UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner.

IPR2024-00332
U.S. Patent No. 10,929,512

IPR2024-00334
U.S. Patent No. 11,514,138

REMOTE DEPOSITION OF MICHAEL T. GOODRICH, Ph.D.

(Taken by Petitioner)

January 8, 2025

12:02 p.m.

Deposition held via Zoom Videoconference

Reported by: F. Renee Finkley, RPR, RMR, CRR, CLR, CCR-B-2289 (Via Videoconference)

1
APPEARANCES OF COUNSEL
2
3
On behalf of the Petitioner:
4
5 HONG SHI, Esq. (Via Videoconference)
6 DAVID W. O'BRIEN, Esq. (Via Videoconference)
7 KELLY LYLE, Esq. (Via Videoconference)
8 Haynes and Boone, LLP
9 98 San Jacinto Boulevard
10 Suite 1500
11 Austin, Texas 78701
12 (512) 867-8440
13 hong.shi@haynesboone.com
14 david.obrien@haynesboone.com
15
16 On behalf of the Patent Owner:
17 GEORGE FISHBACK, Esq. (Via Videoconference)
18 McKool Smith, PC
19 303 Colorado Street, Suite 2100
20 Austin, Texas 78701
21 (512) 692-8700
22 gfishback@mckoolsmith.com
23
24
25

CONTENTS

THE WITNESS: MICHAEL T. GOODRICH, Ph.D.

EXAMINATION Page

By Ms. Shi 4

EXHIBITS

Exhibit No. Page

1 - Table of contents to Introduction to Computer Security 16

(The witness was sworn.)

MICHAEL T. GOODRICH, Ph.D., having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MS. SHI:

Q. Good morning. Again, I'm Hong Shi from Haynes and Boone on behalf of Petitioner Apple.

**A. Good morning.**

Q. Good morning. So I will go over some of the ground rules, similar to what we did yesterday, but this is specific for this deposition. So do you understand that you're under oath today?

**A. Yes.**

Q. And you understand that the oath requires you to answer my questions truthfully and completely?

**A. Yes.**

Q. And you will answer truthfully and completely today; is that right?

**A. That is my plan.**

Q. Is there any reason that you cannot provide truthful, complete, and accurate testimony today?

**A. No.**

Q. Is there any other reason that your

1 deposition should not go forward today, medical or
2 otherwise?
3 **A. I don't anticipate any problems. We're**
4 **having wild fires here in Southern California, but I**
5 **don't think any of them are near to here.**
6 Q. Good to know. But if there's an emergency
7 of the wild fire, let me know. We don't want you to
8 be in danger just for this deposition.
9 **A. Thank you.**
10 Q. I would like to ask you to focus on the
11 questions I asked, and answer that question, not
12 another question; is that fair?
13 **A. I will do my best.**
14 Q. And we can plan the breaks as we go, but
15 let me know if you need a break any time.
16 **A. Okay. Thank you.**
17 Q. So today, we're here discussing the cases
18 for the '512 IPR and the '138 IPR; is that clear?
19 **A. That is my understanding, yes.**
20 Q. So for this set of questions, it applies
21 to both declarations. I won't -- if it goes into the
22 specific of any separate declaration, just let me
23 know, but this set of questions should apply to both;
24 is that clear?
25 **A. Sure.**

Q. So for preparing for those declarations, did you review any documents?

**A. Yes.**

Q. What are they?

**A. I speak to this in my declarations. I list, for example, in my declaration for IPR for U.S. Patent 10,925 -- or 929,512, which we call the '512 patent. I list those in my paragraph 15.**

Q. In addition to those documents listed there, did you review any other documents for preparing your declarations?

**A. I also recall reviewing a declaration from Dr. McDaniel in each IPR. I also reviewed the decision from the board to institute IPR in each case. There may have been some other documents as well I'm just not recalling, as I sit here today.**

Q. To prepare your declarations, did you review the Patent Owner's preliminary responses?

**A. I don't recall, as I sit here today.**

Q. Did you review the petitions in their totality?

**A. I reviewed them. I don't recall if it was the entire documents in each case. In some cases, there oftentimes are legal arguments in these proceedings. And I tried to stick to the technical**

**arguments.**

Q. Did you meet with anyone to prepare for your declaration, either remotely, or by e-mail, or in person?

**A. Yes, I met remotely with Mr. Kamprath from McKool Smith, Mr. Jarrett at McKool Smith, and Mr. Fishback at McKool Smith, who I believe are representing the Patent Owner.**

Q. Did you talk to anyone else?

**A. I don't recall talking to anyone else, as I sit here today.**

Q. Did you do anything else to prepare for the declarations?

**A. I also studied the patents. I did my typical methodology of looking at the arguments, thinking about them, placing myself into the shoes of a person of ordinary skill in the art, in light of the alleged prior art. And then in discussions with counsel, I came to my conclusions.**

Q. Do you remember roughly how many hours you spent to prepare the two declarations?

**A. No, I don't recall that.**

Q. Do you have a rough estimate?

**A. I am not comfortable speculating. I don't recall it.**

Q. So to prepare for the deposition today, have you reviewed any documents?

**A. Yes.**

Q. What documents did you review?

**A. My recollection is that I reviewed my two declarations. I reviewed the declaration -- at least one of the declarations from Dr. McDaniel. I reviewed the institution decision. I reviewed some of the prior art references.**

Q. Did you review the Patent Owner responses?

**A. Not that I recall.**

Q. Did you review any draft of the Patent Owner responses?

**A. Not that I recall, just sitting here today.**

Q. Did you meet with anyone remotely, in person, or through e-mail to prepare for your deposition?

**A. Yes, I met remotely with Mr. Jarrett and Mr. Fishback.**

Q. When was that?

**A. That was on Monday of this week. This was joint with the other depositions that we had yesterday as well.**

Q. And how long was that?

1 **A. It was a few hours.**
2 Q. And did you review the documents you
3 mentioned after your meeting with your counsel?
4 **A. That's my recollection, yes.**
5 Q. When was the last time you reviewed the
6 documents to prepare for today's deposition?
7 **A. I did some review yesterday after our**
8 **deposition from yesterday.**
9 Q. Did you also do some review today before
10 the deposition?
11 **A. No.**
12 Q. Did you review any documents filed or
13 prepared for the District Court?
14 **A. Not that I recall. Only if there's**
15 **potential overlap, for example, with any of the**
16 **alleged prior art references, for example.**
17 Q. But you're not aware there are any
18 documents specific for District Court litigation?
19 **A. That is correct.**
20 Q. Let's -- again, do you have the
21 declarations on your computer?
22 **A. I do. In anticipation of how we did**
23 **things yesterday, I have them on my screen.**
24 Q. Do you have notes on them?
25 **A. There's no notes. There's only some**

1 **sections that may be highlighted in yellow.**
2 Q. So let's go to the -- your declaration,
3 Exhibit 2037, for the '512 IPR?
4 **A. I am there.**
5 Q. Can you go to the last page of your
6 declaration?
7 **A. Yes, I'm there.**
8 Q. Is that your signature on the last page of
9 your declaration?
10 **A. Yes.**
11 Q. Did you sign after reviewing the entirety
12 of the declaration?
13 **A. Yes.**
14 Q. Is there any error in your declaration
15 that you would like to correct?
16 **A. I noticed in reviewing, that there's some**
17 **minor typos, but they are not, in my opinion,**
18 **substantive. There's nothing substantive that I wish**
19 **to change at this time.**
20 Q. Let's go to paragraph 8 of your
21 declaration.
22 **A. I am there.**
23 Q. Can you read the first sentence of
24 paragraph 8?
25 **A. "I have taught undergraduate and graduate**

1 **courses concerning algorithms, data structures,**
2 **software design, networking, and computer security,**
3 **beginning with my work as a graduate student at**
4 **Purdue in 1983, and continuing as a professor at**
5 **Johns Hopkins and University of California, Irvine."**
6 Q. Can you describe the courses you taught
7 concerning algorithms?
8 **A. Sure. So I believe this was also in my**
9 **CV. I will pull that up as well. Yes, the courses**
10 **that I have taught that include discussions and**
11 **lectures on algorithms include computer security**
12 **algorithms, computational geometry, computer**
13 **graphics, cyber fraud detection and prevention, data**
14 **structures, graph algorithms, fundamentals of**
15 **algorithms with applications, introduction to**
16 **algorithms, Internet algorithms, design and analysis**
17 **of algorithms, parallel algorithms, project in**
18 **algorithms and data structures, text processing, and**
19 **pattern matching.**
20 Q. So for the courses you have here, what are
21 the courses that concerns networking?
22 **A. So courses that include networking are**
23 **advanced parallel computing, computer security**
24 **algorithms, cyber fraud detection and prevention,**
25 **graph algorithms, Internet algorithms, parallel**

**algorithms, project in algorithms and data structures, text processing, and pattern matching.**

Q. And what are the courses you have taught concerning computer security?

**A. So courses I've taught that include topics of computer security, in addition to the textbook that I coauthored, include computer security algorithms, cyber fraud detection and prevention, Internet algorithmics, text processing, and pattern matching.**

Q. And you have been teaching these classes since 1983; is that right?

**A. I've taught courses that -- these were part of the whole suite of courses, so they began in 1983, my teaching.**

Q. So for the networking classes, when do you remember you first taught the networking classes?

**A. Courses that included networking, my recollection is they began in the early 1990s.**

Q. And do you remember, when do you first start to teach the computer security classes?

**A. My recollection is I started teaching those classes in the late 1990s, early 2000s.**

Q. So you have one course called computer security algorithms; is that right?

1 **A. That's right.**
2 Q. Is it open to -- what level of students
3 are they directed at?
4 **A. I taught computer security algorithms, as**
5 **I recall, to early undergraduates. So the goal was**
6 **to design it for freshmen and sophomores, but there**
7 **may have been some upper classmen as well.**
8 Q. And the computer security algorithms
9 classes, do they sometimes just be referred to as
10 computer security classes, or is it limited to
11 algorithms?
12 **A. I think people may have also referred to**
13 **that as a computer security course.**
14 Q. What specific topics do you cover in your
15 computer security class?
16 **A. So as I mentioned earlier, I coauthored a**
17 **textbook called Introduction to Computer Security.**
18 **And so as a part of this course on computer security**
19 **algorithms, I -- it's not surprising, since I wrote**
20 **the book, I went through the chapters of my textbook.**
21 **And more advanced topics, I tried to**
22 **explain them to the students, so they could**
23 **understand, 'cause like I said, I was going for**
24 **undergraduates for that class. And so the topics**
25 **that I discussed roughly coincide to the chapters in**

1 **my textbook called Introduction to Computer Security**
2 **coauthored with Roberto Tamassia, T-A-M-A-S-S-I-A.**
3 **And the topics included access control,**
4 **cryptographic concepts, implementation and usability**
5 **issues, physical security, operating system security,**
6 **malware, network security at the lower layers of the**
7 **network stack, network security at the higher layers**
8 **of the network stack, including applications, web**
9 **security, cryptography, including encryption and**
10 **decryption, security models and practice, and**
11 **application security.**
12 Q. Is it correct that you keep the computer
13 security course up to date with the latest
14 developments in computer security?
15 **A. I'm not quite following your question.**
16 **I'm sorry.**
17 Q. Do you make changes every year to your
18 course materials to reflect new trends in computer
19 security?
20 **A. I don't recall the last time I taught this**
21 **class exactly. It's been several years since I've**
22 **taught it. Other people now are teaching that class.**
23 **And I presume that they're teaching more recent**
24 **topics, but I don't know that in detail.**
25 Q. Did you cover social engineering in your

computer security class?

**A. I believe so, because this is one of the topics that is in chapter 1 of my textbook.**

Q. Are you reading the topics from your book?

**A. Yes.**

Q. Do you have -- I would like to ask you without -- don't consult external materials without disclosing it, would that work?

**A. Yes, so I'd like to disclose that I am reading from my textbook to refresh my recollection about the topics that I taught, since I taught from my textbook. And the title, again, is Introduction to Computer Security by Michael T. Goodrich and Roberto Tamassia, published by Pearson with a 2011 copyright. I believe this is available on Amazon, if you'd like to purchase a copy for an exhibit.**

Q. Is it a PDF file?

**A. I do have a PDF, but I don't know if I'm allowed to share that, based on the copyright agreements that I have signed.**

Q. That's okay. Could you please upload in the Zoom just the table of contents, which includes the topics you read from?

**A. I can try to do that.**

Q. Thank you. And, Renee -- Court Reporter,

let's label that as Exhibit 1.

(Exhibit 1 was marked for identification.)

Q. (By Ms. Shi) If you could -- Dr. Goodrich, for that table of contents, if you could also include the cover page and the copyright page, just the initial part, that will be great. Thank you.

**A. All right. Let me see if I can do that. For some reason, I'm not able to submit to the chat window.**

MR. FISHBACK: Dr. Goodrich, if you want to e-mail it to me, I will e-mail it over to Ms. Shi and the court reporter.

THE WITNESS: Okay. This might take a few minutes, but let me prepare that.

MR. FISHBACK: Whatever is easier.

THE WITNESS: Yeah, I can do that right now. It shouldn't take more than two minutes.

(Discussion off the record.)

THE WITNESS: Okay. I've just sent that to Mr. Fishback.

MR. FISHBACK: All right. And I will forward it as soon as I get it.

Q. (By Ms. Shi) So what key concepts of

social engineering do you address in your computer security class?

**A. I talk about generally social engineering as a concept, where, in addition to the topics of security, we now talk about how people can use things that appear to be legitimate, or use subterfuge of other kinds to trick people into doing insecure actions, such as revealing their user name and password, or other credentials, or downloading malicious software without realizing it. These kinds of things.**

Q. Do you cover phishing?

**A. That is my recollection, that we do cover phishing.**

MR. FISHBACK: And for the record, I'm sorry to interrupt, it's phishing, P-H, not F-I-S-H-I-N-G. I just see that in the transcript.

MS. SHI: Thank you for the clarification. Correct. That is what I'm referring as phishing.

Q. (By Ms. Shi) And so, Dr. Goodrich, sorry, I didn't ask you earlier. Is it correct that you don't have your e-mail applications open; is that correct, on your computer?

**A. No, that's incorrect. I would not be able to e-mail the file you just requested if I did not use my e-mail system. You asked me to -- literally, you just asked me to use my e-mail just a minute ago.**

Q. Do you have -- do you communicate, in addition to sending this exhibit to your counsel?

**A. No.**

Q. Do you --

**A. Sorry to interrupt.**

Q. I would like to ask you to close the e-mail applications.

**A. Okay. It is now closed.**

Q. Thank you. And do you have other messaging or communication applications on your computer, other than Zoom, that is open?

**A. No.**

Q. Thank you.

MR. FISHBACK: And, Ms. Shi, I just sent the exhibit over. It might hang up in our e-mail for a second, but it should be on the way.

Q. (By Ms. Shi) Could you confirm, other than Zoom, you don't have other applications running open on your computer?

**A. I also have Adobe Acrobat open, so that**

**you can view the exhibits and documents. I believe I also have the finder application, so that I can find the exhibits on my hard drive. I believe that's it.**

Q. Could you please confirm you don't have Internet browser open?

**A. That is correct.**

Q. And for your PDF browser, can you confirm that you don't have documents other than your '512 declaration open?

**A. I still have my textbook open. Would you like me to close that?**

Q. Yes, please.

**A. Okay, I'm closing my textbook.**

Q. So in addition to phishing, what other types of social engineering tactics did you discuss in your class?

MR. FISHBACK: Objection, form.

THE WITNESS: May I reopen my textbook to answer your question?

Q. (By Ms. Shi) We need to -- is it -- you can open the table of contents that you sent to us, because the portion you relied upon will be -- need to be part of the exhibit.

**A. Right. But now you're asking me about other parts of the textbook. That's what I'm**

**confused about. Maybe the best way to answer is, I include topics that are there in the table of contents. And if you have any other questions about that, I will try my best to remember, but I've been told that a deposition is not a memory test.**

Q. Yes, that would be -- yes, please answer the question without consult the textbook.

**A. Yeah, so just as I sit here today, I already -- I already answered that question. I would answer it the same way I did before.**

Q. Which is --

[Cross-talking.]

THE WITNESS: The same way I did before. Yeah, could you please have the court reporter read my answer back?

MS. SHI: Court Reporter, could you please read Dr. Goodrich's previous response?

(Discussion off the record.)

Q. (By Ms. Shi) Dr. Goodrich, were you referring to your response to my question that --

MR. FISHBACK: Objection -- sorry.

Q. (By Ms. Shi) Let me start with your previous response. And, Dr. Goodrich, please tell me if this is the answer you're referring to. You said, "right, but now you're asking me about other parts of

the textbook." Is that part of your answer that you were referring to?

**A. No. What I was referring to is you had asked me about what topics -- as I recall, you had asked me about what topics of social engineering I had taught. And I had mentioned that, generally, the concept of social engineering is to use social cues and contexts to trick people into revealing confidential or sensitive information.**

**Examples include phishing, P-H-I-S-H, other kinds of disguises to trick people into thinking, for example, that websites are legitimate. And then have them reveal confidential information or download malware as a result of them being tricked.**

**The crucial aspect of social engineering is that it circumvents cryptographic or computer security techniques by tricking somebody into doing something that is insecure, rather than actually breaking a cryptographic system or computer security software.**

Q. Do computer systems -- scratch that.

How do you discuss in your class how to recognize and defend against social engineering attacks?

MR. FISHBACK: Objection, form.

THE WITNESS: I don't recall the details, but my recollection is to tell the students to do their best to verify that websites are legitimate, the e-mail attachments are legitimate, to not click on things unless they know the sender, and verify that the sender is legitimate.

These are all general principles that can be applied, but even then -- as the computer security researchers often acknowledge, even then, there may be ways to trick people using social engineering techniques, even when they're trying to be diligent.

Q. (By Ms. Shi) So in addition to this human awareness prevention, do you also teach students technical solutions to defend against social engineering?

MR. FISHBACK: Objection, form.

THE WITNESS: I don't recall, just sitting here today.

Q. (By Ms. Shi) Are you aware of technical solutions for defending against social engineering?

**A. So in my declarations, I discuss a prior art reference known as Kesanupalli, that includes a technical solution to protect against social**

**engineering.**

Q. Which parts -- is any specific technologies described there, that is used to defend social engineering?

MR. FISHBACK: Objection, form.

MS. SHI: Yeah, let me rephrase my question.

Q. (By Ms. Shi) What specific technologies are described in Kesanupalli that are used to defend social engineering?

**A. So I speak to this in my report, or my declaration, rather, with example for the '512 and the '138 patents, in several paragraphs -- let me just try to list some of them.**

**Yeah, so, for example, in my declaration for the '512 patent, this discussion begins in paragraph 33, goes through paragraph 34. Then it picks up again in paragraph 45, goes through paragraph 60. That's at least inclusive of those discussions. I can read them, if you'd like.**

Q. So, yeah, let's go to paragraph 33 of your declaration for '512. Can you read the first sentence?

**A. What paragraph again?**

Q. 33?

**A. Yes. "Kesanupalli states that passwords are typically used to authenticate user identity in authentication systems and procedures."**

Q. So is it right that passwords is one technique to defend against social engineering?

MR. FISHBACK: Objection, form.

THE WITNESS: That depends on the context.

Q. (By Ms. Shi) Could you please explain how it depends on the context?

**A. Passwords are used in a wide variety of applications, so it depends on the context whether or not they're also being used in the context to defend against social engineering.**

Q. Could you please give one --

**A. In the case of Kesanupalli, Kesanupalli is advocating for longer passwords, as I explained in paragraph 33 of my declaration.**

Q. Is it correct that longer passwords is a technique for defend against social engineering?

**A. Again, that also depends on the context. Generally speaking, longer passwords are considered more secure than shorter passwords. And then in Kesanupalli, there's a system that is taught that shows how you can use longer passwords to defend against social engineering attacks.**

Q. Could you explain how Kesanupalli uses longer password to defend against social engineering attacks?

**A. Sure. At a high level, Kesanupalli is about educating users to use longer passwords, but recognizes that the use of longer passwords is difficult, because they're hard to remember.**

**So it discloses a system where there's a fingerprint sensor that is used to help unlock the longer passwords that go with the user ID, so people can log in to a website more securely.**

**And most importantly, Kesanupalli teaches a binding between the credentials for a website and the website itself. And this also protects against social engineering attacks, because it prevents someone revealing their credentials to another website that might look like a legitimate one, but really is not.**

Q. Is it correct that a longer password is a technique that can be used to improve computer security, other than from social engineering attacks?

