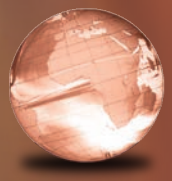
GLOBAL EDITION



Corporate Computer Security

FOURTH EDITION

Randall J. Boyle | Raymond R. Panko

ALWAYS LEARNING

PEARSON

Fourth Edition

Corporate Computer Security

Global Edition

Randall J. Boyle
Longwood University

Raymond R. Panko
University of Hawai`i at Mānoa

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montréal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

To Courtney Boyle, thank you for your patience, kindness, and perspective on what's most important in life.

—Randy Boyle

To Julia Panko, my long-time networking and security editor and one of the best technology minds I've ever encountered.

—Ray Panko

Editor in Chief: Stephanie Wall
Executive Editor: Bob Horan
Program Manager Team Lead: Ashley Santora
Program Manager: Denise Vaughn
Director of Marketing: Maggie Moylan
Executive Marketing Manager: Anne Fahlgren
Project Manager Team Lead: Judy Leale
Project Manager: Tom Benfatti
Operations Specialist: Michelle Klein
Creative Director: Jayne Conte
Head of Learning Asset Acquisition, Global Edition: Laura Dent
Assistant Acquisitions Editor, Global Edition: Debapriya Mukherjee
Project Editor, Global Edition: Amrita Naskar
Media Producer, Global Edition: Vikram Kumar
Senior Manufacturing Controller, Production, Global Edition: Trudy Kimber
Cover Designer: PreMediaGlobal
Cover Image: Devis Da Fre'/Shutterstock
Digital Production Project Manager: Lisa Rinaldi

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text.

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM20 2JE
England

and Associated Companies throughout the world

Visit us on the World Wide Web at: www.pearsonglobaleditions.com

ISBN 10: 1-292-06045-X
ISBN 13: 978-1-292-06045-3 (Print)
ISBN 13: 978-1-292-06659-2 (PDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

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

Typeset in Times, 10/12 by Integra Software Services Pvt. Ltd

Printed and bound by Courier Westford in the United States of America

CONTENTS

PREFACE

The IT security industry has seen dramatic changes in the past decades. Security breaches, data theft, cyber attacks, and information warfare are now common news stories in the mainstream media. IT security expertise that was traditionally the domain of a few experts in large organizations has now become a concern for almost everyone.

These rapid changes in the IT security industry have necessitated more recent editions of this text. Old attacks are being used in new ways, and new attacks are becoming commonplace. We hope the changes to this new edition have captured some of these changes in the industry.

WHAT'S NEW IN THIS EDITION?

If you have used prior editions to this text, you will notice that almost all of the material you are familiar with remains intact. New additions to the text have been driven by requests from reviewers. More specifically, reviewers asked for a text that has a new opening case, business case studies at the end of each chapter, new hands-on projects, updated news articles, and more information related to certifications.

In addition to these changes in content, we have tried to add supplements that make the book easier to use and more engaging for students. Below is a list of the significant changes to this edition of the text.

Opening Case—The opening case in Chapter 1 covers a series of data breaches that resulted in one of the largest known data losses to date. The case looks at the sequence of events surrounding the three data breaches at Sony Corp. It then examines how the attackers were able to steal the data, possible motives behind the attacks, arrests and punishment of the attackers, and the impacts on Sony Corp. This case acts as an illustration of the real-world threat environment corporations face today.

Business Case Studies—This edition has tried to have more of a business focus by adding in a real-world case study at the end of each chapter. The case studies are designed to show how the material presented in the chapter could have a direct impact on an actual corporation. After each case study, there are key findings from prominent annual industry reports related to the case and chapter material. Case studies, combined with key findings from relevant industry reports, should provide ample material for classroom discussion. Open-ended case questions are included to help guide case discussions. They also offer students the opportunity to apply, analyze, and synthesize the material presented in the chapter.

New Hands-on Projects—Each chapter has new, or updated, hands-on projects that use contemporary security software. Each project relates directly to the chapter material. Students are directed to take a screenshot to show they have completed the project. Projects are designed such that each student will have a unique screenshot after completing each project. Any sharing or duplication of project deliverables will be obvious.

Updated News Articles—Each chapter contains expanded and updated IT security news articles. Over 80 percent of the news articles in this book reference stories that have occurred since the prior edition was published.

Expanded Material on Certifications—Reviewers of the prior edition asked for more material related to IT security certifications. We live in a world that relies on credentials as a means of conveying legitimacy, skill, and possibly experience. In this respect, the security field is no different. To this end, we have updated and expanded the certification focus article in Chapter 10. It is likely that students pursuing a career in the IT security industry will seek some type of certification.

Why Use This Book?

INTENDED AUDIENCE This book is written for a one-term introductory course in IT security. The primary audience is upper-division BS majors in Information Systems, Computer Science, or Computer Information Systems. This book is also intended for graduate students in Masters of Information Systems (MSIS), Master of Business Administration (MBA), Master of Accountancy (MAcc), or other MS programs that are seeking a broader knowledge of IT security.

It is designed to provide students with IT security knowledge as it relates to corporate security. It will give students going into the IT security field a solid foundation. It can also serve as a network security text.

PREREQUISITES This book can be used by students who have taken an introductory course in information systems. However, taking a networking course before using this book is strongly advisable. For students who have not taken a networking course, Module A is a review of networking with a special focus on security aspects of network concepts.

Even if networking is a prerequisite or corequisite at your school, we recommend covering Module A. It helps refresh and reinforce networking concepts.

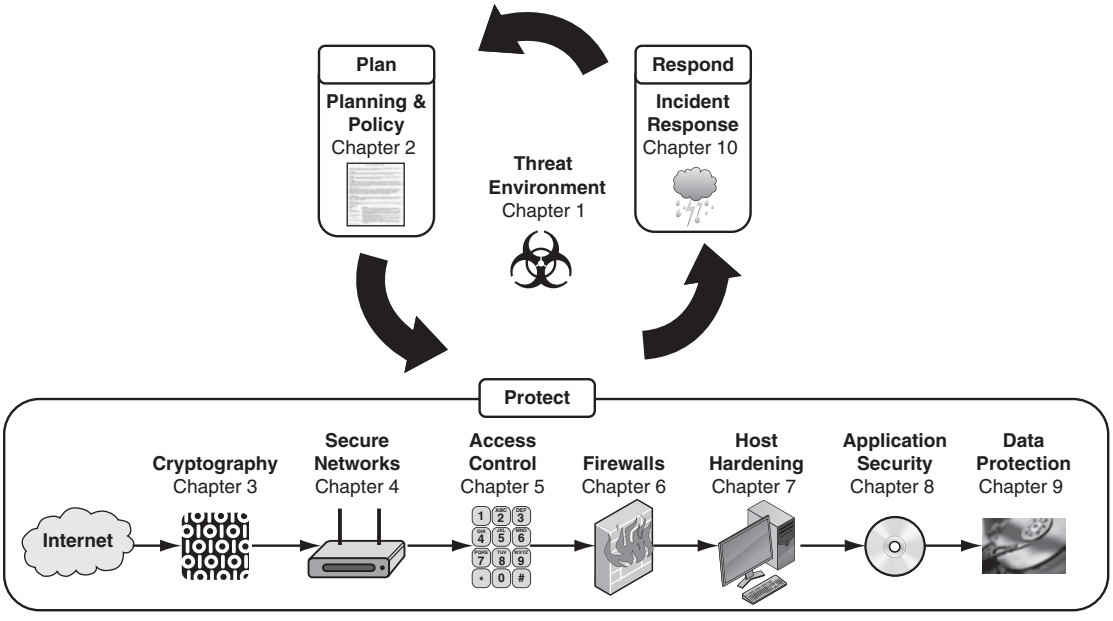
BALANCING TECHNICAL AND MANAGERIAL CONTENT Our students are going to need jobs. When you ask working IT security professionals what they are looking for in a new hire, they give similar responses. They want proactive workers who can take initiative, learn on their own, have strong technical skills, and have a business focus.

