogates one of the payment card applications.

223. Ryan-Abbott-Peart provides these elements. *Supra*, §IX.C.4, Element [1.3], Claim [8].

[9.3]/[21]/[30.3]/[39.3]/[51]/[59.3]/[78.3] the transaction information comprises card-present data. [87.3] the communications data package comprises card-present data.

224. Ryan-Abbott-Peart provides these elements. *Supra*, §IX.D.3, Element [10.4] (track data provides *card-present data*); EX1001, 5:12-36.

(e) Claims 11 and 41

225. Ryan-Abbott-Peart provides Claims 11 and 41. *Supra*, §IX.C.4, Claim 2.

(f) Claims 13 and 43

226. Ryan-Abbott-Peart provides Claims 13 and 43. *Supra*, §IX.C.4, Claim 4.

(g) Claims 16, 46

227. Ryan-Abbott-Peart provides Claims 16, 46. *Supra*, §IX.C.4, Claim 6.

(h) Claims 17, 47

228. Ryan-Abbott-Peart provides Claims 17, 47. *Supra*, §IX.C.4, Claim 7.

(i) Claims 19, 49

229. Ryan-Abbott-Peart provides Claims 19, 49. *Supra*, §IX.C.4, Claim 8.

E. GROUND 2C – Ryan-Abbott-Smets Renders Obvious Claims 65, and 83

1. Ryan-Abbott-Smets Combination

230. As discussed above, Ryan already provides a hardware and software framework capable of performing cryptographic operations and interacting with both contact and contactless payment environments, e.g., “ISO 7816, ISO 14443 and ISO 15693.” *Supra*, §IX.C.1; *see e.g.*, EX1006, 3:18-23, 5:13-30 (“Each electronic certificate includes transaction data and identification data...”), 13:54-57 (“The translation module moves signals between a USB interface and a smart card interface. The smart card interface may be selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.”), 15:11-25, 19:24-40 (“The flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card. (A crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.)”), 28:30-37.

231. Ryan describes crypto capability, e.g., “security features such as Advanced Crypto Engine (ACE)... triple DES encryption and RSA.” EX1006, 2:53-60. This indicates that the hardware platform is suitable for implementing dynamic authentication calculations like CVC3.

232. A POSITA would have been motivated to integrate Smets's backward-compatible formatting of transaction data (e.g., CVC3) into Ryan's smart fob architecture. *Supra*, §IX.A.2; EX1005, [0026] ("payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal... Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number"); EX1006, 3:18-23, 5:13-30, 13:54-57, 14:6-7 ("The fob is capable of interfacing with the Internet and emulating a smart card."), 15:11-25, 19:24-40, 28:30-37. In the combined system, the microprocessor of Ryan's secure element would be responsible for generating the dynamic CVC3, using stored keys and transaction inputs (e.g., unpredictable number, transaction counter), in accordance with Smets. Multiple reasons would have prompted a POSITA to combine the teachings of Ryan, Abbott, and Smets.

233. **First**, a POSITA would have been motivated to implement such combination for enhanced backward compatibility. EX1005, [0014] ("The standardization method and system place...the proximity payment card transaction data...in ISO 7811 byte-level formatted data structures that are commonly used in processing magnetic stripe card transactions."). Doing so in Ryan would facilitate interoperability of the smart fob with legacy payment infrastructure while still leveraging contactless and dynamic authentication capabilities. This aligns with Ryan's goal of bridging environments. EX1006, 16:56-17:2. ("This invention

relates generally to devices, technology and applications for downloading and interacting with data and value from one ‘world’ such as the virtual world of the Internet and, with the device, interacting, typically contactlessly, with another ‘world’ such as the physical world of banking, stores (point of sale), physical access control, and the like... using a standard contactless smart card interface.”). The combination therefore would enhance Ryan’s existing “virtual-to-real-world” transaction model with robust, standardized payment security.

234. **Second**, a POSITA would have been motivated to implement this combination because it would strengthen security and flexibility. Smets emphasizes that dynamic values are transaction-specific, as “[t]he dynamic authentication value changes with each transaction” and “unauthorized person cannot use that CVC3 number as the authentication value for the next or any other transactions.” EX1005, [0010]. Meanwhile, Ryan already supports secure storage and processing, as the token “can generate secret cryptographic keys (Public & Private Key Infrastructure) and store private data.” *See e.g.*, EX1006, 12:5-15. By embedding Smets’s dynamic authentication and bitmap-based placement, Ryan’s token device would gain fraud-resistant, interoperable payment capability, while preserving its modular, multi-interface design. Moreover, Smets highlights flexibility via bitmaps, which complements Ryan’s modular and multi-standard architecture, allowing the same hardware to support multiple issuer-specific

configurations without redesign. *See e.g.*, EX1005, Abstract, [0014]-[0015], [0023] (“The invention provides a standardization method and system for placing proximity card function data or digits in discretionary data fields used for magnetic stripe cards. The digits are stored in available space in the discretionary data fields, which has not been used by card issuers or vendors. The number of such digits and their precise locations within a discretionary data field are flexibly assigned using a bitmap. The bitmap is stored in the card’s discretionary data field. The flexible manner of placing proximity card function data or digits in the card’s discretionary data fields does not have any adverse effect on card functions. Card behavior is independent of vendor usage of the discretionary data fields.”), [0028], [0033], [0040].

235. Furthermore, a POSITA would have expected a high likelihood of success in implementing the combination, because Ryan already provides processing, cryptographic capability, and interface translation layers, while Smets provides a standardized method for encoding dynamic authentication data in legacy-compatible formats. Ryan’s architecture is compatible with Smets’s teaching of generating and placing the dynamic data into existing magnetic-stripe data structures in a backward-compatible manner, because Ryan explicitly includes translation and formatting functionality between interfaces and contemplates direct interaction with contact and contactless standards such as ISO 7816 and ISO

14443. Thus, a POSITA would have found it obvious that a microprocessor would handle the CVC3, UN, and ATC data in a manner compliant with Smets.

2. Analysis

(a) Claims 65, 83

[65]/[83] The token of claim 60/79 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.

236. Ryan-Abbott-Smets provides these claims. As discussed above, the Ryan-Abbott-Smets combination structures its transaction data stored in the secure element, including a dynamic authentication code (e.g., CVC3) (***dynamic card verification code***) computed from the unpredictable number (UN), in accordance with Smets, for compatibility with existing magnetic stripe infrastructure and enhanced security through dynamic authentication. *Supra*, §§IX.A.2-4, IX.C.1-4, IX.E.1; EX1005, [0010], [0014], [0024]-[0026], [0037]-[0039], FIG. 5.

237. As discussed in [60.2], Ryan teaches that the flash memory 150 includes and is managed by a micro-controller (***secure element***), disclosing and rendering obvious a microprocessor. EX1006, 3:9-13; 19:31-40, 29:35-36. A POSITA would have understood a SIM or SD card of the kind Ryan identifies to carry its own microprocessor. EX1006, 2:53-60. In the combined system, the ***microprocessor*** of the secure element uses application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication to calculate the dynamic CVC3

(*dynamic card verification code*), from the UN and optionally “the card’s application transaction counter (ATC),” using a secret encryption key stored on the secure element, in accordance with Smets. *Supra*, §IX.A.2-3, IX.E.1; EX1005, [0010] (“A security solution, which may be utilized in PayPass, is based on generation of a dynamic authentication value or number (CVC3). The dynamic authentication value changes with each transaction.”), [0014], [0024]-[0025] (“The PayPass implementation provides a ‘Pay Pass-Mag Stripe’ application, which can process transactions based on proximity cards and magnetic stripe cards. (See FIG. 5). The PayPass-Mag Stripe application is an extension of the currently available magnetic-stripe applications for debit and credit payments.”), [0026] (“payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal. Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number. Alternatively, payment card 1 may be personalized at the card issuer option to compute the CVC3 number based on a portion of the UN and on the card’s application transaction counter (ATC).”), [0037]-[0039].