**A. So if your question is, do longer passwords generally give higher levels of security, that is correct. Because as I also talk about, as I recall, in my declaration, there are what are known**

**as dictionary attacks that can be used to break security when people use very short passwords, because those passwords may appear in a password dictionary.**

Q. So does dictionary attacks trick people as social engineering did?

**A. No, not usually. Sometimes maybe, but typically not. A dictionary attack is what can be used against weak passwords, hence the advocating for longer passwords in Kesanupalli. And then that's built into its system for preventing social engineering attacks.**

Q. Are you aware of any other techniques that can be used to defend against social engineering?

**A. There may be others, but not immediately coming to mind right now, but, yeah, there's probably others.**

Q. What are the techniques described in the '51 [sic] patent that is used to defend against social engineering?

**A. When you ask about the '512 patent, are you asking about its claims or its specification?**

Q. Both.

**A. So one of the techniques that the '512 patent describes to help guard against all attacks,**

**including social engineering, is it teaches against password reuse and/or the selection of poor quality passwords, which render their credentials less secure against attacks.**

**This is, for example, from the background section of the '512 patent, in column 1, beginning at line 35, and going to line 44.**

Q. Is it correct that the technique you just described in '512 of against -- teaching against password reuse or selection of poor quality passwords are not limited to defend against social engineering attacks?

**A. I agree.**

Q. Any other techniques in the '512 patent that are described to guard against social engineering attacks?

**A. If by your question, you're asking specifically for just social engineering attacks, nothing else is immediately coming to mind. But of course, the claims of the '512 patent would be recognized by a person of ordinary skill in the art as providing improved computer security, generally.**

Q. And would the claims of '512 be recognized by a person of ordinary skill in the art as providing improved computer security specific for social

engineering attacks?

**A. I don't recall that being a question I was asked to opine on. I would want to spend more time to be able to answer that question.**

MS. SHI: Okay. We're close to one hour in the deposition. Can we take a ten-minute break?

MR. FISHBACK: Fine here.

THE WITNESS: Yeah, that's fine with me.

MS. SHI: Thank you.

(A recess was taken.)

Q. (By Ms. Shi) So we were talking about the '51 [sic] patent. Can you please -- do you have the '51 -- '512 patent in front of you?

**A. I do.**

Q. Can you go to figure 1, please?

**A. I am there.**

Q. So could you please describe figure 1?

**A. Sure. So figure 1 is an illustration of an embodiment of an environment in which the authentication translation system disclosed in the '512 patent is provided.**

Q. So where is the authentication translator module is -- in which device is the authenticator translator module is in?

MR. FISHBACK: Objection, form.

THE WITNESS: So if we go to the '512 patent, in column 3, and beginning at line 2, it explains that "also, as will be described in more detail below, authentication translators can be located in a variety of places within an environment. For example, notebook computer 102 includes an authentication translator module 132 that provides authentication translation services. Other devices 104 to 108 can also include, but need not include, their own respective authentication translator modules."

Q. (By Ms. Shi) So is it right that the device 102 communicates -- can communicate with all the other devices on figure 1, including social networking site 120, bank website 122, online camera retailer 124, cloud storage service 140, third-party authentication translator 136; is that correct?

**A. So if we go column 2 in the '512 patent, beginning at line 37, it says, "figure 1 illustrates an embodiment of an environment in which authentication translation is provided. In the examples shown, a variety of client devices 102 to 108 connect via one or more networks represented as a single network cloud 110 to a variety of services 120**

**to 124, also referred to herein as sites 120 to 124."**

**So those are at least inclusive of the other sites that can be communicated with through that network.**

Q. So you discussed 120 to 124. What about 140 cloud storage service, how does the device 102 communicate with cloud storage service 140?

**A. So if we go to column 7, beginning at line 60, it states, "Alice's laptop 102 and phone 104 could both communicate with cloud storage service 140, which would keep their authentication information synchronized."**

Q. So what's the use of cloud storage service 140 here?

**A. In this case, it's talking about keeping their authentication information synchronized. And then it goes on, at line 62, "refreshes can also be made in accordance with user configuration restrictions. For example, Alice's employer could prevent privileged employer data from being stored on shared personal devices or on any device that was not issued by the employer."**

Q. Okay. So in this case, is it correct that the privileged employer data is stored on cloud storage service 140?

MR. FISHBACK: Objection, form.

THE WITNESS: That is not being disclosed here. It may be a possible embodiment, but that's not what's being disclosed.

Instead, what it's saying is that Alice's employer could prevent privileged employer data from being stored on the shared personal devices or any device that was not issued by the employer.

Q. (By Ms. Shi) Can you read the first sentence of this paragraph, starting with "in various embodiments"?

**A. Yes, it says -- beginning in line 56 of column 7, "in various embodiments, cloud storage service 140 is configured to accept backups from multiple devices associated with a single account, and synchronize the updates, so that all devices get automatically refreshed."**

Q. What does "accept backups" mean here?

**A. A person of ordinary skill in the art would understand that to mean just what it says, that you could accept backup of data that, say, is stored on Alice's laptop 102, and then could be backed up to this cloud storage service 140.**

Q. Is it right that the backup is sent from

Alice laptop 102 through the Internet, and then accepted by the cloud storage service 140?

**A. It depends what you mean by sent, because claim 1 speaks of there being a first processor and a second processor. So if now you're asking about claim language, you have to be a little more careful.**

**Also, I don't see any language here at least in this thing about the acceptance or rejection of a backup. So I'm not -- I'm not seeing that here. It may be somewhere else, if you -- if you would be willing to point me to another section in the patent, I'd be happy to review that.**

Q. In the sentence you just read, it says, "cloud storage service 140 is configured to accept backups"?

**A. Right. But the way you asked the question suggested that it could also reject them, so that was the part I was responding to.**

Q. So you don't disagree that cloud storage service 140 can accept backups from multiple devices through Internet; is that right?

MR. FISHBACK: Objection, form.

THE WITNESS: There are multiple embodiments. If now you're asking about other embodiments that may not be in claim 1, I would

not dispute that there may be other embodiments, besides what is in claim 1.

Q. (By Ms. Shi) So let's read this sentence again. I'm not asking this question related to claim 1. Just to clarify, I'm focused on this sentence you read that's from column 7, line 56. Could you please read that first sentence?

**A. Sure. Again, it says, beginning at line 56, "in various embodiments, cloud storage device 140 is configured to accept backups from multiple devices associated with a single account, and synchronize the updates, so that all devices get automatically refreshed."**

Q. Can this sentence -- what's described in the sentence implemented in figure 1?

MR. FISHBACK: Objection, form.

THE WITNESS: So, again, figure 1 is not a flowchart, like steps or even a data flow diagram that would show the flow of data which are in this patent.

So, for example, figure 6, figure 7 are data flow diagrams. And then figure 5 is a flowchart showing logical flow. Instead, figure 1 would be understood by a person of ordinary skill in the art to be an illustration

of an architecture that shows the potential connections that could exist in a system, and is meant to illustrate how, for example, a laptop could be connecting to a bank.

Q. (By Ms. Shi) You mentioned claim 1 recites a first processor and a second processor; is that right?

**A. Yes, that is correct.**

Q. Does the architecture of figure 1 include a first processor and a second processor as recited in claim 1?

MR. FISHBACK: Objection, form.

THE WITNESS: So figure 1 is just an illustration of the devices and the websites and cloud components. Instead, if you want to see an architecture diagram that shows a first processor and a second processor, an example would be figure 3.

Q. (By Ms. Shi) What is figure 3?

**A. So figure 3 is an illustration of an embodiment of a device which secures storage. And it shows both a first processor and a second processor. The first processor is numbered 304, the second processor is number 308.**

Q. Can the embodiment of the device

illustrated in figure 3 implemented in device 102 of figure 1?

**A. A person of ordinary skill in the art would understand that that could be done. That would be possible.**

Q. So is there communication between the processors 304 and 308 in figure 3?

**A. If you're asking about the preferred embodiment of how -- what figure 3 is illustrating, that's discussed, for example, beginning in column 3, starting at line 66, and then continuing into column 4. And one of the disclosures begins at line 5. It says, "however, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API."**

Q. Is it correct that the dedicated processor sensor is 308?

**A. Yes, because if we look just to the part before that, it says, beginning at line 66 of column 3, "one example of a device with secure storage is illustrated in figure 3. In the example shown, a mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to**

**a dedicated processor 308 and a sensor 310, e.g., a camera or fingerprint reader."**

Q. So can a processor 304 communicate directly to the Internet?

MR. FISHBACK: Objection, form.

THE WITNESS: If by communicate directly with the Internet, you mean can that processor be used by a user to access an external resource across the Internet and establish a secure connection with that external source, the answer is yes.

Q. (By Ms. Shi) Can the user do the same with the processor 308?

**A. No. As I read earlier, at line 5 of column 4, it states, "however, users cannot access the secure storage area, and the processor can only communicate with the dedicated processor/sensor via restricted API."**

**And then, of course, that -- it goes on in this passage to talk about how the secure processor can communicate with other entities, but then that is not the user doing that anymore. It's now the secure processor doing it in response to perhaps a communication through the restricted API.**

Q. So the processor 308 can communicate with

other entities, but it needs to go through the restricted API; is that right?

MR. FISHBACK: Objection, form.

THE WITNESS: Not exactly, no. Instead, what is being taught here is that the secure processor -- that the user and the fast processor 304 have restrictions in how they interact with the secure processor. Namely, they must use this restricted API.

But then in this passage in column 4, which then supports the claim language, say, for claim 1, it's disclosing how the secure processor can communicate, for example, with a backup storage service 140 to do a backup.

Q. (By Ms. Shi) So in your class on computer security, how do you define security?

**A. Yeah, so if we go to the table of contents for the book that we now are sharing, and I'm presuming will become an exhibit for this deposition, if we go to the introduction, we see where we discuss -- this is not the text, but this is now the table of contents.**

**We discuss security principles, fundamental concepts. So the concept of computer security is wrapped up into a number of other**

**sub-concepts. The first three go by the initials CIA, which stands for confidentiality, integrity, and availability. And each of those concepts are concepts of computer security.**

**And then we also, in our book, introduce three additional ones, which go by AAA, which deal with assurance, authenticity, and anonymity. So those concepts also relate to computer security. And these are all things that I teach when I teach my course on computer security as being security concept.**

Q. So is it correct that the security of a system has the goals of integrity, confidentiality, and availability?

MR. FISHBACK: Objection, form.

THE WITNESS: Those are three subcomponents of what it can mean to be security. So some systems may provide one or more of those as its goals.

Q. (By Ms. Shi) Can a system have all three of them, integrity, confidentiality, and availability, as its goals?

**A. Yes, that is possible, as well as the other goals we discussed as well, assurance, authenticity, and anonymity.**

Q. What is confidentiality?

**A. Confidentiality is the concept that some data is kept and stored and transmitted in a way that it is kept confidential, so that only people who have the access rights to that data may see it.**

**And those access rights may be embodied, for example, in some type of a secret key, which is a number or password that can unlock the data through some cryptographic means, for example.**

Q. Other than the secret key you mentioned, are there additional tools for implementing confidentiality?

**A. Yes, there's another tool known as public key cryptography. In this case, rather than just having a shared secret key between the two parties, an entity, such as -- we'll call it Bob has a private key that only he knows, and a public key that he publishes widely to everyone.**

**And then if another party, who we'll call Alice, wishes is to send a confidential message to Bob, she can encrypt it using his public key, which is known to everybody. But then after she sends it, or even during transit, anyone else who looks at that -- what we call a cipher text will not be able to determine its value, its true identity.**

**But then once Bob gets it, he can use his private key to decrypt that data, so that he can read it.**

Q. Is authentication also a tool for confidentiality?

MR. FISHBACK: Objection, form.

THE WITNESS: Authentication can be used in conjunction with confidentiality, but it, just by itself, is not a tool for confidentiality. It's instead a tool for authenticating that somebody is who they say they are.

There may be confidential components to any protocol that you do to achieve authenticity, but the concept itself is simply that. Determine that somebody or something is what they say they are. That's authentication.

Q. (By Ms. Shi) Any other tools for confidentiality?

**A. Another tool that can be used for confidentiality is cryptographic hash functions, where you take data, and you run it through this hash function that then produces an output that we referred to as being one way.**

**And what that means is that the output of**

that function is hard to invert. It's easy to compute in one direction, but it's hard to invert. Namely, that if you're given the output from a cryptographic hash function, it's computationally difficult to reverse that and find an input value that would have that output.

Q. Any other tools for confidentiality?

A. There may be others. They're not immediately coming to mind, as I sit here today.

Q. What is integrity?

A. Integrity has to do with the property that the data is unchanged from when it was created. That it's true, has not been altered. So this is different than confidential information. This is information that could be shared with others, but you want to make sure that it has not been altered, say, by some hacker who would be introducing a virus into some software, for example. You'd like to make sure that the software has integrity, that it is as it was originally released, for example.

Q. What are tools for integrity?

A. So example tools in use today for integrity include digital signatures. So the idea there is that perhaps using this public key, private key mechanism we talked about earlier, that an

1 **entity, which we'll call Bob, will digitally sign,**
2 **say, software data. And then send that software**
3 **together with a digital signature to someone like**
4 **Alice. And then she can verify that that message was**
5 **the same that Bob signed by doing a signature**
6 **verification on that.**
7 Q. Are there other tools for integrity?
8 **A. Yes.**
9 Q. What are they?
10 **A. Another tool is something called an HMAC,**
11 **or we pronounce it as HMAC. This is now in a**
12 **scenario where two individuals, for example, Alice**
13 **and Bob, may share a secret key. In this case, what**
14 **you can do is, you can take that original message,**
15 **run it through a cryptographic hash function, where**
16 **you concatenate the message with a secret key, and**
17 **provide that as input to the cryptographic hash**
18 **function.**
19 **And then send the message together with**
20 **this HMAC to the other party, who also knows that**
21 **secret key. So then they can take the message that**
22 **was sent, concatenate the secret key, compute the**
23 **one-way hash function on that, and then compare that**
24 **to the hash value that was also sent. If they match,**
25 **then this is evidence of integrity.**

Q. Any other tools for integrity?

**A. Those are two that are immediately coming to mind. There may be others that I'm just not recalling, as I sit here today.**

Q. What is availability?

**A. So availability is the property that data or a system is available, that people who want to, say, connect to a website and download the web page are able to do that.**

Q. What are some tools for availability?

**A. So tools for availability include redundancy, where you would take a website or web server, and rather than just having one web server, you'd have multiple copies of that web server. So that if one of them goes down, then the other can take over the functionality of that web server. And that general web page would still be available.**

Q. Are there any other tools for availability?

**A. Another tool for availability is the prevention of denial of service attacks. So somebody who is trying to attack a system by overloading it with requests is trying to attack its availability. So tools that, then, would be preventing denial of service attacks would be tools that benefit**

**availability.**

Q. So defending against social engineering attacks helps with which of these goals?

MR. FISHBACK: Objection, form.

THE WITNESS: It helps with at least confidentiality and integrity.

Q. (By Ms. Shi) So Exhibit 1 to this deposition, which is the table of contents of the book, your book, Introduction to Security [sic], chapter 2 says, "physical security." What is physical security?

**A. Physical security is the actual physical protection of computing devices. So, for example, keeping them in locked rooms and in data centers that have physical access controls, so that only authorized people can go into the room.**

Q. Why is physical security important for achieving the security goals?

**A. Because oftentimes, if someone can get access physically to computers, they can disassemble them, which affects availability. They can turn them off, which affects availability. They could potentially even open them up and put in probes. They could compromise confidentiality or they could introduce new data and change things that would**

1 **compromise integrity.**
2 Q. Does physical security help to defend
3 against social engineering?
4 **A. We have a section in this chapter on human**
5 **factors and social engineering, but it was actually**
6 **addressing the opposite question, how can you build**
7 **physical security systems that prevent against social**
8 **engineering, such as somebody being tricked into**
9 **giving their key card to an attacker, and then the**
10 **attacker uses their key card to gain access to a data**
11 **center.**
12 Q. So physical security can be used to defend
13 against a variety of attacks, including social
14 engineering attacks; is that right?
15 **A. I don't -- again, I wouldn't put it that**
16 **way per se. I think the way to say it is, you would**
17 **like to have physical security means that are**
18 **difficult to thwart through social engineering**
19 **attacks.**
20 **So, for example, in this example of having**
21 **a key card, you could have on the key card, a**
22 **physical picture of the person. So that if they**
23 **handed that to a third-party through coercion or**
24 **whatever social engineering was used, that then when**
25 **that third-party shows their key card to the reader**

1 **and their face doesn't match, or a guard can see the**
2 **picture doesn't match, then they will be caught.**
3 MR. FISHBACK: And I'm sorry to interrupt.
4 Is anyone else having connection issues or any
5 lagging?
6 (Discussion off the record.)
7 Q. (By Ms. Shi) You mentioned that it is
8 desirable to have physical security means that are
9 difficult to thwart through social engineering
10 attacks, do you recall?
11 **A. I don't think I said thought through.**
12 Q. What did you say?
13 **A. I thought difficult to attack, something**
14 **along those lines. I think I said thwart, actually.**
15 Q. Are there needs for physical security
16 means that are difficult to --
17 (Discussion off the record.)
18 Q. (By Ms. Shi) Are there physical security
19 means that would be desirable to break through, other
20 than social engineering attacks?
21 **A. When you say break through is desirable,**
22 **you're now taking the perspective of an attacker; is**
23 **that correct.**
24 Q. Let me rephrase. Are there physical
25 security means that would be desirable that is

difficult to break through?

MR. FISHBACK: Objection, form.

Q. (By Ms. Shi) Other than social engineering attacks?

MR. FISHBACK: Same objection.

THE WITNESS: Yes, so we also talk about locks and safes in this chapter, so we talk about how to build locks that are difficult for someone to pick them. That is to be able to unlock the device or the safe without knowing the combination or having a physical key for it.

All of this, of course, is not things I discussed in my declaration. I was not asked to opine on these things.

Q. (By Ms. Shi) What is operating system security?

**A. So an operating system on a computer is the software that manages things like the processes, the memory, the file system, connected devices. And it's generally desirable that the operating system itself also be secure, that someone can't introduce malicious software into the operating system, for example.**

Q. What are tools for operating system security?

1 A. So some example tools to achieve operating
2 system security is to have what is known as access
3 control restrictions, so that the software of the
4 operating system itself can only be modified by
5 system administrators, for example. That's one tool.
6 Other tools are that you build the
7 operating system itself to be robust against attacks
8 that could be trying to break those restrictions or
9 other restrictions that the operating system is
10 trying to enforce.
11 Q. In the table of contents, 3.2, you
12 discussed process security. What is process
13 security?
14 A. So in a computer system, running threads
15 of computer software are known as processes in the
16 context of an operating system. And so what you'd
17 like to do is to protect the processes that are
18 running in an operating system.
19 So, for example, each process will
20 typically have a memory space that is associated with
21 it. And it's desirable, generally, that the memory
22 for one process is not accessible to another process
23 unless that first process gives explicit rights for
24 the other process to access that memory.
25 So, for example, you'd want to have

1 **protections in place to prevent this leakage from one**
2 **process's memory to another process's memory.**
3 Q. Is operating system security used to
4 defend against social engineering attacks?
5 **A. No examples are coming immediately to**
6 **mind, as I'm sitting here today, but that doesn't**
7 **mean that they don't exist. I'm just not having any**
8 **that come up. Again, this whole line of questioning**
9 **is something that is completely outside the scope of**
10 **my declaration.**
11 Q. Section 3.3 is about memory and file
12 system security. Do you see that?
13 **A. Yes.**
14 Q. What is memory in a file system security?
15 **A. So this gets to the issue that, for**
16 **example, certain files oftentimes are sensitive, and**
17 **you would like to restrict who has access to the**
18 **contents of those files. And so what you can do is**
19 **to provide through the operating system, mechanisms**
20 **that protect the contents of files, and only allow**
21 **those who are authorized to see them or to modify**
22 **them to do so.**
23 Q. What is virtual memory security?
24 MR. FISHBACK: Objection, form, scope.
25 THE WITNESS: So, again, we're going far

afield now from my declaration, but in computer science, we oftentimes will give the impression that each process has access to the entire address space of a memory, when, in fact, multiple processes are sharing that memory.

