DECLARATION OF JUNE ANN MUNFORD

1. My name is June Ann Munford. I am over the age of 18, have personal knowledge of the facts set forth herein, and am competent to testify to the same.

2. I earned a Master of Library and Information Science (MLIS) from the University of Wisconsin-Milwaukee in 2009. I have over ten years of experience in the library/information science field. Beginning in 2004, I have served in various positions in the public library sector including Assistant Librarian, Youth Services Librarian and Library Director. I have attached my Curriculum Vitae as Appendix CV.

3. During my career in the library profession, I have been responsible for materials acquisition for multiple libraries. In that position, I have cataloged, purchased and processed incoming library works. That includes purchasing materials directly from vendors, recording publishing data from the material in question, creating detailed material records for library catalogs and physically preparing that material for circulation. In addition to my experience in acquisitions, I was also responsible for analyzing large collections of library materials, tailoring library records for optimal catalog

search performance and creating lending agreements between libraries during my time as a Library Director.

4. I am fully familiar with the catalog record creation process in the library sector. In preparing a material for public availability, a library catalog record describing that material would be created. These records are typically written in Machine Readable Catalog (herein referred to as “MARC”) code and contain information such as a physical description of the material, metadata from the material’s publisher, and date of library acquisition. In particular, the 008 field of the MARC record is reserved for denoting the date of creation of the library record itself. As this typically occurs during the process of preparing materials for public access, it is my experience that an item’s MARC record indicates the date of an item’s public availability.

5. Typically, in creating a MARC record, a librarian would gather various bits of metadata such as book title, publisher and subject headings among others and assign each value to a relevant numerical field. For example, a book’s physical description is tracked in field 300 while title/attribution is tracked in field 245. The 008 field of the MARC record is reserved for denoting the creation of the library record itself. As this is the only date reflecting the inclusion of said materials within the library’s collection, it is my experience

that an item's 008 field accurately indicates the date of an item's public availability.

6. I have reviewed Exhibit 1010, *Security Engineering: A Guide to Building Dependable Distributed Systems* by Ross Anderson, 2nd edition (2008).

7. Attached hereto as Appendix ANDERSON01 is a true and correct copy of the MARC record for *Security Engineering: A Guide to Building Dependable Distributed Systems* as held by the Western Michigan University library. I secured this record myself from the library's public catalog. The MARC record contained within Appendix ANDERSON01 accurately describes the title, author, publisher, and ISBN number of *Security Engineering: A Guide to Building Dependable Distributed Systems.*

8. Attached hereto as Appendix ANDERSON02 is a true and correct copy of selections from *Security Engineering: A Guide to Building Dependable Distributed Systems* as held by the Western Michigan University library. These scans were secured from the library's collection. In comparing Exhibit 1010 to Appendix ANDERSON02, it is my determination that Exhibit 1010 is a true and correct copy of *Security Engineering: A Guide to Building Dependable Distributed Systems* by Ross Anderson.

9. The 008 field of the MARC record in Appendix ANDERSON01 indicates the date of record creation. The 008 field of Appendix ANDERSON01 indicates Western Michigan University library first acquired this book as of April 15, 2008. Considering this information, it is my determination that *Security Engineering: A Guide to Building Dependable Distributed Systems* was made available to the public shortly after its initial acquisition in April 15, 2008.

10. I have been retained on behalf of the Petitioner to provide assistance in the above-illustrated matter in establishing the authenticity and public availability of the documents discussed in this declaration. I am being compensated for my services in this matter at the rate of $200.00 per hour plus reasonable expenses. My statements are objective, and my compensation does not depend on the outcome of this matter.

11. I declare under penalty of perjury that the foregoing is true and correct. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made the knowledge that willful false statements and the like so made are punishable by fine or

imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: 9/19/2023



June Ann Munford

APPENDIX CV

June A. Munford
Curriculum Vitae

Education

University of Wisconsin-Milwaukee - MS, Library & Information Science, 2009
Milwaukee, WI

- Coursework included cataloging, metadata, data analysis, library systems, management strategies and collection development.
- Specialized in library advocacy, cataloging and public administration.

Grand Valley State University - BA, English Language & Literature, 2008
Allendale, MI

- Coursework included linguistics, documentation and literary analysis.
- Minor in political science with a focus in local-level economics and government.

Professional Experience

Researcher / Expert Witness, October 2017 – present
Freelance ● Pittsburgh, Pennsylvania & Grand Rapids, Michigan

- Material authentication and public accessibility determination. Declarations of authenticity and/or public accessibility provided upon research completion. Experienced with appeals and deposition process.

- Research provided on topics of public library operations, material publication history, digital database services and legacy web resources.

- Past clients include Alston & Bird, Arnold & Porter, Baker Botts, Fish & Richardson, Erise IP, Irell & Manella, O'Melveny & Myers, Perkins-Coie, Pillsbury Winthrop Shaw Pittman and Slayden Grubert Beard.

Library Director, February 2013 - March 2015
Dowagiac District Library ● Dowagiac, Michigan

- Executive administrator of the Dowagiac District Library. Located in

Southwest Michigan, this library has a service area of 13,000, an annual operating budget of over $400,000 and total assets of approximately $1,300,000.

● Developed careful budgeting guidelines to produce a 15% surplus during the 2013-2014 & 2014-2015 fiscal years while being audited.

● Using this budget surplus, oversaw significant library investments including the purchase of property for a future building site, demolition of existing buildings and building renovation projects on the current facility.

● Led the organization and digitization of the library's archival records.

● Served as the public representative for the library, developing business relationships with local school, museum and tribal government entities.

● Developed an objective-based analysis system for measuring library services - including a full collection analysis of the library's 50,000+ circulating items and their records.

November 2010 - January 2013
Librarian & Branch Manager, Anchorage Public Library ● Anchorage, Alaska

● Headed the 2013 Anchorage Reads community reading campaign including event planning, staging public performances and creating marketing materials for mass distribution.

● Co-led the social media department of the library's marketing team, drafting social media guidelines, creating original content and instituting long-term planning via content calendars.

● Developed business relationships with The Boys & Girls Club, Anchorage School District and the US Army to establish summer reading programs for children.

June 2004 - September 2005, September 2006 - October 2013
Library Assistant, Hart Area Public Library
Hart, MI

● Responsible for verifying imported MARC records and original MARC

cataloging for the local-level collection as well as the Michigan Electronic Library.

● Handled OCLC Worldcat interlibrary loan requests & fulfillment via ongoing communication with lending libraries.

Professional Involvement

Alaska Library Association - Anchorage Chapter
- Treasurer, 2012

Library Of Michigan
- Level VII Certification, 2008
- Level II Certification, 2013

Michigan Library Association Annual Conference 2014
- New Directors Conference Panel Member

Southwest Michigan Library Cooperative
- Represented the Dowagiac District Library, 2013-2015

Professional Development

Library Of Michigan Beginning Workshop, May 2008
Petoskey, MI
- Received training in cataloging, local history, collection management, children's literacy and reference service.

Public Library Association Intensive Library Management Training, October 2011
Nashville, TN
- Attended a five-day workshop focused on strategic planning, staff management, statistical analysis, collections and cataloging theory.

Alaska Library Association Annual Conference 2012 - Fairbanks, February 2012
Fairbanks, AK
- Attended seminars on EBSCO advanced search methods, budgeting, cataloging, database usage and marketing.

Depositions

2019 ● Fish & Richardson

Apple v. Qualcomm (IPR2018-001281, 39521-00421IP, IPR2018-01282 and 39521-00421IP2)

2019 ● Erise IP

Implicit, LLC v. Netscout Systems, Inc (Civil Action No. 2:18-cv-53-JRG)

2019 ● Perkins-Coie

Adobe Inc. v. RAH Color Technologies LLC (Cases IPR2019-00627, IPR2019-00628, IPR2019-00629 and IPR2019-00646)

2020 ● O'Melveny & Myers

Maxell, Ltd. v. Apple Inc. (Case No. 5:19-cv-00036-RWS)

2021 ● Pillsbury Winthrop Shaw Pittman LLP

Intel v. SRC (IPR2020-1449)

2022 ● Perkins-Coie

Realtek v. Future Link (IPR2021-01182)

2023 ● Fish & Richardson

Neuroderm Ltd. v. Abbvie, Inc (Case No. PGR2022-00040)

2023 ● Fish & Richardson

Nearmap US Inc. v. Pictometry International Corp. (IPR2022-00735)

2023 ● Fish & Richardson

Samsung Electronics v. MemoryWeb LLC (Case No. 39843-0136PS1)

Limited Case History & Potential Conflicts

Alston & Bird

- Ericsson

  v. Collision Communications (IPR2022-01233)

- Nokia

  v. Neptune Subsea, Xtera (Case No. 1:17-cv-01876)

- Universal Electronics Inc

  v. Roku Inc (IPR2022-00818)

Arnold & Porter

- Ivantis

  v. Glaukos (Case No. 8:18-cv-00620)

- Samsung

  v. Jawbone (Case No. 2:21-cv-00186)

Benesch Friedlander Coplan & Aronoff

- Voyis

  v. Cathx (Case No. 5:21-cv-00077-RWS)

Erise I.P.

- Apple

  v. Ericsson Inc. (IPR2022-00715)

v. Future Link Systems (IPRs 6317804, 6622108, 6807505, and 7917680)

v. INVT (Case No. 20-1881)

v. Navblazer LLC (IPR2020-01253)

v. Qualcomm (IPR2018-001281, 39521-00421IP, IPR2018-01282, 39521-00421IP2)

v. Quest Nettech Corp (Case No. 2:19-cv-00118-JRG)

v. Telefonaktiebolaget LM Ericsson (IPR2022-00275)

- Fanduel

  v. CGT (Case No. 19-1393)

- Garmin

  v. Phillips North America LLC (Case No. 2:19-cv-6301-AB-KS)

- Netscout

  v. Longhorn HD LLC (Case No. 2:20-cv-00349)

  v. Implicit, LLC (Civil Action No. 2:18-cv-53-JRG)

- Sony Interactive Entertainment LLC

  v. Bot M8 LLC (IPR2020-01288)

  v. Infernal Technology LLC (Case No. 2:19-CV-00248-JRG)

- Unified Patents

  v. GE Video Compression (Civil Action No. 2:19-cv-248)

Fish & Richardson

- Apple

v. AliveCor (3:21-cv-03958)

v. LBS Innovations (Case No. 2:19-cv-00119-JRG-RSP)

v. Koss Corporation (IPR2021-00305)

v. Masimo (IPR 50095-0012IP1, 50095-0012IP2, 50095-0013IP1, 50095-0013IP2, 50095-0006IP1, 50095-0135IP1)

v. Neonode (Case No. 21-cv-08872-EMC)

v. Qualcomm (IPR2018-001281, 39521-00421IP, IPR2018-01282, 39521-00421IP2)

- Dell

  v. Neo Wireless (IPR2022-00616)

- Dish Network

  v. Realtime Adaptive Streaming (Case No. 1:17-CV-02097-RBJ)

  v. TQ Delta LLC (Case No. 18-1798)

- Evapco Dry Cooling

  v. SPG Dry Cooling (IPR2021-00688)

- Genetec

  v. Sensormatic Electronics (Case No. 1:20-CV-00760)

- Huawei

  v. Bell Northern Research LLC (IPR2019-01174)