A business focus does not mean a purely managerial focus. Companies want a strong understanding of security management. But they also want a really solid understanding of defensive security technology. A common complaint is that students who have taken managerial courses don't even know how stateful packet inspection firewalls operate, or what other types of firewalls are available. "We aren't hiring these kids as security managers" is a common comment. This is usually followed by, "They need to start as worker bees, and worker bees start with technology."

Overall, we have attempted to provide a strong managerial focus along with a solid technical understanding of security tools. Most of this book deals with the technical aspects of protective countermeasures. But even the countermeasure chapters reflect what students need to know to manage these technologies. You can "throttle" the amount of technical content by using or not using the Hands-on Projects at the end of each chapter.

How Is This Book Organized?

The book starts by looking at the threat environment facing corporations today. This gets the students' attention levels up, and introduces terminology that will be used throughout the rest of the book. Discussing the threat environment demonstrates the need for the defenses mentioned in later chapters.



The rest of the book follows the good old plan–protect–respond cycle. Chapter 2 deals with planning, and Chapter 10 deals with incident and disaster response. All of the chapters in the middle deal with countermeasures designed to protect information systems.

The countermeasures section starts with a chapter on cryptography because cryptographic protections are part of many other countermeasures. Subsequent chapters introduce secure networks, access control, firewalls, host hardening, application security, and data protection. In general, the book follows the flow of data from networks, through firewalls, and eventually to hosts to be processed and stored.

USING THE BOOK IN CLASS Chapters in this book are designed to be covered in a semester week. This leaves a few classes for exams, presentations, guest speakers, hands-on activities, or material in the module. Starting each class with a demonstration of one of the hands-on projects is a good way to get students' attention.

It's important for students to read each chapter before it's covered in class. The chapters contain technical and conceptual material that needs to be closely studied. We recommend either giving a short reading quiz or requiring students to turn in Test Your Understanding questions before covering each chapter.

POWERPOINT SLIDES AND STUDY FIGURES The PowerPoint lectures cover nearly everything, as do the study figures in the book. Study figures even summarize main points from the text. This makes the PowerPoint presentations and the figures in the book great study aids.

TEST YOUR UNDERSTANDING QUESTIONS After each section or subsection, there are Test Your Understanding questions. This lets students check if they really understood what they just read. If not, they can go back and master that small chunk of material before going on. The

test item file questions are linked to particular Test Your Understanding questions. If you cut some material out, it is easy to know what multiple-choice questions not to use.

INTEGRATIVE THOUGHT QUESTIONS At the end of each chapter, there are integrative Thought Questions which require students to synthesize what they have learned. They are more general in nature, and require the application of the chapter material beyond rote memorization.

HANDS-ON PROJECTS Students often comment that their favorite part of the course is the Hands-on Projects. Students like the Hands-on Projects because they get to use contemporary IT security software that relates to the chapter material. Each chapter has at least two applied projects and subsequent Project Thought Questions.

Each project requires students to take a unique screenshot at the end of the project as proof they completed the project. Each student's screenshot will include a time stamp, the student's name, or another unique identifier.

CASE STUDY Each chapter includes a real-world case study focused on how IT security affects corporations. More specifically, each case study is designed to illustrate how the material presented in the chapter could impact a corporation. Along with each case study are related key findings from prominent annual industry reports. Links to each industry report are provided and can be used as supplementary reading. Case studies, combined with key findings from relevant industry reports, should provide ample material for classroom discussion.

CASE DISCUSSION QUESTIONS Case studies are followed by a series of open-ended questions to guide case-based classroom discussions. They offer students the opportunity to apply, analyze, and synthesize the material presented in the chapter within the context of a real-world business case.

PERSPECTIVE QUESTIONS There are two general questions that ask students to reflect on what they have studied. These questions give students a chance to think comprehensively about the chapter material at a higher level.

HEY! WHERE'S ALL THE ATTACK SOFTWARE? This book does not teach students how to break into computers. There is software designed specifically to exploit vulnerabilities and gain access to systems. This book does not cover this type of software. Rather, the focus of the book is how to proactively defend corporate systems from attacks.

Effectively securing corporate information systems is a complicated process. Learning how to secure corporate information systems requires the entire book. Once students have a good understanding of how to secure corporate systems, they *might* be ready to look at penetration testing software.

With 10 chapters, you do have time to introduce some offense. However, if you do teach offense, do it carefully. Attack tools are addictive, and students are rarely satisfied using them in small labs that are carefully air-gapped from the broader school network and the Internet. A few publicized attacks by your students can get IT security barred from the curriculum.

Instructor Supplements

This is a hard course to teach. We have tried to build in as much teacher support as possible. Our goal was to reduce the total amount of preparation time instructors had to spend getting ready to teach this course.

Learning new course material, monitoring current events, and managing an active research agenda is time-consuming. We hope the instructor supplements make it easier to teach a high-quality course with less prep time.

ONLINE INSTRUCTOR RESOURCES The Pearson Higher Education website (www.pearsonglobaleditions.com/Boyle) has all of the supplements discussed below. These include the PowerPoint lectures, test item file, TestGen software, teacher's manual, and a sample syllabus.

POWERPOINT LECTURES There is a PowerPoint lecture for each chapter. They aren't "a few selected slides." They are full lectures with detailed figures and explanations. And they aren't made from figures that look pretty in the book but that are invisible on slides. We have tried to create the PowerPoint slides to be pretty self-explanatory.

TEST ITEM FILE The test item file for this book makes creating, or supplementing, an exam with challenging multiple-choice questions easy. Questions in the test item file refer directly to the Test Your Understanding questions located throughout each chapter. This means exams will be tied directly to concepts discussed in the chapter.

TEACHER'S MANUAL The Teacher's Manual has suggestions on how to teach the chapters. For instance, the book begins with threats. In the first class, you could have students list everybody who might attack them. Then have them come up with *ways* each group is likely to attack them. Along the way, the class discussion naturally can touch on chapter concepts such as the distinction between viruses and worms.

SAMPLE SYLLABUS We have included a sample syllabus if you are teaching this course for the first time. It can serve as a guide to structuring the course and reduce your prep time.

STUDENT FILES Study Guide and Homework files in Word are available for download by accessing www.pearsonglobaleditions.com/Boyle.

E-MAIL US Please feel free to e-mail us. You can reach Randy at BoyleRJ@Longwood.edu, or Ray at Ray@Panko.com. Your Pearson Sales Representative can provide you with support, but if you have a question, please also feel free to contact us. We'd also love suggestions for the next edition of the book and for additional support for this edition.

ACKNOWLEDGMENTS

We would like to thank all of the reviewers of prior editions. They have used this book for years and know it well. Their suggestions, recommendations, and criticisms helped shape this edition. This book really is a product of a much larger community of academics and researchers.

We would also like to thank the industry experts who contributed to this edition. Their expertise and perspective added a real-world perspective that can only come from years of practical experience. Thanks to Matt Christensen, Dan McDonald at Utah Valley University, Amber Schroader at Paraben Corp., Chris Larsen at BlueCoat Systems, Inc., David Glod at Grant Thornton, Andrew Yenchik, Stephen Burton, and Susan Jensen at Digital Ranch, Inc., Morpho, and Bruce Wignall at Teleperformance Group.

We thank our editor Bob Horan for his support and guidance. A good editor can produce good books. Bob is a great editor who produces great books. And he has done so for many years. We feel privileged to be able to work with Bob.