To achieve this abstraction for the processes, we use a technique called virtual memory. What this refers to is that the memory space of the process is divided into chunks, we often refer to as pages or segments.

And each page is then brought into the actual memory of the computer when that process needs it. But it may be swapped out, say, to an external drive when the process does not need it. And we refer to this technology as virtual memory.

Q. (By Ms. Shi) What is the virtual memory security techniques used to prevent -- let me rephrase.

What kind of attacks are the virtual memory security tools used to defend against?

**A. So --**

MR. FISHBACK: Same objections.

THE WITNESS: So this, again, is dealing with the issues of protection against someone

trying to access data that they are not authorized to see.

So what you want to do is both protect the memory when it's inside the computer in the main memory, but also when it's been swapped out to the external drive. And so this virtual memory security techniques would be used to protect the address space of a process, both when it's being used inside the internal memory of a computer, as well as when it has been swapped out to the external memory.

This is like office hours. This is so much fun. Thank you for all these wonderful questions, of course, that are completely outside the scope of my declaration for this matter.

Q. (By Ms. Shi) So in section 3.4, you listed a few attacks. 3.4.2 says, "simple buffer overflow attacks." What kind of attacks are you discussing here?

**A. So this is referring to an attack known as a buffer overflow attack. So a buffer in an operating system is a piece of memory that's allocated for, say, inputs, outputs, communications between two entities, could even be a buffer that's**

1 **used for a website, for text that's being input into**
2 **a graphical user interface, that then is processed by**
3 **the operating system.**
4 **And what can happen, though, is that an**
5 **attacker can give an input into the buffer that is**
6 **bigger than the size of the buffer itself. And this**
7 **is known as a buffer overflow attack. And then what**
8 **the attacker can do is by giving it input that's so**
9 **large, that then the computer that is not defending**
10 **against a buffer overflow attack will do is it just**
11 **accepts that, and overwrites memory.**
12 **But then continues overwriting memory**
13 **beyond the space of the buffer, which then can damage**
14 **other memory. And it gets to that issue of damaging**
15 **memory that you want to otherwise protect.**
16 Q. So are these attacks -- scratch that.
17 So the next chapter is malware, and
18 section 4.1 is about insider attacks. Were the
19 attacks we just described in section 3 outsider
20 attacks?
21 **A. Not necessarily.**
22 Q. So section 3 and 4 can overlap; is that
23 right?
24 **A. Yes.**
25 Q. So why is insider attacks an issue that

computer security need to deal with?

**A. Because to achieve computer security goals, it's oftentimes useful to limit the access rights of users, and to have roles assigned to the user, such as system administrator, accountant, manager, these kinds of roles in an enterprise.**

**And you want to oftentimes restrict the access, or the types of things each person and these different roles can achieve. But if you have an insider inside your company, let's say, who is actively trying to thwart the security and break it, and introduce issues that are bad, this is something that you should defend against.**

**And this is especially true for the programmers who are programming the software for an enterprise. Those are the ultimate insiders. And so you want to put in place procedures for software development that help reduce the possibility that a programmer could introduce malicious software while they're writing their programs. And that has to do with insider attacks.**

Q. And the malware attacks can come from insider or outsider; is that right?

**A. That is correct. This section is about insiders.**

Q. Section 1.4 is about insiders; is that right?

**A. Section 4.1 is about insiders.**

Q. Thank you. And is it desirable to have security against malware against both insider attacks and outsider attacks?

MR. FISHBACK: Objection, form.

THE WITNESS: I would generally agree with that, depending on the system.

MR. FISHBACK: Ms. Shi, we've been going for about an hour. When you get a good chance, could we take a break?

MS. SHI: Yeah, let's take a ten-minute break.

MR. FISHBACK: Awesome. Thank you.

MS. SHI: Thank you. Let's go off record.

(A recess was taken.)

Q. (By Ms. Shi) So before the break, we were talking about chapter 4, malware; is that right?

**A. Yes, I recall that.**

Q. What is a worm?

**A. So a computer worm is software that can spread itself without intervention from any human. So it can spread itself from computer to computer, and infect the computers, and doesn't need a user to**

1 **click on an e-mail. Those kind of things.**
2 Q. So what does a computer worm usually will
3 do?
4 **A. It will try to infect multiple computers**
5 **to then potentially set them up as what we call bots,**
6 **B-O-T-S, where then they can be used for themselves**
7 **to then attack other computers, perhaps do a denial**
8 **of service attack on a website.**
9 Q. What are the tools to -- against worms?
10 MR. FISHBACK: Objection to form, scope.
11 THE WITNESS: Example tools to protect
12 against computer worms are to have improved and
13 robust authenticity and authorization. So, for
14 example, if somebody is logging in to your
15 computer, you want to make sure that they're
16 logging in with correct and valid credentials.
17 And this would then prevent, say, a worm coming
18 in to attack with what would presumably be
19 invalid credentials.
20 Q. (By Ms. Shi) Can signature -- digital
21 signature used to fight against malware?
22 **A. Yes.**
23 Q. How would it work?
24 **A. So, for example, another type of malware**
25 **is something called a computer virus, which is**

1 **malicious software that injects itself into other**
2 **software. And then is sent, say, through e-mails or**
3 **other means, where people would click on something**
4 **and then install it, not knowing that it has this**
5 **virus inside of it.**
6 **But what you can do to protect against**
7 **that is that a software designer, such as Microsoft,**
8 **could digitally sign their software. In fact, they**
9 **do today digitally sign all their software, so that**
10 **when you install your software from, say, Microsoft,**
11 **before you do the installation, you first check that**
12 **the software has a valid digital signature. And if**
13 **it does, then that's evidence that it has not been**
14 **tampered with. Hence, it is unlikely to have a**
15 **computer virus.**
16 Q. So I've -- personally, I've used some
17 antivirus software. Is that a technique pretty
18 commonly used on my device to protect against
19 malware?
20 MR. FISHBACK: Objection, form, scope.
21 THE WITNESS: I don't know how common it
22 is. And, again, we're talking about things
23 today, not in the scope of the patents, but the
24 idea of much of the computer virus software of
25 today, it is doing something called signature

checking, which is a -- I have to apologize for my colleagues -- a different type of a signature than a digital signature that's used to sign and protect software, so you know it's from a good source.

Here, what we're referring to, in using this word "signature," to be a pattern, that certain viruses tend to have a certain pattern in the actual binary bits of the software. And so we look for a certain pattern of zeros and ones here, a certain pattern of things over there.

And that pattern of software that tends to go with certain computer viruses, we call that a signature. But it's a different signature than the digital signature we were talking about earlier today.

Q. (By Ms. Shi) So is it correct that the antivirus software installed on my device is using a specific type of --

(Discussion off the record.)

Q. (By Ms. Shi) So let me ask my question again. How does checking a digital signature of code protect a device?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: So this what we talked about earlier, what I was referring to earlier. Again, there's this digital signature, where a software developer or a company will digitally sign the software that they release, such as Microsoft releasing its software.

So that then, when you install it, you check the digital signature, that this is a way of achieving integrity, that the software that was sent is the same software that you're installing. Hence, it's unlikely to include a computer virus in that software. So that's a technique that's very common today for protecting against computer viruses in distributed software.

Q. (By Ms. Shi) So we discussed encryption before. Can we use encrypted -- can we use encryption to fight against malware?

**A. Yes. So one of the ways that you can do -- you can perform digital signatures is through a type of encryption. We talked earlier about public key encryption, how Bob can have a public key that he shares with everyone. And anyone who wants to encrypt a message for Bob can use that. And then he uses his private key to decrypt that.**

1 **There are some types of public key**
2 **cryptography, where those keys can be reversed. Bob**
3 **can use his private key to encrypt something. And**
4 **then everybody else can use his public key to decrypt**
5 **it. And this could then be a form of a digital**
6 **signature for Bob.**
7 **You can take his software he just wrote,**
8 **encrypt it with his private key. Send both that and**
9 **original unencrypted software to you. And then you**
10 **will then encrypt the software using his public key,**
11 **and see if that matches what he had encrypted with**
12 **his private key, or likewise, you could decrypt his**
13 **encrypted software, and see that it matches the**
14 **software he sent you.**
15 **And this is a form of a digital signature.**
16 **And something akin to this is used today, in fact,**
17 **for digital signatures.**
18 Q. So can I use encryption in my computer to
19 protect my files?
20 MR. FISHBACK: Objection, form, scope.
21 THE WITNESS: Yes, that's something you
22 can use today. There's a number of tools that
23 are available today to encrypt the files on your
24 computer, say, using a password that you know.
25 And then what that would do is anyone who

would then gain access to your computer, who does not know that password or key, they can see the encrypted files on your computer, but they would not be able to either modify them without breaking the encryption, and then it would just be garbage when you tried to decrypt it, or they would not be able to see the unencrypted version of them.

Q. (By Ms. Shi) Are there commercially available tools like that?

**A. Yes, there are today.**

Q. Can you give some examples?

**A. Yes. So, for example, on the Mac, the Apple Company provides a tool where you could have all of your files on your hard drive encrypted, if you'd like. And then there's other third-party software that does similar things.**

**In fact, it was with -- working with law firms that I discovered some of these that are being used today, 'cause oftentimes, law firms will want to protect the software of their clients. And then only send that on a flash drive that is protected using one of these third-party tools.**

Q. I think we discussed access control a while back. Is it correct that providing different

levels of access control is another way to provide protection of the device?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: Generally speaking, today, that's another tool that is being used to protect sensitive data. That if you don't have access rights to the data, then the operating system should have mechanisms in place to prevent you from getting at the data.

Q. (By Ms. Shi) Are you aware of other tools for protecting sensitive data?

**A. We already talked about encryption. Encryption and access controls are probably the most widely used today. I'm not thinking of any other examples, as I sit here today.**

Q. The next chapter, chapter 5 is titled "network security, 1." Do you see that?

**A. Yes.**

Q. Of your book table of contents, Exhibit 1 of this deposition. Why is network security important for computer security?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: So generally speaking, today, computers are connected through networks to oftentimes perform operations, do

communications of various types. Hence, protecting the network that the computers use and that the -- the protocols that occur in the network is also protecting both the computers and their data as well.

Q. (By Ms. Shi) Is it correct that encryption is a technique that can be used to increase network security?

**A. Yes, encryption is used in some cases today for achieving various goals of network security.**

Q. How does that work?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: There's a number of ways that encryption is used. So probably the most common, actually, technically, is something that we discuss in chapter 6 is when you go to a web page nowadays, you typically are going to use a protocol called HTTPS.

And what this does is when you use this protocol, it encrypts the session you have between your computer and the website, so that all the packets that are being sent between them are encrypted, the data in them is encrypted. So if anyone were to eavesdrop on your

communication, say, through your wifi, they would not learn the contents of those packets, the data portion.

Q. (By Ms. Shi) Can the transmission -- the security of the transmission of the data be improved by using multilayer of encryption? For example, I encrypt it first before I send it on to network, and then use the HTTPS protocol to communicate that encrypted data?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: That one is a more slippery slope today, unfortunately. Namely, one of the ways that attackers now are introducing computer viruses on to computers is to be sending them through encrypted sessions, such as with HTTPS.

And so what some systems are doing to protect against that is that they are inside of a processor known as a proxy. They will decrypt the packets, check them for a computer virus, and then re-encrypt them using HTTPS back to send it back to you.

And so encrypting inside of an HTTPS protocol can protect data when you know what you're doing, but it could also potentially be hiding a computer viruses that your proxy might

not catch. That's a problem that exists today.

Q. (By Ms. Shi) So there are techniques using encrypted data for transmission, and there are techniques that communicate using unencrypted data; is that right?

**A. Generally speaking, there's things that can use encrypted data, and there's things that can use unencrypted data, yes. That's a very broad question. And various techniques exist today for that.**

Q. So in the network sections 5 and 6, you have listed many types of attacks. Do you see those?

**A. Yes.**

Q. Are those attacks mainly attacking the content that is communicated -- sorry, scratch that.

Are those attacks -- the attacks described in sections 5 and 6 directed at the cloud portion of a network, instead of attacking the end devices?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: No, I would not characterize it that way. Instead, the way that we wrote these two sections was organized, based on something known as the network stack, which is a set of layers of how networks are designed starting with the hardware at the bottom layer.

And then going up to the applications at the top layer.

And what we talk about in these chapters are attacks that can occur at every layer. Some of those attacks are attacking the protocols themselves, and trying to achieve denial of service. Some of those attacks are trying to hijack a communication. Some of them are about eavesdropping on communications. There's a whole variety of possible attacks that we talk about in these chapters.

Q. (By Ms. Shi) Can you give one example that attacks the end user computer, instead of attacking the Internet devices?

MR. FISHBACK: Objection, form.

THE WITNESS: Sure. So in section 6.4.4, we talk about an attack known as port scanning. This, at first, might seem like it's not even an attack, but it potentially is setting up another attack.

So what this refers to is how an attacking computer can scan the various ports on your computer, to see which of them are accepting connections. And in some cases, if you are accepting connections on certain ports, and you

may even be using old software to accept those connections, then an attacker can then do an intrusion attack on your computer through that port. That's a risk that exists today, for example.

Q. (By Ms. Shi) Is it correct that network security is tied pretty closely with web security taught in section 7?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: Actually, no, as it turns out. I mean, technically, in order to connect to a website, you have to go through the network. But then what we're talking about here in chapter 7 is the security of websites themselves. So the software that's running on the website itself, how do you protect the servers. These kinds of things.

Q. (By Ms. Shi) So web security is really about protecting the devices, while network security is more broadly directed at the network connections; is that correct at all?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: No. Actually, again, the way that we organized these chapters was yet again based on this network stack abstraction.

So chapter 5 and 6 were specifically looking at the different layers of the network stack, the top layer of which is the application layer. And then one of the applications that can exist at that layer is HTTP and HTTPS, which are the protocols that you use for websites.

And so chapter 7 really is just diving in on that, how do you protect websites, how do you protect clients that connect to websites, how do you connect servers from malicious clients.

MS. SHI: Well, thank you. Can we go off record? I think we can take the break now, and go off record.

(A recess was taken.)

Q. (By Ms. Shi) Let's just go over some questions not really related to network technology. So do -- you have reviewed the declaration of Dr. Patrick McDaniel; is that right?

**A. Yes.**

Q. Do you know Mr. McDaniel in person?

**A. I know Dr. McDaniel in person, yes.**

Q. How do you know each other?

**A. We've met at computer security conferences.**

Q. Do you know Jack Hobson, the inventor of

the '512 patent?

**A. Not personally. We may have had interactions in the past, though, on other cases, as I recall.**

Q. For the -- another case, are you talking about the case -- cases we took deposition yesterday?

**A. No, unrelated cases.**

Q. Do you know any of the inventors of the prior art references?

**A. Could you be more specific, please?**

Q. Sure. So Exhibit 1006 is a patent by Kesanupalli. Am I saying it right?

**A. I don't know, because I don't know Kesanupalli. So I would just say it, the way I just said it.**

Q. Okay. And so you don't know the inventor, Kesanupalli?

**A. I'm not personally -- met him, but I am familiar with his work, his achievements, his reputation. I speak to that in my declaration.**

Q. And Exhibit 1007 is a patent by Challener. Do you see that?

**A. Yes.**

Q. Do you know Challener, personally?

**A. I do not know David Challener personally,**

1 **but I also know of his work, his reputation. And I**
2 **speak of that in my declarations.**
3 Q. Exhibit 1008 is by Cheng, C-H-E-N-G. Do
4 you know Mr. or Mrs. Cheng?
5 **A. I don't know David Cheng. That does not**
6 **ring a bell, as I sit here today.**
7 Q. We have cited in the petition, additional
8 supporting references. Any of the author of those
9 supporting references, do you know them, personally?
10 **A. We'd already mentioned Patrick McDaniel.**
11 **I can't remember if he was an author of one of your**
12 **supporting references. And then there's a number of**
13 **other supporting references. I don't recall every**
14 **single one, but for example, there's a supporting**
15 **reference, Exhibit 1009, which is a patent to Brown,**
16 **et al. And I do not know, personally, any of the**
17 **authors of the Brown reference.**
18 Q. So let's talk a little bit about your
19 personal experience with defending against social
20 engineering attacks. Could you please describe any
21 real world social engineering attacks that you have
22 dealt with in your work?
23 **A. Sure. So going now to my CV. Yeah, so**
24 **there's a publication, one of my earliest**
25 **publications in the computer security area, which is**

1 listed in my CV as C-80, which is on a system
2 called -- we called TRICERT, T-R-I-C-E-R-T, all
3 capitals, which is getting at the issue of phishing
4 in e-mails.
5 So one of the ways that social engineering
6 occurs is that someone will send an e-mail to a
7 potential victim, where an attachment in that e-mail
8 is containing a computer virus, let's say. And they
9 try to trick, through whatever message is in the
10 e-mail, you know, we're the IRS or we're your
11 security company or your boss, whatever, click here
12 to find the important thing. And then people click.
13 This is called -- this is one of the ways
14 that phishing occurs. And I talk about that also in
15 my declarations. For example, in the paragraph that
16 talks about phishing attacks through e-mail.
17 And in this paper, we give a technique
18 that would prevent that through a certification
19 process, where only somebody who really is your boss
20 and now is certified to be your boss is sending you
21 this message. So it's something that presumably you
22 can trust as coming from your boss, rather than
23 somebody just pretending to be your boss, and trying
24 to get you to click it.
25 Q. So that's your research paper, right?

1 **A. Yes, dealing with the real world attack of**
2 **phishing through e-mails.**
3 Q. Did you implement your technology in any
4 real world organizations or project?
5 **A. I believe we did implement a prototype.**
6 **The student, D. Medarios, one of the coauthors on**
7 **that paper, my recollection is that he did do an**
8 **implementation prototype.**
9 Q. Have you been involved in the education in
10 organizations or individuals to recognize and respond
11 to these types of attacks by social engineering?
12 **A. Yes. So as we talked about earlier, I**
13 **have written a textbook on Introduction to Computer**
14 **Security. I've taught courses using that textbook**
15 **myself. And then I've been honored that this**
16 **textbook has been used at a number of other**
17 **universities to teach courses of how to protect**
18 **systems and people from all kinds of attacks,**
19 **including social engineering attacks, including**
20 **courses at Berkeley, University -- Brown University,**
21 **Virginia Tech University, and others.**
22 Q. Any involvement other than the textbook?
23 **A. Yes, I've also taught in -- here at UCI,**
24 **we have what we call a professional master's degree,**
25 **that is directed to professionals or future**

1 **professionals in the computing sphere. And I've**
2 **taught my computer security course with similar kinds**
3 **of topics to either existing professionals or future**
4 **professionals in that course.**
5 Q. So is it correct that a lot of your
6 research work is directed at cryptographic
7 technologies?
8 **A. I have a number of papers that either**
9 **directly or indirectly utilize cryptographic**
10 **techniques.**
11 Q. For computer security, could you provide
12 some examples of how crypto concepts can be used?
13 **A. Sure. So the paper we just discussed was**
14 **C-80, TRICERT. That used cryptographic techniques to**
15 **do this certification, what we called certified**
16 **e-mail, where you could be assured that the e-mail**
17 **was from somebody who was trusted.**
18 **Another very influential paper that was a**
19 **part of a big -- over a million dollars grant from**
20 **DARPA is publication C-83. And this is the system**
21 **behind the prototype that we ultimately developed**
22 **through the company I talked about yesterday called**
23 **Algomagic, that was all about certifying the digital**
24 **certificates that are used in -- for example, as a**
25 **part of the HTTPS protocol.**

**So, for example, one of the ways you can protect against phishing attacks is to verify that when you use this HTTPS protocol, that you're going to a website that has a valid digital certificate that's used to encrypt that session.**

**And our system described here first in C-83, and then we did a technology transfer to the company. And, in fact, got an award -- technology transfer award for, was for that technology. That was a cryptographic technique. And I could go on. I mean, there's dozens of other papers I could discuss as well.**

Q. Yeah, I think one thing is -- one technique I read about security is called message authentication codes. Does that -- is that familiar tell you?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: Yes, we talked about them earlier today, if you recall. They're already on the record for today.