- Kianxis

  v. Blue Yonder (Case No. 3:20-cv-03636)

- LG Electronics
  - v. Bell Northern Research LLC (Case No. 3:18-cv-2864-CAB-BLM)

- Metaswitch
  - v. Sonus Networks (IPR2018-01719)

- Microsoft
  - v. Throughputer Inc (IPR2022-00757)

- MLC Intellectual Property
  - v. MicronTech (Case No. 3:14-cv-03657-SI)

- Nearmap Inc
  - v. EagleView Technologies (IPR2022-01009)

- Neuroderm Ltd.
  - v. Abbvie, Inc (Case No. PGR2022-00040)

- Realtek Semiconductor
  - v. Future Link (IPR2021-01182)

- Quectel
  - v. Koninklijke Philips (Case No. 1:20-cv-01710)

- Samsung
  - v. Aire Technology (IPR2022-00877)
  - v. Bell Northern Research (Case No. 2:19-cv-00286-JRG)
  - v. Communication Technologies Inc (IPR2022-01221)

v. Jawbone Innovations (IPR2022-00865)

v. MemoryWeb LLC (IPR2022-00885)

v. Telefonaktiebolaget LM Ericsson (IPR2021-00615)

- Texas Instruments

  v. Vantage Micro LLC (IPR2020-01261)

- Xilinx

  v. Sentient Sensors LCC (Case No. 1:22-cv-00173)

Irell & Manella

- Curium

O'Melveny & Myers

- Apple

  v. Maxell (Case No. 5:19-cv-00036-RWS)

- Samsung

  v. Daedalus Prime LLC (1335 Investigation)

Perkins-Coie

- Heru Industries

  v. The UAB Research Foundation (IPR2022-01148)

- Intel Corporation

  v. BitMICRO (Case No. 5:23-cv-00625)

- Realtek Semiconductor

  v. Future Link (IPR2021-01182)

- Twitter Inc

  v. VOIP-Pal.com (Case No. 3:20-cv-02397-JD)

- TCL Industries

  v. Koninklijke Philips NV (IPR2021-00495, IPR2021-00496 and IPR2021-00497)

Pillsbury Winthrop Shaw Pittman

- Intel

  v. FG SRC LLC (Case No. 6:20-cv-00315)

- Gravel Rating Systems

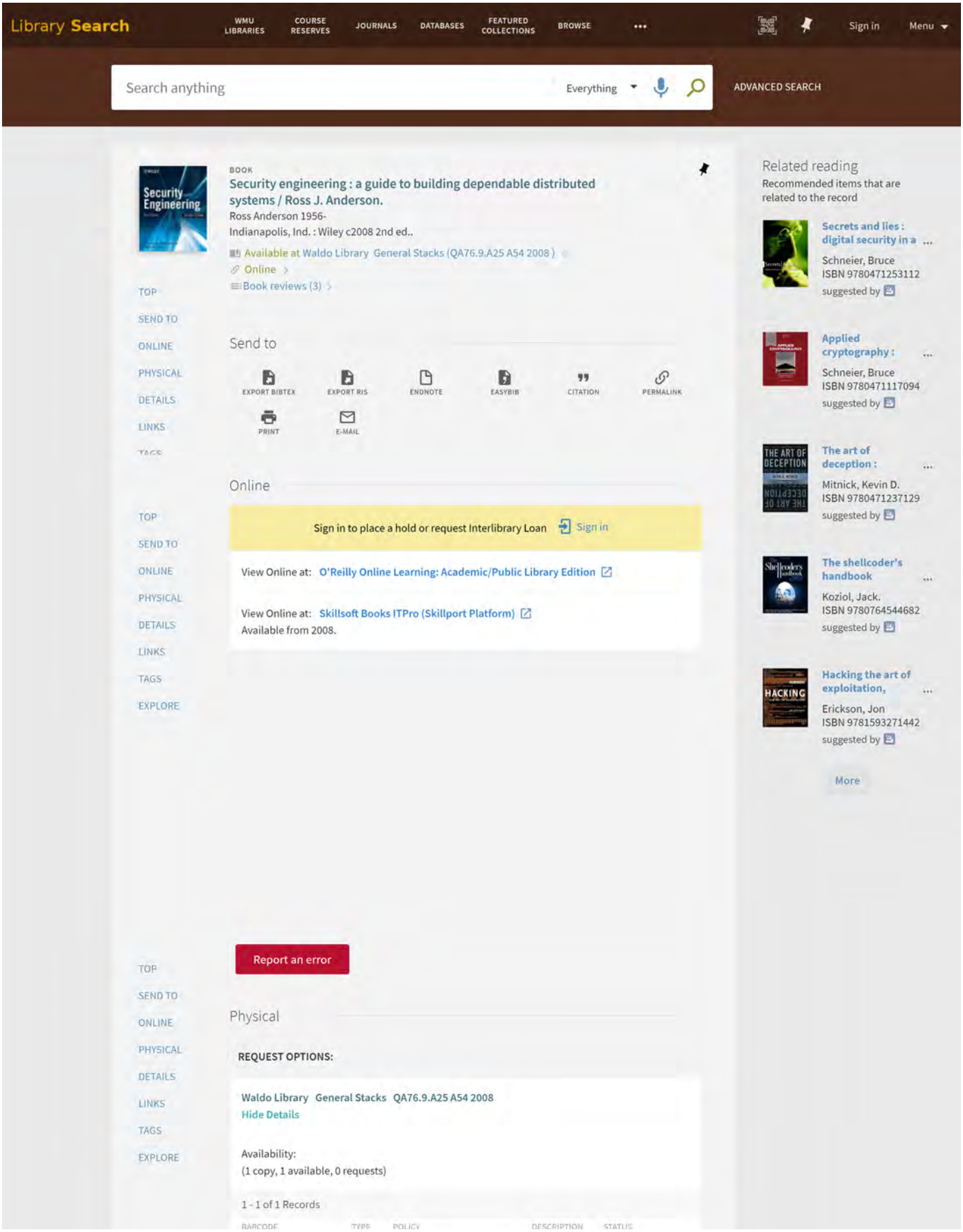
  v. Costco (Case No. 4:21-cv-149)
  v. Lowe's Home Centers (Case No. 4:21-cv-150)
  v. T-Mobile USA (Case No. 4:21-cv-152)
  v. Kohl's Inc. (Case No. 4:21-cv-258)
  v. Under Armor (Case No. 4:21-cv-356)

APPENDIX ANDERSON01

screenshot-primo-pmtna01.hosted.exlibrisgroup.com-2023.09.11-14_51_29
https://primo-pmtna01.hosted.exlibrisgroup.com/primo-explore/sourceRecord?vid=01WMU&docId=dedupmrg2738221330
11.09.2023

```
Leader 01575cam a2200445Ia 4500
001    9919997043802436
005    20160317101458.0
008    080415s2008    inua     b    001 0 eng
010    ##$a  2008006392
019    ##$a154798563
020    ##$a9780470068526 (cloth)
020    ##$a0470068523 (cloth)
029    1#$aNLGGC$b309703875
035    ##$a(OCoLC)ocn192045774
035    ##$a(MiKW)1999704-wmichdb
035    ##$z(OCoLC)154798563
040    ##$aDLC$cDLC$dBAKER$dBTCTA$dYDXCP$dC#P$dUtOrBLW
049    ##$aEXWZ
050    00$aQA76.9.A25$bA54 2008
082    00$a005.1$222
100    1#$aAnderson, Ross,$d1956-$0http://id.loc.gov/authorities/names/n94047247$0http://viaf.org/viaf/sourceID/LC|n94047247
245    10$aSecurity engineering :$ba guide to building dependable distributed systems /$cRoss J. Anderson.
250    ##$a2nd ed.
264    #1$aIndianapolis, Ind. :$bWiley Pub.,$c[2008]
264    #4$c©2008
300    ##$axl, 1040 pages :$billustrations ;$c25 cm
336    ##$atext$btxt$2rdacontent
337    ##$aunmediated$bn$2rdamedia
338    ##$avolume$bnc$2rdacarrier
504    ##$aIncludes bibliographical references (pages 893-996) and index.
650    #0$aComputer security.$0http://id.loc.gov/authorities/subjects/sh90001862
650    #0$aElectronic data processing$xDistributed processing.$0http://id.loc.gov/authorities/subjects/sh85042293
856    42$3Publisher description$uhttp://www.loc.gov/catdir/enhancements/fy0827/2008006392-d.html
856    41$3Table of contents only$uhttp://www.loc.gov/catdir/enhancements/fy0827/2008006392-t.html
910    ##$aMARS
948    ##$a2008;07;30$bpln$cL
960    ##$o1$q06-20-08$s70.00$tbnapcatfor$uBISf$zUSD
980    ##$e58.88$f11263211$g1
981    ##$aBISf$bbnapcatfor
994    ##$aC0$bEXW
AVA    ##$0991999704380243 6$822115923110002436$a01WMU_INST$bwaldo$cGeneral Stacks$dQA76.9.A25 A54 2008$eavailable$f1$g0$jgeneral$k0$p1$qWaldo Library
CAT    ##$aEngineering_Applied_Sciences$bComputer_Science
INST   ##$a01WMU_INST
INT    ##$aP
PLK    ##$aAdditional Form.$b99509306551102436$mSecurity engineering :$ea guide to building dependable distributed systems /$fRoss J. Anderson.
```

screenshot-primo-pmtna01.hosted.exlibrisgroup.com-2023.09.11-14_53_50
https://primo-pmtna01.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=01WMU_ALMA51183983860002436&vid=01WMU&search_scope=EVERYTHING&tab=default_tab&context=L
11.09.2023



31141018498084	Book	Sign in for availability	Item in place

TOP
SEND TO
ONLINE
PHYSICAL
DETAILS
LINKS
TAGS
EXPLORE

Details

Title	Security engineering : a guide to building dependable distributed systems / Ross J. Anderson.
Author	Ross Anderson 1956-
Subjects	Computer security Electronic data processing -- Distributed processing
Description	What is security engineering? -- Usability and psychology -- Protocols -- Access control -- Cryptography -- Distributed systems -- Economics -- Multilevel security -- Multilateral security -- Banking and bookkeeping -- Physical protection -- Monitoring and metering -- Nuclear command and control -- Security printing and seals -- Biometrics -- Physical tamper resistance -- Emission security -- API attacks -- Electronic and information warfare -- Telecom system security -- Network attack and defense -- Copyright and DRM -- The bleeding edge -- Terror, justice and freedom -- Managing the development of secure systems -- System evaluation and assurance. The world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here?s straight talk on critical topics such as technical engineering basics, types of attack, specialized protection mechanisms, security psychology, policy, and more.
Publisher	Indianapolis, Ind. : Wiley
Publication Date	c2008
Format	xi, 1040p. : ill..
Language	English
Identifier	ISBN : 1-118-00836-7 ISBN : 1-282-82294-2 ISBN : 9786612822940 ISBN : 1-118-00838-3
Source	Library Catalog Library Catalog
Alma MMS ID	99509306551102436 9919997043802436

TOP
SEND TO
ONLINE
PHYSICAL
DETAILS
LINKS
TAGS
EXPLORE

Links

Table of contents only
Click for more information on this title (from Syndetics)
Get this for me in MELCAT
Publisher description
This item in WorldCat®
Display Source Record

Tags

ADD YOUR OWN TAGS

Explore Syndetics Unbound

Summary | About The Author | Librarian Lists | Reader Reviews
Also Available As | Tags | Browse Shelf

SUMMARY

The world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced (read more)

TOP
SEND TO
ONLINE
PHYSICAL
DETAILS
LINKS
TAGS

ABOUT THE AUTHOR



Ross J. Anderson

Ross Anderson is Professor of Security Engineering at Cambridge University and a pioneer of security economics. Widely recognized as one of the world's

foremost authorities on security, he has published many studies of how real security systems fail and made trailblazing contributions to numerous technologies from peer-to-peer systems and API analysis through hardware security.