Special thanks go to Denise Vaughn, Karin Williams, Ashley Santora, and the production team that actually makes the book. Most readers won't fully appreciate the hard work and dedication it takes to transform the "raw" content provided by authors into the finished copy you're holding in your hands. Denise, Karin, Ashley, and the Pearson production team's commitment and attention to detail have made this into a great book.

Lastly, and most importantly, I (Randy) would like to thank Ray. Like many of you, I have used Ray's books for years. Ray has a writing style that students find accessible and intuitive. Ray's books are popular and widely adopted by instructors across the country. His books have been the source of networking and security knowledge for many workers currently in the industry.

I'm grateful that Ray trusted me enough to work on one of his books. I hope this edition continues in the legacy of great texts Ray has produced. It's an honor to work with a generous person like Ray.

Randy Boyle
Ray Panko

The publishers would like to thank the following for their contribution to the Global Edition:

Contributor

Sahil Raj, Punjabi University

Reviewers

Fabian Ng Yaw Tong, School of InfoComm Technology, Ngee Ann Polytechnic

Lucas Chi Kwong HUI, The University of Hong Kong

Ng Hu, Multimedia University

ABOUT THE AUTHORS

Randy Boyle is a professor at the College of Business and Economics at Longwood University. He received his PhD in Management Information Systems (MIS) from Florida State University in 2003. He also has a master's degree in Public Administration and a BS in Finance. His research areas include deception detection in computer-mediated environments, information assurance policy, the effects of IT on cognitive biases, and the effects of IT on knowledge workers. He has received college teaching awards at the University of Alabama in Huntsville, the University of Utah, and Longwood University. His teaching is primarily focused on information security, networking, and management information systems. He is the author of *Applied Information Security* and *Applied Networking Labs*.

Ray Panko is a professor of IT Management at the University of Hawai`i's Shidler College of Business. His main courses are networking and security. Before coming to the university, he was a project manager at Stanford Research Institute (now SRI International), where he worked for Doug Englebart (the inventor of the mouse). He received his BS in Physics and his MBA from Seattle University. He received his doctorate from Stanford University, where his dissertation was conducted under contract to the Office of the President of the United States. He has been awarded the Shidler College of Business's Dennis Ching award as the outstanding teacher among senior faculty. He is also a Shidler Fellow.

This page is intentionally left blank.

CHAPTER 1

The Threat Environment

Chapter Outline

Learning Objectives

After studying this chapter, you should be able to:

- Define the term *threat environment*.
- Use basic *security terminology*.
- Describe threats from *employees* and ex-employees.
- Describe threats from *malware* writers.
- Describe traditional external hackers and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks.
- Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation.
- Distinguish between *cyberwar* and *cyberterror*.

1.1 INTRODUCTION

The world today is a dangerous place for corporations. The Internet has given firms access to billions of customers and other business partners, but it has also given criminals access to hundreds of millions of corporations and individuals. Criminals are able to attack websites, databases, and critical information systems without ever entering the corporation's host country.

Corporations have become critically dependent on information technology (IT) as part of their overall competitive advantage. In order to protect their IT infrastructure from a variety of threats, and subsequent profitability, corporations must have comprehensive IT security policies, well-established procedures, hardened applications, and secure hardware.

Basic Security Terminology

THE THREAT ENVIRONMENT If companies are to be able to defend themselves, they need an understanding of the **threat environment**—that is, the types of attackers and attacks companies face. "Understanding the threat environment" is a fancy way of saying "Know your enemy." If you do not know how you may be attacked, you cannot plan to defend yourself. This chapter will focus almost exclusively on the threat environment.

The threat environment consists of the types of attackers and attacks that companies face.

The Threat Environment
- The threat environment consists of the types of attackers and attacks that companies face

Security Goals
- **Confidentiality**
  - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network
- **Integrity**
  - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data
- **Availability**
  - Availability means that people who are authorized to use information are not prevented from doing so

Compromises
- Successful attacks
- Also called incidents and breaches

Countermeasures
- Tools used to thwart attacks
- Also called safeguards, protections, and controls
- Types of countermeasures
  - Preventative
  - Detective
  - Corrective

FIGURE 1-1 Basic Security Terminology (Study Figure)

SECURITY GOALS Corporations and subgroups in corporations have **security goals**—conditions that the security staff wishes to achieve. Three common core goals are referred to collectively as **CIA**. This is not the Central Intelligence Agency. Rather, CIA stands for confidentiality, integrity, and availability.

- ***Confidentiality***—Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.
- ***Integrity***—Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.
- ***Availability***—Availability means that people who are authorized to use information are not prevented from doing so. Neither a computer attack nor a network attack will keep them away from the information they are authorized to access.

Many security specialists are unhappy with the simplistic CIA goal taxonomy because they feel that companies have many other security goals. However, the CIA goals are a good place to begin thinking about security goals.

COMPROMISES When a threat succeeds in causing harm to a business, this is called an **incident**, **breach**, or **compromise**. Companies try to deter incidents, of course, but they usually have to face several breaches each year, so response to incidents is a critical skill. In terms of the business process model, threats push the business process away from meeting one or more of its goals.

When a threat succeeds in causing harm to a business, this is called an incident, breach, or compromise.

COUNTERMEASURES Naturally, security professionals try to stop threats. The methods they use to thwart attacks are called **countermeasures**, **safeguards**, **protections**, or **controls**. The goal of countermeasures is to keep business processes on track for meeting their business goals despite the presence of threats and actual compromises.

Tools used to thwart attacks are called countermeasures, safeguards, or controls.

Countermeasures can be technical, human, or (most commonly) a mixture of the two. Typically, countermeasures are classified into three types:

- ***Preventative***—Preventative countermeasures keep attacks from succeeding. Most controls are preventative controls.
- ***Detective***—Detective countermeasures identify when a threat is attacking and especially when it is succeeding. Fast detection can minimize damage.
- ***Corrective***—Corrective countermeasures get the business process back on track after a compromise. The faster the business process can get back on track, the more likely the business process will be to meet its goals.

TEST YOUR UNDERSTANDING

1. **a.** Why is it important for firms to understand the threat environment?
   b. Name the three common security goals.
   c. Briefly explain each goal.
   d. What is an incident?

e. What are the synonyms for *incidents*?
f. What are countermeasures?
g. What are the synonyms for *countermeasure*?
h. What is the goal of countermeasures?
i. What are the three types of countermeasures?

CASE STUDY

The Sony Data Breaches

If this terminology seems abstract, it may help to look at a specific attack to put these terms into context and to show how complex security attacks can be. We will begin with one of the largest losses of private customer information. These were a series of data breaches at Sony Corporation.

Sony Corporation

Sony Corporation is a Japanese multinational corporation founded in 1946 that focuses on electronics, game, entertainment, and financial services. It employs about 146,300 people and has annual revenues of about $72.3 billion. Sony is widely known for its televisions, digital imaging, audio/video hardware, PCs, semiconductors, electronic components, and gaming platform.

The First Attack

The first of three attacks on Sony occurred on April 17–19, 2011, just weeks after the catastrophic earthquake, tsunami, and subsequent reactor meltdowns in Japan. Attackers used SQL injection to steal 77 million accounts containing personally identifiable information (PII) including names, addresses, dates of birth, usernames, passwords, security questions, and some credit card numbers.[1] Considering the amount and sensitive nature of the data stolen, this attack is easily one of the most severe losses of consumer data to date.

Sony detected unusual server activity on April 19 and brought in forensic examiners to determine if data may have been stolen.[2] On April 20, Sony turned off access to the entire 77 million-user Sony PlayStation Network (PSN) fearing that the attackers accessed user accounts. Sony then provided the FBI with information about the attack.