F. GROUND 2D – Ryan-Abbott-Peart-Smets Renders Obvious Claims 15, 20, 45, 50

238. A POSITA would have been motivated to combine Ryan with Abbott, Peart, and Smets for the reasons described above. *Supra*, §§IX.C.3 (Ryan-Abbott

Combination), IX.D.2 (Ryan-Abbott-Peart Combination), IX.E.1 (Ryan-Abbott-Smets Combination).

1. Analysis

(a) Claims 15, 20, 45, 50

239. Ryan-Abbott-Peart-Smets provides Claims 15, 20, 45, 50. *Supra*, §IX.G.2, Ground 2C, Claim [65]; *see also id.* (the combination’s “‘PayPass-MagStripe’ application” providing *an application level protocol* for dynamic authentication of the secure element).

G. GROUND 2E/2F – Ryan-Abbott-Smets-Kisliakov Renders Obvious Claims 2, 23, 32, 53, 61, 80 / Ryan-Abbott-Peart-Smets-Kisliakov Renders Obvious Claims 11, 41

1. Ryan-Abbott-Smets-Kisliakov (Ground 2E) / Ryan-Abbott-Peart-Smets-Kisliakov (Ground 2F) Combinations

240. As discussed above for the Huomo-Smets-Kisliakov combination under Ground 1B, Smets describes commands and responses of a type similar to ISO 7816-4. *Supra*, §IX.B.2. Similarly, Abbott describes an ISO 7816 compliant interface (324) between the smartcard processor (320) and smartcard reader emulator module (SREM) (316) and communications between the two components in “commands” and “responses” “according to the S/C [short for smartcard] protocol.” EX1009, 9:12-25, 10:8-16 (“SREM 316 provides all instructions and commands to the smartcard processor 320 and receives messages and responses from the smartcard processor 320 according to the S/C [smartcard] protocol.”),

12:26-13:19 (“after the reset signal is applied by the smartcard reader, the smartcard processor 320 responds with an answer-to-reset message....the smartcard reader emulation module activates the RST signal path in the smartcard interface 324, thus providing the RST command to the smartcard processor 320. The smartcard processor 320 responds with an answer-to-reset message, sends the message via the serial I/O line of the smartcard interface 324 to the interface processor 314. The message is then packaged by the translation module 318 and transmitted to the host computer 102 via the USE-compliant interface 326.”), 14:7-15 (“after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320.”), 15:29-16:12 (“If the sma; *supra*, §IX.C.2; *see also*, §IX.F. Additionally, Ryan’s token already implements ISO 7816 messaging among its modules. EX1006, 14:30-35, 27:19-23, 34:66-35:3.

241. Even if Ryan, Abbott, Smets, and/or Peart, did not disclose transaction data communications comprising communications formatted according to ISO 7816-4, the combinations render obvious based on Kisliakov’s express teachings. Kisliakov provides express implementation details of the ISO 7816-4 file-system form Ryan’s memory addressing takes, and confirms organization of the stored cardholder data in separately selectable elementary files. EX1006, 19:24-30, 19:31-40; EX1010, [0126], [0351]. A POSITA would have formatted the

commands and responses on that link — the processor module and the flash memory it addresses — as ISO 7816-4 APDUs, in accordance with Kisliakov, promoting a defined addressing scheme for the secure element's storage such that distinct categories of cardholder data occupy separate files the reader can select individually. EX1010, [0268], [0323], [0326], [0351], [0414]. To be clear, a POSITA would have combined each set of references for reasons described above. *Supra*, Grounds 2A-2D.

2. Analysis

(a) Claims 2, 11, 23, 32, 41, 53, 61, 80

242. Even if Ryan-Abbott-Smets (or Ryan-Abbott-Peart-Smets) did not disclose or make obvious *ISO 7816-4* type of commands and responses (APDUs) (*plurality of transaction data communications*) between the secure element and the secure element interrogator (the processor module and the memory it addresses), the combination provides such features through Kisliakov's express disclosure. *Supra*, §§IX.B.1-2, IX.G.1, IX.G.1.

X. CONCLUSION

243. For all the reasons I have noted in the foregoing paragraphs, claims 1-25 of the '924 Patent are obvious in view of the references discussed above.

244. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain

supplemental insights that may result in added observations.

APPENDIX A

Patrick Gerard Traynor

Professor

Interim Department Chair in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

1889 Museum Rd,

Gainesville, FL 32611 USA

traynor@cise.ufl.edu

<http://www.cise.ufl.edu/~traynor>

Table of Contents

EDUCATIONAL BACKGROUND	4
EMPLOYMENT HISTORY	4
CURRENT FIELDS OF INTEREST	4
I. TEACHING	6
A. Courses Taught	6
B. Continuing Education	6
C. Curriculum Development	6
D. Individual Student Guidance	7
E. Teaching Honors and Awards	12
II. RESEARCH AND CREATIVE SCHOLARSHIP	13
A. Thesis	13
B. Published Journal Papers (Refereed)	13
C. Published Books and Parts of Books	15
D. Edited Proceedings	15
E. Conference Presentations	15
E.1. Conference Papers with Proceedings (Refereed)	15
E.2. Conference Presentations with Proceedings (Non-Refereed)	23
E.3. Conference Presentations without Proceedings	23
F. Other	23
F.1. Submitted Journal Papers	23
F.2. Refereed Research Reports	23
F.3. Software	23
F.4. Published Papers (Non-Refereed)	23
F.5. Books in Preparation	24
F.6. Workshops and External Courses	24
G. Research Proposals and Grants (Principal Investigator)	24
H. Research Proposals and Grants (Contributor)	27
I. Research Honors and Awards	29
III. SERVICE	30
A. Professional Activities	30
A.1. Memberships and Activities in Professional Societies	30
A.2. Conference Committee Activities	30
B. On-Campus Committees	31
B.1. University of Florida	31
B.2. Georgia Tech	32
C. Special Assignments	32
D. Ph.D. Examining Committees	32
E. External Member of M.S. Examining Committee	36
F. Consulting and Advisory Appointments	36
G. Civic Activities	36
IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION	37
A. Honors and Awards	37
B. Invited Conference Session Chairmanships	37
C. Professional Registration	37
D. Patents	37
E. Editorial and Reviewer Work for Technical Journals and Publishers	38
F. Expert Witness Services	40
V. OTHER CONTRIBUTIONS	42
A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)	42

B. Special Activities	46
---------------------------------	----

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA <i>Dissertation:</i> Characterizing the Impact of Ridigity on the Security of Cellular Telecommunications Networks <i>Advisors:</i> Thomas F. La Porta and Patrick D. McDaniel	Computer Science & Engineering
M.S.	2004	Pennsylvania State University State College, PA	Computer Science & Engineering
B.S.	2002	University of Richmond Richmond, VA <i>Minors:</i> Biology, Business Admin	Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Interim Department Chair	University of Florida	July 2025–Present
Associate Chair for Research	University of Florida	August 2018–Present
Professor	University of Florida	August 2018–Present
Associate Professor	University of Florida	August 2014–July 2018
Associate Professor	Georgia Institute of Technology	March 2014–August 2014
Assistant Professor	Georgia Institute of Technology	2008–March 2014
Research Assistant	Pennsylvania State University	2004–2008
Teaching Assistant	Pennsylvania State University	2004

CURRENT FIELDS OF INTEREST

My research focuses on the security of cellular/telephony networks and mobile systems. The security of these systems generally relies on their closed nature and trust in the honest behavior of users. However, with the recent disintegration of these assumptions and with over than six billion subscribers around the world, cellular and mobile systems represent the next great expansion in global critical infrastructure and, because of their unique characteristics, require new and different approaches to security.