More by Ross J. Anderson



LIBRARIAN RECOMMENDS

Related Lists



Technology
by Unbound Trends

SEE MORE LISTS

READER REVIEWS

★★★★½ Reviewed by 3 people

Wow! This is one of the most comprehensive books on security (particularly computer security) that I've ever read! Anderson takes the reader on a journey across all the different distributed systems we now take for granted, and explains in very clear language, how each and every single on is flawed, and in some cases, even shows the flaws. While this is a pretty thick tome, it's right (read more)

Review by aethercowboy (LibraryThing) ★★★★

What do you think? Write your own review

This is an updating of Anderson's previous work, which was a standard for the field (it can be obtain in PDF for free on-line). I highly recommend it for those into security. The discipline and thorough treatment of a wide breath of areas that Anderson provides is just what a true security professional needs.

Review by ittai (LibraryThing) ★★★★★

SEE MORE REVIEWS

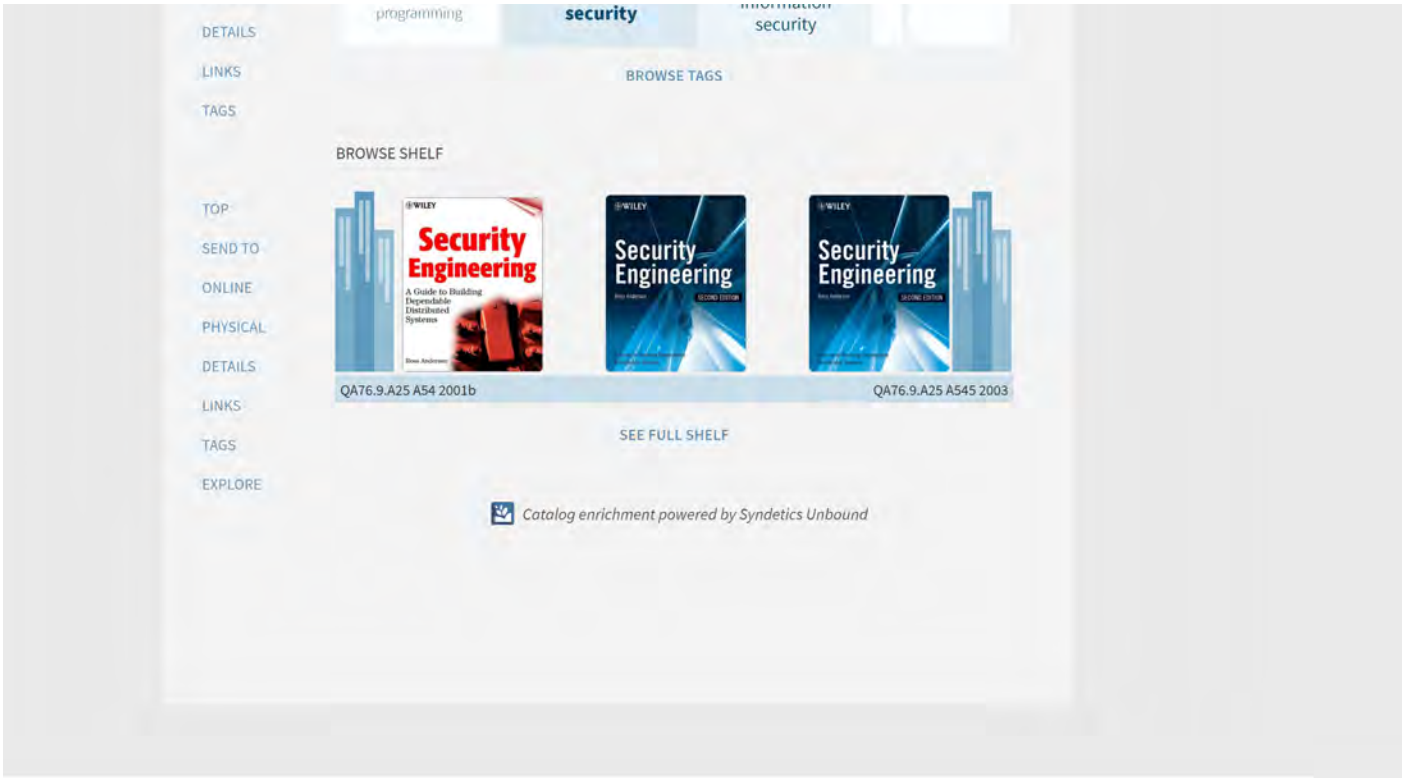
ALSO AVAILABLE AS



Paper Book Paper Book Ebook

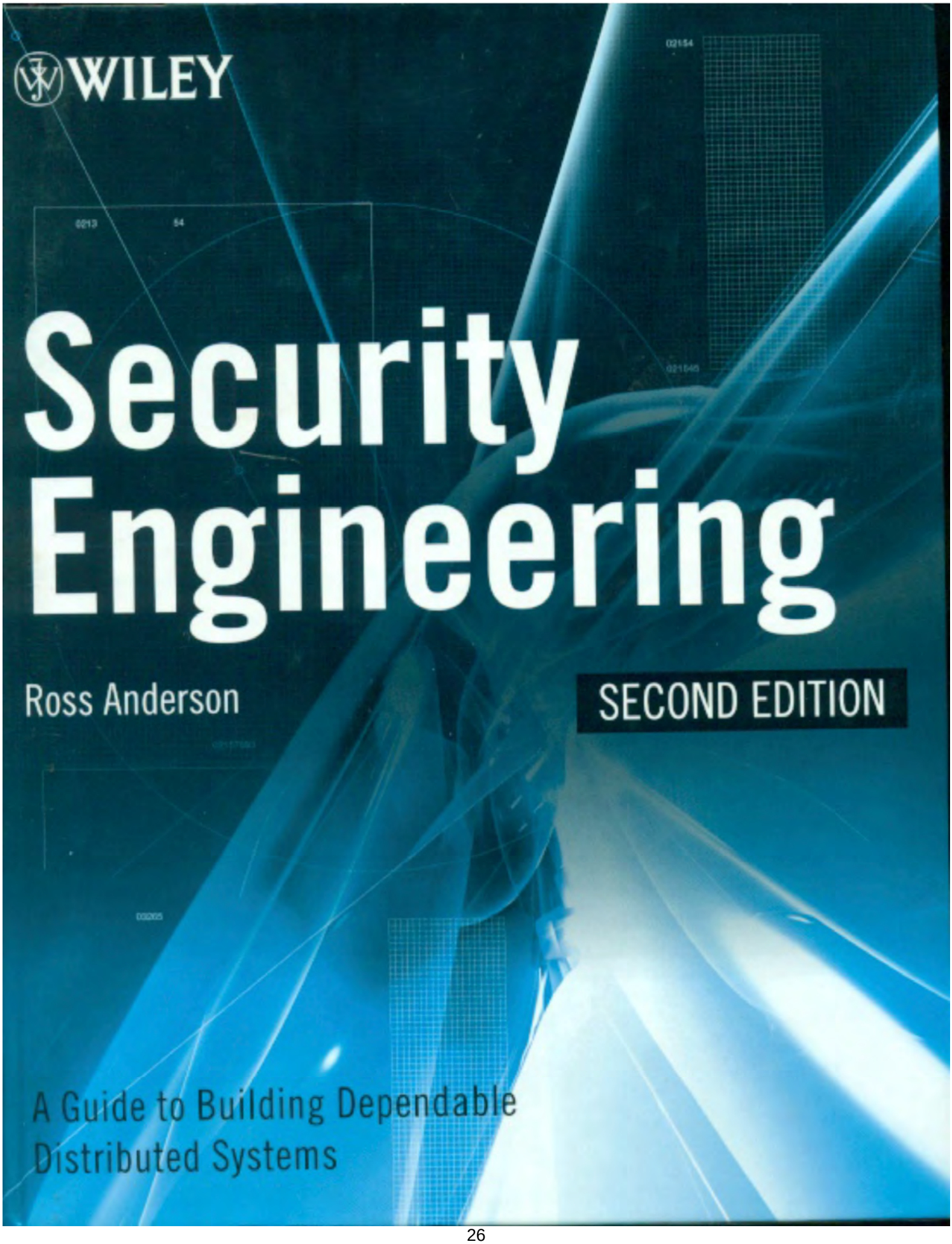
TAGS




programming
security
security
DETAILS
LINKS
TAGS
BROWSE TAGS
BROWSE SHELF
TOP
SEND TO
ONLINE
PHYSICAL
DETAILS
LINKS
TAGS
EXPLORE
Security Engineering
A Guide to Building Dependable Distributed Systems
Security Engineering
Security Engineering
QA76.9.A25 A54 2001b
QA76.9.A25 A545 2003
SEE FULL SHELF
Catalog enrichment powered by Syndetics Unbound

APPENDIX ANDERSON02


Anderson
Security Engineering
SECOND EDITION
QA
76.9
.A25
A54
2008


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems

WESTERN MICHIGAN UNIVERSITY LIBRARIES
KALAMAZOO, MICHIGAN 49008

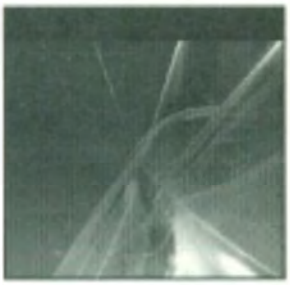
WESTERN MICHIGAN UNIVERSITY
3 1141 01849 8084

DATE DUE | RET'D

WALD NOV 21 '10
NOV 19 2010
MEL MAR 04 2011
MEL APR 04 2011
APR 20 2011
MEL AUG 20 2012
AUG 08 2012
WALD SEP 17 '15
SEP 04 2015

ALL ITEMS ARE SUBJECT TO RECALL AFTER 2 WEEKS

QA
76.9
.A25
A54
2008



Security Engineering

A Guide to Building Dependable Distributed Systems Second Edition

Ross J. Anderson

WILEY

Wiley Publishing, Inc.

Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256

Copyright © 2008 by Ross J. Anderson. All Rights Reserved.