Sony publicly acknowledged the intrusion on April 26, more than a week after it became aware of it. Sony would later face scrutiny about its decision to delay telling its customers that attackers had access to their account information for a full week.

On April 30, the CEO of Sony, Kazuo Hirai, apologized to PSN gamers for the loss of their account information and the continuing PSN outage.[3] At the press conference Hirai said,

> These illegal attacks obviously highlight the widespread problem with cybersecurity. We take the security of our consumers' information very seriously and are committed to helping our consumers protect their personal data. In addition,

[1] Shane Richmond and Christopher Williams. "Millions of Internet Users Hit by Massive Sony PlayStation Data Theft," *The Telegraph*, April 26, 2011. http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html.
[2] Dean Takahashi, "Chronology of the Attack on Sony's PlayStation Network," *VentureBeat.com*, May 4, 2011. http://venturebeat.com/2011/05/04/chronology-of-the-attack-on-sonys-playstation-network/#QuSrgtEootxXhtil.99.
[3] Dean Takahashi, "Sony Executive Kaz Hirai Apologizes for PlayStation Network Outage," *VentureBeat.com*, April 30, 2011. http://venturebeat.com/2011/04/30/psn-outage-apolog/.

Sony Corporation

Multinational corporation focused on electronics, game, entertainment, and financial services

Has approximately 146,300 employees and $72.3 billion in revenue

The First Attack

Occurred weeks after a catastrophic earthquake, tsunami, and subsequent reactor meltdowns in Japan

SQL injection was used to steal 77 million accounts with personally identifiable information

PlayStation Network shutdown for weeks

More than a week delay in notifying users about the data loss

Increased level of security

The Second Attack

Additional 24.6 million accounts stolen from Sony Online Entertainment

Similar SQL injection attack

Greatly enhanced security put in place

PlayStation Network offline for about three weeks

The Third Attack

One million additional user accounts stolen from SonyPictures.com

Weeks after PlayStation Network comes back online

LulzSec takes credit

Attackers claim to have used a simple SQL injection technique

The Attack Method—SQL Injection

Sending modified SQL statements through web application

Unexpected values passed

Attempts to alter how SQL statement is processed

Can be used to manipulate stored data

Attackers and Their Motives

Members of LulzSec and Anonymous

Possibly motivated by Sony's lawsuit against George Hotz for jailbreaking PlayStation 3

Multiple arrests, convictions, prison sentences, and fines

Informant help identify other attackers

The Fallout

Sony provided free identity theft services and online games

£250,000 fine from the UK

Estimated losses at $171 million

FIGURE 1-2 The Sony Data Breaches (Study Figure)

(*continued*)

the organization has worked around the clock to bring these services back online, and are doing so only after we had verified increased levels of security across our networks.

The Second Attack

The ink wasn't dry from the humbling press conference when Sony found evidence of a new attack on May 1.[4] On May 2, forensic investigators found evidence that an *additional* 24.6 million user accounts were compromised in a similar SQL injection attack on Sony Online Entertainment. In addition to the user account information, more than 12,700 credit card numbers and 10,700 debit card numbers had been stolen. Sony later clarified that only 900 of the possible 12,700 credit card numbers were still active.[5]

All of Sony Online Entertainment servers were immediately taken down. The total number of lost accounts was now over 100 million. Hundreds of servers were shut down, gaming services were unavailable for millions of users, and future compensation costs were mounting.

On May 4, Kazuo Hirai submitted a written response to the U.S. Congress about the attacks.[6] He specifically mentioned the steps that Sony was taking to prevent future breaches including enhanced "data protection and encryption enhanced ability to detect software intrusions, unauthorized access and unusual activity patterns; additional firewalls; establishment of a new data center in an undisclosed location with increased security; and the naming of a new Chief Information Security Officer."

On May 15, some PSN services started coming online in select countries after being offline for about three weeks. Sony estimated that the costs related to the attacks would be over $171 million.[7] According to Sony, credit card companies had not reported any fraudulent transactions associated with the intrusion.

The Third Attack

Sony was besieged by yet another online SQL injection attack only a few weeks after PSN services started coming back online.[8] On June 2, a group named LulzSec posted a press release and multiple data files, claiming to have stolen over 1 million user accounts from SonyPictures.com.[9] The following is part of the LulzSec press release:

> Greetings folks. We're LulzSec, and welto Sownage. Enclosed you will find various collections of data stolen from internal Sony networks and websites, all of which we accessed easily and without the need for outside support or money.
>
> We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, e-mail addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts. Among other things, we also compromised all admin

[4] Jason Schreier, "Sony Hacked Again; 25 Million Entertainment Users' Info at Risk," Wired.com, May 2, 2011. http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.
[5] Dan Pearson, "24.6 Million SOE Accounts Potentially Compromised," *GameIndustry.biz*, May 3, 2011. http://www.gamesindustry.biz/articles/2011-05-03-24-6-million-soe-accounts-potentially-compromised.
[6] Patrick Seybold, "Sony's Response to the U.S. House of Representatives," *PlayStation.com*, May 4, 2011. http://blog.us.playstation.com/2011/05/04/sonys-response-to-the-u-s-house-of-representatives/.
[7] Mark Hachman, "Play Station Hack to Cost Sony $171M; Quake Costs far Higher," *PCMag.com*, May 23, 2011. http://www.pcmag.com/article2/0,2817,2385790,00.asp.
[8] Christina Warren, "Sony Pictures Website Hacked, 1 Million Accounts Exposed," *Mashable.com*, June 2, 2011. http://mashable.com/2011/06/02/sony-pictures-hacked/.
[9] Julianne Pepitone, "Group Claims Fresh Hack of 1 Million Sony Accounts," *CNN Money*, June 2, 2011. http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm.

details of Sony Pictures (including passwords) along with 75,000 "music codes" and 3.5 million "music coupons."[10]

The press release went on to give more details about the attack and the contents of the associated data files. The attackers used a simple SQL injection technique to extract the stolen information. They were also critical of Sony's security efforts.

> What's worse is that every bit of data we took wasn't encrypted. Sony stored over 1,000,000 passwords of its customers in plaintext, which means it's just a matter of taking it. This is disgraceful and insecure: they were asking for it.

The Attack Method—SQL Injection

What is SQL injection? SQL injection is an attack that involves sending modified SQL statements to a web application that will, in turn, modify a database. Attackers can send unexpected input through their web browser that will enable them to read from, write to, and even delete entire databases. SQL injection can even be used to execute commands on the server. SQL injection is a common attack method for many of the high-profile attacks seen in the news.

Below is a simple example of how SQL injection could be used.

****Warning***SQL injection can cause tremendous damage and harm. It is illegal to do on other systems and you will be prosecuted. Do not use SQL injection on any system without permission.*

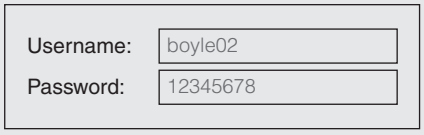


FIGURE 1-3 Normal Login

Normal SQL Statement for Login

Login screens require users to enter a username and password. These values are then passed to the web application and checked against values in the database. The SQL statement below shows how these parameters might be passed to a database for a legitimate login.

Information from this login is used to make the following SQL statement:

```
SELECT FROM Users WHERE
username='boyle02' AND
password='12345678';
```

Both the username (boyle02) and password (12345678) are strings that can include letters, numbers, and characters. They are both enclosed by single quotes, and the SQL statement ends with a semicolon.

Malformed SQL Statement for Login

In the SQL statement below, the password (12345678) is replaced with text (whatever' or 1=1—). This will alter how the SQL query is interpreted. Note that the additional single quote after the word "whatever" encloses the password. Since the actual password

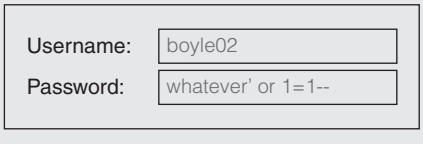


FIGURE 1-4 SQL Injection

(*continued*)

[10] The original press release was posted on http://lulzsecurity.com/. At the time of this writing, all content from the site had been removed.