Recognizing this, my research focuses on three specific themes: (1) developing efficient techniques to allow telephony providers and customers to authenticate the origin of incoming calls; (2) measuring and

improving the security of emerging mobile financial systems and (3) efficient and strong privacy-preserving techniques for mobile devices. Additionally, I have significant expertise in fraud detection, particularly for payment systems.

I have a strong interest in solutions that can be deployed in both the short and long terms, and am actively engaging both industry and government in this capacity. My research, if successful, will help to not only improve the general security of networked devices, but also to maintain the historical reliability of telephony networks as they become the dominant digital access technology.

I. TEACHING

A. Courses Taught

Semester/Year	Course Number & Title	Number of Students	Comments
Fall 2024	CNT 4007 Computer Networks 1	310	Revamped Course
Fall 2023	CIS 6930 Cellular and Mobile Network Security	19	New Topics
Fall 2022	CNT 5410 Computer and Network Security	75	New Topics
Fall 2021	CNT 5410 Computer and Network Security	45	New Topics
Fall 2019	CNT 5410 Computer and Network Security	28	New Topics
Fall 2018	CIS 6930 Cellular and Mobile Network Security	16	New Course
Fall 2017	CNT 5410 Computer and Network Security	27	New Topics
Fall 2016	CNT 5410 Computer and Network Security	60	New Topics
Spring 2016	CNT 5410 Computer and Network Security	13	New Topics
Spring 2015	CNT 5410 Computer and Network Security	12	New Topics
Fall 2014	CNT 5410 Computer and Network Security	30	New Course
Spring 2014	CS 6262 Network Security	55	New Projects
Fall 2013	CS 3251 Computer Networks I	73	Expanded Syllabus
Spring 2013	CS 6262 Network Security	65	All New Projects
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2012	CS 8803 Cellular & Mobile Network Security	17	New Topics
	CS 8001 Information Security Seminar	20	New Speakers
Spring 2011	CS 8001 Information Security Seminar	20	New Speakers
Fall 2011	CS 6262 Network Security	27	Expanded Syllabus
	CS 8001 Information Security Seminar	35	New Speakers
Spring 2011	CS 3251 Computer Networks I	61	Expanded Syllabus
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2010	CS 8803/4803 Cellular & Mobile Network Security	16	New Course
	CS 8001 Information Security Seminar	31	New Speakers
Fall 2009	CS 6262 Network Security	55	Expanded Syllabus
Spring 2009	CS 3251 Computer Networks I	45	Expanded Syllabus
Fall 2008	CS 8003 Destructive Research	10	New Course

Guest lecturer for CS 4235 (Introduction to Information Security) and CS 8803 (e-Democracy) in Fall 2008.

Advised ECE 4811/CS 4802 (Vertically Integrated Project) with Ed Coyle

B. Continuing Education

None.

C. Curriculum Development

University of Florida

CNT 4007 Computer Networks 1: *Fall 2024.* Provided the first major overhaul to this course in a number of years. While I have relied on the same book used by other faculty, I have created new homeworks, projects, and slides to better represent the current state of computer networks. I have also significantly expanded the discussion of security in this course.

CIS 6930 Cellular and Mobile Network Security: *Fall 2018, 2023.* Developed an entirely new course around security issues facing cellular and mobile networks. Students learned about wireless basics, spectrum issues, core network architectures (GSM, ISDN, IMS, SIP), air interfaces (2G-5G), mobility management, voice-driven systems, authentication, mobile phone operating systems (Android, iPhone), Android security, congestion and denial of service, privacy and eavesdropping. Students also complete a research project and aim towards publishing this work at a major venue. My aim is for this class to become part of the regular offering of security courses. Semester projects were also judged and encouraged using a “venture capital” model, in which students had to pretend as if they were pitching their ideas for a start-up company to potential investors.

CNT 5410 Computer and Network Security: *Fall 2014-2022.* Totally rewrote the syllabus and slide material, giving the class its first major overhaul in a number of years. While many old themes remain, new lecture blocks including Web Security, Cellular Security and Social Engineering were developed from scratch. This new course material was made available to all other faculty members teaching this class, who have since used my slides and syllabus.

Georgia Tech In addition to the above courses, I also developed the following course while serving as a faculty member at Georgia Tech.

CS 3251 Computer Networks I: *Spring 2009.* Modified undergraduate networking course to include a persistent focus on security at all layers of the protocol stack. I have also created new lectures focusing on the physical layer and cellular networks and new exams to include all of the abovementioned changes.

CS 8803 Destructive Research: *Fall 2008.* Developed course based around understanding how so-called secure systems have been defeated by attackers. With such knowledge, students would have the context to develop the next generation of more secure systems. I delivered more than 1/3 of the lectures in this seminar course and paid special focus on vulnerabilities in cellular networks, analog telecommunications and electronic voting. Students were also instructed on techniques for performing research, writing technical papers and making conference and lecture-style presentations. I have offered these slides to future 7001 classes to help impact a wider audience.

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Hadi Abdullah University of Florida

Fall 2016–Summer 2022

Evaluating the security of ML-driven voice interfaces. Now: Research Scientist at Visa Research

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

Her research discovered vulnerabilities in mobile web browsers and developed techniques to detect malicious mobile web pages. First: Oracle in Spring 2014. Now: Google.

Nathaniel Bennett University of Florida

Fall 2022–Summer 2006

Finding vulnerabilities in cellular core networks via fuzzing. Now: Assistant Professor, Brigham Young University

Logan Blue University of Florida

Fall 2016–Summer 2022

Investigated biological feature reconstruction from voice recordings. Now: Research Scientist at Harbor Experts

Jasmine Bowers University of Florida

Fall 2015–Summer 2020

Her research focuses on mobile applications, and the development of tools for building secure systems. Now: Research Scientist, MITRE

Henry “Hank” Carter Georgia Institute of Technology

Fall 2010–Spring 2016

Developing techniques for secure function evaluation for privacy-preserving applications on constrained mobile devices. First: Assistant Professor, Villanova University.

Italo Dacosta Georgia Institute of Technology

Fall 2008–Summer 2012

Co-advised with Mustaque Ahamad. Research on scaling performance of SIP network components. Now: Senior Data Protection Engineer at UBS.

David Dewey Georgia Institute of Technology

Fall 2011–Summer 2015

Investigated compiler techniques to remove software vulnerabilities from code. Now: CTO of MailChimp.

Cassidy Gibson University of Florida

Fall 2019–Spring 2025

Investigated the use of AI in generating non-consensual imagery. Now: Research Scientist at Alice.

Seth Layton University of Florida

Fall 2020–Summer 2025

Detecting deepfakes in audio samples. Now: Research Scientist at PinDrop.

Daniel Olszewski University of Florida

Fall 2019–Spring 2026

Improving reproducibility and replicability in computer security research. Now: Research Scientist at Harbor Experts

Christian Peeters University of Florida

Fall 2016–Summer 2022

Develop techniques to detect and defend against call and message interception attacks in cellular networks. Now: Research Scientist at Harbor Experts

Brad Reaves University of Florida

Fall 2014–Spring 2017

Develop strong authentication techniques for cellular networks. Now: Associate Professor at North Carolina State University.

Nolen Scaife University of Florida

Fall 2014–Spring 2019

Developed techniques to detect credit card skimming. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart

Imani Sherman University of Florida

Fall 2018–Summer 2021

Developing usable interfaces against robocalls. Co-advised with Juan Gilbert. Now: Assistant Professor at the University of California, San Diego

Tyler Tucker University of Florida

Fall 2021–Summer 2025

Evaluating the security of Bluetooth/cellular radios. Now: Associate at the Analysis Group.