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-06852-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Library of Congress Cataloging-in-Publication Data
Anderson, Ross, 1956-
Security engineering : a guide to building dependable distributed systems / Ross J Anderson. — 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-06852-6 (cloth)
1. Computer security. 2. Electronic data processing–Distributed processing. I. Title.
QA76.9.A25A54 2008
005.1–dc22 2008006392

Trademarks: Wiley, the Wiley logo, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc. is not associated with any product or vendor mentioned in this book.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Contents at a Glance

Preface to the Second Edition		xxv
Foreword by Bruce Schneier		xxvii
Preface		xxix
Acknowledgments		xxxv
Part I		
Chapter 1	What Is Security Engineering?	3
Chapter 2	Usability and Psychology	17
Chapter 3	Protocols	63
Chapter 4	Access Control	93
Chapter 5	Cryptography	129
Chapter 6	Distributed Systems	185
Chapter 7	Economics	215
Part II		
Chapter 8	Multilevel Security	239
Chapter 9	Multilateral Security	275
Chapter 10	Banking and Bookkeeping	313
Chapter 11	Physical Protection	365
Chapter 12	Monitoring and Metering	389
Chapter 13	Nuclear Command and Control	415

Chapter 14	Security Printing and Seals	433
Chapter 15	Biometrics	457
Chapter 16	Physical Tamper Resistance	483
Chapter 17	Emission Security	523
Chapter 18	API Attacks	547
Chapter 19	Electronic and Information Warfare	559
Chapter 20	Telecom System Security	595
Chapter 21	Network Attack and Defense	633
Chapter 22	Copyright and DRM	679
Chapter 23	The Bleeding Edge	727
Part III		
Chapter 24	Terror, Justice and Freedom	769
Chapter 25	Managing the Development of Secure Systems	815
Chapter 26	System Evaluation and Assurance	857
Chapter 27	Conclusions	889
Bibliography		893
Index		997

CHAPTER

20

Telecom System Security

I rarely had to resort to a technical attack. Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses or reveals the information they were seeking.

— Kevin Mitnick

There are two kinds of fools. One says, "This is old, therefore it is good." The other one says, "This is new, therefore it is better".

— Dean William Inge

20.1 Introduction

The protection of telecommunications systems is an important case study for a number of reasons. First, many distributed systems rely on the fixed or mobile phone network in ways that are often not obvious, and the dependability of these networks is declining. For example, POTS — the 'plain old telephone system' — typically required exchanges to have backup generators with enough diesel to survive a six-week outage in the electricity supply, while mobile systems typically use batteries that will last at most 48 hours. What's more, the electicity companies rely on mobile phones to direct their engineers when repairing faults. When people realised that this could cause serious problems where outages lasted more than two days, the electricity companies started buying satellite phones as a backup.

Second, the history of telecomms security failures is very instructive. Early attacks were carried out on phone companies by enthusiasts ('phone phreaks') to get free calls; then the phone system's vulnerabilities started to be

exploited by crooks to evade police wiretapping; then premium rate calls were introduced, which created the motive for large-scale fraud; then when telecomms markets were liberalized, some phone companies started conducting attacks on each other's customers; and some phone companies have even attacked each other. At each stage the defensive measures undertaken were not only very expensive but also tended to be inadequate for various reasons. The same pattern is repeating with the Internet — only with history much speeded up. A number of the policy issues that arose with wireline phones, such as wiretapping, have played themselves out again on the Internet.

Finally, the latest developments in telecomms, from VOIP at the consumer level to the adoption of IP networks as the underlying technology by telecomms providers, create further interactions. Skype's two-day failure in August 2007 following Microsoft's Patch Tuesday is just one case in point. Systems are becoming much more complex and interdependent, and are generally not being engineered to the old standards.

20.2 Phone Phreaking

The abuse of communication services goes back centuries. Before Sir Rowland Hill invented the postage stamp, postage was paid by the recipient. Unsolicited mail became a huge problem — especially for famous people — so recipients were allowed to inspect a letter and reject it rather than paying for it. People soon worked out schemes to send short messages on the covers of letters which their correspondents rejected. Regulations were brought in to stop this, but were never really effective [979].

A second set of abuses developed with the telegraph. The early optical telegraphs, which worked using semaphores or heliographs, were abused by people to place foreknowledge bets on races; if you could learn which horse had won before the bookmaker did, you were well away. People would bribe operators, or 'hack the local loop' by observing the last heliograph station through a telescope. Here too, attempts to legislate the problem away were a failure [1215]. The problems got even more widespread when the electric telegraph brought costs down; the greater volumes of communication, and the greater flexibility that got built into and on top of the service, led to greater complexity and volume of abuse.

The telephone was to be no different.

20.2.1 Attacks on Metering

Early metering systems were wide open to abuse.

- In the 1950's, the operator in some systems had to listen for the sound of coins dropping on a metal plate to tell that a callbox customer had paid

so some people acquired the knack of hitting the coinbox with a piece of metal that struck the right note.

- Initially, the operator had no way of knowing which phone a call had come from, so she had to ask the caller his number. He could give the number of someone else — who would be charged. This was risky to do from your own phone, so people did it from call boxes. Operators started calling back to verify the number for international calls, so people worked out social engineering attacks ('This is IBM here, we'd like to book a call to San Francisco and because of the time difference can our Managing Director take it at home tonight? His number's xxx-yyyy'). So call box lines had a feature added to alert the operator. But in the UK implementation, there was a bug: a customer who had called the operator from a callbox could depress the rest for a quarter second or so, whereupon he'd be disconnected and reconnected (often to a different operator), with no signal this time that the call was from a callbox. He could then place a call to anywhere and bill it to any local number.
- Early systems also signalled the entry of a coin by one or more pulses, each of which consisted of the insertion of a resistance in the line followed by a brief open circuit. At a number of colleges, enterprising students installed 'magic buttons' which could simulate this in a callbox in the student union so people could phone for free. (The bill in this case went to the student union, for which the magic button was not quite so amusing.)

Attacks on metering mechanisms continue. Many countries have moved their payphones to chip cards in order to cut the costs of coin collection and vandalism. Some of the implementations have been poor (as I remarked in the chapter on tamper resistance) and villains have manufactured large quantities of bogus phone cards. Other attacks involve what's called *clip-on*: physically attaching a phone to someone else's line to steal their service.

In the 1970's, when international phone calls were very expensive, foreign students would clip their own phone on to a residential line in order to call home; an unsuspecting home owner could get a huge bill. Despite the fact that in most countries the cable was the phone company's legal responsibility up to the service socket in the house, phone companies were mostly adamant that householders should pay and could threaten to blacklist them if they didn't. Now that long distance calls are cheap, the financial incentive for clip-on fraud has largely disappeared. But it's still enough of a problem that the Norwegian phone company designed a system whereby a challenge and response are exchanged between a wall-socket mounted authentication device and the exchange software before a dial tone is given [673].

Clip-on fraud had a catastrophic effect on a family in Cramlington, a town in the North East of England. The first [illegible]

a conversation on their line. The next was a visit from the police who said there'd been complaints of nuisance phone calls. The complainants were three ladies, all of whom had a number one digit different from a number to which this family had supposedly made a huge number of calls. When the family's bill was examined, there were also calls to clusters of numbers that turned out to be payphones; these had started quite suddenly at the same time as the nuisance calls. When the family had complained later to the phone company about a fault, their connection was rerouted and this had solved the problem.

But the phone company denied the possibility of a tap, despite the report from their maintenance person which noted that the family's line had been tampered with at the distribution cabinet. (The phone company later claimed this report was in error.) It turned out that a drug dealer had lived close by, and it seemed a reasonable inference that he'd tapped their line in order to call his couriers at the payphones. By using an innocent family's phone line instead of his own, he not only saved on the phone bill, but also had a better chance of evading police surveillance. But both the police and the local phone company refused to go into the house where the dealer had lived, claiming it was too dangerous — even though the dealer had by now got six years in jail. The Norwegian phone company declined an invitation to testify about clip-on for the defence. The upshot was that the subscriber was convicted of making harassing phone calls, in a case widely believed to have been a miscarriage of justice. There was discussion at the time about whether the closing of ranks between the phone company and the police was a bureaucratic reflex — or something more sinister. Since 9/11, it's emerged that many phone companies have been giving the police easy access to systems for years, often without warrants, in return for favours. The logical consequence was a policy of covering up anything that could stray into this territory — even if the cover-up caused collateral damage. I'll discuss all this later in the third part of this book.

Stealing dial tone from cordless phones is another variant on the theme. In the 1990s, this became so widespread in Paris that France Telecom broke with phone company tradition and announced that it was happening, claiming that the victims were using illegally imported cordless phones which were easy to spoof [745]. Yet to this day I am unaware of any cordless phones — authorised or not — with decent air link authentication. The new digital cordless phones use the DECT standard which allows for challenge-response mechanisms [1283] but the equipment sold so far seems to simply send a handset serial number to the base station.

Social engineering is also widespread. A crook calls you pretending to be from AT&T security and asks whether you made a large number of calls to Peru on your calling card. When you deny this, he says that they were obviously fake and, in order to reverse out the charges, can he confirm that your card number is 123-456-7890-6543? No, you say (if you're not really

it's 123-456-7890-5678. Now 123-456-7890 is your phone number and 5678 your password, so you've just given that caller the ability to bill calls to you.

The growth of premium rate phone services during the 1990s also led to scamsters developing all sorts of tricks to get people to call them: pager messages, job ads, fake emergency messages about relatives, 'low cost' calling cards with 0900 access numbers, you name it. (In fact, the whole business of tricking people into calling expensive premium numbers enabled crooks to develop a lot of the techniques we now see used in email as part of phishing attacks.) The 809 area code for the Caribbean used to be a favourite cover for crooks targeting U.S. subscribers; many people weren't aware that 'domestic' numbers (numbers within the USA's +1 international direct dialling code) extend outside the relatively cheap USA (and Canada). Even though many people have now learned that +1 809 is 'foreign' and more expensive, the introduction of still more Caribbean area codes, such as +1 345 for the Cayman Islands, has made it even harder to spot premium rate numbers.

Phone companies advised their customers 'Do not return calls to unfamiliar telephone numbers' and 'Beware of faxes, e-mail, voice mail and pages requesting a return call to an unfamiliar number' [22] — but how practical is that? Just as banks now train their customers to click on links in marketing emails and thus make them vulnerable to phishing attacks, so I've had junk marketing calls from my phone company — even though I'm on the do-not-call list. And as for governments, they have tended to set up weak regulators to oversee phone system abuses at home, and avoid anything that might get them involved in trying to regulate premium rate scams overseas. For example, they let phone companies harass their customers into paying bills for overseas services even when they knew that the overseas traffic was fraudulent.

Indeed, by no means all premium-rate scams involved obviously dodgy companies running sex lines; as I write in 2007, the British press are full of stories about how TV companies rip off their customers by getting them to call premium lines in order to compete, and vote, in all sorts of shows. It's turned out that many of these are recorded, so the calls are totally futile; and even the live ones are managed so that people who live in the wrong part of the country or speak with the wrong accent have no chance. The authorities tried to leave this to 'self-regulation' and on-air apologies from TV bosses, until a public outcry (whipped up by their competitors) led to the file being sent to the police in October 2007. It's a recurring pattern that the biggest scams are often run by 'respectable' companies rather than by Russian gangsters.

20.2.2 Attacks on Signaling

The term 'phone phreaking' refers to attacks on signaling as well as pure toll fraud. Until the 1980s, phone companies used signalling systems that worked by sending tone pulses in the same circuit that carried the speech. The

first attack I've heard of dates back to 1952, and by the mid-to-late 1960s many enthusiasts in both America and Britain had worked out ways of rerouting calls. One of the pioneers, Joe Engresia, had perfect pitch and discovered as a child that he could make free phone calls by whistling a tone he'd heard in the background of a long-distance call. His less gifted colleagues typically used home-made tone generators, of which the most common were called *blue boxes*. The trick was to call an 0800 number and then send a 2600Hz tone that would *clear down* the line at the far end — that is, disconnect the called party while leaving the caller with a trunk line connected to the exchange. The caller could now enter the number he really wanted and be connected without paying. Phone phreaking was one of the roots of the computer hacker culture that took root in the Bay Area and was formative in the development and evolution of personal computers [835]. For example, Steve Jobs and Steve Wozniak first built blue boxes before they diversified into computers [502].