Q. (By Ms. Shi) Is it related to digital signature?

**A. In some contexts, it could be thought of as like a poor man's digital signature, because it only works for the purpose of integrity if two**

**parties share a secret key.**

**And so it's not truly -- I mean, it's kind of like -- it has some overlap with, like, a digital signature, but it's not exactly that, because they have to share the secret key in order to both produce the MAC, the HMAC, as well as to verify a message using an HMAC at the other end. They have to have a key in order to achieve it.**

Q. So is it fair to say that the message authentication codes help to achieve the integrity goal for security?

**A. Yes, generally speaking, that's how they are used today.**

Q. So can message authentication codes be used to protect sensitive files that are saved on a computer?

**A. I think that depends on the context, and how they would be used.**

Q. So is it correct that, in some contexts, message authentication codes can be used to protect sensitive files on a computer device?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: It, again, depends what you mean by protect. So if by protect, you mean to achieve some level of integrity that the files

have not been changed, then there may be -- it may be possible, in some cases, to come up with a scheme based on hashed message authentication codes to achieve that.

Q. (By Ms. Shi) And can message authentication codes be used to -- for multiple parties on the network to verify the integrity of a file?

**A. Yes, that's something that could be done using message authentication codes, in some contexts.**

Q. So what are some other techniques that are used for file protection?

**A. We talked about some of them already today. So one we talked about was encryption. Another we talked about was access rights and access control. Another one is memory protections. And another one we also talked about is encryption, if I haven't mentioned that already. There's a number of techniques that are in use today for that purpose.**

Q. What do you mean by memory?

**A. I mean memory for computers, so either the main memory in RAM for a computer or it's external drives.**

Q. Sorry if I missed that, I don't recall we talked about memory protections -- memory protection

1 techniques?
2 **A. Okay. So this is now when I get to**
3 **pretend to be the professor scolding the student**
4 **during office hours, that we did talk about that.**
5 **Namely, we talked about virtual memory protection.**
6 Q. Okay.
7 **A. We talked about file system protection,**
8 **which is another form of memory. We talked about**
9 **process memory protections between multiple**
10 **processors. So we did talk about those as techniques**
11 **in use today that protect memory. Sorry to be the**
12 **scolding professor.**
13 Q. Okay. So is the memory protection
14 different from file system protection?
15 MR. FISHBACK: Objection, form, scope.
16 THE WITNESS: So memory protection is
17 broader, because a file system is a specific
18 organization for memory into a file system. So
19 memory protection is a broader concept, the way
20 that we discussed it today with respect to
21 memory protection.
22 Q. (By Ms. Shi) So is memory protection the
23 same as data protection?
24 MR. FISHBACK: Objection, form, scope.
25 THE WITNESS: No, not the way that -- I

mean, of course, that depends on the context. But data protection is yet another overlapping concept of protecting the contents of data, which could be in memory, so it definitely overlaps.

But now moving it to another memory, you still want to protect that same data. So it's an overlapping concept. It's not identical. It, again, depends on the context, but generally speaking, that would be true.

Q. (By Ms. Shi) So are techniques protecting data different from techniques protecting memory?

**A. They overlap. So some techniques are used for both, and then some might be used for one and not the other.**

Q. So we talked about authentication techniques. Is that a technique that can be used for both data protection and memory protection?

**A. It could be a component in a system that is being used for either or both, depending on the context.**

Q. We also talked about access control. Is access control a technique that can be used to protect both memory and data?

**A. Yes, that's something that also is in use**

**today for potentially protecting either or both.**

Q. We also talked about encryption. Is encryption a technique that can be used to protect both memory and data?

**A. Yes, that's also a technique that I believe is in use today for protecting either or both.**

Q. So what are some techniques that only protect data, but are not applicable to protection of memory?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: So nothing specific is coming to mind, but it could depend, for example, on how you use those other techniques, the specific ways that you're doing the, say, encryption versus how you're using it with memory or for data.

Q. (By Ms. Shi) Are there techniques that only apply to memory protection, but not applicable to data protection?

MR. FISHBACK: Objection, form, scope.

THE WITNESS: Yeah, I would need more time to think about that. Nothing is specifically coming to mind, but there may be some things.

MS. SHI: Okay. I would like to take a

1 break, if that works for you.
2 THE WITNESS: Yeah, now we can take the
3 lunch break, and then be back in an hour.
4 MS. SHI: Okay, that will work. So we
5 will be back here at my 3:20.
6 THE WITNESS: Sounds good.
7 MR. FISHBACK: Ms. Shi, just for my own
8 planning purposes, do you know how long you plan
9 on taking today? And if you don't, that's
10 completely fine, but I'm just trying to plan out
11 something after 5:00 today, so --
12 MS. SHI: Yeah, 5:00 Central, right?
13 MR. FISHBACK: Yeah.
14 MS. SHI: I expect to wrap up definitely
15 before 5:00.
16 MR. FISHBACK: Awesome. Thank you.
17 THE WITNESS: All right. See you guys at
18 3:20 your time.
19 MS. SHI: Thank you.
20 (A luncheon recess was taken.)
21 Q. (By Ms. Shi) So we have taken multiple
22 breaks today. Have you spoken with anyone during
23 those breaks?
24 **A. Not about anything to do with my**
25 **testimony.**

Q. Did you review any documents during the breaks?

**A. Not that I recall.**

Q. Did you communicate with anyone about this deposition today?

**A. No.**

Q. So at the beginning of this deposition, you had your e-mail application open and used that e-mail application to send Exhibit 1; is that right?

**A. Yes.**

Q. After you closed that e-mail application, did you use any other applications, other than PDF and the finder tool?

**A. Not on this computer.**

Q. Did you consult any documents other than Exhibit 1 on your computer today?

**A. I consulted other exhibits that we discussed today on my computer, including exhibit -- not during breaks, but during the time on the record that we discussed. So all the exhibits we discussed on the record, I consulted on my computer.**

Q. Did you consult any other documents on your computer today?

**A. Not that I recall.**

Q. Did you consult any other documents not on

your computer today?

**A. No.**

MS. SHI: I don't have additional questions. I pass the witness.

MR. FISHBACK: Nothing further from me. Thank you, Dr. Goodrich.

(Whereupon, at 4:24 p.m., the deposition concluded.)

1 E R R A T A S H E E T
2 Pursuant to Rule 30(e) of the Federal
3 Rules of Civil Procedure and/or Official Code of
4 Georgia Annotated 9-11-30(e), any changes in form or
5 substance which you desire to make to your deposition
6 testimony shall be entered upon the deposition with a
7 statement of the reasons given for making them.
8 To assist you in making any such
9 corrections, please use the form below. If
10 supplemental or additional pages are necessary,
11 please furnish same and attach them to this errata
12 sheet.
13 * * *
14 I, the undersigned,MICHAEL T. GOODRICH,
15 Ph.D., do hereby certify that I have read the
16 foregoing deposition, and that to the best of my
17 knowledge, said deposition is true and accurate (with
18 the exception of the following corrections listed
19 below).
20 Page____Line____should read:_____
21 Reason for change:_____
22 Page____Line____should read:_____
23 Reason for change:_____
24 Page____Line____should read:_____
25 Reason for change:_____

1 Page____Line____should read:_____
2 Reason for change:_____
3 Page____Line____should read:_____
4 Reason for change:_____
5 Page____Line____should read:_____
6 Reason for change:_____
7 Page____Line____should read:_____
8 Reason for change:_____
9 Page____Line____should read:_____
10 Reason for change:_____
11 Page____Line____should read:_____
12 Reason for change:_____
13 Page____Line____should read:_____
14 Reason for change:_____
15
16
17 _____
Signature
18
19
_____, Notary Public.
20 This, the_____day of_____, 2025.
My Commission Expires:_____.
21
22
23
24
25

1 D I S C L O S U R E

2

STATE OF GEORGIA ) DEPOSITION OF

3

HENRY COUNTY ) MICHAEL T. GOODRICH, PH.D.

4

5

Pursuant to Article 10.B of the Rules and
6 Regulations of the Board of Court Reporting of the Judicial Council of Georgia, I make the following
7 disclosure:

8 I am a Georgia Certified Court Reporter. I am here as a representative of Henderson Legal Services,
9 Inc.

10 Henderson Legal Services, Inc. was contacted by the offices of Haynes and Boone, LLP to provide court
11 reporting services for this deposition. Henderson Legal Services, Inc. will not be taking this
12 deposition under any contract that is prohibited by O.C.G.A. 9-11-28 (c).

13

Henderson Legal Services, Inc. has no contract
14 or agreement to provide court reporting services with any party to the case, or any reporter or reporting
15 agency from whom a referral might have been made to cover the deposition.

16

Henderson Legal Services, Inc. will charge its
17 usual and customary rates to all parties in the case, and a financial discount will not be given to any
18 party in this litigation.

19

20

21

22 F. Renee Finkley, RPR, CRR, CLR

23 Georgia CCR-B-2289

24

25

C E R T I F I C A T E

STATE OF GEORGIA:
COUNTY OF HENRY:

I, F. Renee Finkley, a Certified Court Reporter in and for the State of Georgia, do hereby Certify:

That prior to being examined, the witness named in the foregoing deposition was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth.

That said deposition was taken before me at the time and place set forth and was taken down by me in shorthand and thereafter reduced to computerized transcription under my direction and supervision, and I hereby certify the foregoing deposition is a full, true and correct transcript of my shorthand notes so taken.

I further certify that I am not of kin or counsel to the parties in the case, and I am not in the regular employ of counsel for any of the said parties, nor am I in any way financially interested in the result of said case.

IN WITNESS WHEREOF, I have hereunto subscribed my name this 8th day of January, 2025.

F. Renee Finkley, RPR, CRR, CLR
Georgia CCR-B-2289

A
**AAA** 38:6
**able** 16:10 18:1 28:4 39:24 43:9 47:9 60:4,7
**abstraction** 50:6 66:25
**accept** 31:15 31:19,22 32:14,20 33:10 66:1
**acceptance** 32:8
**accepted** 32:2
**accepting** 65:23,25
**accepts** 52:11
**access** 14:3 35:13 36:8 36:15 39:5,6 44:15,20 45:10 48:2 48:24 49:17 50:3 51:1 53:3,8 60:1 60:24 61:1,7 61:13 75:15 75:15 77:22 77:23
**accessible** 48:22
**account** 31:16 33:11
**accountant** 53:5
**accurate** 4:22 82:17
**achieve** 40:14 48:1 50:6 53:2,9 65:6 74:8,10,25 75:4
**achievements** 68:19
**achieving** 44:18 58:9 62:10
**acknowledge** 22:10
**Acrobat** 18:25
**actions** 17:8
**actively** 53:11
**actual** 44:12 50:12 57:9
**addition** 6:9 12:6 17:4 18:6 19:14 22:14
**additional** 38:6 39:11 69:7 81:3 82:10
**address** 17:1 50:4 51:8
**addressing** 45:6
**administrator** 53:5
**administrato...** 48:5
**Adobe** 18:25
**advanced** 11:23 13:21
**advocating** 24:16 26:9
**afield** 50:1
**agency** 84:15
**ago** 18:4
**agree** 27:13 54:8
**agreement** 84:14
**agreements** 15:20
**akin** 59:16
**al** 69:16
**Algomagic** 72:23
**algorithmics** 12:9
**algorithms** 11:1,7,11,12 11:14,15,16 11:16,17,17 11:18,24,25 11:25 12:1,1 12:8,25 13:4 13:8,11,19
**Alice** 32:1 39:20 42:4 42:12
**Alice's** 30:9,19 31:5,23
**alleged** 7:18 9:16
**allocated** 51:24
**allow** 49:20
**allowed** 15:19
**altered** 41:13 41:16
**Amazon** 15:15
**analysis** 11:16
**and/or** 27:2 82:3
**Annotated** 82:4
**anonymity** 38:7,25
**answer** 4:16 4:18 5:11 19:19 20:1,6 20:10,15,24 21:1 28:4 36:10
**answered** 20:9
**anticipate** 5:3
**anticipation** 9:22
**antivirus** 56:17 57:19
**anymore** 36:22
**API** 35:16 36:18,24 37:2,9
**apologize** 57:1
**APPEAL** 1:3
**appear** 17:6 26:3
**APPEARAN...** 2:1
**Apple** 1:6 4:8 60:14
**applicable** 78:9,19
**application** 14:11 19:2 67:3 80:8,9 80:11
**applications** 11:15 14:8 17:24 18:11 18:14,23 24:11 65:1 67:4 80:12
**applied** 22:9
**applies** 5:20
**apply** 5:23 78:19
**architecture** 34:1,9,16
**area** 35:14 36:16 69:25
**arguments** 6:24 7:1,15
**art** 7:17,18 8:9 9:16 22:24 27:21,24 31:20 33:25 35:3 68:9
**Article** 84:5
**asked** 5:11 18:3,4 21:4,5 28:3 32:16 47:13
**asking** 19:24 20:25 26:22 27:17 32:5 32:24 33:4 35:8
**aspect** 21:15
**assigned** 53:4
**assist** 82:8
**associated** 31:16 33:11 48:20
**assurance** 38:7,24
**assured** 72:16
**attach** 82:11
**attached** 35:24 35:25
**attachment** 70:7
**attachments** 22:4
**attack** 26:8 43:22,23 46:13 51:21 51:22 52:7 52:10 55:7,8 55:18 65:17 65:19,20 66:3 71:1
**attacker** 45:9 45:10 46:22 52:5,8 66:2
**attackers** 63:13
**attacking** 64:14,18 65:5,14,21
**attacks** 21:24 24:25 25:3 25:15,21 26:1,5,12,25 27:4,12,16 27:18 28:1 43:21,25

44:3 45:13 45:14,19 46:10,20 47:4 48:7 49:4 50:20 51:18,19,19 52:16,18,19 52:20,25 53:21,22 54:5,6 64:12 64:14,16,16 65:4,5,7,10 65:13 69:20 69:21 70:16 71:11,18,19 73:2
**Austin** 2:11,20
**authenticate** 24:2
**authenticating** 40:11
**authentication** 24:3 28:21 28:23 29:5,8 29:9,12,18 29:22 30:11 30:16 40:4,7 40:17 73:15 74:10,14,20 75:3,6,10 77:16
**authenticator** 28:24
**authenticity** 38:7,25 40:15 55:13
**author** 69:8,11
**authorization** 55:13
**authorized** 44:16 49:21 51:2
**authors** 69:17
**automatically** 31:18 33:12
**availability** 38:3,14,22 43:5,6,10,11 43:19,20,23 44:1,21,22
**available** 15:15 43:7 43:17 59:23 60:10
**award** 73:8,9
**aware** 9:17 22:21 26:13 61:10
**awareness** 22:15
**Awesome** 54:15 79:16

**B**

**B-O-T-S** 55:6
**back** 20:15 60:25 63:20 63:21 79:3,5
**backed** 31:23
**background** 27:5
**backup** 31:22 31:25 32:9 37:14,14
**backups** 31:15 31:19 32:15 32:20 33:10
**bad** 53:12
**bank** 29:16 34:4
**based** 15:19 64:22 66:25 75:3
**began** 12:14 12:19
**beginning** 11:3 27:6 29:3,20 30:8 31:13 33:8 35:10,20 80:7
**begins** 23:16 35:12
**behalf** 2:3,16 4:8
**believe** 7:7 11:8 15:2,15 19:1,3 71:5 78:6
**bell** 69:6
**benefit** 43:25
**Berkeley** 71:20
**best** 5:13 20:1 20:4 22:3 82:16
**beyond** 52:13
**big** 72:19
**bigger** 52:6
**binary** 57:9
**binding** 25:13
**BIOMETRICS** 1:9
**bit** 69:18
**bits** 57:9
**board** 1:3 6:14 84:6
**Bob** 39:16,21 40:1 42:1,5 42:13 58:22 58:24 59:2,6
**book** 13:20 15:4 37:18 38:5 44:9,9 61:19
**Boone** 2:8 4:8 84:10
**boss** 70:11,19 70:20,22,23
**bots** 55:5
**bottom** 64:25
**Boulevard** 2:9
**break** 5:15 26:1 28:7 46:19,21 47:1 48:8 53:11 54:12 54:14,18 67:12 79:1,3
**breaking** 21:19 60:5
**breaks** 5:14 79:22,23 80:2,19
**broad** 64:8
**broader** 76:17 76:19
**broadly** 66:20
**brought** 50:11
**Brown** 69:15 69:17 71:20
**browser** 19:5 19:7
**buffer** 51:18 51:22,22,25 52:5,6,7,10 52:13
**build** 45:6 47:8 48:6
**built** 26:11

**C**

**c** 84:1,12 85:1 85:1
**C-80** 70:1 72:14
**C-83** 72:20 73:7
**C-H-E-N-G** 69:3
**California** 5:4 11:5
**call** 6:7 39:16 39:19,24 42:1 55:5 57:14 71:24
**called** 12:24 13:17 14:1 42:10 50:7 55:25 56:25 62:19 70:2,2 70:13 72:15 72:22 73:14
**camera** 29:16 36:2
**capitals** 70:3
**CARBYNE** 1:9
**card** 45:9,10 45:21,21,25
**careful** 32:6
**case** 6:15,23 24:15 30:15 30:23 39:14 42:13 68:5,6 84:14,17 85:12,13
**cases** 5:17 6:23 62:9 65:24 68:3,6 68:7 75:2
**catch** 64:1
**caught** 46:2
**cause** 13:23 60:20
**CCR-B-2289** 1:25 84:22 85:20
**center** 45:11
**centers** 44:14
**Central** 79:12
**certain** 49:16 57:8,8,10,11 57:14 65:25
**certificate** 73:4
**certificates** 72:24
**certification** 70:18 72:15
**certified** 70:20