Luis Vargas University of Florida

Fall 2016–Summer 2021

Developing techniques for network-based detection and mitigation of malware in a healthcare environment. Now: Data Scientist at Harbor Experts

Kevin Warren University of Florida

Fall 2019–Summer 2025

Detecting deepfake audio through linguistic information. Now: Associate at the Analysis Group.

2. Ph.D. Students Supervised

Jordan Greene University of Florida

Fall 2025–Present

Defending voice-driven systems and cellular network security.

Allison Lu University of Florida

Fall 2022–Present

Measuring repeatability in computer security.

3. Ph.D. Students - Other

Saurabh Chakradeo Georgia Institute of Technology

Fall 2010–Spring 2013

Research exploring malicious mobile applications. Left to join Facebook.

Brendan Dolan-Gavitt Georgia Institute of Technology

Spring 2009

Research project on using kernel type graphs to detect dummy structures.

Ryon Kennedy University of Florida

Fall 2020–Spring 2023

Finding vulnerabilities in cellular core networks via fuzzing. Left to join UFIT.

Eric (Yu) Liu Georgia Institute of Technology

Fall 2008

Research on the spread of malware through cellular infrastructure.

Chaz Lever Georgia Institute of Technology

Fall 2011–Spring 2014

Developing techniques to measure the spread of malware in cellular networks. Left Georgia Tech to create a startup.

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology
Fall 2009–Summer 2010
Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

Aviva Smith University of Florida
Fall 2025–Spring 2026
Detecting attacks on voice-driven systems and deepfakes. Left program for industry.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2008–Spring 2009
Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida
Fall 2015–Spring 2016
Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology
Fall 2009–Spring 2010
Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology
Fall 2012–Fall 2013
Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology
Fall 2012–Fall 2013
Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology
Fall 2008–Summer 2009
Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology
Fall 2011–Spring 2012
Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology
Fall 2009–Present
Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now Raytheon

Rishikesh Naik Georgia Institute of Technology
Fall 2008–Spring 2010
Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal University of Florida

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

Research on creating provably anonymous networks on a base of secure function evaluation. Now with VMWare.

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

Developed the OnionDNS architecture, which prevents domain delisting attacks by leveraging a Tor hidden service. Joined Ph.D. program at UF.

Tyler Tucker University of Florida

Fall 2018–Spring 2021

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology

Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology

Spring 2011

Developed mobile phone-based tools for measuring performance and reachability throughout the Internet.

Ashwin Narasimhan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

Aamir Poonawalla Georgia Institute of Technology

Spring 2010

Helped develop a call provenance infrastructure, which included both networking and machine learning components.

Erin Reddick Georgia Institute of Technology

Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology

Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology

Fall 2011–Spring 2012

Developed a mobile phone application for taking measurements of cellular networks.

Dane Van Dyck Georgia Institute of Technology

Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

1. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Fall 2013.
2. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Fall 2012.
3. United State Army Signal Corps, “Helmet” Award, 2010.
4. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Spring 2009.
5. Pennsylvania State University CSE Graduate Student Teaching Award, 2005

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

1. Patrick Gerard Traynor. *Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks*. PhD thesis, The Pennsylvania State University, May 2008.

B. Published Journal Papers (Refereed)

1. Kevin Butler, Kurt Hugenberg, Eakta Jain, Apu Kapadia Tadayoshi Kohno, Elissa Redmiles, Franziska Roesner, Mattea Sim, Patrick Traynor, and Hanna Barakat. Extending the Heilmeier Catechism to Evaluate Security and Privacy Systems: Who is Left Out? *IEEE Security and Privacy*, May/June 2025.
2. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022. (Acceptance rate: 24%).
3. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.
4. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Security Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.
5. Nolen Scaife, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.
6. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Security (TOPS)*, 2017.
7. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.
8. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.
9. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.
10. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.
11. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.
12. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.
13. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.

14. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.
15. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.
16. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.
17. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.
18. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous networkRking in Delay tolErant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.
19. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.
20. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.
21. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.
22. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010.
23. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points. *Journal of Security and Communication Networks (SCN)*, 2(3):102–113, 2010.
24. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.
25. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12):1803–1815, 2009.
26. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.
27. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TIS-SEC)*, 2008.
28. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.
29. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.
2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Papers with Proceedings (Refereed)

1. Seaver Thorn, Nathaniel Bennett, Kevin Butler, Patrick Traynor, and William Enck. ASN1spect: Uncovering ASN.1 Compiler-Generated Vulnerabilities in Critical Infrastructure. In *ACM Secure Development (SecDev) Conference*, 2026.
2. Eric Pauley and Yohan Beugin and Paul Barford and Patrick Traynor and Patrick McDaniel. Honey Configs: Measuring the Disclosure and Exploitation of Cloud IP Address Reuse. In *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2026.
3. Nathaniel Bennett, Tyler Tucker, Carson Stillman, William Enck, Patrick Traynor, and Kevin Butler. Fizzle: A Framework for Deterministic and Reproducible Network Fuzzing. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2026.
4. Seth Layton, Bernardo Medeiros, Kevin Butler, and Patrick Traynor. AI Wrote My Paper and All I Got Was This False Negative: Measuring the Efficacy of Commercial AI Text Detectors. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2026.
5. Carson Stillman, Jennifer Sheldon, Ian Garrett, Patrick Traynor, Ryan Gerdes, Sara Rampazzi, and Kevin Butler. EM-Flow: Advanced Electromagnetic Control Flow Verification for Embedded Systems. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2025.
6. Daniel Olszewski, Tyler Tucker, Kevin Butler, and Patrick Traynor. SoK: Towards a Unified Approach to Applied Replicability for Computer Security. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.
7. Daniel Olszewski, Allison Lu, Anna Crowder, Nathaniel Bennett, Seth Layton, Sri Hrushikesh Varma Bhupathiraju, Tyler Tucker, Siddhant Kalgutkar, Hunter Ver Helst, Carson Stillman, Kevin Butler, Sara Rampazzi, and Patrick Traynor. Reproducibility in Applied Security Conferences: An 11-Year Review on Artifacts and Evaluation Committees. In *Proceedings of ACM Conference on Reproducibility and Replicability (REP)*, 2025.
8. Cassidy Gibson and Daniel Olszewski and Natalie Grace Brigham and Anna Crowder and Kevin R. B. Butler and Patrick Traynor and Elissa M. Redmiles and Tadayoshi Kohno. Analyzing the AI Nudification Application Ecosystem. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.

9. Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin Butler, and Patrick Traynor. Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
10. Anna Crowder, Allison Lu, Kevin Childs, Carson Stillman, Patrick Traynor, and Kevin Butler. Data to Infinity and Beyond: Examining Data Sharing and Reuse Practices in the Computer Security Community. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2025.
11. Magdalena Pasternak, Kevin Warren, Daniel Olszewski, Susan Nittroueri, Patrick Traynor, and Kevin Butler. Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant Simulated Audio. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
12. Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2024. (Acceptance Rate 21.8%).
13. Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa Redmiles, Eakta Jain, Patrick Traynor, and Kevin Butler. “I Had Sort of a Sense that I Was Always Being Watched... Since I Was”: Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
14. Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, William Enck, Patrick Traynor, and Kevin Butler. RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
15. Kevin Warren, Tyler Tucker, Anna Crowder, Daniel Olszewski, Allison Lu, Caroline Fedele, Magdalena Pasternak, Seth Layton, Kevin Butler, Carrie Gates, and Patrick Traynor. Better Be Computer or I’m Dumb”: A Large-Scale Evaluation of Humans as Audio Deepfake Detectors. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
16. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. Examining Cryptography and Randomness Failures in Open-Source Cellular Cores. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2024. (Acceptance rate: 21.3%)(Best Paper).
17. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
18. Imani Munyaka, Daniel Delgado, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. “I used to live in Florida”: Exploring the Impact of Spam Call Warning Accuracy on Callee Decision-Making. In *Symposium on Usable Security and Privacy (USEC)*, 2024.
19. Jianliang Wu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).

20. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. “Get in Researchers; We’re Measuring Reproducibility”: A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2023. (Acceptance rate: 19.8%).
21. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023. (Acceptance rate: 21%).
22. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue’s Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023. (Acceptance rate: 14%).
23. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023. (Acceptance rate: 16%).
24. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.
25. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).
26. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O’Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).
27. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)*, 2022. (Acceptance rate: 16.2%).
28. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).
29. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.
30. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
31. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).

32. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear “No Evil”, See “Kenansville”: Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
33. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.
34. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).
35. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
36. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 22.0% for all papers).
37. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY’19)*, 2019. (Acceptance rate: 23.5%).
38. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).
39. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).
40. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
41. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
42. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.
43. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.

44. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. AT-tention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
45. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szajda, and Patrick Traynor. Mitigating Risk while Complying with Data Retention Laws. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.
46. Logan Blue, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2018.
47. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).
48. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
49. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
50. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).
51. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).
52. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).
53. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
54. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
55. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).
56. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).
57. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).

58. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).
59. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).
60. Nolen Scaife, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
61. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
62. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
63. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).
64. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
65. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).
66. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).
67. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).
68. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).
69. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).
70. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).

71. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).
72. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).
73. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).
74. Yacin Nadjji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
75. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
76. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).
77. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).
78. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingerin Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).
79. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).
80. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).
81. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).
82. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).
83. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).
84. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).

85. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
86. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
87. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).
88. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).
89. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).
90. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).
91. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).
92. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).
93. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).
94. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).
95. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).
96. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).
97. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).

98. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).
99. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).
100. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

E.2. Conference Presentations with Proceedings (Non-Refereed)

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).
3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator*: Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.
2. *Malicious Telephony Load Tester*: Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.

2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop, CCSW '20*, 2020.
2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.
3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.
4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.
5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.
7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.
8. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **Artus Protocol STTR Phase II - Extension**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$300,000 over 2 years
Awarded: August 2023
2. **Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler

Amount: \$150,000 over 1 year
Awarded: August 2023

3. **Reconstructing Human Physiological Features from Audio Samples**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$700,000 over 3 years
Awarded: August 2021
4. **Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$274,000 over 2 years
August 2021
5. **Deploying Defenses for Cellular Networks Using the AWARE Testbed**
Sponsor: Department of Homeland Security: CISA:
Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P. R. Kumar
Amount: \$3,100,000 over 4 years
Awarded: October 2019
6. **SaTC: CORE: Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler
Amount: \$1,199,999 over 4 years
Awarded: October 2019
7. **Artus Protocol STTR Phase II**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$800,000 over 4 years
Awarded: August 2019
8. **Evaluating the Security of QR Code-Based Payments**
Sponsor: Discover Financial
Investigator(s): Patrick Traynor (PI)
Amount: \$50,000 over 1 year
Awarded: September 2018
9. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$50,000 over 1 year
Awarded: September 2017
10. **Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded: July 2016
11. **Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem**

Sponsor: National Science Foundation
Investigator(s): Patrick Traynor (PI), Kevin Butler, Shigang Chen
Amount: \$1,200,000 over 4 years
Awarded: June 2016

12. Evaluating and Improving Security in Emerging Branchless Banking Systems

Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded July 2015

13. Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems

Sponsor: CISE-ECE Harris Endowed Seed Fund Program
Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
Amount: \$40,000 over 1 year
Awarded December 2014

14. Mobile Excursion Study Support

Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
Amount: \$280,000 over 3 months
Awarded July 2012

15. Characterizing the Security Limitations of Accessing the Mobile Web

Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
Amount: \$334,000 over 3 years
Awarded July 2012

16. Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure

Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
Amount: \$210,081 over 1 year
Awarded June 2011

17. Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation

Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
Amount: \$580,000 over 4 years
Awarded May 2011

18. Security for Converged IMS Networks

Sponsor: US Department of Defense
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
Amount: \$242,401 over 1 year
Awarded August 2010

19. CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$400,000 over 5 years
Awarded: May 2010

20. **Provably Anonymous Networking Through Secure Function Evaluation**

Sponsor: NSF Trustworthy Computing

Investigator(s): Patrick Traynor (PI)

Amount: \$200,000 over 2 years

Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **RADIOBEAR**

Sponsor: Nightwing Intelligence / US Air Force

Investigator(s): Kevin Butler (PI), Patrick Traynor

Amount: \$249,327 for 1 year

Awarded September 2025

2. **Artus Protocol STTR Phase II - Extension**

Sponsor: Office of Naval Research

Investigator(s): Kevin Butler (PI), Patrick Traynor

Amount: \$300,000 over 1 year

Awarded: August 2024

3. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**

Sponsor: NSF SaTC

Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franz Roesner, Apu Kapadia, Eakta Jain.

Amount: \$7,500,000 for 5 years

Awarded October 2022

4. **Mobile Interface Security Analysis**

Sponsor: Office of Naval Research

Investigator(s): Kevin Butler (PI), Patrick Traynor

Amount: \$700,000 over 3 years

January 2020

5. **AFOSR University Center of Excellence in Assured Autonomy in Contested Environments (AACOE)**

Sponsor: Air Force Office of Scientific Research and Air Force Research Labs

Investigator(s): Warren Dixon (PI), Patrick Traynor

Amount: \$5,999,515 for 5 years

March 2019

6. **ROCKY: Reliable Obfuscated Communications Kit for everyOne**

Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement

Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger

Amount: \$1,600,000 over 4 years

Awarded May 2019

7. **Smartphones and Mobile Money: Analysis and Recommendations for Security**
Sponsor: GSMA Mobile For Development Foundation
Investigator(s): Kevin Butler (PI), Patrick Traynor
Amount: \$28,500
December 2017
8. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: \$300,000 for 2 years
December 2016
9. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: \$532,952 for 2 years
October 2016
10. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: \$200,000 for 2 years
September 2015
11. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: \$500,000 for 3 years
Submitted: December 2012
12. **Facilitating Free and Open Access to Information on the Internet**
Sponsor: NSF Trustworthy Computing
Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
Amount: \$1,500,000 for 4 years
Awarded: June 2011
13. **Monitoring Free and Open Access to Information on the Internet**
Sponsor: Google Focus Program
Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
Amount: \$1,000,000 for 2 years
Awarded: November 2011
14. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
Sponsor: Health Systems Institute (HSI) Seed Grant Program
Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
Amount: \$50,000 over 1 year
Awarded: August 2009
15. **Federal Cyber Service Scholarships at Georgia Tech**
Sponsor: NSF SFS Scholarships
Investigator(s): Seymour Goodman (PI), Patrick Traynor
Amount: \$1,250,682 over 5 years
Awarded: June 2009

16. Security for IMS-Enabled Converged Applications

Sponsor: US Department of Defense

Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark

Amount: \$146,121 for 1 year

Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

1. Social Impact Award, New York University CSAW Applied Research Competition, 2025.
2. Distinguished Paper (Runner Up), USENIX Security Symposium, 2025.
3. Best Paper Award, ACM Conference on Reproducibility and Replicability (REP), 2025.
4. Distinguished Paper, ACM Conference on Computer and Communications Security (CCS), 2024.
5. Best Paper Award, ACM Conference on Data and Application security and Privacy (CODASPY), 2024.
6. Distinguished Paper, USENIX Security Symposium, 2018.
7. Fellow, Center for Financial Inclusion at Accion, 2017.
8. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.
9. Best Paper, The ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); Budapest, Hungary, 2013.
10. Best Student Paper, The Information Security Conference (ISC); Passau, Germany, 2012
11. Lockheed Inspirational Young Faculty Award, 2012
12. Best Demo, "Is Browsing the Internet on Your Mobile Phone Secure?" Chaitrali Amrutkar (Ph.D Advisee), CoC Research Day, 2011
13. Best Poster, "(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers" Arunabh Verma, Henry Carter (MS, Ph.D Advisees), CoC Research Day, 2011
14. National Science Foundation CAREER Award, 2010
15. Pennsylvania State University Alumni Association Dissertation Award, 2007
16. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
17. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