Phone phreaking started out with a strong ideological element. In those days most phone companies had monopolies. They were large, faceless and unresponsive. In America, AT&T was such an abusive monopoly that the courts eventually broke it up; most phone companies in Europe were government departments. People whose domestic phone lines had been involved in a service theft found they were stuck with the charges. If the young man who had courted your daughter was (unknown to you) a phone phreak who hadn't paid for the calls he made to her, you would suddenly find the company trying to extort either the young man's name or a payment. Phone companies were also aligned with state security. Phone phreaks in many countries discovered signalling codes or switch features that would enable the police or the spooks to tap your phone from the comfort of their desks, without having to send out a lineman to install a wiretap. Back in the days of Vietnam and student protests, this was inflammatory stuff. Phone phreaks were counterculture heroes, while phone companies were hand-in-hand with the forces of darkness.

As there was no way to stop blue-box type attacks so long as telephone signalling was carried in-band, the phone companies spent years and many billions of dollars upgrading exchanges so that the signaling was moved out-of-band, in separate channels to which the subscribers had no easy access. Gradually, region by region, the world was closed off to blue box attacks. There are still a few places left. For example, the first time that USAF operations were disrupted by an 'information warfare' attack by noncombatants was in 1994 when two British hackers broke into the Rome Air Force Base via an analog link through an ancient phone system in Argentina which they used to hold up investigators [1202]. There's also an interesting legacy vulnerability in wiretapping systems: common phone-tapping equipment was designed to be backwards compatible with in-band signalling, with the result that you can evade surveillance by using a blue box to convince the police equipment

you've hung up. The telephone exchange ignores this signal, so you remain on the phone but with the police recording stopped [1151].

But to defeat a modern telephone network — as opposed to its law-enforcement add-ons — different techniques are needed.

20.2.3 Attacks on Switching and Configuration

The second wave of attacks targeted the computers that did the switching. Typically these were Unix machines on a LAN in the exchange, which also had machines with administrative functions such as scheduling maintenance. By hacking one of these less well guarded machines, a phreak could go across the LAN and break into the switching equipment — or in to other secondary systems such as subscriber databases. For a survey of PacBell's experience of this, see [271]; for Bellcore's, see [722].

Using these techniques, unlisted phone numbers could be found, calls could be forwarded without a subscriber's knowledge, and all sorts of mischief became possible. A Californian phone phreak called Kevin Poulsen got root access to many of PacBel's switches and other systems in 1985–88: this apparently involved burglary as much as hacking (he was eventually convicted of conspiring to possess fifteen or more counterfeit, unauthorized and stolen access devices.) He did petty things like obtaining unlisted phone numbers for celebrities and winning a Porsche from Los Angeles radio station KIIS-FM. Each week KIIS would give a Porsche to the 102nd caller, so Poulsen and his accomplices blocked out all calls to the radio station's 25 phone lines save their own, made the 102nd call and collected the Porsche. He was also accused of unlawful wiretapping and espionage; these charges were dismissed. In fact, the FBI came down on him so heavily that there were allegations of an improper relationship between the agency and the phone companies, along the lines of 'you scratch our backs with wiretaps when needed, and we'll investigate your hacker problems' [472].

Although the unauthorized wiretapping charges against Poulsen were dismissed, the FBI's sensitivity does highlight the possibility that attacks on phone company computers can be used by foreign intelligence agencies to conduct remote wiretaps. Some of the attacks mentioned in [271] were from overseas, and the possibility that such tricks might be used to crash the whole phone system in the context of an information warfare attack has for some years worried the NSA [495, 754]. Countries that import their telephone exchanges rather than building their own are in an even worse position; a prudent nations will assume that its telephone switchgear has vulnerabilities known to the government of the country from which they bought it. (It was notable that during the invasion of Afghanistan in 2001, Kabul had two exchanges: an old electromechanical one and a new electronic one. The USAF bombed only the [illegible] of these.)

But although high-tech attacks do happen, and newspaper articles on phone phreaking tend to play up the 'evil hacker' aspects, most real attacks are much simpler. Many involve insiders, who deliberately misconfigure systems to provide free calls from (or through) favored numbers. This didn't matter all that much when the phone company's marginal cost of servicing an extra phone call was near zero, but with the modern proliferation of value-added services, people with access to the systems can be tempted to place (or forge) large numbers of calls to accomplices' sex lines. Deregulation, and the advent of mobile phones, have also made fraud serious as they give rise to cash payments between phone companies [317]. Insiders also get up to mischief with services that depend on the security of the phone network. In a hack reminiscent of Poulsen, two staff at British Telecom were dismissed after they each won ten tickets for Concorde from a phone-in offer at which only one randomly selected call in a thousand was supposed to get through [1266].

As for outsiders, the other 'arch-hacker' apart from Poulsen was Kevin Mitnick, who got arrested and convicted following a series of break-ins, many of which involved phone systems and which made him the target of an FBI manhunt. They initially thought that he was a foreign agent who was abusing the U.S. phone system in order to wiretap sensitive U.S. targets. As I mentioned in Chapter 2, he testified after his release from prison that almost all of his exploits had involved social engineering. He came out with the quote at the head of this chapter: 'Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses or reveals the information they were seeking' [895]. So phone company systems are vulnerable to careless insiders as well as malicious insiders — just like hospital systems and many others we've discussed.

A worrying recent development is the emergence of switching exploits by organisations. The protocols used between phone companies to switch calls — notably 5ESS — aren't particularly secure, as the move from in-band to out-of-band signaling was supposed to restrict access to trusted parties. But once again, changing environments undermine security assumptions. Now that there are many entrepreneurial phone companies rather than a handful of large ones, all sorts of people have access to the switching. An example is location service. This is provided for a fee by mobile networks; you can register your child's mobile, or your employees' mobiles, and trace them through a website. One entrepreneur undercut this service in the UK by using the switching interface exported by a local telco. While such issues can generally be resolved by contracts, litigation and regulation, there remains a lingering worry that attackers might bring down a telco by exploiting access to its switching and network management. This worry increases as telcos [illegible]

their networks to IP, and they start to converge with VOIP services that give users access to the IP layer. I'll return to VOIP later.

20.2.4 Insecure End Systems

After direct attacks on the systems kept on phone company premises, the next major vulnerabilities of modern phone systems are insecure terminal equipment and feature interaction.

There have been a number of cases where villains exploited people's answering machines. The same technique can be used for at least two different purposes: the relatively innocuous one of tricking someone into dialling a premium rate number, or the somewhat more sinister one of using their answering machine as a covert remailer for a voicemail message. The problem arises from phone company switches that give you dial tone twelve seconds after the other party hangs up. So a terrorist who wants to send an untraceable instruction to a colleague can record on your answering machine thirteen blank seconds, followed by the tones needed to dial his colleague's number and the secret message. He then calls again, gets the machine to play back its messages, and hangs up on it.

But the really big frauds using insecure end systems are directed against companies and government departments. Attacks on corporate *private branch exchange* systems (PBXes) had become big business by the mid-1990's and cost business billions of dollars a year [322]. PBXes are usually supplied with facilities for *refiling* calls, also known as *direct inward system access* (DISA). The typical application is that the company's sales force can call in to an 0800 number, enter a PIN or password, and then call out again taking advantage of the low rates a large company can get for long distance calls. As you'd expect, these PINs become known and get traded by villains [911]. The result is known as *dial-through* fraud.

In many cases, the PINs are set to a default by the manufacturer, and never changed by the customer. In other cases, PINs are captured by crooks who monitor telephone traffic in hotels anyway on order to steal credit card numbers; phone card numbers and PBX PINs are a useful sideline. Many PBX designs have fixed engineering passwords that allow remote maintenance access, and prudent people reckon that any PBX will have at least one back door installed by the manufacturer to give easy access to law enforcement and intelligence agencies (it's said, as a condition of export licensing). Of course such features get discovered and abused. In one case, the PBX at Scotland Yard was compromised and used by villains to refile calls, costing the Yard a million pounds, for which they sued their telephone installer. The crooks were never caught [1244]. This was particularly poignant, as one of the criminals' motivations in such cases is to get access to communications that will not be tapped. Businesses who're the victims of such crimes nevertheless find

the police reluctant to investigate, and one reason for this is that the phone companies aren't particularly helpful — presumably as they don't like having their bills disputed [1088].

In another case, Chinese gangsters involved in labor market racketeering — smuggling illegal immigrants from Fujian, China, into Britain where they were put to work in sweatshops, on farms and so on — hacked the PBX of an English district council and used it to refile over a million pounds' worth of calls to China. The gang was tackled by the police after a number of its labourers died; they were picking shellfish in Morecambe Bay when the tide came in and drowned them. The council had by now discovered the discrepancy in its phone bills and sued the phone company for its money back. The phone company argued that it wasn't to blame, even although it had supplied the insecure PBX. Here, too, the gangsters were interested not just in saving money but in evading surveillance. (Indeed, they routed their calls to China via a compromised PBX in Albania, so that the cross-border segment of the call, which is most likely to be monitored by the agencies, was between whitelisted numbers; the same trick seems to have been used in the Scotland Yard case, where the crooks made their calls via the USA.)

Such cases apart, dial-through fraud is mostly driven by premium rate services: the main culprits are crooks who are in cahoots with premium line owners. Most companies don't understand the need to guard their 'dial tone' and don't know how to even if they wanted to. PBXes are typically run by company telecomms managers who know little about security, while the security manager often knows little about phones. This is changing, albeit slowly, as VOIP technologies take over and the company phone network merges with the data network.

Exploits of insecure end-systems sometimes affect domestic subscribers too. A notorious case was the Moldova scam. In 1997, customers of a porn site were told to download a 'viewer' program that dropped their phone line and connected them to a phone number in Moldova (having turned off their modem speakers so they wouldn't notice). The new connection stayed up until they turned off their computers; thousands of subscribers incurred hundreds of thousands of dollars in international long distance charges at over $2 per minute. Their phone companies tried to collect this money but there was an outcry. Eventually the subscribers got their money back, and the Federal Trade Commission enjoined and prosecuted the perpetrators [456]. Since then there have been a number of copycat scams [870]; but as more and more people move to cable modems or broadband, and their PCs are no longer able to dial out on the plain old telephone system, this kind of abuse is getting less common. The latest twist is premium-rate mobile malware: in 2006, for example, the Ikee Browser worm cashed out by sending $5 SMSs to Russia [633].

Premium rate scams and anonymous calling are not the only motives. Now that phones are used more and more for tasks such as voting, securing entry into apartment buildings, checking that offenders are observing their parole terms, and authenticating financial transactions, more motives are created for ever more creative kinds of mischief, and especially for hacks that defeat caller line ID. For example, caller-line ID hacks make middleperson attacks on payment systems easier; SMS spoofing and attacks on the SS7 signaling in the underlying network can have similar effects [897].