72:15 84:8 85:4
**certify** 82:15 85:5,10,11
**certifying** 72:23
**Challener** 68:21,24,25
**chance** 54:11
**change** 10:19 44:25 82:21 82:23,25 83:2,4,6,8,10 83:12,14
**changed** 75:1
**changes** 14:17 82:4
**chapter** 15:3 44:10 45:4 47:7 52:17 54:19 61:16 61:16 62:17 66:14 67:1,7
**chapters** 13:20,25 65:3,11 66:24
**characterize** 64:20
**charge** 84:16
**chat** 16:10
**check** 56:11 58:8 63:19
**checking** 57:1 57:23
**Cheng** 69:3,4 69:5
**chunks** 50:9
**CIA** 38:2
**cipher** 39:24
**circumvents** 21:16
**cited** 69:7
**Civil** 82:3
**claim** 32:4,6 32:25 33:2,5 34:5,11 37:11,12
**claims** 26:22 27:20,23
**clarification** 17:19
**clarify** 33:5
**class** 13:15,24 14:21,22 15:1 17:2 19:16 21:22 37:15
**classes** 12:11 12:16,17,21 12:23 13:9 13:10
**classmen** 13:7
**clear** 5:18,24
**click** 22:5 55:1 56:3 70:11 70:12,24
**client** 29:23
**clients** 60:21 67:9,10
**close** 18:10 19:11 28:5
**closed** 18:12 80:11
**closely** 66:7
**closing** 19:13
**cloud** 29:17,25 30:6,7,10,13 30:24 31:14 31:24 32:2 32:14,19 33:9 34:15 64:17
**CLR** 1:24 84:22 85:19
**coauthored** 12:7 13:16 14:2
**coauthors** 71:6
**code** 57:23 82:3
**codes** 73:15 74:10,14,20 75:4,6,10
**coercion** 45:23
**coincide** 13:25
**colleagues** 57:2
**Colorado** 2:19
**column** 27:6 29:3,19 30:8 31:14 33:6 35:10,12,21 36:15 37:10
**combination** 47:11
**come** 49:8 53:22 75:2
**comfortable** 7:24
**coming** 26:16 27:19 41:9 43:2 49:5 55:17 70:22 78:13,24
**commercially** 60:9
**Commission** 83:20
**common** 56:21 58:13 62:16
**commonly** 56:18
**communicate** 18:5 29:14 30:7,10 35:15 36:3,6 36:17,21,25 37:13 63:8 64:4 80:4
**communicat...** 30:3 64:15
**communicat...** 29:14
**communicat...** 18:14 35:6 36:24 63:1 65:8
**communicat...** 51:24 62:1 65:9
**company** 53:10 58:4 60:14 70:11 72:22 73:8
**compare** 42:23
**complete** 4:22
**completely** 4:16,19 49:9 51:14 79:10
**component** 77:19
**components** 34:15 40:13
**compromise** 44:24 45:1
**computational** 11:12
**computation...** 41:4
**compute** 41:2 42:22
**computer** 3:9 9:21 11:2,11 11:12,23 12:4,6,7,21 12:24 13:4,8 13:10,13,15 13:17,18 14:1,12,14 14:18 15:1 15:13 17:1 17:25 18:15 18:24 21:16 21:19,21 22:9 25:20 27:22,25 29:7 37:15 37:24 38:4,8 38:10 47:17 48:14,15 50:1,12 51:4 51:9 52:9 53:1,2 54:22 54:24,24 55:2,12,15 55:25 56:15 56:24 57:14 58:12,14 59:18,24 60:1,3 61:21 62:22 63:13 63:19,25 65:13,22,23 66:3 67:23 69:25 70:8 71:13 72:2 72:11 74:16 74:21 75:22 80:14,16,18 80:21,23 81:1
**computerized** 85:9
**computers** 44:20 54:25 55:4,7 61:24 62:2,4 63:14 75:21
**computing** 11:23 44:13 72:1
**concatenate** 42:16,22
**concept** 17:4 21:7 37:24

38:11 39:2 40:15 76:19 77:3,8
**concepts** 14:4 16:25 37:24 38:3,4,8 72:12
**concerning** 11:1,7 12:4
**concerns** 11:21
**concluded** 81:8
**conclusions** 7:19
**conferences** 67:24
**confidential** 21:9,13 39:4 39:20 40:13 41:14
**confidentiality** 38:2,13,21 39:1,2,12 40:5,8,10,19 40:21 41:7 44:6,24
**configuration** 30:18
**configured** 31:15 32:14 33:10
**confirm** 18:22 19:4,7
**confused** 20:1
**conjunction** 40:8
**connect** 29:24 43:8 66:11 67:9,10
**connected** 47:19 61:24
**connecting** 34:4
**connection** 36:10 46:4
**connections** 34:2 65:24 65:25 66:2 66:20
**considered** 24:21
**consult** 15:7 20:7 80:15 80:22,25
**consulted** 80:17,21
**contacted** 84:10
**containing** 70:8
**content** 64:15
**contents** 3:1,8 15:22 16:5 19:21 20:3 37:17,22 44:8 48:11 49:18,20 61:19 63:2 77:3
**context** 24:7,9 24:11,12,20 48:16 74:17 77:1,9,21
**contexts** 21:8 73:23 74:19 75:10
**continues** 52:12
**continuing** 11:4 35:11
**contract** 84:12 84:13
**control** 14:3 48:3 60:24 61:1 75:16 77:22,23
**controls** 44:15 61:13
**copies** 43:14
**copy** 15:16
**copyright** 15:15,19 16:6
**correct** 9:19 10:15 14:12 17:20,23,25 19:6 24:18 25:19,24 27:8 29:18 30:23 34:8 35:17 38:12 46:23 53:24 55:16 57:18 60:25 62:6 66:6,21 72:5 74:19 85:10
**corrections** 82:9,18
**Council** 84:6
**counsel** 2:1 7:19 9:3 18:6 85:12,12
**COUNTY** 84:3 85:2
**course** 12:24 13:13,18 14:13,18 27:20 36:19 38:10 47:12 51:14 72:2,4 77:1
**courses** 11:1,6 11:9,20,21 11:22 12:3,5 12:13,14,18 71:14,17,20
**court** 9:13,18 15:25 16:14 20:14,16 84:6,8,10,14 85:4
**cover** 13:14 14:25 16:6 17:12,13 84:15
**created** 41:12
**credentials** 17:9 25:13 25:16 27:3 55:16,19
**Cross-talking** 20:12
**CRR** 1:24 84:22 85:19
**crucial** 21:15
**crypto** 72:12
**cryptographic** 14:4 21:16 21:19 39:9 40:21 41:4 42:15,17 72:6,9,14 73:10
**cryptography** 14:9 39:14 59:2
**cues** 21:7
**customary** 84:17
**CV** 11:9 69:23 70:1
**cyber** 11:13,24 12:8

**D**

**D** 71:6 84:1
**damage** 52:13
**damaging** 52:14
**danger** 5:8
**DARPA** 72:20
**data** 11:1,13 11:18 12:1 30:20,24 31:6,22 33:18,19,22 39:3,5,8 40:2 40:22 41:12 42:2 43:6 44:14,25 45:10 51:1 61:6,7,9,11 62:5,24 63:3 63:5,9,23 64:3,4,7,8 76:23 77:2,3 77:7,12,18 77:24 78:4,9 78:17,20
**date** 14:13
**David** 2:6 68:25 69:5
**david.obrien...** 2:14
**day** 83:20 85:14
**deal** 38:6 53:1
**dealing** 50:24 71:1
**dealt** 69:22
**decision** 6:14 8:8
**declaration** 5:22 6:6,12 7:3 8:6 10:2 10:6,9,12,14 10:21 19:9 23:12,15,22 24:17 25:25 47:13 49:10 50:1 51:15 67:17 68:20
**declarations** 5:21 6:1,5,11 6:17 7:13,21 8:6,7 9:21 22:23 69:2 70:15
**decrypt** 40:2

58:25 59:4 59:12 60:6 63:18
**decryption** 14:10
**dedicated** 35:15,17 36:1,17
**defend** 21:23 22:16 23:3,9 24:5,12,19 24:24 25:2 26:14,19 27:11 45:2 45:12 49:4 50:21 53:13
**defending** 22:22 44:2 52:9 69:19
**define** 37:16
**definitely** 77:4 79:14
**degree** 71:24
**denial** 43:21 43:24 55:7 65:6
**depend** 78:13
**depending** 54:9 77:20
**depends** 24:7 24:9,11,20 32:3 74:17 74:23 77:1,9
**deposition** 1:17,22 4:12 5:1,8 8:1,18 9:6,8,10 20:5 28:6 37:19 44:8 61:20 68:6 80:5,7 81:7 82:5,6 82:16,17 84:2,11,12 84:15 85:6,8 85:10
**depositions** 8:23
**describe** 11:6 28:18 69:20
**described** 23:3,9 26:18 27:9,15 29:4 33:14 52:19 64:16 73:6
**describes** 26:25
**design** 11:2,16 13:6
**designed** 64:24
**designer** 56:7
**desirable** 46:8 46:19,21,25 47:20 48:21 54:4
**desire** 82:5
**detail** 14:24 29:5
**details** 22:1
**detection** 11:13,24 12:8
**determine** 39:25 40:16
**developed** 72:21
**developer** 58:4
**development** 53:18
**developments** 14:14
**device** 28:24 29:14 30:6 30:21 31:8 33:9 34:21 34:25 35:1 35:21 47:10 56:18 57:19 57:24 61:2 74:21
**devices** 29:10 29:15,23 30:21 31:7 31:16,17 32:20 33:10 33:12 34:14 44:13 47:19 64:18 65:14 66:19
**diagram** 33:19 34:16
**diagrams** 33:22
**dictionary** 26:1,4,5,8
**different** 41:14 53:9 57:2,15 60:25 67:2 76:14 77:12
**difficult** 25:7 41:5 45:18 46:9,13,16 47:1,8
**digital** 41:23 42:3 55:20 56:12 57:3 57:16,23 58:3,8,20 59:5,15,17 72:23 73:4 73:21,24 74:3
**digitally** 42:1 56:8,9 58:4
**diligent** 22:13
**directed** 13:3 64:17 66:20 71:25 72:6
**direction** 41:2 85:9
**directly** 36:4,6 72:9
**disagree** 32:19
**disassemble** 44:20
**disclose** 15:9
**disclosed** 28:21 31:2,4
**discloses** 25:8
**disclosing** 15:8 37:12
**disclosure** 84:7
**disclosures** 35:12
**discount** 84:17
**discovered** 60:19
**discuss** 19:15 21:22 22:23 37:21,23 62:17 73:11
**discussed** 13:25 30:5 35:10 38:24 47:13 48:12 58:16 60:24 72:13 76:20 80:18,20,21
**discussing** 5:17 51:20
**discussion** 16:20 20:18 23:16 46:6 46:17 57:21
**discussions** 7:18 11:10 23:20
**disguises** 21:11
**dispute** 33:1
**distributed** 58:15
**District** 9:13 9:18
**divided** 50:9
**diving** 67:7
**documents** 6:2,9,10,15 6:23 8:2,4 9:2,6,12,18 19:1,8 80:1 80:15,22,25
**doing** 17:7 21:17 36:22 36:23 42:5 56:25 63:16 63:24 78:15
**dollars** 72:19
**download** 21:14 43:8
**downloading** 17:9
**dozens** 73:11
**Dr** 6:13 8:7 16:5,12 17:22 20:17 20:19,23 67:18,21 81:6
**draft** 8:12
**drive** 19:3 50:14 51:6 60:15,22
**drives** 75:23
**duly** 4:3 85:6

**E**

**E** 82:1,1,1 84:1 85:1,1
**e-mail** 7:3 8:17 16:13,13 17:24 18:2,3 18:4,11,20 22:4 55:1 70:6,7,10,16 72:16,16 80:8,9,11

**e-mails** 56:2 70:4 71:2
**e.g** 36:1
**earlier** 13:16 17:23 36:14 41:25 57:17 58:2,2,21 71:12 73:19
**earliest** 69:24
**early** 12:19,23 13:5
**easier** 16:17
**easy** 41:1
**eavesdrop** 62:25
**eavesdroppi...** 65:9
**educating** 25:5
**education** 71:9
**either** 7:3 60:4 72:3,8 75:21 77:20 78:1,6
**embodied** 39:6
**embodiment** 28:20 29:21 31:3 34:21 34:25 35:9
**embodiments** 31:12,14 32:24,25 33:1,9
**emergency** 5:6
**employ** 85:12
**employer** 30:19,20,22 30:24 31:6,6 31:9
**encrypt** 39:21 58:24 59:3,8 59:10,23 63:7 73:5
**encrypted** 58:17 59:11 59:13 60:3 60:15 62:24 62:24 63:9 63:15 64:3,7
**encrypting** 63:22
**encryption** 14:9 58:16 58:18,21,22 59:18 60:5 61:12,13 62:7,9,15 63:6 75:14 75:17 78:2,3 78:16
**encrypts** 62:21
**enforce** 48:10
**engineering** 14:25 17:1,3 19:15 21:5,7 21:15,23 22:12,17,22 23:1,4,10 24:5,13,19 24:25 25:2 25:15,21 26:6,12,14 26:20 27:1 27:11,16,18 28:1 44:2 45:3,5,8,14 45:18,24 46:9,20 47:4 49:4 69:20 69:21 70:5 71:11,19
**entered** 82:6
**enterprise** 53:6,16
**entire** 6:23 50:3
**entirety** 10:11
**entities** 36:21 37:1 51:25
**entity** 39:16 42:1
**environment** 28:20 29:7 29:21
**errata** 82:11
**error** 10:14
**especially** 53:14
**Esq** 2:5,6,7,17
**establish** 36:9
**estimate** 7:23
**et** 69:16
**everybody** 39:22 59:4
**evidence** 42:25 56:13
**exactly** 14:21 37:4 74:4
**EXAMINATI...** 3:3 4:5
**examined** 4:3 85:6
**example** 6:6 9:15,16 21:12 23:12 23:15 27:5 29:7 30:19 33:21 34:3 34:17 35:10 35:21,22 37:13 39:7,9 41:18,20,22 42:12 44:13 45:20,20 47:23 48:1,5 48:19,25 49:16 55:11 55:14,24 60:13 63:6 65:12 66:5 69:14 70:15 72:24 73:1 78:14
**examples** 21:10 29:23 49:5 60:12 61:15 72:12
**exception** 82:18
**exhibit** 3:7 10:3 15:16 16:1,2 18:6 18:19 19:23 37:19 44:7 61:19 68:11 68:21 69:3 69:15 80:9 80:16,19
**exhibits** 3:6 19:1,3 80:17 80:20
**exist** 34:2 49:7 64:9 67:5
**existing** 72:3
**exists** 64:1 66:4
**expect** 79:14
**experience** 69:19
**Expires** 83:20
**explain** 13:22 24:8 25:1
**explained** 24:16
**explains** 29:4
**explicit** 48:23
**external** 15:7 36:8,10 50:14 51:6 51:11 75:22

**F**

**F** 1:24 84:22 85:1,4,19
**F-I-S-H-I-N-G** 17:17
**face** 46:1
**fact** 50:4 56:8 59:16 60:18 73:8
**factors** 45:5
**fair** 5:12 74:9
**familiar** 68:19 73:15
**far** 49:25
**fast** 35:14,24 37:6
**Federal** 82:2
**fight** 55:21 58:18
**figure** 28:16 28:18,19 29:15,20 33:15,17,21 33:21,22,24 34:9,13,18 34:19,20 35:1,2,7,9,22
**file** 15:17 18:2 47:19 49:11 49:14 75:8 75:12 76:7 76:14,17,18
**filed** 9:12
**files** 49:16,18 49:20 59:19 59:23 60:3 60:15 74:15 74:21,25
**financial** 84:17
**financially** 85:13
**find** 19:2 41:5 70:12
**finder** 19:2 80:13
**fine** 28:8,9 79:10
**fingerprint**

25:9 36:2
**Finkley** 1:24 84:22 85:4 85:19
**fire** 5:7
**fires** 5:4
**firms** 60:19,20
**first** 4:3 10:23 12:17,20 23:22 31:10 32:4 33:7 34:6,10,16 34:22,23 38:1 48:23 56:11 63:7 65:18 73:6
**Fishback** 2:17 7:7 8:20 16:12,17,22 16:23 17:15 18:18 19:17 20:21 21:25 22:18 23:5 24:6 28:8 29:1 31:1 32:22 33:16 34:12 36:5 37:3 38:15 40:6 44:4 46:3 47:2,5 49:24 50:23 54:7,10,15 55:10 56:20 57:25 59:20 61:3,22 62:13 63:10 64:19 65:15 66:9,22 73:17 74:22 76:15,24 78:11,21 79:7,13,16 81:5
**flash** 60:22
**flow** 33:18,19 33:22,23
**flowchart** 33:18,23
**focus** 5:10
**focused** 33:5
**following** 14:15 82:18 84:6
**follows** 4:4
**foregoing** 82:16 85:6 85:10
**form** 19:17 21:25 22:18 23:5 24:6 29:1 31:1 32:22 33:16 34:12 36:5 37:3 38:15 40:6 44:4 47:2 49:24 54:7 55:10 56:20 57:25 59:5,15,20 61:3,22 62:13 63:10 64:19 65:15 66:9,22 73:17 74:22 76:8,15,24 78:11,21 82:4,9
**forth** 85:8
**forward** 5:1 16:24
**fraud** 11:13,24 12:8
**freshmen** 13:6
**front** 28:14
**full** 85:10
**fun** 51:13
**function** 40:23 41:1,4 42:15 42:18,23
**functionality** 43:16
**functions** 40:21
**fundamental** 37:24
**fundamentals** 11:14
**furnish** 82:11
**further** 81:5 85:11
**future** 71:25 72:3

G

**gain** 45:10 60:1
**garbage** 60:6
**general** 22:8 43:17
**generally** 17:3 21:6 24:21 25:23 27:22 47:20 48:21 54:8 61:4,23 64:6 74:12 77:9
**geometry** 11:12
**GEORGE** 2:17
**Georgia** 82:4 84:2,6,8,22 85:2,4,20
**getting** 61:9 70:3
**gfishback@...** 2:22
**give** 24:14 25:23 50:2 52:5 60:12 65:12 70:17
**given** 41:3 82:7 84:17
**gives** 48:23
**giving** 45:9 52:8
**go** 4:10 5:1,14 10:2,5,20 23:21 25:10 28:16 29:2 29:19 30:8 37:1,17,20 38:1,6 44:16 54:16 57:14 62:17 66:12 67:11,13,15 73:10
**goal** 13:5 74:11
**goals** 38:13,19 38:22,24 44:3,18 53:3 62:10
**goes** 5:21 23:17,18 30:17 36:19 43:15
**going** 13:23 27:7 49:25 54:10 62:18 65:1 69:23 73:3
**good** 4:7,9,10 5:6 54:11 57:4 79:6
**Goodrich** 1:17 3:2 4:2 15:13 16:5,12 17:22 20:19 20:23 81:6 82:14 84:3
**Goodrich's** 20:17
**graduate** 10:25 11:3
**grant** 72:19
**graph** 11:14 11:25
**graphical** 52:2
**graphics** 11:13
**great** 16:7
**ground** 4:11
**guard** 26:25 27:15 46:1
**guys** 79:17

H

**H** 82:1
**hacker** 41:17
**handed** 45:23
**hang** 18:19
**happen** 52:4
**happy** 32:12
**hard** 19:3 25:7 41:1,2 60:15
**hardware** 64:25
**hash** 40:21,22 41:4 42:15 42:17,23,24
**hashed** 75:3
**Haynes** 2:8 4:8 84:10
**held** 1:22
**help** 25:9 26:25 45:2 53:18 74:10
**helps** 44:3,5
**Henderson** 84:8,10,11 84:13,16
**HENRY** 84:3 85:2
**hereunto** 85:14
**hiding** 63:25
**high** 25:4
**higher** 14:7 25:23
**highlighted**

**hijack** 65:8
**HMAC** 42:10 42:11,20 74:6,7
**Hobson** 67:25
**Hong** 2:5 4:7
**hong.shi@h...** 2:13
**honored** 71:15
**Hopkins** 11:5
**hour** 28:5 54:11 79:3
**hours** 7:20 9:1 51:12 76:4
**HTTP** 67:5
**HTTPS** 62:19 63:8,15,20 63:22 67:5 72:25 73:3
**human** 22:14 45:4 54:23