1. Senior Member, Association for Computing Machinery (ACM)
2. Senior Member, Institute of Electrical and Electronics Engineers (IEEE)
3. Member, USENIX Advanced Computing Systems Association (USENIX)

A.2. Conference Committee Activities

1. Program co-Chair, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2023, 2024
2. Program co-Chair, *USENIX Security Symposium (SECURITY)*: 2019
3. Program co-Chair, *Network and Distributed System Security Symposium (NDSS)*: 2017, 2018
4. Program Chair, *USENIX Workshop on Offensive Technologies (WOOT)*: 2016
5. Program Chair, *ACM Conference on Wireless Network Security (WiSec)*: 2014
6. Program Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*: 2012, 2013
7. Program Chair, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2012
8. Chair Invited Talks Committee, *USENIX Security Symposium (SECURITY)*: 2014
9. Workshops Chair, *IEEE Conference on Communications and Network Security (CNS)*: 2016
10. Program Committee, *USENIX Security Symposium (SECURITY)*: 2008, 2009, 2010, 2013, 2015-2018, 2020-2022
11. Program Committee, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2009-2014, 2022.
12. Program Committee, *ACM Conference On Computer and Communications Security (CCS)*: 2009, 2013-2015, 2017
13. Program Committee, *Network and Distributed System Security Symposium (NDSS)*: 2010, 2013-2016, 2020-2021
14. Program Committee, *IEEE European Symposium on Security and Privacy (Euro S&P)*: 2016
15. Program Committee, *Annual Computer Security Applications Conference (ACSAC)*: 2008, 2009, 2010, 2011, 2015
16. Program Committee, *ACM Conference on Wireless Network Security (WiSec)*: 2009, 2010, 2013, 2015-2021
17. Program Committee, *International Conference on Financial Cryptography and Data Security (FC)*: 2010, 2013
18. Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*: 2016.
19. Program Committee, *ICST Conference on Security and Privacy in Communication Networks (SecureComm)*: 2009, 2010
20. Program Committee, *Privacy Enhancing Technologies Symposium (PETS)*: 2015, 2016

21. Program Committee, *International World Wide Web Conference (WWW)*: 2016
22. Program Committee, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2011
23. Program Committee, *ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds (MOBIHELD)*: 2010
24. Program Committee, *International Workshop on Mobile Security (WMS)*: 2010
25. Program Committee, *European Symposium on Research in Computer Security (ESORICS)*: 2009, 2011
26. Program Committee, *IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS)*: 2009, 2010
27. Program Committee, *Information Security Conference (ISC)*: 2010
28. Program Committee, *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*: 2009
29. Program Committee, *Computer Security Architecture Workshop (CSAW)*: 2008
30. Program Committee, *IWCMC Computer and Network Security Symposium*: 2009
31. Program Committee, *IARIA International Conference on Internet Monitoring and Protection (ICIMP)*: 2009
32. Program Committee, *IEEE Workshop on Network Security and Privacy (NSP)*: 2008
33. Program Committee, *IEEE International Workshop on Wireless and Sensor Networks Security (WSNS)*: 2008, 2009
34. Program Committee, *IEEE Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC)*: 2008
35. Program Committee, *ACM Conference on Computer and Communications Security, Industry and Government Track (CCS I&G)*: 2006, 2007
36. Program Committee, *Workshop on Secure Network Protocols (NPsec)*: 2006
37. Program Committee, *International Conference on Information Systems Security (ICISS)*: 2006, 2009, 2010
38. Program Committee, *IEEE LCN Workshop on Network Security (WNS)*: 2006, 2007, 2008

B. On-Campus Committees

B.1. University of Florida

1. Member, Computer and Information Science and Engineering Steering Committee, 2015-2017.
2. Member, Graduate Recruiting Committee, 2015-2017.
3. Chair, Computer and Information Science and Engineering Industrial Advisory Board, 2014-2015.

B.2. Georgia Tech

1. Member, Massive Open Online Master's (MOOMS) Investigation Committee, 2012-2013.
2. Chair, School of Computer Science Ph.D. Review Committee, 2012.
3. Member, School of Computer Science Ph.D Review Committee, 2011.
4. Faculty Advisor, Grey H@T - Georgia Tech Undergraduate Security Club, 2011-2014.
5. Member, School of Computer Science Ph.D. Review Committee, 2011.
6. Member, School Advisory Committee, School of Computer Science, 2011-2013.
7. Member, School of Computer Science Chair Recruiting Committee, 2011.
8. Member, School of Computer Science Faculty Recruiting Committee, 2010, 2011.
9. Chair, College of Computing Ph.D. Welcome Weekend Committee, 2009, 2010, 2011 (co-chair).
10. Member, College of Computing Ph.D. Recruiting Committee, 2009.
11. Member, Georgia Tech Computer and Network Usage Security Policy (CNUSP) Evaluation Group, 2009.

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, University of Florida, Summer 2017.
Advisor: Professor Patrick Traynor.
2. Adam Bates, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
4. Henry Carter, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
5. David Dewey, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
6. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2014.
Advisor: Professor Umakishore Ramachandran.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Patrick Traynor.
8. Long Lu, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Wenke Lee.

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Patrick Traynor.
12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Alexandra Boldyreva.
13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Nick Feamster.
14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Mustaque Ahamad.
15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Wenke Lee.
16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Jon Giffin.
17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
Advisor: Professor Alexandra Boldyreva.
18. David Cash, College of Computing, Georgia Tech, Fall 2009.
Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
Advisor: Professor Kelly Jordan.
2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
Advisor: Professor Alan George.
3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
Advisor: Professor Srdjan Capkun.
4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
Advisor: Professor Srdjan Capkun.
5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, Spring 2016.
Advisor: Professor Patrick Traynor.
2. Maliheh Shirvanian, University of Alabama, Birmingham, Spring 2016.
Advisor: Professor Nitesh Saxena.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
4. Adam Bates, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
5. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Umakishore Ramachandran.
6. Long Lu, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2012.
Advisor: Professor Patrick Traynor.
8. Junjie Zhang, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
9. Italo Dacosta, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
10. Manos Antonakakis, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
11. Abhinav Srivastava, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Jon Giffin.
12. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mustaque Ahamad.
13. Kapil Singh, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Wenke Lee.
14. Anirudh Ramachandran, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
15. Adam O'Neill, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Alexandra Boldyreva.
16. David Cash, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.

Ph.D. Qualifying Exam Committees—Georgia Tech

1. Byoungyoung Lee, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
2. Yizheng Chen, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professors Mustaque Ahamad and Roberto Perdesi.
7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Jon Giffin.
10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
14. Ikpeeme Erete, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Alex Orso.
15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Patrick Traynor.
16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Wenke Lee and Professor Jon Giffin.
17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.
19. Partha Kanuparth, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Constantine Dorvolis.
20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Wenke Lee.
21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.
22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Patrick Traynor.

23. Italo Dacosta, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Mustaque Ahamad and Professor Patrick Traynor.
24. Adam O'Neill, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Alexandra Boldyreva.