And sometimes attacks are conducted by upstanding citizens for perfectly honorable motives. A neat example, due to Udi Manber, is as follows. Suppose you have bought something which breaks, and the manufacturer's helpline only has an answering machine. To get service, you have to take the answering machine out of service. This can often be done by recording its message, and playing it back so that it appears as the customer message. With luck the machine's owner will think it's broken and it'll be sent off for maintenance.

20.2.5 Feature Interaction

More and more cases of telephone manipulation involve feature interaction.

- Inmates at the Clallam Bay Correctional Center in Washington state, who were only allowed to make collect calls, found an interesting exploit of a system which the phone company ('Fone America') introduced to handle collect calls automatically. The system would call the dialled number and a synthesised voice would say: 'If you will accept a collect call from ... (name of caller) ... please press the number 3 on your telephone twice'. Prisoners were supposed to state their name for the machine to record and insert. The system had, as an additional feature, the ability to have the greeting delivered in Spanish. Inmates did so, and when asked to identify themselves, said 'If you want to hear this message in English, press 33'. This worked often enough that they could get through to corporate PBXes and talk the operator into giving them an outside line. The University of Washington was hit several times by this scam [476].
- A number of directory-enquiry services will connect you to the number they've just given you, as a service to motorists who can't dial while driving. But this can often be used to defeat mechanisms that depend on endpoint identification. Adulterers use it to prevent their spouses seeing lovers' numbers on the family phone bill, and naughty children use it to call sex lines despite call barring [977].

- Call forwarding is a source of many scams. In the old days, it was used for pranks, such as kids social-engineering a phone company operator to forward calls for someone they didn't like to a sex line. Nowadays, it's quite often both professional and nasty. For example, a fraudster may tell a victim to confirm her phone number with the bank by dialing a sequence of digits — which forwards her incoming calls to a number controlled by the attacker. So the bank's callback machanisms are defeated when the customer isn't aware that a certain sequence of dialed numbers can alter the behavior of her phone.
- British Telecom launched a feature called 'Ringback'. If you dial an engaged number, you can then enter a short code and as soon as the called number is free, both your phone and theirs will ring. The resulting call is billed to you. However, when you used ringback used from a pay phone, it was the phone's owner who ended up with the bill. People with private pay phones, such as pub landlords and shopkeepers, lost a lot of money, which the phone company was eventually obliged to refund [652].
- Conference calls also cause a lot of trouble. For example, football hooligans in some countries are placed under a curfew that requires them to be at home during a match, and to prove this by calling the probation service, which verifies their number using caller ID. The trick is to get one of your kids to set up a conference call with the probation service and the mobile you've taken to the match. If the probation officer asks about the crowd noise, you tell him it's the TV and you can't turn it down or your mates will kill you. (And if he wants to call you back, you get your kids to forward the call.)

This brings us to the many problems with mobile phones.

20.3 Mobile Phones

Since their beginnings as an expensive luxury in the early 1980s, mobile phones have become one of the big technological success stories. By 2007, we now have over a billion subscribers; it's said that over a billion phones will be sold this year and the total subscriber base may rise to two billion. In developed countries, most people have at least one mobile, and many new electronic services are being built on top of them. Scandinavia has led here: you get a ferry ticket in Helsinki by sending a text message to the vending machine, and you get a can of Coke the same way. You can also scan a bar code at a bus stop with your phone camera, and get sent a text message 90 seconds before the next bus arrives: that way you don't have to stand out in the snow.

Growth is rapid in developing countries too, where the wireline network is often dilapidated and people used to wait years for phone service to be installed. In some places it's the arrival of mobile phone service that's connected villages to the world. Criminals also make heavy use of mobiles, and not just for communications: and in large tracts of the third world, mobile phone units have become a de facto currency. If you get kidnapped in Katanga, the kidnappers will tell your relatives in Kinshasa to buy mobile phone units and text them the magic numbers. In developed countries, the criminal interest is largely in communications, and most police wiretaps are now on mobile numbers.

So mobile phones are very important to the security engineer, both as part of the underlying infrastructure and as a channel for service delivery. They can also teach us a lot about fraud techniques and countermeasures.

20.3.1 Mobile Phone Cloning

The first generation of mobile phones used analog signals with no real authentication. The handset simply sent its serial numbers in clear over the air link. (In the U.S. system, there were two of them: one for the equipment, and one for the subscriber.) So villains built devices to capture these numbers from calls in the neighborhood. (I've even seen a phone that a student had reprogrammed to do this by a simple software hack.) One of the main customers was the *call-sell operation* that would steal phone service and resell it cheaply, often to immigrants or students who wanted to call home. The call-sell operators would hang out at known pitches with cloned mobiles, and their customers would queue up to phone home for a few dollars.

So a black market developed in phone serial numbers. The call-sell market was complemented by the market for anonymous communications for criminals: enterprising engineers built mobile phones which used a different identity for each call. Known as *tumblers*, these were particularly hard for the police to track [636]. The demand for serial numbers grew rapidly and satisfying it was increasingly difficult, even by snooping at places like airports where lots of mobiles were turned on. So prices rose, and as well as passive listening, active methods started to get used.

Modern mobile phones are cellular, in that the operator divides the service area up into cells, each covered by a base station. The mobile uses whichever base station has the strongest signal, and there are protocols for handing off calls from one cell to another as the customer roams. (For a survey of mobile phone technology, see [1061].) The active attack consists of a fake base station, typically at a place with a lot of passing traffic such as a freeway bridge. As phones pass by, they hear a stronger base station signal and attempt to register by sending their serial numbers.

A number of mechanisms were tried to cut the volume of fraud. Most operators developed or bought intrusion detection systems, which watch out

for suspicious patterns of activity. A number of heuristics were developed. For example, genuine mobiles which roam and call home regularly, but then stop calling home, have usually been stolen; other indicators include too-rapid movement (such as calls being made from New York and LA within an hour of each other) and even just a rapid increase in call volume or duration.

In the chapter on electronic warfare, I mentioned RF fingerprinting — a formerly classified military technology in which signal characteristics that arise from manufacturing variability in the handset's radio transmitter are used to identify individual devices and tie them to the claimed serial numbers [534]. Although this technique works — it was used by Vodafone in the UK to almost eliminate cloning fraud from analogue mobiles — it is expensive as it involves modifying the base stations. (Vodafone also used an intrusion detection system that tracked customer call patterns and mobility, described in [1283]; their competitor Cellnet simply blocked international calls from analogue mobiles, which helped move its high value customers to its more modern digital network.) Another proposed solution was to adopt a cryptographic authentication protocol, but there are limits on how much can be done without changing the whole network. For example, one can use a challenge-response protocol to modify the serial number [485]. But many of the mechanisms people proposed to fortify the security of analog cellular phones have turned out to be weak [1305].

Eventually the industry decided to upgrade to a new digital system. Revenue protection was an issue, but far from the only one; digital systems offered more efficient use of bandwidth, and a whole host of new features — including easier international roaming (important in Europe with lots of small countries jammed close together), and the ability to send and receive short text messages. (Text messages were almost an afterthought; the designers didn't realise they'd be hugely popular.) From the operators' viewpoint, the move to standard digital equipment cut costs and enabled rapid, wide-scale deployment.

20.3.2 GSM Security Mechanisms

The second generation of mobile phones adopted digital technology. Most handsets worldwide use the *Global System for Mobile Communications*, or GSM, which was designed from the start to facilitate international roaming; it was founded when 15 companies signed up to the GSM Association in 1987, and service was launched in 1992. As of 2007, the GSM system extends to over two billion handsets in over 200 countries; a typical developed country has more handsets in service than it has people [133]. The USA, Japan, Korea and Israel had different second-generation digital standards (although the USA has GSM service too). Since about 2001, most countries also have a third-generation service, which I'll describe in the next section.

The designers of GSM set out to secure the system against cloning and other attacks: their goal was that GSM should be at least as secure as the wireline system. What they did, how they succeeded and where they failed, make an interesting case history.

The authentication protocols are described in a number of places, such as [232] (which also describes the mechanisms in an incompatible U.S. system). The industry initially tried to keep secret the cryptographic and other protection mechanisms which form the core of the GSM protocols. This didn't work: some eventually leaked and the rest were discovered by reverse engineering. I'll describe them briefly here.

Each network has two databases, a *home location register* (HLR) that contains the location of its own mobiles, and a *visitor location register* (VLR) for the location of mobiles which have roamed in from other networks. These databases enable incoming calls to be forwarded to the correct cell.

The handsets are commodity items. They are personalised using a *subscriber identity module* (SIM) — a smartcard you get when you sign up for a network service, and which you load into your handset. The SIM can be thought of as containing three numbers:

1. there may be a personal identification number that you use to unlock the card. In theory, this stops stolen mobiles being used. In practice, many networks set an initial PIN of 0000, and most users never change it or even use it;
2. there's an *international mobile subscriber identification* (IMSI), a unique number that maps on to your mobile phone number;
3. finally there is a *subscriber authentication key* K_i, a 128-bit number that serves to authenticate that IMSI and is known to your home network.

Unlike the banks, which used master keys to generate PINs, the phone companies decided that master keys were too dangerous. So instead of diversifying a master key KM to manufacture the authentication keys as $K_i = \{\text{IMSI}\}_{KM}$, the keys are generated randomly and kept in an authentication database attached to the HLR.

The protocol used to authenticate the handset to the network runs as follows (see Figure 20.1). On power-up, the SIM may request the customer's PIN; if this isn't configured, or once it's entered correctly, the SIM emits the IMSI, which the handset sends to the nearest base station. It's relayed to the subscriber's HLR, which generates five *triplets*. Each triplet consists of:

- RAND, a random challenge;
- SRES, a response; and
- K_c, a ciphering key

The relationship between these values is that RAND, encrypted under the SIM's authentication key K_i, gives an output which is SRES concatenated with K_c:

$$\{RAND\}_{K_i} = (SRES|K_c)$$

The standard way to do this encryption is using a one-way function called Comp128, or A3/A8. (A3 refers to the SRES output and A8 to the K_c output). Comp128 is a hash function with 40 rounds, described in detail in [226], and like most proprietary algorithms that were designed in the shadows and fielded quietly in the 1980s and 90s, it turns out to be vulnerable to cryptanalysis. The basic design of the function is much like in Figure 5.9 — each round consists of table lookups followed by mixing. There are five tables, with 512, 256, 128, 64 and 32 byte entries each, and the hash function uses them successively in each block of five rounds; there are eight of these blocks. This may seem very complex, but once its design became public, a vulnerability was soon noticed. Four of the bytes at the output of the second round depend only on the value of the same bytes of the input. This four-byte to four-byte channel is called a *narrow pipe* and it's possible to probe it by tweaking input bytes until you detect a collision. Once all the details have been worked out, it turns out that you need about 150,000 suitably chosen challenges to extract the key [1306, 1307]. The effect is that given access to a SIM issued by a network that uses Comp128, the authentication key can be extracted in several hours using software that is now freely available.

This attack is yet another example of the dangers of using a secret crypto primitive that has been evaluated by only a few friends; the cryptanalytic techniques necessary to find the flaw were well known [1287] and if Comp128 had been open to hostile public scrutiny, the flaw would most probably have been found. Thankfully, a phone company can replace Comp128 with a proper hash function such as SHA-256 without affecting anyone else; the hash function is present only in the SIM cards it issues to its customers and the software at its HLR. In any case, there don't seem to be any industrial-scale attacks based on a vulnerable hash function; the normal user doesn't have any incentive to crack his K_i out from his SIM as it doesn't let him bill calls to (or steal calls from) anyone else.