**I**

**ID** 25:10
**idea** 41:23 56:24
**identical** 77:8
**identification** 16:3
**identity** 24:2 39:25
**illustrate** 34:3
**illustrated** 35:1,22
**illustrates** 29:20
**illustrating** 35:9
**illustration** 28:19 33:25 34:14,20
**immediately** 26:15 27:19 41:9 43:2 49:5
**implement** 71:3,5
**implementat...** 14:4 71:8
**implemented** 33:15 35:1
**implementing** 39:11
**important** 44:17 61:21 70:12
**importantly** 25:12
**impression** 50:2
**improve** 25:20
**improved** 27:22,25 55:12 63:5
**include** 11:10 11:11,22 12:5,7 16:6 20:2 21:10 29:11,11 34:9 41:23 43:11 58:11
**included** 12:18 14:3
**includes** 15:22 22:24 29:8 35:23
**including** 14:8 14:9 27:1 29:15 45:13 71:19,19 80:18
**inclusive** 23:19 30:2
**incorrect** 18:1
**increase** 62:8
**indirectly** 72:9
**individuals** 42:12 71:10
**infect** 54:25 55:4
**influential** 72:18
**information** 21:9,13 30:12,16 41:14,15
**initial** 16:7
**initials** 38:1
**injects** 56:1
**input** 41:5 42:17 52:1,5 52:8
**inputs** 51:24
**insecure** 17:7 21:18 35:24
**inside** 51:4,9 53:10 56:5 63:17,22
**insider** 52:18 52:25 53:10 53:21,23 54:5
**insiders** 53:16 53:25 54:1,3
**install** 56:4,10 58:7
**installation** 56:11
**installed** 57:19
**installing** 58:11
**institute** 6:14
**institution** 8:8
**integrity** 38:2 38:13,21 41:10,11,19 41:21,23 42:7,25 43:1 44:6 45:1 58:9 73:25 74:10,25 75:7
**interact** 37:8
**interactions** 68:3
**interested** 85:13
**interface** 52:2
**internal** 51:9
**Internet** 11:16 11:25 12:9 19:5 32:1,21 36:4,7,9 65:14
**interrupt** 17:16 18:9 46:3
**intervention** 54:23
**introduce** 38:5 44:25 47:21 53:12,19
**introducing** 41:17 63:13
**introduction** 3:8 11:15 13:17 14:1 15:12 37:20 44:9 71:13
**intrusion** 66:3
**invalid** 55:19
**inventor** 67:25 68:16
**inventors** 68:8
**invert** 41:1,2
**involved** 71:9
**involvement** 71:22
**IPR** 5:18,18 6:6,13,14 10:3
**IPR2024-003...** 1:12
**IPR2024-003...** 1:13
**IRS** 70:10
**Irvine** 11:5
**issue** 49:15 52:14,25 70:3
**issued** 30:22 31:8
**issues** 14:5 46:4 50:25 53:12

**J**

**Jacinto** 2:9
**Jack** 67:25
**January** 1:19 85:14
**Jarrett** 7:6 8:19
**Johns** 11:5
**joint** 8:23
**Judicial** 84:6

**K**

**Kamprath** 7:5
**keep** 14:12 30:11
**keeping** 30:15 44:14
**KELLY** 2:7
**kept** 39:3,4
**Kesanupalli** 22:24 23:9 24:1,15,15 24:23 25:1,4 25:12 26:10 68:12,14,17
**key** 16:25 39:7 39:10,14,15 39:17,17,21 40:2 41:24 41:25 42:13 42:16,21,22 45:9,10,21 45:21,25 47:11 58:22 58:22,25 59:1,3,4,8,10

59:12 60:2 74:1,5,8
**keys** 59:2
**kin** 85:11
**kind** 50:20 51:19 55:1 74:2
**kinds** 17:7,10 21:11 53:6 66:17 71:18 72:2
**know** 5:6,7,15 5:23 14:24 15:18 22:6 56:21 57:4 59:24 60:2 63:23 67:20 67:21,22,25 68:8,13,13 68:16,24,25 69:1,4,5,9,16 70:10 79:8
**knowing** 47:10 56:4
**knowledge** 82:17
**known** 22:24 25:25 39:13 39:22 48:2 48:15 51:21 52:7 63:18 64:23 65:17
**knows** 39:17 42:20

**L**

**L** 84:1
**label** 16:1
**lagging** 46:5
**language** 32:6 32:7 37:11
**laptop** 30:9 31:23 32:1 34:3
**large** 35:23 52:9
**late** 12:23
**latest** 14:13
**law** 60:18,20
**layer** 64:25 65:2,4 67:3,4 67:5
**layers** 14:6,7 64:24 67:2
**leakage** 49:1
**learn** 63:2
**lectures** 11:11
**legal** 6:24 84:8 84:10,11,13 84:16
**legitimate** 17:6 21:12 22:4,5 22:7 25:17
**let's** 9:20 10:2 10:20 16:1 23:21 33:3 53:10 54:13 54:16 67:15 69:18 70:8
**level** 13:2 25:4 74:25
**levels** 25:23 61:1
**light** 7:17
**likewise** 59:12
**limit** 53:3
**limited** 13:10 27:11
**line** 27:7,7 29:3,20 30:8 30:17 31:13 33:6,8 35:11 35:13,20 36:14 49:8 82:20,22,24 83:1,3,5,7,9 83:11,13
**lines** 46:14
**list** 6:6,8 23:14
**listed** 6:9 51:18 64:12 70:1 82:18
**literally** 18:3
**litigation** 9:18 84:18
**little** 32:6 69:18
**LLC** 1:9
**LLP** 2:8 84:10
**located** 29:6
**locked** 44:14
**locks** 47:7,8
**log** 25:11
**logging** 55:14 55:16
**logical** 33:23
**long** 8:25 79:8
**longer** 24:16 24:18,21,24 25:2,5,6,10 25:19,22 26:10
**look** 25:17 35:19 57:10
**looking** 7:15 67:2
**looks** 39:23
**lot** 72:5
**lower** 14:6
**lunch** 79:3
**luncheon** 79:20
**LYLE** 2:7

**M**

**Mac** 60:13 74:6
**main** 51:4 75:22
**making** 82:7,8
**malicious** 17:10 47:22 53:19 56:1 67:10
**malware** 14:6 21:14 52:17 53:22 54:5 54:19 55:21 55:24 56:19 58:18
**man's** 73:24
**manager** 53:6
**manages** 47:18
**marked** 16:2
**master's** 71:24
**match** 42:24 46:1,2
**matches** 59:11 59:13
**matching** 11:19 12:2 12:10
**materials** 14:18 15:7
**matter** 51:16
**McDaniel** 6:13 8:7 67:18,20 67:21 69:10
**McKool** 2:18 7:6,6,7
**mean** 31:19,21 32:3 36:7 38:17 49:7 66:11 73:11 74:2,24,24 75:20,21 77:1
**means** 39:9 40:25 45:17 46:8,16,19 46:25 56:3
**meant** 34:3
**mechanism** 41:25
**mechanisms** 49:19 61:8
**Medarios** 71:6
**medical** 5:1
**meet** 7:2 8:16
**meeting** 9:3
**memory** 20:5 47:19 48:20 48:21,24 49:2,2,11,14 49:23 50:4,5 50:8,8,12,16 50:17,21 51:4,5,6,9,11 51:23 52:11 52:12,14,15 75:16,20,21 75:22,25,25 76:5,8,9,11 76:13,16,18 76:19,21,22 77:4,6,12,18 77:24 78:4 78:10,17,19
**mentioned** 9:3 13:16 21:6 34:5 39:10 46:7 69:10 75:18
**message** 39:20 42:4 42:14,16,19 42:21 58:24 70:9,21 73:14 74:6,9 74:14,20 75:3,5,10
**messaging** 18:14
**met** 7:5 8:19 67:23 68:18
**methodology** 7:15
**Michael** 1:17 3:2 4:2 15:13

84:3
**Microsoft** 56:7 56:10 58:6
**million** 72:19
**mind** 26:16 27:19 41:9 43:3 49:6 78:13,24
**minor** 10:17
**minute** 18:4
**minutes** 16:16 16:19
**missed** 75:24
**mobile** 35:23
**models** 14:10
**modified** 48:4
**modify** 49:21 60:4
**module** 28:24 28:25 29:8
**modules** 29:12
**Monday** 8:22
**morning** 4:7,9 4:10
**moving** 77:6
**multilayer** 63:6
**multiple** 31:16 32:20,23 33:10 43:14 50:5 55:4 75:6 76:9 79:21

**N**

**name** 17:8 85:14
**named** 85:6
**near** 5:5
**necessarily** 52:21
**necessary** 82:10
**need** 5:15 19:20,22 29:11 50:14 53:1 54:25 78:22
**needs** 37:1 46:15 50:13
**network** 14:6,7 14:7,8 29:25 30:4 61:17 61:20 62:2,4 62:8,10 63:7 64:11,18,23 66:6,13,19 66:20,25 67:2,16 75:7
**networking** 11:2,21,22 12:16,17,18 29:16
**networks** 29:24 61:24 64:24
**new** 14:18 44:25
**Notary** 83:19
**notebook** 29:7
**notes** 9:24,25 85:11
**noticed** 10:16
**nowadays** 62:18
**number** 34:24 37:25 39:8 59:22 62:14 69:12 71:16 72:8 75:18
**numbered** 34:23

**O**

**O** 84:1
**O'BRIEN** 2:6
**O.C.G.A** 84:12
**oath** 4:13,15
**objection** 19:17 20:21 21:25 22:18 23:5 24:6 29:1 31:1 32:22 33:16 34:12 36:5 37:3 38:15 40:6 44:4 47:2,5 49:24 54:7 55:10 56:20 57:25 59:20 61:3 61:22 62:13 63:10 64:19 65:15 66:9 66:22 73:17 74:22 76:15 76:24 78:11 78:21
**objections** 50:23
**occur** 62:3 65:4
**occurs** 70:6,14
**office** 1:1 51:12 76:4
**offices** 84:10
**Official** 82:3
**oftentimes** 6:24 44:19 49:16 50:2 53:3,7 60:20 61:25
**okay** 5:16 15:21 16:15 16:21 18:12 19:13 28:5 30:23 68:16 76:2,6,13 78:25 79:4
**old** 66:1
**once** 40:1
**one-way** 42:23
**ones** 38:6 57:11
**online** 29:16
**open** 13:2 17:24 18:15 18:24,25 19:5,9,10,21 44:23 80:8
**operating** 14:5 47:15,17,20 47:22,24 48:1,4,7,9,16 48:18 49:3 49:19 51:23 52:3 61:7
**operations** 61:25
**opine** 28:3 47:14
**opinion** 10:17
**opposite** 45:6
**order** 66:11 74:5,8
**ordinary** 7:17 27:21,24 31:20 33:25 35:3
**organization** 76:18
**organizations** 71:4,10
**organized** 64:22 66:24
**original** 42:14 59:9
**originally** 41:20
**output** 40:23 40:25 41:3,6
**outputs** 51:24
**outside** 49:9 51:15
**outsider** 52:19 53:23 54:6
**overflow** 51:19 51:22 52:7 52:10
**overlap** 9:15 52:22 74:3 77:13
**overlapping** 77:2,8
**overlaps** 77:5
**overloading** 43:22
**overwrites** 52:11
**overwriting** 52:12
**Owner** 1:10 2:16 7:8 8:10 8:13
**Owner's** 6:18

**P**

**P-H** 17:16
**P-H-I-S-H** 21:10
**p.m** 1:20 81:7
**packets** 62:23 63:2,19
**page** 3:3,7 10:5,8 16:6,7 43:8,17 50:11 62:18 82:20,22,24 83:1,3,5,7,9 83:11,13
**pages** 50:10 82:10
**paper** 70:17,25 71:7 72:13 72:18
**papers** 72:8 73:11
**paragraph** 6:8 10:20,24 23:17,17,18 23:19,21,24

24:17 31:11 70:15
**paragraphs** 23:13
**parallel** 11:17 11:23,25
**part** 12:14 13:18 16:7 19:23 21:1 32:18 35:19 72:19,25
**parties** 39:15 74:1 75:7 84:17 85:12 85:13
**parts** 19:25 20:25 23:2
**party** 39:19 42:20 84:14 84:18
**pass** 81:4
**passage** 36:20 37:10
**password** 17:9 25:2,19 26:3 27:2,10 39:8 59:24 60:2
**passwords** 24:1,4,10,16 24:18,21,22 24:24 25:5,6 25:10,23 26:2,3,9,10 27:3,10
**patent** 1:1,3,10 1:12,14 2:16 6:7,8,18 7:8 8:10,12 23:16 26:19 26:21,25 27:6,14,20 28:13,14,22 29:3,19 32:11 33:20 68:1,11,21 69:15
**patents** 7:14 23:13 56:23
**Patrick** 67:18 69:10
**pattern** 11:19 12:2,9 57:7,8 57:10,11,13
**PC** 2:18
**PDF** 15:17,18 19:7 80:12
**Pearson** 15:14
**people** 13:12 14:22 17:5,7 21:8,11 22:11 25:10 26:2,5 39:4 43:7 44:16 56:3 70:12 71:18
**perform** 58:20 61:25
**person** 7:4,17 8:17 27:21 27:24 31:20 33:24 35:3 45:22 53:8 67:20,21
**personal** 30:21 31:7 69:19
**personally** 56:16 68:2 68:18,24,25 69:9,16
**perspective** 46:22
**petition** 69:7
**Petitioner** 1:7 1:18 2:3 4:8
**petitions** 6:20
**Ph.D** 1:17 3:2 4:2 82:15 84:3
**phishing** 17:12,14,16 17:21 19:14 21:10 70:3 70:14,16 71:2 73:2
**phone** 30:9 35:23
**physical** 14:5 44:10,11,12 44:12,15,17 45:2,7,12,17 45:22 46:8 46:15,18,24 47:11
**physically** 44:20
**pick** 47:9
**picks** 23:18
**picture** 45:22 46:2
**piece** 51:23
**place** 49:1 53:17 61:8 85:8
**places** 29:6
**placing** 7:16
**plan** 4:20 5:14 79:8,10
**planning** 79:8
**please** 15:21 19:4,12 20:6 20:14,16,23 24:8,14 28:13,16,18 33:7 68:10 69:20 82:9 82:11
**point** 32:11
**poor** 27:2,10 73:24
**port** 65:17 66:4
**portion** 19:22 63:3 64:17
**ports** 65:22,25
**possibility** 53:18
**possible** 31:3 35:5 38:23 65:10 75:2
**potential** 9:15 34:1 70:7
**potentially** 44:23 55:5 63:24 65:19 78:1
**practice** 14:10
**preferred** 35:8
**preliminary** 6:18
**prepare** 6:17 7:2,12,21 8:1 8:17 9:6 16:16
**prepared** 9:13
**preparing** 6:1 6:11
**presumably** 55:18 70:21
**presume** 14:23
**presuming** 37:19
**pretend** 76:3
**pretending** 70:23
**pretty** 56:17 66:7
**prevent** 30:20 31:6 45:7 49:1 50:18 55:17 61:9 70:18
**preventing** 26:11 43:24
**prevention** 11:13,24 12:8 22:15 43:21
**prevents** 25:15
**previous** 20:17,23
**principles** 22:8 37:23
**prior** 7:18 8:9 9:16 22:23 68:9 85:6
**private** 39:16 40:2 41:24 58:25 59:3,8 59:12
**privileged** 30:20,24 31:6
**probably** 26:16 61:13 62:15
**probes** 44:23
**problem** 64:1
**problems** 5:3
**Procedure** 82:3
**procedures** 24:3 53:17
**proceedings** 6:25
**process** 48:12 48:12,19,22 48:22,23,24 50:3,9,12,14 51:8 70:19 76:9
**process's** 49:2 49:2
**processed** 52:2
**processes** 47:18 48:15 48:17 50:5,7

**processing** 11:18 12:2,9
**processor** 32:4,5 34:6,6 34:10,10,17 34:17,22,22 34:23,24 35:14,17,24 36:1,3,7,13 36:16,20,23 36:25 37:6,7 37:8,13 63:18
**processor/s...** 35:15 36:17
**processors** 35:7 76:10
**produce** 74:5
**produces** 40:23
**professional** 71:24
**professionals** 71:25 72:1,3 72:4
**professor** 11:4 76:3,12
**programmer** 53:19
**programmers** 53:15
**programming** 53:15
**programs** 53:20
**prohibited** 84:12
**project** 11:17 12:1 71:4
**pronounce** 42:11
**property** 41:11 43:6
**protect** 22:25 48:17 49:20 51:3,7 52:15 55:11 56:6 56:18 57:4 57:24 59:19 60:21 61:6 63:17,23 66:16 67:8,9 71:17 73:2 74:15,20,24 74:24 76:11 77:7,24 78:3 78:9
**protected** 60:22
**protecting** 58:14 61:11 62:2,4 66:19 77:3,11,12 78:1,6
**protection** 44:13 50:25 61:2 75:12 75:25 76:5,7 76:13,14,16 76:19,21,22 76:23 77:2 77:18,18 78:9,19,20
**protections** 49:1 75:16 75:25 76:9
**protects** 25:14
**protocol** 40:14 62:19,21 63:8,23 72:25 73:3
**protocols** 62:3 65:5 67:6
**prototype** 71:5 71:8 72:21
**provide** 4:22 38:18 42:17 49:19 61:1 72:11 84:10 84:14
**provided** 28:22 29:22
**provides** 29:9 60:14
**providing** 27:22,24 60:25
**proxy** 63:18,25
**public** 39:13 39:17,21 41:24 58:21 58:22 59:1,4 59:10 83:19
**publication** 69:24 72:20
**publications** 69:25
**published** 15:14
**publishes** 39:18
**pull** 11:9
**purchase** 15:16
**Purdue** 11:4
**purpose** 73:25 75:19
**purposes** 79:8
**Pursuant** 82:2 84:5
**put** 44:23 45:15 53:17

**Q**

**quality** 27:2,10
**question** 5:11 5:12 14:15 19:19 20:7,9 20:20 23:7 25:22 27:17 28:2,4 32:16 33:4 45:6 57:22 64:9
**questioning** 49:8
**questions** 4:16 5:11,20 5:23 20:3 51:14 67:16 81:4
**quite** 14:15

**R**

**R** 82:1,1 84:1 85:1
**RAM** 75:22
**rates** 84:17
**re-encrypt** 63:20
**read** 10:23 15:23 20:15 20:17 23:20 23:22 31:10 32:13 33:3,6 33:7 36:14 40:2 73:14 82:15,20,22 82:24 83:1,3 83:5,7,9,11 83:13
**reader** 36:2 45:25
**reading** 15:4 15:10
**real** 69:21 71:1 71:4
**realizing** 17:10
**really** 25:18 66:18 67:7 67:16 70:19
**reason** 4:21,25 16:10 82:21 82:23,25 83:2,4,6,8,10 83:12,14
**reasons** 82:7
**recall** 6:12,19 6:22 7:10,22 7:25 8:11,14 9:14 13:5 14:20 21:4 22:1,19 25:25 28:2 46:10 54:20 68:4 69:13 73:19 75:24 80:3,24
**recalling** 6:16 43:4
**recess** 28:11 54:17 67:14 79:20
**recited** 34:10
**recites** 34:6
**recognize** 21:23 71:10
**recognized** 27:21,23
**recognizes** 25:6
**recollection** 8:5 9:4 12:19 12:22 15:10 17:13 22:2 71:7
**record** 16:20 17:15 20:18 46:6,17 54:16 57:21 67:12,13 73:20 80:20 80:21
**reduce** 53:18
**reduced** 85:9
**redundancy** 43:12
**refer** 50:10,15
**reference** 22:24 69:15 69:17

**references** 8:9 9:16 68:9 69:8,9,12,13
**referral** 84:15
**referred** 13:9 13:12 30:1 40:24
**referring** 17:20 20:20,24 21:2,3 51:21 57:6 58:2
**refers** 50:8 65:21
**reflect** 14:18
**refresh** 15:10
**refreshed** 31:18 33:13
**refreshes** 30:17
**regular** 85:12
**Regulations** 84:6
**reject** 32:17
**rejection** 32:8
**relate** 38:8
**related** 33:4 67:16 73:21
**release** 58:5
**released** 41:20
**releasing** 58:6
**relied** 19:22
**remember** 7:20 12:17 12:20 20:4 25:7 69:11
**REMOTE** 1:17
**remotely** 7:3,5 8:16,19
**render** 27:3
**Renee** 1:24 15:25 84:22 85:4,19
**reopen** 19:18
**rephrase** 23:6 46:24 50:19
**report** 23:11
**Reported** 1:24
**reporter** 15:25 16:14 20:14 20:16 84:8 84:14 85:4
**reporting** 84:6 84:11,14,14
**representative** 84:8
**represented** 29:24
**representing** 7:8
**reputation** 68:20 69:1
**requested** 18:2
**requests** 43:23
**requires** 4:15
**research** 70:25 72:6
**researchers** 22:10
**resource** 36:8
**respect** 76:20
**respective** 29:12
**respond** 71:10
**responding** 32:18
**response** 20:17,20,23 36:23
**responses** 6:18 8:10,13
**restrict** 49:17 53:7
**restricted** 35:16 36:18 36:24 37:2,9
**restrictions** 30:19 37:7 48:3,8,9
**result** 21:14 85:13
**retailer** 29:17
**reuse** 27:2,10
**reveal** 21:13
**revealing** 17:8 21:8 25:16
**reverse** 41:5
**reversed** 59:2
**review** 6:2,10 6:18,20 8:4 8:10,12 9:2,7 9:9,12 32:12 80:1
**reviewed** 6:13 6:22 8:2,5,6 8:8,8 9:5 67:17
**reviewing** 6:12 10:11,16
**right** 4:19 12:12,25 13:1 16:9,18 16:23 19:24 20:25 24:4 26:16 29:13 31:25 32:16 32:21 34:7 37:2 45:14 52:23 53:23 54:2,19 64:5 67:18 68:12 70:25 79:12 79:17 80:9
**rights** 39:5,6 48:23 53:4 61:7 75:15
**ring** 69:6
**risk** 66:4
**RMR** 1:24 84:22 85:19
**Roberto** 14:2 15:14
**robust** 48:7 55:13
**roles** 53:4,6,9
**room** 44:16
**rooms** 44:14
**rough** 7:23
**roughly** 7:20 13:25
**RPR** 1:24 84:22 85:19
**Rule** 82:2
**rules** 4:11 82:3 84:5
**run** 40:22 42:15
**running** 18:23 48:14,18 66:15