(12345678) is not "whatever" the login should fail. However, the additional parameters will ensure that the login succeeds.

The rest of the injected SQL statement is processed normally. The logical operator "or" is used to create a two-part WHERE clause. The first part of the clause will return a false value for the WHERE clause. The second part of the clause, 1=1, will *always* return a *true* value. This *guarantees* that the login will succeed.

Information from this login is used to make the following malformed SQL statement:

```
SELECT FROM Users WHERE
username='boyle02' AND
password='whatever' or 1=1--';
```

In this case, SQL injection was used as a simple authentication bypass. In the case of the Sony data breaches, SQL injection was used to extract information from corporate databases through a web interface. SQL injection is covered in greater depth in Chapter 8.

Attackers and Their Motives

Members of two affiliated hacking groups, Anonymous and LulzSec, were likely behind the attacks on Sony. The Anonymous hacking group released a press statement denying involvement after Sony claimed to have found a file named "Anonymous" containing the text "We are Legion" after the first two attacks.[11]

Just before the Sony attacks, Anonymous said it was launching operation "#OpSony" in response to Sony's lawsuit against George Hotz.[12] Sony was suing George Hotz for jailbreaking its PlayStation 3. In a statement from Anonymous it said Sony would "experience the wrath of Anonymous."[13]

While LulzSec took credit for the third attack, on SonyPictures.com,[14] it's likely that the attackers were members of both groups. Numerous members of Anonymous and LulzSec were arrested for a variety of computer crimes. One such arrest occurred on September 22, 2011, when the FBI arrested Arizona native Cody Andrew Kretsinger.[15]

Kretsinger, AKA "recursion," pled guilty and was sentenced to one year and one day in federal prison after being convicted of federal computer hacking charges related to his involvement in the Sony attacks.[16] He was also ordered to perform 1,000 hours of community service and pay $605,663 in restitution.

Another LulzSec member, Hector Monsegur, AKA "Sabu," was awaiting sentencing at the time of this writing. Monsegur faces a possible 122 years in prison for various computer crimes. Federal investigators will likely recommend a greatly reduced sentence because he was the key informant who helped identify numerous other members of LulzSec.[17]

---

[11] Chris Davies, "Anonymous Denies Sony PSN 'We Are Legion' Calling Card," *SlashGear.com*, May 5, 2011. http://www.slashgear.com/anonymous-denies-sony-psn-we-are-legion-calling-card-05150280/.
[12] Sarah Purewal, "Sony Sues PS3 Hackers," *PCWorld.com*, January 12, 2011. http://www.pcworld.com/article/216547/Sony_Sues_PS3_Hackers.html.
[13] Michael Stone, "Anonymous #OpSony: DDoS Attacks Against Play Station Succeed," *Examin-er.com*, April 6, 2011. http://www.examiner.com/article/anonymous-opsony-ddos-attacks-against-playstation-succeed.
[14] Julianne Pepitone, "Group Claims Fresh Hack of 1 Million Sony Accounts," *CNN Money*, June 2, 2011. http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm.
[15] Kim Zetter, "FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous also Targeted," *Wired.com*, September 22, 2011. http://www.wired.com/threatlevel/2011/09/sony-hack-arrest/.
[16] Salvador Rodriquez, "LulzSec Hacker Sentenced to a Year in Federal Prison," *Los Angles Times*, April 18, 2013. http://articles.latimes.com/2013/apr/18/business/la-fi-tn-lulzsec-hacker-year-sentence-20130418.
[17] N. R. Kleinfield and Somini Sengupta, "Hacker, Informant and Party Boy of the Projects," *The New York Times*, March 8, 2012. http://www.nytimes.com/2012/03/09/technology/hacker-informant-and-party-boy-of-the-projects.html.

The Fallout

Following the data breaches, Sony offered its users compensation in the form of one year of free identity theft services, a month of free online gaming service, and couple games from a limited selection of games.[18] To date, no known credit fraud has occurred as a direct result of the Sony data breaches.

Sony was fined £250,000 (about $395,000) by the Information Commissioner's Office in the UK. Deputy Commissioner David Smith said that "the security measures were simply not good enough."[19] Other losses related to the attack are harder to quantify. While Sony estimates its direct losses at $171 million, it may be more difficult to quantify the impact of the series of data breaches on Sony's reputation.

TEST YOUR UNDERSTANDING

2. a. Who were the victims in the Sony breach?
b. How did the attackers steal the information from Sony? Explain.
c. What likely motivated the attackers?
d. What is SQL injection?
e. Were Sony's security measures strong enough? Why or why not?

1.2 EMPLOYEE AND EX-EMPLOYEE THREATS

Having looked at threats in general, at key security terminology, and at a particular compromise, we will now look at specific elements of the corporate threat environment. We will begin by looking inside the firm, at the threats created by employees. When firms began getting their own computers in the 1960s, they soon found that disgruntled and greedy employees and ex-employees are serious security threats. As firms have become more dependent on information technology, the threats from insiders have become more perilous.

Why Employees Are Dangerous

Employees and ex-employees are very dangerous for four reasons:

- They usually have extensive *knowledge* of systems.
- They often have the credentials needed to *access* sensitive parts of systems.
- They know corporate control mechanisms and so often know how to *avoid* detection.
- Finally, companies tend to *trust* their employees. In fact, when security insists that an employee behave in a particular way or explain an apparent security violation, it is common for the employee's manager to protect the employee against "security interference."

Employees and ex-employees are very dangerous because they have extensive knowledge of systems, have the credentials needed to access sensitive parts of systems, often know how to avoid detection, and can benefit from the trust that usually is accorded to "our people."

[18] Sony Online Entertainment LLC, "Customer Service Notification," *SOE.com*, May 2, 2011. https://www.soe.com/securityupdate/.
[19] BBC, "Sony Fined over 'Preventable' PlayStation Data Hack," *BBC.co.uk*, January 24, 2013. http://www.bbc.co.uk/news/technology-21160818.

Employees and Ex-Employees Are Dangerous

- Dangerous because
  - They have knowledge of internal systems
  - They often have the permissions to access systems
  - They often know how to avoid detection
  - Employees generally are trusted
- IT and especially IT security professionals are the greatest employee threats (*Quis custodiet custodes?*)

Employee Sabotage

- Destruction of hardware, software, or data
- Plant time bomb or logic bomb on computer

Employee Hacking

- Hacking is intentionally accessing a computer resource without authorization or in excess of authorization
- Authorization is the key

Employee Financial Theft

- Misappropriation of assets
- Theft of money

Employee Theft of Intellectual Property (IP)

- Copyrights and patents (formally protected)
- Trade secrets: plans, product formulations, business processes, and other info that a company wishes to keep secret from competitors

Employee Extortion

- Perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest

Sexual or Racial Harassment of Other Employees

- Via e-mail
- Displaying pornographic material

Employee Computer and Internet Abuse

- Downloading pornography, which can lead to sexual harassment lawsuits and viruses
- Downloading pirated software, music, and video, which can lead to copyright violation penalties
- Excessive personal use of the Internet at work

Non-Internet Computer Abuse

- Access to sensitive personal information motivated by curiosity
- In one survey at a security conference, one in three admitted to looking at confidential or personal information in ways unrelated to their jobs

Data Loss

- Loss of laptops and storage media

Other "Internal" Attackers

- Contract workers
- Workers in contracting companies

FIGURE 1-5 Employee and Ex-Employee Threats (Study Figure)

These factors often eliminate the need for sophisticated computer knowledge. In fact, in 23 financial services' cybercrimes committed between 1996 and 2002, 87 percent were accomplished without any sophisticated programming.[20]

IT employees are particularly dangerous because of their extraordinary knowledge and access. IT security employees are the most dangerous of all. The Department of Justice has a website, http://www.cybercrime.gov, which lists federal cybercrime prosecutions. Roughly half the cases have defendants who are IT professionals and even security employees and ex-employees. The Romans asked, *Quis custodiet custodes*? This translates as "Who watches the watchers?" This is one of the most difficult issues in IT security management.