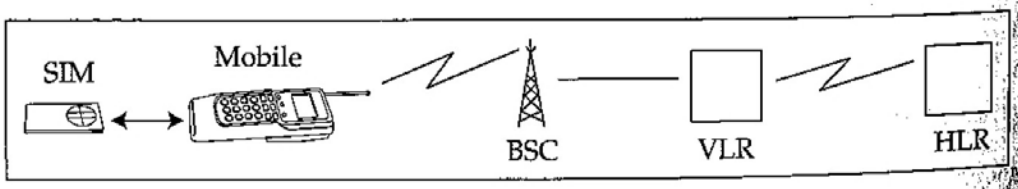


Figure 20.1: GSM authentication system components

Anyway, the triplets are sent to the base station, which now presents the first RAND to the mobile. It passes this to the SIM, which computes SRES. The mobile returns this to the base station and if it's correct the mobile and the base station can now communicate using the ciphering key K_c. So the whole authentication protocol runs as in Figure 20.2.

SIM → HLR	IMSI
HLR → BSC	(RAND, SRES, K_c), ...
BSC → SIM	RAND
SIM → BSC	SRES
BSC → mobile	$\{traffic\}_{K_c}$

Figure 20.2: GSM authentication protocol

There are several vulnerabilities in this protocol. In most countries the communications between base stations and the VLR pass unencrypted on microwave links[1]. So an attacker could send out an IMSI of his choice and then intercept the triplet on the microwave link back to the local base station. A German mobile operator, which offered a reward of 100,000 Deutschmarks to anyone who could bill a call to a mobile number whose SIM card was held in their lawyer's office, backed down when asked for the IMSI [44].

Second, triples can be replayed. An unscrupulous foreign network can get five triples while you are roaming on it and then keep on reusing them to allow you to phone as much as you want. (Home networks could stop this by contract but they don't.) So the visited network doesn't have to refer back to your home network for further authorisation — and even if they do, it doesn't protect you as the visited network might not bill you for a week or more. So your home network can't reliably shut you down while you roam and it may still be liable to pay the roamed network the money. Dishonest networks also defraud roaming customers by *cramming* — by creating false billing records, a practice I'll describe in more detail later. So even if you thought you'd limited your liability by using a pre-paid SIM, you might still end up with your network trying to collect money from you. This is why, to enable roaming with a pre-paid SIM, you're normally asked for a credit card number. You can end up being billed for more than you expected.

[1] The equipment can encrypt traffic, but the average phone company has no incentive to switch the cryptography on. Indeed, as intelligence agencies often monitor the backhaul near major switching nodes as an efficient means of getting warrantless access to traffic, a phone company that did switch on the crypto might find that persons unknown started jamming the link to make them stop.

The introduction of GSM caused significant shifts in patterns of crime generally. The authentication mechanisms made phone cloning difficult, so the villains switched their modus operandi to buying phones using stolen credit cards, using stolen identities or bribing insiders [1352]. Robbery was another issue. We've had a spate of media stories in Britain about kids being mugged for their phones. Mobile phone crime did indeed increase 190% between 1995 and 2002, but to keep this in context, the number of subscribers went up 600% in the same period [583]. Some of the theft is bullying — kids taking smaller kids' phones; some is insurance fraud by subscribers who've dropped their phones in the toilet and report them as stolen as their insurance doesn't cover accidental damage; but there is a hard core of theft where muggers take phones and sell them to fences. Many of the fences either work at mobile phone shops that have authorised access to tools for reprogramming the International Mobile Equipment Identifier (IMEI), the serial number in the handset, or else have links to organised criminals who ship the handsets abroad. Things are worse in Brazil, where kidnapping is endemic: there are now fake kidnappings in which a child's phone is snatched by a criminal who phones its parents to demand a ransom[2].

From about 1997, prepaid mobile phones were introduced. This kicked off a period of rapid growth in the industry as the technology became available to people without credit ratings. For example, prepaids make up 90% of the market in Mexico but 15% in the USA. Worldwide, they're over half, and growing. They also made anonymous communication much more practical, and many criminals have started using them. The issues include not just evading police wiretapping but stalking, extortion, bullying and other kinds of harassment. Prepaids also facilitate simple frauds; if your identity isn't checked when you buy a phone, there's little risk to you if you recharge it with a stolen credit card [343].

It must be said though that most people who use prepaid phones for crime are only getting lightweight anonymity, and remain undetected only because the police don't put serious effort into catching petty crooks. If a really serious crime is committed, traffic analysis will be used, and most criminals don't have any clue of the level of operational discipline needed to stop this. As I already remarked, the alleged 9/11 mastermind Khalid Shaikh Mohammed was caught when he used a prepaid SIM from the same batch as one that had been used by another Al-Qaida member; and after the failed 21/7 London bombings, the would-be bomber Husein Osman fled to Rome, where he was promptly caught. He had changed the SIM in his mobile phone en route, but

[2]There are also completely fake kidnappings in which the bad guys just lie: they say they've snatched the child, and if they call its phone it will be killed. The perpetrators of these crimes are often in prison and have little to lose. 20% of parents still pay up rather than take the risk.

call records show not just the IMSI from the SIM, but also the IMEI from the handset. If you've got all the world's police after you, just changing the SIM isn't anything like enough. Operational security requires a detailed technical understanding of how networks operate, and levels of training and discipline that are most unusual outside national intelligence agencies.

Finally, prepaid mobiles were a gift to crooked call-sell operators. As the billing infrastructure is only invoked when a phone goes on-hook, it's possible for a bad guy to make a call last all day: the numbers called by each of his clients are simply added to a long conference call one after the other. At the end of the day, the phone goes on-hook, a bill for thousands of dollars is generated, the alarm goes off, and the crook tosses the phone in the river. The following day he buys another. That's why network operators typically tear down any call that lasts more than a few hours.

In addition to authentication, the GSM system is supposed to provide two further kinds of protection — location security and call content confidentiality.

The location security mechanism is that once a mobile is registered to a network, it is issued with a *temporary mobile subscriber identification* (TMSI), which acts as its address as it roams through the network. The attack on this mechanism uses a device called an *IMSI-catcher*, which is sold to police forces [488]. The IMSI-catcher, which is typically operated in a police car tailing a suspect, pretends to be a GSM base station. Being closer than the genuine article, its signal is stronger and the mobile tries to register with it. The IMSI catcher claims not to understand the TMSI, so the handset helpfully sends it the cleartext IMSI. This feature is needed if mobiles are to be able to roam from one network to another without the call being dropped, and to recover from failures at the VLR [1283]. The police can now get a warrant to intercept the traffic to that mobile or — if they're in a hurry — just do a middleperson attack in which they pretend to be the network to the mobile and the mobile to the network.

The GSM system is supposed to provide call content confidentiality by encrypting the traffic between the handset and the base station once the authentication and registration are completed. The speech is digitized, compressed and chopped into packets; each packet is encrypted by xor-ing it with a pseudorandom sequence generated from the ciphering key K_c and the packet number. The algorithm commonly used in Europe is A5/1.

A5/1, like Comp128, was originally secret; like Comp128, it was leaked and attacks were quickly found on it. The algorithm is shown in Figure 20.3. There are three linear feedback shift registers of lengths 19, 22 and 23 and their outputs are combined using exclusive-or to form the output keystream. The nonlinearity in this generator comes from a majority-clocking arrangement whereby the middle bits c_i of the three shift registers are compared and the two or three shift registers whose middle bits agree are clocked

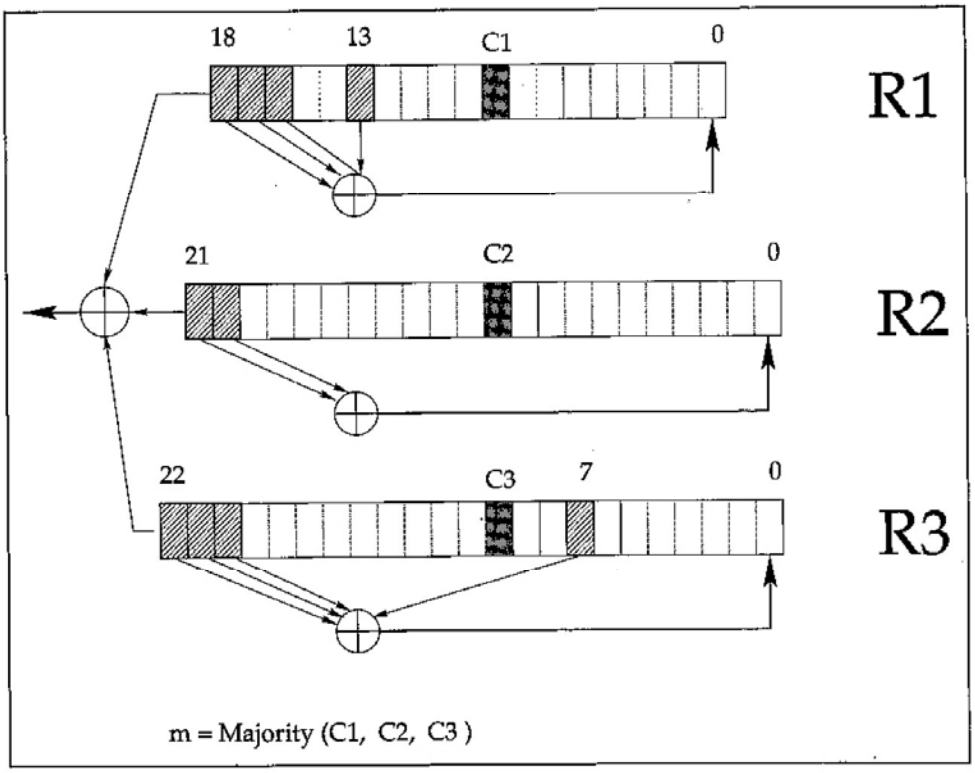


Figure 20.3: A5 (courtesy of Alex Biryukov and Adi Shamir)

The obvious attack on this arrangement is to guess the two shorter registers and then work out the value of the third. As there are 41 bits to guess, one might think that about 2^{40} computations would be needed on average. It's slightly more complex than this, as the generator loses state; many states have more than one possible precursor, so more guesses are needed. This led to an attack using a lot of FPGAs that is sold for about $1m[3]. Then Biryukov and Shamir found some optimizations and tradeoffs that let A5 be broken with much less effort. Their basic idea is to compute a large file of special points to which the state of the algorithm converges, and then look for a match with the observed traffic. Given this precomputed file, the attack can use several seconds of traffic and several minutes' work on a PC, or several minutes of traffic and several seconds' work [173]. Reverse engineering actual systems also showed that the keying of A5 was deliberately weakened. Although in theory A5 has a 64-bit key (the initial loads for the shift registers) the actual implementations set the ten least significant key bits to zero. Anyway, the response of the GSM vendors to these disclosures was to introduce a third cipher, A5/3, which is based on a strong block cipher known as Kasumi that's also used in third-generation mobile phones.

[3]A system of 15 boxes, each with 20 cards, each with 18 ICs, each with 32 cores, each running ... 150 MHz, and burning 7.5 ... per key and burns 15KW.