**S**

**S** 82:1 84:1,1
**safe** 47:10
**safes** 47:7
**San** 2:9
**saved** 74:15
**saying** 31:5 68:12
**says** 29:20 31:13,21 32:13 33:8 35:13,20 44:10 51:18
**scan** 65:22
**scanning** 65:17
**scenario** 42:12
**scheme** 75:3
**science** 50:2
**scolding** 76:3 76:12
**scope** 49:9,24 51:15 55:10 56:20,23 57:25 59:20 61:3,22 62:13 63:10 64:19 66:9 66:22 73:17 74:22 76:15 76:24 78:11 78:21
**scratch** 21:21 52:16 64:15
**screen** 9:23
**se** 45:16
**second** 18:20 32:5 34:6,10 34:17,22,23
**secret** 39:7,10 39:15 42:13 42:16,21,22 74:1,5
**section** 27:6 32:11 45:4 49:11 51:17 52:18,19,22 53:24 54:1,3 65:16 66:8
**sections** 10:1 64:11,17,22
**secure** 24:22 27:3 35:14 35:21,25 36:9,16,20 36:22 37:5,8 37:12 47:21
**securely** 25:11
**secures** 34:21
**security** 3:9 11:2,11,23 12:4,6,7,21 12:25 13:4,8 13:10,13,15 13:17,18 14:1,5,5,6,7 14:9,10,11 14:13,14,19

15:1,13 17:2 17:5 21:17 21:19 22:10 25:21,23 26:2 27:22 27:25 37:16 37:16,23,25 38:4,8,10,10 38:12,18 44:9,10,11 44:12,17,18 45:2,7,12,17 46:8,15,18 46:25 47:16 47:25 48:2 48:12,13 49:3,12,14 49:23 50:18 50:21 51:7 53:1,2,11 54:5 61:17 61:20,21 62:8,11 63:5 66:7,7,14,18 66:19 67:23 69:25 70:11 71:14 72:2 72:11 73:14 74:11
**see** 16:9 17:17 32:7 34:15 37:20 39:5 46:1 49:12 49:21 51:2 59:11,13 60:2,7 61:17 64:12 65:23 68:22 79:17
**seeing** 32:9
**segments** 50:10
**selection** 27:2 27:10
**send** 39:20 42:2,19 59:8 60:22 63:7 63:21 70:6 80:9
**sender** 22:6,6
**sending** 18:6 63:14 70:20
**sends** 39:22
**sensitive** 21:9 49:16 61:6 61:11 74:15 74:21
**sensor** 25:9 35:18 36:1
**sent** 16:21 18:18 19:21 31:25 32:3 42:22,24 56:2 58:10 59:14 62:23
**sentence** 10:23 23:23 31:11 32:13 33:3,6,7,14 33:15
**separate** 5:22
**server** 43:13 43:13,14,16
**servers** 66:17 67:10
**service** 29:17 30:6,7,10,13 30:25 31:15 31:24 32:2 32:14,20 37:14 43:21 43:25 55:8 65:7
**services** 29:10 29:25 84:8 84:10,11,11 84:13,14,16
**session** 62:21 73:5
**sessions** 63:15
**set** 5:20,23 55:5 64:24 85:8
**setting** 65:19
**share** 15:19 42:13 74:1,5
**shared** 30:21 31:7 39:15 41:15
**shares** 58:23
**sharing** 37:18 50:5
**sheet** 82:12
**Shi** 2:5 3:4 4:6 4:7 16:4,14 16:25 17:19 17:22 18:18 18:22 19:20 20:16,19,22 22:14,21 23:6,8 24:8 28:5,10,12 29:13 31:10 33:3 34:5,19 36:12 37:15 38:20 40:18 44:7 46:7,18 47:3,15 50:17 51:17 54:10,13,16 54:18 55:20 57:18,22 58:16 60:9 61:10 62:6 63:4 64:2 65:12 66:6 66:18 67:11 67:15 73:21 75:5 76:22 77:11 78:18 78:25 79:4,7 79:12,14,19 79:21 81:3
**shoes** 7:16
**short** 26:2
**shorter** 24:22
**shorthand** 85:9,11
**show** 33:19
**showing** 33:23
**shown** 29:23 35:23
**shows** 24:24 34:1,16,22 45:25
**sic** 26:19 28:13 44:9
**sign** 10:11 42:1 56:8,9 57:3 58:5
**signature** 10:8 42:3,5 55:20 55:21 56:12 56:25 57:2,3 57:7,15,15 57:16,23 58:3,8 59:6 59:15 73:22 73:24 74:4 83:17
**signatures** 41:23 58:20 59:17
**signed** 15:20 42:5
**similar** 4:11 60:17 72:2
**simple** 51:18
**simply** 40:15
**single** 29:25 31:16 33:11 69:14
**sit** 6:16,19 7:11 20:8 41:9 43:4 61:15 69:6
**site** 29:16
**sites** 30:1,3
**sitting** 8:14 22:19 49:6
**size** 52:6
**skill** 7:17 27:21,24 31:20 33:25 35:3
**slippery** 63:11
**slope** 63:12
**smaller** 35:25
**Smith** 2:18 7:6 7:6,7
**social** 14:25 17:1,3 19:15 21:5,7,7,15 21:23 22:12 22:16,22,25 23:4,10 24:5 24:13,19,25 25:2,15,21 26:6,11,14 26:20 27:1 27:11,15,18 27:25 29:15 44:2 45:3,5,7 45:13,18,24 46:9,20 47:3 49:4 69:19 69:21 70:5 71:11,19
**software** 11:2 17:10 21:20 41:18,19 42:2,2 47:18 47:22 48:3 48:15 53:15 53:17,19 54:22 56:1,2 56:7,8,9,10 56:12,17,24 57:4,9,13,19 58:4,5,6,9,10

58:12,15 59:7,9,10,13 59:14 60:17 60:21 66:1 66:15
**solution** 22:25
**solutions** 22:16,22
**somebody** 21:17 40:11 40:16 43:21 45:8 55:14 70:19,23 72:17
**soon** 16:24
**sophomores** 13:6
**sorry** 14:16 17:16,22 18:9 20:21 46:3 64:15 75:24 76:11
**Sounds** 79:6
**source** 36:10 57:5
**Southern** 5:4
**space** 48:20 50:4,9 51:8 52:13
**speak** 6:5 23:11 68:20 69:2
**speaking** 24:21 61:4 61:23 64:6 74:12 77:10
**speaks** 32:4
**specific** 4:12 5:22 9:18 13:14 23:2,8 27:25 57:20 68:10 76:17 78:12,15
**specifically** 27:18 67:1 78:23
**specification** 26:22
**speculating** 7:24
**spend** 28:3
**spent** 7:21
**sphere** 72:1
**spoken** 79:22
**spread** 54:23 54:24
**stack** 14:7,8 64:23 66:25 67:3
**stands** 38:2
**start** 12:21 20:22
**started** 12:22
**starting** 31:11 35:11 64:25
**State** 84:2 85:2 85:4
**statement** 82:7
**states** 1:1 24:1 30:9 36:15
**steps** 33:18
**stick** 6:25
**storage** 29:17 30:6,7,10,13 30:25 31:14 31:24 32:2 32:14,19 33:9 34:21 35:14,22,24 35:25 36:16 37:14
**stored** 30:20 30:24 31:7 31:22 39:3
**Street** 2:19
**structures** 11:1,14,18 12:2
**student** 11:3 71:6 76:3
**students** 13:2 13:22 22:2 22:15
**studied** 7:14
**sub-concepts** 38:1
**subcompon...** 38:17
**submit** 16:10
**subscribed** 85:14
**substance** 82:5
**substantive** 10:18,18
**subterfuge** 17:6
**suggested** 32:17
**suite** 2:10,19 12:14
**supervision** 85:10
**supplemental** 82:10
**supporting** 69:8,9,12,13 69:14
**supports** 37:11
**sure** 5:25 11:8 25:4 28:19 33:8 41:16 41:18 55:15 65:16 68:11 69:23 72:13
**surprising** 13:19
**swapped** 50:13 51:5 51:10
**sworn** 4:1,3 85:7
**synchronize** 31:17 33:11
**synchronized** 30:12,16
**system** 14:5 18:3 21:19 24:23 25:8 26:11 28:21 34:2 38:13 38:20 43:7 43:22 47:15 47:17,19,20 47:22,24 48:2,4,5,7,9 48:14,16,18 49:3,12,14 49:19 51:23 52:3 53:5 54:9 61:8 70:1 72:20 73:6 76:7,14 76:17,18 77:19
**systems** 21:21 24:3 38:18 45:7 63:16 71:18

**T**

**T** 1:17 3:2 4:2 15:13 82:1,1 82:14 84:3 85:1,1
**T-A-M-A-S-S...** 14:2
**T-R-I-C-E-R-T** 70:2
**table** 3:8 15:22 16:5 19:21 20:2 37:17 37:22 44:8 48:11 61:19
**tactics** 19:15
**take** 16:15,19 28:6 40:22 42:14,21 43:12,16 54:12,13 59:7 67:12 78:25 79:2
**taken** 1:18 28:11 54:17 67:14 79:20 79:21 85:8,8 85:11
**talk** 7:9 17:3,5 25:24 36:20 47:6,7 65:3 65:10,17 69:18 70:14 76:4,10
**talked** 41:25 58:1,21 61:12 71:12 72:22 73:18 75:13,14,15 75:17,25 76:5,7,8 77:16,22 78:2
**talking** 7:10 28:12 30:15 54:19 56:22 57:16 66:13 68:5
**talks** 70:16
**Tamassia** 14:2 15:14
**tampered** 56:14
**taught** 10:25 11:6,10 12:3 12:5,13,17 13:4 14:20 14:22 15:11 15:11 21:6

24:23 37:5 66:8 71:14 71:23 72:2
**teach** 12:21 22:15 38:9,9 71:17
**teaches** 25:12 27:1
**teaching** 12:11 12:15,22 14:22,23 27:9
**Tech** 71:21
**technical** 6:25 22:16,21,25
**technically** 62:16 66:11
**technique** 24:5,19 25:20 27:8 50:7 56:17 58:13 62:7 70:17 73:10 73:14 77:17 77:23 78:3,5
**techniques** 21:17 22:12 26:13,18,24 27:14 50:18 51:7 64:2,4,9 72:10,14 75:11,19 76:1,10 77:11,12,13 77:17 78:8 78:14,18
**technologies** 23:3,8 72:7
**technology** 50:15 67:16 71:3 73:7,8,9
**tell** 20:23 22:2 73:16
**ten-minute** 28:6 54:13
**tend** 57:8
**tends** 57:13
**test** 20:5
**testified** 4:4
**testify** 85:7
**testimony** 4:22 79:25 82:6
**Texas** 2:11,20
**text** 11:18 12:2 12:9 37:21 39:24 52:1
**textbook** 12:6 13:17,20 14:1 15:3,10 15:12 19:10 19:13,18,25 20:7 21:1 71:13,14,16 71:22
**thank** 5:9,16 15:25 16:8 17:19 18:13 18:17 28:10 51:13 54:4 54:15,16 67:11 79:16 79:19 81:6
**thing** 32:8 70:12 73:13
**things** 9:23 17:5,11 22:5 38:9 44:25 47:12,14,18 53:8 55:1 56:22 57:11 60:17 64:6,7 66:17 78:24
**think** 5:5 13:12 45:16 46:11 46:14 60:24 67:12 73:13 74:17 78:23
**thinking** 7:16 21:12 61:14
**third-party** 29:17 45:23 45:25 60:16 60:23
**thought** 46:11 46:13 73:23
**threads** 48:14
**three** 38:1,6,16 38:20
**thwart** 45:18 46:9,14 53:11
**tied** 66:7
**time** 5:15 9:5 10:19 14:20 28:3 78:22 79:18 80:19 85:8
**title** 15:12
**titled** 61:16
**today** 4:13,19 4:23 5:1,17 6:16,19 7:11 8:1,15 9:9 20:8 22:20 41:9,22 43:4 49:6 56:9,23 56:25 57:17 58:13 59:16 59:22,23 60:11,20 61:4,14,15 61:24 62:10 63:12 64:1,9 66:4 69:6 73:19,20 74:13 75:14 75:19 76:11 76:20 78:1,6 79:9,11,22 80:5,16,18 80:23 81:1
**today's** 9:6
**told** 20:5
**tool** 39:13 40:4 40:9,10,20 42:10 43:20 48:5 60:14 61:5 80:13
**tools** 39:11 40:18 41:7 41:21,22 42:7 43:1,10 43:11,18,24 43:25 47:24 48:1,6 50:21 55:9,11 59:22 60:10 60:23 61:10
**top** 65:1 67:3
**topics** 12:5 13:14,21,24 14:3,24 15:3 15:4,11,23 17:4 20:2 21:4,5 72:3
**totality** 6:21
**TRADEMARK** 1:1
**transcript** 17:18 85:10
**transcription** 85:9
**transfer** 73:7,9
**transit** 39:23
**translation** 28:21 29:9 29:22
**translator** 28:23,25 29:8,12,18
**translators** 29:5
**transmission** 63:4,5 64:3
**transmitted** 39:3
**trends** 14:18
**TRIAL** 1:3
**TRICERT** 70:2 72:14
**trick** 17:7 21:8 21:11 22:11 26:5 70:9
**tricked** 21:14 45:8
**tricking** 21:17
**tried** 6:25 13:21 60:6
**true** 39:25 41:13 53:14 77:10 82:17 85:10
**truly** 74:2
**trust** 70:22
**trusted** 72:17
**truth** 85:7,7,7
**truthful** 4:22
**truthfully** 4:16 4:18
**try** 15:24 20:4 23:14 55:4 70:9
**trying** 22:13 43:22,23 48:8,10 51:1 53:11 65:6,7 70:23 79:10
**turn** 44:21
**turns** 66:10
**two** 7:21 8:5 16:19 39:15 42:12 43:2 51:25 64:22 73:25
**type** 39:7 55:24 57:2 57:20 58:21
**types** 19:15 53:8 59:1 62:1 64:12

71:11
**typical** 7:15
**typically** 24:2 26:8 48:20 62:18
**typos** 10:17

**U**

**U** 84:1
**U.S** 1:12,14 6:6
**UCI** 71:23
**ultimate** 53:16
**ultimately** 72:21
**unchanged** 41:12
**undergradu...** 10:25
**undergradu...** 13:5,24
**undersigned...** 82:14
**understand** 4:13,15 13:23 31:21 35:4
**understandi...** 5:19
**understood** 33:24
**unencrypted** 59:9 60:7 64:4,8
**unfortunately** 63:12
**UNITED** 1:1
**universities** 71:17
**University** 11:5 71:20 71:20,21
**unlock** 25:9 39:8 47:10
**unrelated** 68:7
**updates** 31:17 33:12
**upload** 15:21
**upper** 13:7
**usability** 14:4
**use** 17:5,6 18:3,4 21:7 24:24 25:5,6 26:2 30:13 37:9 40:1 41:22 50:7 58:17,17,24 59:3,4,18,22 62:2,19,20 63:8 64:7,8 67:6 73:3 75:19 76:11 77:25 78:6 78:14 80:12 82:9
**useful** 53:3
**user** 17:8 24:2 25:10 30:18 36:8,12,22 37:6 52:2 53:5 54:25 65:13
**users** 25:5 35:13 36:15 53:4
**uses** 25:1 45:10 58:25
**usual** 84:17
**usually** 26:7 55:2
**utilize** 72:9

**V**

**v** 1:8
**valid** 55:16 56:12 73:4
**value** 39:25 41:5 42:24
**variety** 24:10 29:6,23,25 45:13 65:10
**various** 31:11 31:14 33:9 62:1,10 64:9 65:22
**verification** 42:6
**verify** 22:3,6 42:4 73:2 74:6 75:7
**version** 60:7
**versus** 78:16
**victim** 70:7
**Videoconfer...** 1:22,25 2:5,6 2:7,17
**view** 19:1
**Virginia** 71:21
**virtual** 49:23 50:7,15,17 50:20 51:6 76:5
**virus** 41:17 55:25 56:5 56:15,24 58:12 63:19 70:8
**viruses** 57:8 57:14 58:14 63:14,25

**W**

**W** 2:6
**want** 5:7 16:12 28:3 34:15 41:16 43:7 48:25 51:3 52:15 53:7 53:17 55:15 60:20 77:7
**wants** 58:23
**way** 18:21 20:1 20:10,13 32:16 39:3 40:24 45:16 45:16 58:8 61:1 64:21 64:21 66:24 68:14 76:19 76:25 85:13
**ways** 22:11 58:19 62:14 63:13 70:5 70:13 73:1 78:15
**we'll** 39:16,19 42:1
**we're** 5:3,17 28:5 49:25 56:22 57:6 66:13 70:10 70:10
**we've** 54:10 67:23
**weak** 26:9
**web** 14:8 43:8 43:12,13,14 43:16,17 62:18 66:7 66:18
**website** 25:11 25:13,14,17 29:16 43:8 43:12 52:1 55:8 62:22 66:12,16 73:4
**websites** 21:12 22:3 34:14 66:14 67:6,8,9
**week** 8:22
**went** 13:20
**WHEREOF** 85:14
**wide** 24:10
**widely** 39:18 61:14
**wifi** 63:1
**wild** 5:4,7
**willing** 32:11
**window** 16:11
**wish** 10:18
**wishes** 39:20
**witness** 3:2 4:1 16:15,18 16:21 19:18 20:13 22:1 22:19 24:7 28:9 29:2 31:2 32:23 33:17 34:13 36:6 37:4 38:16 40:7 44:5 47:6 49:25 50:24 54:8 55:11 56:21 58:1 59:21 61:4 61:23 62:14 63:11 64:20 65:16 66:10 66:23 73:18 74:23 76:16 76:25 78:12 78:22 79:2,6 79:17 81:4 85:6,14
**wonderful** 51:13
**word** 57:7
**work** 11:3 15:8 55:23 62:12 68:19 69:1 69:22 72:6 79:4
**working** 60:18
**works** 73:25 79:1
**world** 69:21

71:1,4
**worm** 54:21,22 55:2,17
**worms** 55:9,12
**wouldn't** 45:15
**wrap** 79:14
**wrapped** 37:25
**writing** 53:20
**written** 71:13
**wrote** 13:19 59:7 64:21

**X**

**Y**

**yeah** 16:18 20:8,14 23:6 23:15,21 26:16 28:9 37:17 54:13 69:23 73:13 78:22 79:2 79:12,13
**year** 14:17
**years** 14:21
**yellow** 10:1
**yesterday** 4:11 8:24 9:7,8,23 68:6 72:22