Employee Sabotage

One of the oldest concerns about employees is **sabotage**, which is the destruction of hardware, software, or data. *Sabotage* comes from the French word for *shoe* because disgruntled workers in the early years of the Industrial Revolution supposedly threw their wooden shoes into machines to stop production.

IN THE NEWS

Tim Lloyd, a computer systems administrator, was fired for being threatening and disruptive. In retaliation, Lloyd planted a logic bomb program on a critical server. When pre-set conditions occurred, the logic bomb destroyed the programs that ran the company's manufacturing machines. Lloyd also took home and erased the firm's backup tapes to prevent recovery. Lloyd's sabotage resulted in $10 million in immediate business losses, $2 million in reprogramming costs, and 80 layoffs. The attack led to a permanent loss of the company's competitive status in the high-tech instruments and measurements market because the company could not rebuild the proprietary design software it had been using.[21]

Sabotage can also have *financial* motives. When Roger Duronio sabotaged 2,000 servers at UBS PaineWebber, he was not just punishing his ex-employer. He also sold UBS PaineWebber shares short to take advantage of the subsequent drop in the company's share price. Although the attack did extensive damage, the stock price did not drop, and Duronio lost money. Found guilty of computer sabotage and securities fraud, 63-year-old Duronio was sentenced to eight years in federal prison.[22]

---

[20] Marissa R. Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," U.S. Secret Service and the Carnegie Mellon Software Engineering Institute, August 2004.

[21] Sharon Gaudin, "Computer Saboteur Sentenced to Federal Prison," *Computerworld*, February 26, 2002. http://www.computerworld.com/s/article/68624/Computer_saboteur_sentenced_to_federal_prison.

[22] Sharon Gaudin, "Ex-UBS Systems Admin Sentenced to 97 Months in Jail," *InformationWeek*, December 13, 2006. http://www.informationweek.com/news/showArticle.jhtml?articleID=196603888.

IN THE NEWS

Two traffic engineers working for the city of Los Angeles plead guilty to hacking the city's traffic center and disconnecting signals at four of LA's busiest intersections. They locked out the controls for these intersections, so that it took four days to restore control. They did this a few hours before their union's scheduled job action against the city in support of contract negotiations. For this infraction, they received 240 days of community service and were required to have their computers at home and work monitored.[23]

Employee Hacking

Another concern is that employees will hack (break into) the company's computers using stolen credentials, flaws in internal systems, or some other fraudulent scheme. They can then embezzle money, steal intellectual property, or just look up embarrassing information.

As we will see in Chapter 10, U.S. law provides the following definition of **hacking**—intentionally accessing a computer resource without authorization or in excess of authorization. Definitions of hacking in other jurisdictions tend to be very similar.[24]

Hacking is intentionally accessing a computer resource without authorization or in excess of authorization.

Note that the key issue is **authorization**.[25] Were you explicitly (or implicitly) authorized to use the resource that you accessed? Were you authorized to use part of the resource but not the specific part that you accessed? The motivation for hacking is irrelevant. Penalties are the same whether you were attempting to steal a million dollars or were merely "testing security."[26]

Employee Financial Theft and Theft of Intellectual Property

There are many reasons for employees to access resources without permission or in excess of permission. Sometimes employees do so out of mere curiosity or to find information that could embarrass the company. At other times, however, they have purely criminal goals, such as **financial theft**, which involves the misappropriation of assets (say by assigning them via computer to themselves) or the theft of money (such as the manipulation of an application in order to be paid a bonus).

---

[23] Dan Goodin, "LA Engineers Cop to Traffic System Sabotage," *The Register*, November 6, 2008. http://www.theregister.co.uk/2008/11/06/traffic_control_system_sabotage/.

[24] The first documented use of the term *hacker* was in Steve Levy's book *Hackers*, in 1984 (Penguin Books). Levy actually decried the use of the term *hacker* to mean someone who breaks into computers illicitly. Rather, he argued that hackers were people who managed to hack out creative solutions to difficult computer problems. Some people in security continue to argue for Levy's viewpoint, using the term *cracker* as someone who breaks into computers. However, this is not the dominant usage in security and is certainly not widespread in the popular literature. The term *cracking* is now used primarily to refer to the breaking of passwords or encryption keys.

[25] In their defense, hackers can claim that they did not realize that authorization was required because the computer system that they hacked was public, like a free news website. Consequently, firms that have login screens or even public home pages should have a prominent warning that specific authorization is needed to use a site.

[26] Most hacking laws require damage to pass a certain level before the hacking can be prosecuted. However, it is quite possible for a hacker to do the requisite amount of damage accidentally, even if he or she did not intend to do so. While access has to be intentional, damage does not.

IN THE NEWS

In one case of financial theft, two accountants at Cisco Systems illegally accessed a corporate computer to issue themselves $8 million worth of Cisco stock. In fact, they successfully issued themselves stocks three times before being caught. They committed the crime by exploiting the company's poorly controlled procedures for issuing stock to employees.[27]

Another criminal motive is the theft of the company's **intellectual property (IP)**, which is information owned by the company and protected by law. IP includes formally protected information such as copyrights, patents, trade names, and trademarks. Although many companies have no such formal intellectual assets, IP also includes **trade secrets**, which are pieces of sensitive information that a firm acts to keep secret. These include plans, product formulations, business processes, price lists, customer lists, and many other types of information that a company wishes to keep secret from competitors. If another company obtains trade secrets in an illicit way, that company will be subject to prosecution. Nevertheless, some employees steal trade secrets to sell to another company.

Intellectual property (IP) is information that is owned by the company and protected by law. Trade secrets are pieces of sensitive information that a firm acts to keep secret.

IN THE NEWS

When scientists and engineers change jobs, there is always a danger that they will take trade secret information with them. One former DuPont research scientist admitted downloading trade secrets worth $400 million. Only when he announced his intention to leave was his downloading behavior analyzed. The analysis found that he had downloaded 16,700 documents and even more abstract—15 times the volume of the second-highest downloader. Most of these documents had nothing to do with his primary research area.[28]

Employee Extortion

In some cases, an employee or ex-employee will use his or her ability to damage systems or access confidential information to extort the firm. In **extortion**, the perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest. For instance, an employee might plant a logic bomb on the company's computer. If the

[27] U.S. Department of Justice, "Former Cisco Systems Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue $8 Million in Cisco Stock to Themselves," November 26, 2001. http://www.justice.gov/criminal/cybercrime/press-releases/2001/Osowski_TangSent.htm.

[28] Jaikumar Vijayan, "Scientist Admits Stealing Valuable Trade Secrets," *PC World*, February 16, 2007. http://www.pcworld.com/article/129116-1/article.html?tk=nl_dnxnws.

employee or ex-employee tells the company to pay money to avoid suffering damage, this is extortion. Stealing intellectual property and demanding money in exchange for not passing on the information is also extortion.

In extortion, the perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest.

Employee Sexual or Racial Harassment

Although hacking, theft, and extortion are critical issues, employee sexual or racial harassment is an even more common problem. Sexual harassment, for example, can include making physical threats, taking revenge after a romantic breakup, downloading and displaying pornography, or retaliating against an unwilling sexual partner by withholding promotions and raises.