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

1. Skim Reaper, *Co-Founder and CEO*, 2019-Present.
2. CryptoDrop Anti-Ransomware, *Co-Founder and CEO*, 2017-2018.
3. Pindrop Security, *Research Fellow and Co-Founder*, Spring 2012 - Spring 2014.
4. United States Army (via US Falcon), *Information Assurance Officer Training Program*, Spring 2010.
5. 3G Americas, *Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Systems*, Fall 2008.

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

1. Fellow, Kavli Foundation, 2017.
2. Fellow, Center for Financial Inclusion at Accion, 2016.
3. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.

B. Invited Conference Session Chairmanships

1. Session Chair, *Work-in-Progress* at the *USENIX Security Symposium (SECURITY)*, 2016.
2. Session Chair, *Mobile Security* at the *USENIX Security Symposium (SECURITY)*, 2013.
3. Poster Chair, *USENIX Security Symposium (SECURITY)*, 2010, 2011.
4. Session Chair, *Privacy and Anonymity* at the *USENIX Workshop on Hot Topics in Security (HotSec)*, 2011.
5. Session Chair, *Security of Authentication and Protection Mechanisms* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2011.
6. Session Chair, *Information Abuse* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2010.
7. Session Chair, *RFID Security* at the *ACM Conference on Computer and Communications Security (CCS)*, 2009.
8. Session Chair, *Browser Security Session* at the *USENIX Security Symposium (SECURITY)*, 2009.
9. Session Chair, *Information Security Session* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
10. Session Chair, *Work-in-Progress* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
11. Session Chair, *Work/Opinions-in-Progress* at the *ISOC Network and Distributed Systems Security (NDSS) Symposium*, 2009.
12. Session Chair, *Privacy Session* at the *USENIX Security Symposium (SECURITY)*, 2008.

C. Professional Registration

None.

D. Patents

1. Patrick G. Traynor, Christian Peeters, Bradley G. Reaves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife, "Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding", United State Patent # 11,265,717, Filed March 2019, Issued March 2022.
2. Patrick G. Traynor, Logan E. Blue, Luis Vargas, "Method and Apparatus for Differentiating Between Human and Electronic Speaker for Voice Interface Security", United State Patent # 11,176,960, Filed June 2019, Issued November 2021.
3. Patrick G. Traynor, Bradley G. Reaves, Logan E. Blue Practical End-to-End Cryptographic Authentication for Telephony Over Voice Channels, United State Patent # 11,329,831, Filed November 2018, Issued May 2022.

4. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)
5. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.
6. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.
7. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.
8. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)
9. Patrick G. Traynor, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

- *ACM Transactions on Information and System Security (TISSEC)* 2015-present

Guest Editor:

Journals

- *IEEE Security and Privacy Magazine (S&P)* 2013

Reviewer for:

Journals

- *ACM Transactions on Information and System Security (TISSEC)* 2008, 2009, 2010, 2011, 2012, 2013
- *IEEE Transactions on Dependable and Secure Computing (TDSC)* 2012, 2013
- *IEEE Security and Privacy Magazine (S&P)* 2010, 2011
- *Communications of the ACM (CACM)* 2010
- *Journal of Anesthesia & Analgesia* 2009
- *IEEE Transactions on Mobile Computing (TMC)* 2008, 2010, 2011, 2012, 2013
- *IEEE Transactions on Internet Technology (TOIT)* 2009, 2010
- *ACM Mobile Computing and Communications Review (MC2R)* 2008
- *IEEE/ACM Transactions on Networking (TON)* 2007, 2008
- *Journal of Pervasive and Mobile Computing (PMC)* 2009, 2010

- *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2005, 2009, 2010
- *IEEE Transactions on Computers (TOC)* 2010
- *Journal of Security and Communication Networks (SCN)* 2008
- *IEEE Communications Letters (CL)* 2007, 2009
- *IEEE Transactions on Wireless Communications (TWC)* 2007
- *Pervasive and Mobile Computing (PMC)* 2007
- *IEEE Transactions on Software Engineering (TSE)* 2007, 2008
- *Journal of Wireless Networks (WiNet)* 2006, 2007, 2008, 2009
- *Journal of Wireless Communications and Mobile Computing* 2006
- *ACM Computing Surveys (ACMCS)* 2006
- *Information Processing Letters (IPL)* 2006
- *IEEE Transactions on Very Large Scale Integration Systems (TVLSIS)* 2006

Conferences and Workshops

- *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2011
- *ACM Conference on Computer and Communications Security (CCS)*, 2008, 2011
- *IEEE Symposium on Security and Privacy (OAKLAND)* 2007, 2008
- *Computer Security Foundations (CSF)*, 2011
- *IFIP Conference on Data and Applications Security (DBSec)* 2008
- *Financial Cryptography (FC)* 2007, 2008
- *International Conference on VLSI Design (VLSI)* 2007
- *Annual Computer Security Applications Conference (ACSAC)* 2005, 2006, 2007
- *USENIX Workshop on Hot Topics in Security (HotSec)* 2007
- *International Conference on Information Systems Security (ICISS)* 2007
- *IEEE International Conference on Computer Engineering & Systems (ICCES)* 2007
- *International Workshop on Security (IWSec)* 2006, 2007
- *USENIX Security Symposium (SECURITY)* 2006, 2007
- *IEEE Sarnoff Symposium (SARNOFF)* 2007
- *International Conference on New Technologies, Mobility and Security (NTMS)* 2007
- *IEEE Infocom (INFOCOM)* 2007
- *Network and Distributed System Security Symposium (NDSS)* 2007
- *International Workshop on Storage Security and Survivability (IWSSS)* 2006
- *ACM Conference on Computer and Communications Security (CCS)* 2006

- *IEEE GLOBECOM (GLOBECOM) 2006*
- *International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS) 2006*
- *IFIP Conference on Data and Applications Security (DBSec) 2006*
- *Emerging Trends in Information and Communications Security (ETRICS) 2006*
- *International Conference on Applied Cryptography and Network Security (ACNS) 2006*
- *ACM Symposium on Access Control Models and Technology (SACMAT) 2006*
- *IEEE Conference on Communication Systems Software & Middleware (COMSWARE) 2006*
- *International Conference on Cryptology in India (IndoCrypt) 2005*
- *IEEE Symposium on New Frontiers in Dynamic Spectrum Access (DySPAN) 2005*
- *European Symposium on Research in Computer Security (ESORICS) 2005*

F. Expert Witness Services

1. *KAIFI LLC v. Apple Inc., No. 1:25-cv-1372 (W.D. Tex.):* Expert witness for the Defense (via Gibson, Dunn & Crutcher, LLP). *March 2026 - Present.*
2. *Natalie Delgado, et al. v. Meta Platforms Inc., Case No.: 23-cv-04181 (N.D. Cal.):* Expert witness for the Defense (via Gibson, Dunn & Crutcher, LLP). *October 2025 - Present.*
3. *Google LLC v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Wolf, Greenfield & Sacks, P.C.). *August 2025 - Present.*
4. *Amazon v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Perkins Coie, LLP). *August 2025 - Present.*
5. *HBCU Messaging US LP v. Apple, Inc. et al., Civil No. 1:24-cv-1199,:* Expert witness for the Defense (via Fish & Richardson, LLP). *June 2025 - June 2026.*
6. *PACid v. Citibank, N.A., 1:24-cv-00272-DAE (W.D. Tex.):* Expert witness for the Defense (via Troutman Pepper Locke LLP). *April 2025 - November 2025.*
7. *Facebook Inc. Derivative Litigation., Consolidated C.A. No. 2018-0307-JTL (Del. Ch.):* Expert witness for the Defense (via Wachtell, Lipton, Rosen & Katz, LLP) *January 2025 - July 2025.*
8. *Averon US, Inc. vs AT&T Inc., Case No. 1:22-cv-01341-TMH:* Expert witness for the Defense (via O'Melveny & Myers, LLP). *November 2024 - September 2025.*
9. *RightQuestion, LLC v. AT&T Inc. et al.,, Case No. 2-24-cv-00094 -JRG:* Expert witness for the Defense (via Duane Morris, LLP). *September 2024 - November 2025.*
10. *ByteDance Ltd. vs CellSpin Soft, Inc.:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *February 2024 - October 2024.*
11. *Bank of America, N.A., vs PACid:* Expert witness for the Plaintiff for Inter Partes Review (via McNish PLLC). *December 2023 - March 2024.*
12. *Microsoft vs Proxense, LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *November 2023 - July 2025.*