**Z**

**zeros** 57:10
**Zoom** 1:22 15:22 18:15 18:23

**0**

**1**

**1** 3:8 15:3 16:1 16:2 27:6 28:16,18,19 29:15,20 32:4,25 33:2 33:5,15,17 33:24 34:5,9 34:11,13 35:2 37:12 44:7 61:17 61:19 80:9 80:16
**1.4** 54:1
**10,925** 6:7
**10,929,512** 1:12
**10.B** 84:5
**1006** 68:11
**1007** 68:21
**1008** 69:3
**1009** 69:15
**102** 29:7,14,23 30:6,9 31:23 32:1 35:1
**104** 29:10 30:9
**108** 29:10,24
**11,514,138** 1:14
**110** 29:25
**12:02** 1:20
**120** 29:16,25 30:1,5
**122** 29:16
**124** 29:17 30:1 30:1,5
**132** 29:8
**136** 29:18
**138** 5:18 23:13
**140** 29:17 30:6 30:7,11,14 30:25 31:15 31:24 32:2 32:14,20 33:9 37:14
**15** 6:8
**1500** 2:10
**16** 3:9
**1983** 11:4 12:12,15
**1990s** 12:19 12:23

**2**

**2** 29:4,19 44:10
**2000s** 12:23
**2011** 15:14
**2025** 1:19 83:20 85:14
**2037** 10:3
**2100** 2:19

**3**

**3** 29:3 34:18 34:19,20 35:1,7,9,10 35:21,22 52:19,22
**3.2** 48:11
**3.3** 49:11
**3.4** 51:17
**3.4.2** 51:18
**3:20** 79:5,18
**30(e)** 82:2
**300** 35:23
**302** 35:24
**303** 2:19
**304** 34:23 35:7 35:25 36:3 37:7
**306** 35:25
**308** 34:24 35:7 35:18 36:1 36:13,25
**310** 36:1
**33** 23:17,21,25 24:17
**34** 23:17
**35** 27:7
**37** 29:20

**4**

**4** 3:4 35:12 36:15 37:10 52:22 54:19
**4.1** 52:18 54:3
**4:24** 81:7
**44** 27:7
**45** 23:18

**5**

**5** 33:22 35:13 36:14 61:16 64:11,17 67:1
**5:00** 79:11,12 79:15
**51** 26:19 28:13 28:14
**512** 2:12,21 5:18 6:7 10:3 19:8 23:12 23:16,22 26:21,24 27:6,9,14,20 27:23 28:14 28:22 29:3 29:19 68:1
**56** 31:13 33:6 33:9

**6**

**6** 33:21 62:17 64:11,17 67:1
**6.4.4** 65:16
**60** 23:19 30:9
**62** 30:17
**66** 35:11,20
**692-8700** 2:21

**7**

**7** 30:8 31:14 33:6,21 66:8 66:14 67:7
**78701** 2:11,20

**8**

**8** 1:19 10:20 10:24
**867-8440** 2:12
**8th** 85:14

**9**

**9-11-28** 84:12
**9-11-30(e)** 82:4
**929,512** 6:7
**98** 2:9

EXHIBIT
1

INTRODUCTION TO

# Computer Security

Michael T. GOODRICH & Roberto TAMASSIA

*Editorial Director*: Marcia Horton
*Editor-in-Chief*: Michael Hirsch
*Acquisitions Editor*: Matt Goldstein
*Editorial Assistant*: Chelsea Bell
*Marketing Manager*: Yezan Alayan
*Marketing Coordinator*: Kathryn Ferranti
*Managing Editor*: Jeff Holcomb
*Senior Operations Supervisor*: Alan Fischer
*Art Director*: Linda Knowles
*Cover Designer*: Joyce Cosentino Wells
*Cover Photograph*: © Fotolia
*Media Editor*: Daniel Sandin
*Copyeditor*: Jeri Warner
*Proofreader*: Richard Camp
*Printer/Binder*: Edwards Brothers
*Cover Printer*: Lehigh-Phoenix Color/Hagerstown

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on pages iii and iv of this book.

Copyright © 2011 Michael T. Goodrich and Roberto Tamassia. All rights reserved. Manufactured in the United States of America. This publication is protected by Copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission(s) to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, 501 Boylston Street, Suite 900, Boston, Massachusetts 02116.

Many of the designations by manufacturers and seller to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed in initial caps or all caps.

**Library of Congress Cataloging-in-Publication Data**

Goodrich, Michael T.
Introduction to computer security / Michael T. Goodrich, Roberto Tamassia.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-321-51294-9 (alk. paper)
ISBN-10: 0-321-51294-4 (alk. paper)
1. Computer security. I. Tamassia, Roberto, 1960- II. Title.
QA76.9.A25G655 2011
005.8--dc22
2010028536

10 9 8 7 6 5 4 3 2 1—EB—14 13 12 11 10

# Contents


**1 Introduction** **1**

1.1 Fundamental Concepts . . . . . 2

1.1.1 Confidentiality, Integrity, and Availability . . . . . 3

1.1.2 Assurance, Authenticity, and Anonymity . . . . . 9

1.1.3 Threats and Attacks . . . . . 14

1.1.4 Security Principles . . . . . 15

1.2 Access Control Models . . . . . 19

1.2.1 Access Control Matrices . . . . . 19

1.2.2 Access Control Lists . . . . . 20

1.2.3 Capabilities . . . . . 22

1.2.4 Role-Based Access Control . . . . . 23

1.3 Cryptographic Concepts . . . . . 25

1.3.1 Encryption . . . . . 25

1.3.2 Digital Signatures . . . . . 31

1.3.3 Simple Attacks on Cryptosystems . . . . . 32

1.3.4 Cryptographic Hash Functions . . . . . 35

1.3.5 Digital Certificates . . . . . 37

1.4 Implementation and Usability Issues . . . . . 39

1.4.1 Efficiency and Usability . . . . . 39

1.4.2 Passwords . . . . . 41

1.4.3 Social Engineering . . . . . 43

1.4.4 Vulnerabilities from Programming Errors . . . . . 44

1.5 Exercises . . . . . 46

**2 Physical Security** **55**
2.1 Physical Protections and Attacks . . . . . 56
2.2 Locks and Safes . . . . . 57
2.2.1 Lock Technology . . . . . 57
2.2.2 Attacks on Locks and Safes . . . . . 62
2.2.3 The Mathematics of Lock Security . . . . . 68
2.3 Authentication Technologies . . . . . 71
2.3.1 Barcodes . . . . . 71
2.3.2 Magnetic Stripe Cards . . . . . 72
2.3.3 Smart Cards . . . . . 74
2.3.4 RFIDs . . . . . 79
2.3.5 Biometrics . . . . . 83
2.4 Direct Attacks Against Computers . . . . . 88
2.4.1 Environmental Attacks and Accidents . . . . . 88
2.4.2 Eavesdropping . . . . . 89
2.4.3 TEMPEST . . . . . 94
2.4.4 Live CDs . . . . . 96
2.4.5 Computer Forensics . . . . . 96
2.5 Special-Purpose Machines . . . . . 99
2.5.1 Automated Teller Machines . . . . . 99
2.5.2 Voting Machines . . . . . 101
2.6 Physical Intrusion Detection . . . . . 103
2.6.1 Video Monitoring . . . . . 103
2.6.2 Human Factors and Social Engineering . . . . . 105
2.7 Exercises . . . . . 106

**3 Operating Systems Security** **113**
3.1 Operating Systems Concepts . . . . . 114
3.1.1 The Kernel and Input/Output . . . . . 115
3.1.2 Processes . . . . . 116
3.1.3 The Filesystem . . . . . 121
3.1.4 Memory Management . . . . . 124
3.1.5 Virtual Machines . . . . . 128
3.2 Process Security . . . . . 130
3.2.1 Inductive Trust from Start to Finish . . . . . 130
3.2.2 Monitoring, Management, and Logging . . . . . 132
3.3 Memory and Filesystem Security . . . . . 136
3.3.1 Virtual Memory Security . . . . . 136
3.3.2 Password-Based Authentication . . . . . 137
3.3.3 Access Control and Advanced File Permissions . . . . 140
3.3.4 File Descriptors . . . . . 146
3.3.5 Symbolic Links and Shortcuts . . . . . 148

3.4 Application Program Security . . . . . 149
3.4.1 Compiling and Linking . . . . . 149
3.4.2 Simple Buffer Overflow Attacks . . . . . 150
3.4.3 Stack-Based Buffer Overflow . . . . . 152
3.4.4 Heap-Based Buffer Overflow Attacks . . . . . 159
3.4.5 Format String Attacks . . . . . 162
3.4.6 Race Conditions . . . . . 163
3.5 Exercises . . . . . 166

**4 Malware 173**
4.1 Insider Attacks . . . . . 174
4.1.1 Backdoors . . . . . 174
4.1.2 Logic Bombs . . . . . 177
4.1.3 Defenses Against Insider Attacks . . . . . 180
4.2 Computer Viruses . . . . . 181
4.2.1 Virus Classification . . . . . 182
4.2.2 Defenses Against Viruses . . . . . 185
4.2.3 Encrypted Viruses . . . . . 186
4.2.4 Polymorphic and Metamorphic Viruses . . . . . 187
4.3 Malware Attacks . . . . . 188
4.3.1 Trojan Horses . . . . . 188
4.3.2 Computer Worms . . . . . 190
4.3.3 Rootkits . . . . . 195
4.3.4 Zero-Day Attacks . . . . . 199
4.3.5 Botnets . . . . . 200
4.4 Privacy-Invasive Software . . . . . 202
4.4.1 Adware . . . . . 202
4.4.2 Spyware . . . . . 204
4.5 Countermeasures . . . . . 208
4.5.1 Best Practices . . . . . 208
4.5.2 The Impossibility of Detecting All Malware . . . . . 211
4.5.3 The Malware Detection Arms Race . . . . . 213
4.5.4 Economics of Malware . . . . . 214
4.6 Exercises . . . . . 215

**5 Network Security I 221**
5.1 Network Security Concepts . . . . . 222
5.1.1 Network Topology . . . . . 222
5.1.2 Internet Protocol Layers . . . . . 223
5.1.3 Network Security Issues . . . . . 227
5.2 The Link Layer . . . . . 229
5.2.1 Ethernet . . . . . 229

5.2.2 Media Access Control (MAC) Addresses . . . . . 232
5.2.3 ARP Spoofing . . . . . 233
5.3 The Network Layer . . . . . 236
5.3.1 IP . . . . . 236
5.3.2 Internet Control Message Protocol . . . . . 240
5.3.3 IP Spoofing . . . . . 242
5.3.4 Packet Sniffing . . . . . 244
5.4 The Transport Layer . . . . . 246
5.4.1 Transmission Control Protocol (TCP) . . . . . 246
5.4.2 User Datagram Protocol (UDP) . . . . . 250
5.4.3 Network Address Translation (NAT) . . . . . 251
5.4.4 TCP Session Hijacking . . . . . 253
5.5 Denial-of-Service Attacks . . . . . 256
5.5.1 ICMP Attacks . . . . . 256
5.5.2 SYN Flood Attacks . . . . . 258
5.5.3 Optimistic TCP ACK Attack . . . . . 260
5.5.4 Distributed Denial-of-Service . . . . . 261
5.5.5 IP Traceback . . . . . 262
5.6 Exercises . . . . . 264

**6 Network Security II 269**
6.1 The Application Layer and DNS . . . . . 270
6.1.1 A Sample of Application-Layer Protocols . . . . . 270
6.1.2 The Domain Name System (DNS) . . . . . 271
6.1.3 DNS Attacks . . . . . 278
6.1.4 DNSSEC . . . . . 285
6.2 Firewalls . . . . . 287
6.2.1 Firewall Policies . . . . . 288
6.2.2 Stateless and Stateful Firewalls . . . . . 289
6.3 Tunneling . . . . . 292
6.3.1 Secure Shell (SSH) . . . . . 293
6.3.2 IPsec . . . . . 294
6.3.3 Virtual Private Networking (VPN) . . . . . 297
6.4 Intrusion Detection . . . . . 299
6.4.1 Intrusion Detection Events . . . . . 302
6.4.2 Rule-Based Intrusion Detection . . . . . 305
6.4.3 Statistical Intrusion Detection . . . . . 306
6.4.4 Port Scanning . . . . . 308
6.4.5 Honeypots . . . . . 312
6.5 Wireless Networking . . . . . 313
6.5.1 Wireless Technologies . . . . . 314
6.5.2 Wired Equivalent Privacy (WEP) . . . . . 315

6.5.3 Wi-Fi Protected Access (WPA) . . . . . 318
6.6 Exercises . . . . . 322

**7 Web Security 327**
7.1 The World Wide Web . . . . . 328
7.1.1 HTTP and HTML . . . . . 328
7.1.2 HTTPS . . . . . 334
7.1.3 Dynamic Content . . . . . 339
7.1.4 Sessions and Cookies . . . . . 342
7.2 Attacks on Clients . . . . . 347
7.2.1 Session Hijacking . . . . . 347
7.2.2 Phishing . . . . . 349
7.2.3 Click-Jacking . . . . . 351
7.2.4 Vulnerabilities in Media Content . . . . . 352
7.2.5 Privacy Attacks . . . . . 356
7.2.6 Cross-Site Scripting (XSS) . . . . . 357
7.2.7 Cross-Site Request Forgery (CSRF) . . . . . 364
7.2.8 Defenses Against Client-Side Attacks . . . . . 366
7.3 Attacks on Servers . . . . . 368
7.3.1 Server-Side Scripting . . . . . 368
7.3.2 Server-Side Script Inclusion Vulnerabilities . . . . . 370
7.3.3 Databases and SQL Injection Attacks . . . . . 372
7.3.4 Denial-of-Service Attacks . . . . . 378
7.3.5 Web Server Privileges . . . . . 379
7.3.6 Defenses Against Server-Side Attacks . . . . . 380
7.4 Exercises . . . . . 382

**8 Cryptography 387**
8.1 Symmetric Cryptography . . . . . 388
8.1.1 Attacks . . . . . 389
8.1.2 Substitution Ciphers . . . . . 391
8.1.3 One-Time Pads . . . . . 393
8.1.4 Pseudo-Random Number Generators . . . . . 395
8.1.5 The Hill Cipher and Transposition Ciphers . . . . . 397
8.1.6 The Advanced Encryption Standard (AES) . . . . . 399
8.1.7 Modes of Operation . . . . . 402
8.2 Public-Key Cryptography . . . . . 406
8.2.1 Modular Arithmetic . . . . . 406
8.2.2 The RSA Cryptosystem . . . . . 410
8.2.3 The Elgamal Cryptosystem . . . . . 413
8.2.4 Key Exchange . . . . . 415
8.3 Cryptographic Hash Functions . . . . . 417

6.5.3 Wi-Fi Protected Access (WPA) . . . . . 318
6.6 Exercises . . . . . 322

**7 Web Security 327**
7.1 The World Wide Web . . . . . 328
7.1.1 HTTP and HTML . . . . . 328
7.1.2 HTTPS . . . . . 334
7.1.3 Dynamic Content . . . . . 339
7.1.4 Sessions and Cookies . . . . . 342
7.2 Attacks on Clients . . . . . 347
7.2.1 Session Hijacking . . . . . 347
7.2.2 Phishing . . . . . 349
7.2.3 Click-Jacking . . . . . 351
7.2.4 Vulnerabilities in Media Content . . . . . 352
7.2.5 Privacy Attacks . . . . . 356
7.2.6 Cross-Site Scripting (XSS) . . . . . 357
7.2.7 Cross-Site Request Forgery (CSRF) . . . . . 364
7.2.8 Defenses Against Client-Side Attacks . . . . . 366
7.3 Attacks on Servers . . . . . 368
7.3.1 Server-Side Scripting . . . . . 368
7.3.2 Server-Side Script Inclusion Vulnerabilities . . . . . 370
7.3.3 Databases and SQL Injection Attacks . . . . . 372
7.3.4 Denial-of-Service Attacks . . . . . 378
7.3.5 Web Server Privileges . . . . . 379
7.3.6 Defenses Against Server-Side Attacks . . . . . 380
7.4 Exercises . . . . . 382

**8 Cryptography 387**
8.1 Symmetric Cryptography . . . . . 388
8.1.1 Attacks . . . . . 389
8.1.2 Substitution Ciphers . . . . . 391
8.1.3 One-Time Pads . . . . . 393
8.1.4 Pseudo-Random Number Generators . . . . . 395
8.1.5 The Hill Cipher and Transposition Ciphers . . . . . 397
8.1.6 The Advanced Encryption Standard (AES) . . . . . 399
8.1.7 Modes of Operation . . . . . 402
8.2 Public-Key Cryptography . . . . . 406
8.2.1 Modular Arithmetic . . . . . 406
8.2.2 The RSA Cryptosystem . . . . . 410
8.2.3 The Elgamal Cryptosystem . . . . . 413
8.2.4 Key Exchange . . . . . 415
8.3 Cryptographic Hash Functions . . . . . 417

8.3.1 Properties and Applications . . . . . 417
8.3.2 Birthday Attacks . . . . . 419
8.4 Digital Signatures . . . . . 421
8.4.1 The RSA Signature Scheme . . . . . 422
8.4.2 The Elgamal Signature Scheme . . . . . 423
8.4.3 Using Hash Functions with Digital Signatures . . . . . 424
8.5 Details of AES and RSA Cryptography . . . . . 425
8.5.1 Details for AES . . . . . 425
8.5.2 Details for RSA . . . . . 431
8.6 Exercises . . . . . 439

**9 Security Models and Practice 445**
9.1 Policy, Models, and Trust . . . . . 446
9.1.1 Security Policy . . . . . 446
9.1.2 Security Models . . . . . 447
9.1.3 Trust Management . . . . . 448
9.2 Access-Control Models . . . . . 450
9.2.1 The Bell-La Padula Model . . . . . 450
9.2.2 Other Access-Control Models . . . . . 454
9.2.3 Role-Based Access Control . . . . . 456
9.3 Security Standards and Evaluation . . . . . 460
9.3.1 Orange Book and Common Criteria . . . . . 460
9.3.2 Government Regulations and Standards . . . . . 462
9.4 Software Vulnerability Assessment . . . . . 464
9.4.1 Static and Dynamic Analysis . . . . . 465
9.4.2 Exploit Development and Vulnerability Disclosure . . . 468
9.5 Administration and Auditing . . . . . 470
9.5.1 System Administration . . . . . 470
9.5.2 Network Auditing and Penetration Testing . . . . . 473
9.6 Kerberos . . . . . 475
9.6.1 Kerberos Tickets and Servers . . . . . 475
9.6.2 Kerberos Authentication . . . . . 476
9.7 Secure Storage . . . . . 479
9.7.1 File Encryption . . . . . 479
9.7.2 Disk Encryption . . . . . 481
9.7.3 Trusted Platform Module . . . . . 482
9.8 Exercises . . . . . 484

**10 Distributed-Applications Security 487**
10.1 Database Security . . . . . 488
10.1.1 Tables and Queries . . . . . 489
10.1.2 Updates and the Two-Phase Commit Protocol . . . . . 491

10.1.3 Database Access Control . . . . . 493
10.1.4 Sensitive Data . . . . . 497
10.2 Email Security . . . . . 500
10.2.1 How Email Works . . . . . 500
10.2.2 Encryption and Authentication . . . . . 502
10.2.3 Spam . . . . . 507
10.3 Payment Systems and Auctions . . . . . 513
10.3.1 Credit Cards . . . . . 513
10.3.2 Digital Cash . . . . . 516
10.3.3 Online Auctions . . . . . 518
10.4 Digital-Rights Management . . . . . 519
10.4.1 Digital-Media Rights Techniques . . . . . 520
10.4.2 Digital-Media Rights Practice . . . . . 523
10.4.3 Software Licensing Schemes . . . . . 525
10.4.4 Legal Issues . . . . . 527
10.5 Social Networking . . . . . 528
10.5.1 Social Networks as Attack Vectors . . . . . 528
10.5.2 Privacy . . . . . 529
10.6 Voting Systems . . . . . 531
10.6.1 Security Goals . . . . . 531
10.6.2 ThreeBallot . . . . . 532
10.7 Exercises . . . . . 535