IN THE NEWS

One such case began when a female employee spurned a male employee, Washington Leung. He left the firm and later logged into his ex-firm's servers using passwords given to him while employed there. He deleted over 900 files related to employee compensation. To frame the female employee, he gave her a $40,000 annual raise and a $100,000 bonus. In addition, he created a Hotmail account in her name and used the account to send senior managers at the company an e-mail containing some information from the deleted files. However, the frame failed. In his work computer at his new place of employment, authorities found evidence of the e-mail he sent to senior managers.[29]

Employee Computer and Internet Abuse

INTERNET ABUSE The term **abuse** is used for activities that violate a company's IT use policies or ethics policies. In some cases, employees abuse their Internet access, most commonly by downloading pornography, downloading pirated media or software, or wasting many hours surfing the Internet for personal purposes. Abuse ranges from mildly damaging behavior to criminal acts.

Abuse consists of activities that violate a company's IT use policies or ethics policies.

Downloading pornography can lead to sexual harassment lawsuits against the firm as well as against the responsible individual. Downloading pirated music, videos, and software, in turn, can result in extensive copyright violation penalties.[30] Downloading any unapproved files can also lead to expensive malware infections.

---

[29] U.S. Department of Justice, "U.S [sic] Sentences Computer Operator for Breaking into Ex-Employer's Database," March 27, 2002. http://www.justice.gov/criminal/cybercrime/press-releases/2002/leungSent.htm.

[30] In addition, pirated software often contains viruses that infect the downloader's computer and then infect other computers in the firm.

While many employers do not mind a small amount of personal Internet use, some employees become addicted to Internet use and spend tens of hours a week on personal websurfing at work.[31] In addition, when employees download numerous files from the Internet, they are likely to download a virus or some other malicious software.

IT security departments usually dislike searching for evidence of pornography and excessive personal websurfing, but this is part of the job in most firms.

NON-INTERNET COMPUTER ABUSE Another aspect of employee abuse is unauthorized access to private personal data on internal systems by curious employees. This type of behavior was detected in the 2008 U.S. presidential election campaign and in several celebrity hospitalizations.[32]

IN THE NEWS

During the 2008 presidential campaign, contract employees at the State Department looked at the passport histories of candidates Obama, Clinton, and McCain without permission.[33] "According to Infoworld.com: a breach was flagged by the State Department's in-house computer system; but supervisors downplayed the alarm."[34] Two of the contract workers have been fired by their employers. Later, Verizon announced that Obama's phone records had been accessed illegally.[35]

The abuse of internal corporate systems for voyeuristic purposes is not limited to general office employees. For example, a survey of 300 senior IT administrators in a London security conference and trade show found that one in three admitted to looking at confidential or personal information in ways unrelated to their jobs.[36]

Data Loss

The damaging employee behaviors we have looked at so far involve deliberate improper actions. Employees can also endanger the security of their firms through simple carelessness, by losing laptops, optical disks, and USB drives. The unauthorized release of data on these computers and media can be devastating to the firm. Even if the data is not actually used, the fact that it could be used may require the firm to take expensive actions.

---

[31] Raymond R. Panko and Hazel Beh, "Monitoring for Performance and Sexual Harassment," *Communications of the ACM*, in a special section on Internet Abuse in the Workplace, January 2002.
[32] Charles Ornestein, "UCLA Workers Snooped in Spears' Medical Records," *Los Angeles Times*, March 15, 2008. http://www.latimes.com/news/local/la-me-britney15mar15,0,1421107.story.
[33] Anne Flaherty and Desmond Butler, "Obama, Clinton and McCain's Passports Breached: Two State Dept Officials Fired, Investigation Underway," *Associated Press*, March 21, 2008 07:53 p.m. EST; published in the *Huffington Post*, January 14, 2009.
[34] Prolog, "Obama's Phone Records, Passport Documents Breached by Verizon Employees, Department of State Contractors," *Press Release*, December 14, 2008.
[35] Ibid.
[36] Gregg Keizer, "One in Three IT Admins Admit Snooping," *Computerworld*, June 22, 2008. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9101498.

A Ponemon survey in 2010 found that the average cost of a noncatastrophic data breach was $4 million. Primary causes of data loss were malicious or criminal attacks, negligence, system glitches, or third-party errors.[37]

Other "Internal" Attackers

Employees are not the only threats inside a firm's walls. Many businesses hire **contract workers**, who work for the firm for brief periods of time. Contract workers often get access credentials that are not deleted after their engagement ends. In fact, companies often hire other companies to do contracting work that takes place inside the original company's walls. These contracting companies and their employees also often receive temporary credentials. These contract workers and contracting firms create risks almost identical to those created by employees.

TEST YOUR UNDERSTANDING

3. a. Give four reasons why employees are especially dangerous.
b. What type of employee is the most dangerous?
c. What is sabotage?
d. Give the book's definition of hacking.
e. What is intellectual property?
f. What two types of things are employees likely to steal?
g. Distinguish between intellectual property in general and trade secrets.
h. What is extortion?
i. What is employee computer and Internet abuse?
j. Who besides employees constitute potential "internal" threats?

1.3 MALWARE

Although employees and other "internal" threats can be extremely dangerous, firms must also be concerned with traditional external attackers, who use the Internet to send malware into corporations, hack into corporate computers, and do other damage.

Malware Writers

The first external malware attackers were malware writers. The term **malware** generically means "evil software." The most widely known type of malware is the computer virus. Malware also includes worms, Trojan horses, RATs (remote access Trojans), spam, and several other types that we will see in this section.

Malware is a generic term for evil software.

Malware is a very serious threat. In June 2006, Microsoft reported results from a survey of users who allowed their computers to be scanned for malware. The scan found 16 million pieces of malware on the 5.7 million machines examined.

Viruses

Viruses are programs that attach themselves to legitimate programs on the victim's machine. Later, when infected programs are transferred to other computers and run, the virus attaches itself to other programs on those machines.

[37] Ponemon Institute, "Global Cost of a Data Breach," April 19, 2010. http://www.ponemon.org/data-security.

Viruses are programs that attach themselves to legitimate programs.

Initially, most viruses were spread through the transfer of programs via floppy disks. Today, viruses are spread via e-mail with infected attachments, instant messaging, file sharing programs, infected programs from malicious websites, and users deliberately downloading "free software" or pornography. Virus writers target popular operating systems and applications in order to maximize their damage. Through networked applications, viruses can spread very rapidly today.

IN THE NEWS

When Macintosh users searched BitTorrent sites in early 2009, they found that they were able to download the newly released Adobe Photoshop CS4. They would also download a program installed on the download CS4 on the downloader's computer. The copy of CS4 was clean, but when the downloader ran the cracking program, he or she got a dialog box saying that "Adobe CS4 Crack [intel] requires that you type your password." The dialog box had Name and Password data entry boxes, plus some cryptic details that made it look more authentic.[38]

FIGURE 1-6 Code for the ILOVEYOU Virus

[38] Andrew Nusca, "Mac Trojan Horse Found in Pirated Adobe Photoshop CS4," *ZDNet*, January 26, 2009. http://blogs.zdnet.com/gadgetreviews/?p=856&tag=nl.e539.

Malware

A generic name for any "evil software"

Viruses

Programs that attach themselves to legitimate programs on the victim's machine

Spread today primarily by e-mail

Also by instant messaging, file transfers, etc.

Worms

Full programs that do not attach themselves to other programs

Also spread by e-mail, instant messaging, and file transfers

In addition, direct-propagation worms can jump to from one computer to another without human intervention on the receiving computer

Computer must have a vulnerability for direct propagation to work

Direct-propagation worms can spread extremely rapidly

Blended Threats

Malware propagates in several ways—like worms, viruses, compromised webpages containing mobile code, etc.