13. *Samsung vs Headwater Research LLC*: Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). August 2023 - October 2025.
14. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.*: Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). July 2023 - September 2023.
15. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021*: Expert witness for the Defendant (via Corrs Chambers Westgarth). January 2023 - June 2024.
16. *Rubin vs KAHOOT! ASA and KAHOOT! EDU*: Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). December 2022 - June 2024.
17. *Telefonaktiebolaget LM Ericsson vs Apple, Inc.*: Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). February 2022 - December 2022.
18. *Wepay Global Payments, LLC v. Bank of America N. A.*: Expert Witness for the Defendant (via WilmerHale LLP) September 2022 - November 2022.
19. *Apple vs. R.N Nehushtan Trust Ltd.*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). August 2022 - June 2023.
20. *Apple/Microsoft vs. Zipit Wireless*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). May 2021 - November 2022.
21. *Blackberry Inc v MobileIron, Inc.*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). January 2021 - March 2021.
22. *Apple Inc v Seven Networks, LLC*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). August 2019 - November 2020.
23. *mSIGNIA, Inc. v. InAuth, Inc.*: Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity, Trade Secrets (via Quinn Emanuel Urquhart and Sullivan, LLP). October 2017 - December 2018.
24. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) June 2016 - December 2017.
25. *Telefonaktiebolaget LM Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). June 2015 - December 2015.
26. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). June 2015 - November 2015.
27. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). January 2014 - August 2014.
28. *Maxim Integrated Products v Comerica Inc, et al.*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). June 2014 - August 2014.
29. *William Grecia v. Apple Inc. et al.*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). July 2014 - August 2014.
30. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). October 2013 - February 2014.
31. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) April 2013 - June 2013.
32. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), October 2012 - February 2015.

V. OTHER CONTRIBUTIONS

A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)

1. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. Learning from Authoritative Security Experiment Results (LASER) Workshop, December 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
2. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
3. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
4. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. EPFL Summer Research Institute (SURI), July 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
5. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. North Central Florida Institute of Internal Auditors (IIA), May 2024.
6. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. UF Quest 2: Siri is my Superpower: Communicating with AI, March 2024. University of Florida.
7. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. Federal Information Integrity Research and Development (FIIRD) Interworking Group (IWG), March 2024. via NITRD, OSTP.
8. AI driven voice cloning scams. Discussion at the White House with Anne Neuberger (Deputy National Security Advisor for Cyber and Emerging Technologies), Jessica Rosenworcel (Chair of the Federal Communications Commission) and Lina Khan (Chair of the Federal Trade Commission), January 2024. Lead Academic facilitator.
9. Keynote: Well, It Worked on My Computer: Reproducibility, Tech Transfer, and Computer Security Research. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Vision 2.0 Workshop, March 2023. University of Texas at Dallas.
10. Humans vs The Computer Interfaces: Separating Deepfakes/Bots from People Using Psychoacoustics. UCLA Electrical and Computer Engineering Distinguished Seminar, February 2023. University of California, Los Angeles.
11. Keynote: Exploiting the Gaps Between Human and Machine Understanding of Audio: Frameworks, Attacks, and Defenses. ISCA Symposium on Security and Privacy in Speech Communication (SPSC), November 2021. Virtual.
12. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
13. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. North Carolina State University Department of Computer Science Colloquium, January 2020. Raleigh, NC.
14. Moving from research to practice: How to maximize the impact of SaTC projects. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) PI Meeting, October 2019. Alexandria, VA.
15. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Purdue University Computer Science Excellence Lecture Series, October 2019. West Lafayette, IN.

16. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
17. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. CISP – Helmholtz Center for Information Security, Saarland University, February 2019. Saarbrücken, Germany.
18. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.
19. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
20. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
21. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
22. Why Caller-ID Spoofing Is So Easy (and Why End-To-End Solutions Are the Way Forward). IEEE Workshop on Technology and Consumer Protection (ConPro'18), May 2018. San Francisco, CA.
23. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
24. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
26. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
27. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
28. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
29. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
30. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
31. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.
32. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
33. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.

34. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.
35. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.
36. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.
37. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
38. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
39. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
40. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
41. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
42. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.
43. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2013. Belfast, Northern Ireland.
44. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
45. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
46. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.
47. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
48. Chasing Telephony Security: Where the Wild Things... Are? University of Washington Department of Electrical Engineering, Network Security Lab (NSL): Invited Talk, November 2012. Seattle, WA.
49. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
50. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
51. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

52. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.
53. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.
54. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.
55. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.
56. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.
57. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.
58. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.
59. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.
60. Privacy and Security Concerns for Personal and Mobile Health Devices. Invited Talk: Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies, October 2009. Indianapolis, IN.
61. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.
62. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.
63. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.
64. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.
65. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.
66. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.
67. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.
68. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.
69. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.
70. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.
71. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.

72. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.
73. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.
74. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.
75. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.
76. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.
77. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
78. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
79. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

B. Special Activities

Presentations to Lay Media

1. How technology can fight digital fakery. The Babbage Podcast/The Economist <https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake>, January 2023.
2. Deepfake audio has a tell and researchers can spot it. Ars Technica <https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/>, September 2022.
3. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie <https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/>, July 2016.
4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - <http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255>, July 2016.
5. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
6. Ransomware 'stopped' by new software. BBC - <http://www.bbc.com/news/technology-36772461>, July 2016.
7. Researchers create effective anti-ransomware solution. Help Net Security - <https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/>, July 2016.
8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.

9. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
10. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - <http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/>, July 2016.
11. Desarrollan una solución para detener el ransomware. ComputerHoy - <http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972>, July 2016.
12. Why your antivirus software can't stop ransomware. Futurity - <http://www.futurity.org/ransomware-computer-files-1198242-2/>, July 2016.
13. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - <http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml>, July 2016.
14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - <https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomware-threat-071116.html>, July 2016.
15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - <https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem>, July 2016.
17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured - Researchers. <http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/>, August 2015.
18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. <http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmsQ.twitter>, August 2015.
19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>, August 2015.
20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.
21. N. V. The Economist - The Threat in the Pocket. <http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket>, October 2013.

22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. <http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move>, October 2013.
23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.
25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. <http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/>, June 2013.
26. Jim Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.
27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuId, December 2012.
31. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.
35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.

36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-siphone-smartphones-accelerometer-track.html>, October 2011.
40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.
41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. <http://www.sciencedaily.com/releases/2010/10/101005121820.htm>, October 2010.
44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.
45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - <http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies-iphone-users-cripple-att/story?id=9355447>, December 2009.
46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - http://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.
47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - <http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html>, November 2009.
48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - <http://www.scmagazineus.com/remote-repair-for-infected-phones-in-development/article/157504/>, November 2009.
49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - <http://www.networkworld.com/news/2009/111109-smartphone-security-georgia-tech.html?hpg1=bn>, November 2009.

50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11/2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - <http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3>, July 2009.
53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - <http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/>, June 2009.
55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.
56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.
58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - <http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml>, October 2008.
59. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.
61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.
64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.
65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine <http://www.slate.com/id/2161402/>, 2007.

66. Jamming Cellphones with Text Messages. Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
67. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
68. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times <http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss>, 2005.