However, this attempt to fix the content-confidentiality problem has been undermined by an attack that exploits the underlying authentication protocol and that is now coming into widespread use by police and surveillance folks. It relies on the fact that phone companies in many countries use a weakened version of A5/1, called A5/2. Mobile phones are generally able to use either algorithm, so that they can roam freely. The attack was invented by Elad Barkan, Eli Biham and Nathan Keller [117], and runs as follows. If you're following a suspect who uses his mobile, you record the call, including the initial protocol exchange of challenge and response. Once he's finished, you switch on your IMSI-catcher and cause him to register with your bogus base station. The IMSI-catcher tells his phone to use A5/2 rather than A5/1, and a key is duly set up — with the IMSI-catcher sending the challenge that was used before. So the mobile phone generates the same key K_c as before. As this is now being used in a weak cipher, it can be cracked quickly, giving access to the target conversation recorded previously. In fact it doesn't matter whether that was protected using the medium-security A5/1 or the high-security A5/3. The facts that there's a low-security algorithm, that keys are determined by one of the two principals, and that keys are shared between algorithms, together make the whole system weak.

The A5/1 vulnerability was introduced following pressure from Europe's intelligence agencies, and the ostensible justification was that they didn't want even halfways decent security exported to potentially hostile countries, as it would be harder to spy on them. The conspiracy theorists had a field day with all this — for example, there was a political row in Australia when it turned out that A5/2 was being used there, as it was seen as implying that European governments saw Australia as an intelligence target rather than an ally.

The truth is, as always, more subtle. Weak ciphers can definitely help in some tactical situations. Consider the case I mentioned in the chapter on electronic warfare, where the New Zealand navy sent a frigate to monitor a coup in Fiji. If the Fijian phone company had been allowed to use A5/1 rather than A5/2, this would not have frustrated the mission: the sigint officers could snatch the triplets off the microwave links, hack the location register, and if all else fails, brute force a key. But being able to break traffic quickly is very convenient.

On the other hand, imposing weak cipher security on less developed countries can also have operational costs. In 2007, the Taleban started tapping mobile phone calls made by British soldiers to friends and relatives back home, whom they then called. The wife of one RAF officer was told: 'You'll never see your husband alive — we have just killed him'. It was some hours before she could confirm that he was still safe and well [603]. British troops have now been banned from using mobile phones — which doesn't exactly help morale.

In domestic or friendly-country operations, it's even more complex. The agencies can get lawful access to cleartext from phone companies, but sometimes the warrantry procedures are (or are felt to be) too cumbersome. Hence

the sweetheart deals with some phone companies to get access without warrants; this has led to a number of scandals recently. For example, it emerged that AT&T had been giving the US authorities access to itemised billing data for years. Sweetheart deals were common with companies that used to be monopolies, but are becoming less common as most countries have now deregulated telecomms and have hundreds of phone companies, not just one. Some phone companies are distrusted by the authorities because they're owned by foreigners or even by gangsters. Others are tiny, have never been tapped before, the police just don't know who to talk to. Other companies are respectable and willing to comply with warrants, but unable to do so. One of Britain's most closely guarded law-enforcement and intelligence secrets for several years was that one of the mobile phone networks couldn't be conveniently tapped. Engineers tried to hook up their complex, messy systems to the intelligence community's complex, messy systems but the project went off the rails and they just could not get the thing to work. The police were really scared that crooks might find this out, and migrate en masse to that network.

How are we to make sense of this mess? It's as well to admit that there are many reasons, some honourable and some less so, why government employees may want to get access to traffic by technical means rather than by using the lawful interfaces provided for the purpose. But that doesn't mean that such access should be allowed. The huge improvements in liberty, prosperity and quality of life that the West has enjoyed since the Enlightenment and the Industrial Revolution are due in large part to our replacing the divine right of kings with freedom under the law in a democracy. We elect legislators to make the rules, and if we decide through them that the police can't torture suspects any more, then they'd better not try. Similarly, if our legislators decide that police and intelligence agencies should get warrants to wiretap, then the agencies must obey the law like anyone else. The GSM security story provides a good example of how the deliberate insertion of vulnerabilities can have wide-ranging and unforeseen engineering consequences. It must also be said that the facilities that phone companies and ISPs are now being compelled to provide for properly warranted law-enforcement access are often so poorly engineered that they can be abused [1151]. In 2004–5, persons unknown tapped the mobile phones of the Greek Prime Minister and about a hundred of that country's political, law enforcement and military elite, by subverting the wiretapping facilities built into Vodafone's Greek network. Both Vodafone and their equipment supplier Ericsson, where heavily fined [1042]. Colleagues and I warned about this problem years ago [4] and I expect it to get worse. I'll discuss it at greater length in Part III.

There are further policy issues with location privacy. There was a storm in Switzerland in 1997 when the press found that the phone company was routinely giving location data to the police [1030], while in the USA, the FCC ordered mobile phone companies to be able to locate people 'so that 911

could be dispatched to the right place'. This was imposed on every user of mobile phone service, rather than letting users decide whether to buy mobile location services or not. Privacy activists were not happy with this.

Anyway, the net effect is that the initial GSM security mechanisms provided slightly better protection than the wireline network in countries allowed to use A5/1, and slightly worse protection elsewhere, until the protocol attacks were discovered and exploited. Now privacy is slightly worse everywhere, as people with the right equipment can get fairly straightforward access to traffic. But it's probably not a big deal. Relatively few people ever get followed around by an investigator with professional snooping equipment — and if you're such a person, then ways to detect and prevent semi-active attacks on your mobile phone are just a small part of the tradecraft you need to know. If you're an average subscriber, the privacy threat comes from possible abuse of data collected by the phone company, such as itemized billing data. From that viewpoint, the vulnerabilities in the communications security mechanisms neither expose you to additional wiretapping, nor prevent the frauds that are likely to cause you the most grief.

20.3.3 Third Generation Mobiles – 3gpp

The third generation of digital mobile phones was initially known as the *Universal Mobile Telecommunications System* (UMTS) and now as the *Third Generation Partnership Project* (3gpp, or just 3g). These systems are now available almost everywhere, the exception being in China which is working on its own proprietary variant. Elsewhere, the security is much the same as GSM, but upgraded to deal with a number of GSM's known vulnerabilities. Third generation systems entered service in 2003–2004; the main advantage of 3g over GSM is higher data rates; instead of the 9.6kb/s of GSM and the tens of kilobits per second of GPRS, third-generation data rates are in the hundreds of thousands to millions of bits per second. The vision is that 3g will enable all sorts of mobile services, from mobile TV to laptops that just go online anywhere.

The overall security strategy is described in [1310], and the security architecture is at [1298]. The crypto algorithms A5/1, A5/2 and Comp128 are replaced by various modes of operation of a block cipher called Kasumi [696]. Kasumi is public and is based on a design by Mitsuru Matsui called Misty, which was properly peer-reviewed and has now withstood public scrutiny for a decade [844]. All keys are now 128 bits. Cryptography is used to protect the integrity and confidentiality of both message content and signalling data, rather than just content confidentiality, and the protection at least runs from the handset to a fairly central node, rather than simply to the local base station. This means the picking up the triples, or the plaintext, from the microwave backhaul is no longer an attack. The authentication is now two-way rather

than one-way, ending the vulnerability to rogue base stations; so IMSI-catchers don't work against third generation mobiles. Instead, there is a properly engineered interface for lawful interception [1299]. This can supply key material as well as plaintext, so that if the police follow a suspect, record a call and identify the mobile in the process, they can decrypt that call later, rather than being limited to the plaintext of calls recorded by the phone company after they get their warrant approved.

The protocol mechanics work as follows (see Figure 20.4). In the basic 3gpp protocol, the authentication is pushed back from the base station controller to the visitor location register. The home location register is now known as the *home environment* (HE) and the SIM as the *UMTS SIM* (USIM). The home environment chooses a random challenge RAND as before and enciphers it with the USIM authentication key K to generate a response RES, a confidentiality key CK, and integrity key IK, and an anonymity key AK.

$$\{RAND\}_K = (RES|CK|IK|AK)$$

There is also a sequence number SEQ known to the HE and the USIM. A MAC is computed on RAND and SEQ, and then the sequence number is masked by exclusive-or'ing it with the anonymity key. The challenge, the expected response, the confidentiality key, the integrity key, and the masked sequence number made up into an *authentication vector* AV which is sent from the HE to the VLR. The VLR then sends the USIM the challenge, the masked sequence number and the MAC; the USIM computes the response and the keys, unmasks the sequence number, verifies the MAC, and if it's correct returns the response to the VLR.

USIM → HE	IMSI (this can optionally be encrypted)
HE → VLR	RAND, XRES, CK, IK, $SEQ \oplus AK$, MAC
VLR → USIM	RAND, $SEQ \oplus AK$, MAC
USIM → VLR	RES

Figure 20.4: 3gpp authentication protocol

The UMTS standards set out are many other features, including details of sequence number generation, identity and location privacy mechanisms, backwards compatibility with GSM, mechanisms for public-key encryption of authentication vectors in transit from HEs to VLRs, and negotiation of various optional cryptographic mechanisms.

The net effect is that confidentiality will be improved over GSM: eavesdropping on the air link is prevented by higher-quality mechanisms, and the current attacks on the backbone network, or by bogus base stations, are excluded. Police wiretaps are done at the VLR. In a number of countries third-generation mobiles were hard for the police to tap in the first few years

as they had to learn to operate through formal channels and also to integrate their systems with those of the network operators. In the second phase, it's proposed to have end-to-end encryption, so that the call content and some of the associated signaling will be protected from one handset to another. This led to government demands for a *key escrow protocol* — a protocol to make keys available to police and intelligence services on demand. The catch is that if a mobile phone call takes place from a British phone company's subscriber using a U.S. handset, roaming in France, to a German company's subscriber roaming in Switzerland using a Finnish handset, and the call goes via a long distance service based in Canada and using Swedish exchange equipment, then which of these countries' intelligence agencies will have access to the keys? [1299] (Traditionally, most of them would have had access to the call content one way or another.)

One solution pushed by the agencies in Britain and France is the so-called Royal Holloway protocol [663], designed largely by Vodafone, which gives access to the countries where the subscribers are based (so in this case, Britain and Germany). This is achieved by using a variant of Diffie-Hellman key exchange in which the users' private keys are obtained by encrypting their names under a super-secret master key known to the local phone company and/or intelligence agency. Although this protocol has been adopted in the British civil service and the French health service, it is at odds with the phone company security philosophy that master keys are a bad thing. The protocol is also clunky and inefficient [76].

So 3gpp won't provide a revolution in confidentiality, merely a modest improvement. As with GSM, its design goal is that security should be comparable with that of the wired network [621] and this looks like being achieved.

20.3.4 Platform Security

The final point I need to make here is that as mobile phones become more widespread and more programmable, they may suffer from the malware problems that have plagued the PC. They have followed the pattern predicted by security economics. At first, the platform vendors — the firms selling operating systems, such as Symbian, Microsoft and Linux — didn't incorporate much security, as it would have got in application developers' way and appealing to complementers is vital when building share in a new market with network externalities. Then, as one platform pulled ahead of the others, the malware writers targeted it. In 2007, viruses and worms are being detected at the rate of about 300 per annum for Symbian phones, and one or two a year for the others. Symbian has started a program of hardening their platform, with progressively more sophisti[illegible]