Payloads

Pieces of code that do damage

Implemented by viruses and worms after propagation

Malicious payloads are designed to do heavy damage

FIGURE 1-7 Classic Malware: Viruses and Worms (Study Figure)

Worms

Viruses are not the only type of malware. One particularly important type of malware is the worm. Unlike viruses, worms are stand-alone programs that do not attach themselves to other programs.

Worms are stand-alone programs that do not attach themselves to other programs.

In general, worms act much like viruses and can propagate in many of the same ways. However, some worms have a far more aggressive spreading mode—jumping directly from one computer to another without user intervention on the receiving computer. Such **direct-propagation worms** take advantage of vulnerabilities (security weaknesses) in software. When a direct-propagation worm jumps to a computer that has the specific vulnerability for which the worm was designed, the worm can install itself on that computer and use that computer as a base to jump to other computers—all without any action on the user's part.

Direct-propagation worms jump directly to computers that have vulnerabilities; they then use these computers to jump to other computers.

IN THE NEWS

In September 2010, Iranian officials disclosed that 30,000 computers were infected with the Stuxnet worm. The worm was designed to infect industrial control systems produced by Siemens. This was the first known virus made specifically for industrial sabotage. The worm infected communication systems, electrical plants, and the Bushehr nuclear facility.[39]

Direct propagation can be very rapid, enabling the worm to do tremendous damage before it is detected and stopped. Researchers at the University of California at Berkeley estimated that a worst-case direct-propagation worm could do $50 billion in damage in the United States alone.[40]

Direct propagation requires no user action, so direct-propagation worms can spread extremely rapidly.

IN THE NEWS

On January 25, 2003, the Slammer worm exploded across the Internet. In 10 minutes—before more than a handful of people knew it existed—Slammer had infected 90 percent of all vulnerable computers on the entire Internet.[41] Despite the fact that Slammer did not erase hard disks or do other deliberate damage to the computers it infected, Slammer still caused massive damage by spreading so rapidly that it overwhelmed parts of the Internet.

Around the world, ATMs became unusable, police departments lost their ability to communicate, and most Internet users in Korea lost their service.[42] Had Slammer been deliberately malicious, it could have produced tens of billions of dollars in damage worldwide. Although Slammer's rapid flooding of the Internet was unprecedented, we now know that even faster "blitz worms" are possible.[43] Worms and related threats such as viruses are no longer weapons of mere mass annoyance. They can cause incredible losses.

---

[39] Thomas Erdbrink and Ellen Nakashima, "Iran Struggling to Contain 'Foreign-made' Computer Worm," September 28, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706606.html.
[40] Gregg Keizer, "Worst-Case Worm Could Rack Up $50 Billion in U.S. Damages," *CMP Techweb*, June 4, 2004. http://www.techweb.com/wire/story/TWB20040604S0006.
[41] David Moore, Vern Paxson, Stephan Savage, Colleen Shannon, Stuart Stainford, and Nicolas Weaver. "The Spread of the Sapphire/Slammer Worm," 2003. (Slammer was also called Sapphire.) http://www.caida.org/publications/papers/2003/saphire/saphire.html.
[42] Raymond R. Panko, "Slammer: The First Blitz Worm," *Communications of the AIS,* 11(12), February 2003, pp. 30–33.
[43] Vern Paxson, Stuart Stainford, and Nicholas Weaver, "How to Own the Internet in Your Spare Time," *Proceedings of the 11th USENIX Security Symposium (Security '02)*, 2002.

Blended Threats

If viruses and worms were not bad enough, a growing number of **blended threats** propagate both as viruses and worms. They can also post themselves on websites for people to download unwittingly. By propagating in multiple ways, blended threats increase their likelihood of success.

MessageLabs (http://www.messagelabs.com) keeps data on viruses, worms, and blended threats. In September 2010, MessageLabs reported that 1 in 218 e-mail messages contained viruses, worms, or blended threats. Phishing scams accounted for 1 in every 382 e-mails sent, and 92 percent of all e-mail was spam.[44]

Payloads

After viruses and worms propagate, they often execute **payloads**, which are pieces of code that do damage. Benign payloads merely pop up a message on the user's screen or do some other annoying but nonlethal damage. Unfortunately, some viruses and worms that have apparently benign payloads or even no payloads at all can do substantial damage. For example, although Slammer did not contain a payload, it spread so rapidly that it clogged networks with so much traffic that it effectively shut down parts of the Internet.

By contrast, **malicious payloads** can do extreme damage, for example, by randomly deleting files from the victim's hard disk drive or by installing some of the other types of malware described later in this section.

Virus and worm payloads also frequently "soften up" the computer by disabling its antivirus software and taking other actions that leave it highly vulnerable to subsequent virus and worm attacks.

TEST YOUR UNDERSTANDING

4. **a.** What is malware?
   b. Distinguish between viruses and worms.
   c. How do most viruses spread between computers today?
   d. Describe how directly propagating worms move between computers.
   e. Why are directly propagating worms especially dangerous?
   f. What is a virus or worm payload?

Trojan Horses and Rootkits

NONMOBILE MALWARE Viruses, worms, and blended threats are not the only types of malware, but they are the only types of malware that can forward themselves to other victims. Other forms of malware can spread to a machine only if they are placed there. Examples of ways to get nonmobile malware include the following:

- Having a hacker place it there
- Having a virus or worm place it there as part of its payload
- Enticing the victim to download the malware from a website or FTP site by portraying the malware as a useful program or data file
- Attaching hostile mobile code (described later) to a webpage and executing it on a victim's computer when the victim downloads the webpage.

---

[44] Symantec Corporation. "MessageLabs Intelligence September 2010," *MessageLabs*, September 2010. http://www.messagelabs.com/intelligence.aspx.

TROJAN HORSES Most nonmobile malware programs are Trojan horses. Early Trojan horses were programs that pretended to be one thing, such as a game or a pirated version of a commercial program, but really were malware. Many of these classic Trojan horses still exist. Today, however, when we talk about a **Trojan horse**, we mean a program that hides itself by deleting a system file and taking on the system file's name. Trojan horses are difficult to detect because they look like legitimate system files.

A Trojan horse is a program that hides itself by deleting a system file and taking on the system file's name. Trojan horses are difficult to detect because they look like legitimate system files.

REMOTE ACCESS TROJANS One common type of Trojan horse is the **remote access Trojan (RAT)**. A RAT gives the attacker remote control of your computer. The attacker can remotely do pranks, such as opening and closing your CD drive or typing things on your screen. However, they can also engage in more malicious activities. There are many legitimate remote access programs that allow a remote user to work on a machine or do diagnostics. However, RATs typically are stealthy in order to avoid detection by the owner of the machine.

Nonmobile Malware
- Usually placed on the user's computer through one of a growing number of attack techniques
  - Placed on computer by hackers
  - Placed on computer by virus or worm as part of its payload
  - The victim can be enticed to download the program from a website or FTP site
  - Mobile code executed on a webpage can download the nonmobile malware

Trojan Horses
- A program that replaces an existing system file, taking its name

Remote Access Trojans
- Allow the attacker to control your computer remotely

Downloaders
- Small Trojan horses that download larger Trojan horses after the downloader is installed

Spyware
- Programs that gather information about you and make it available to the adversary
- Cookies that store too much sensitive personal information
- Keystroke loggers
- Password-stealing spyware
- Data mining spyware

Rootkits
- Take control of the super user account (root, administrator, etc.)
- Can hide themselves from file system detection
- Can hide malware from detection
- Extremely difficult to detect (ordinary antivirus programs find few rootkits)

FIGURE 1-8 Trojan Horses and Rootkits (Study Figure)

Mobile Code
- Executable code on a webpage
- Code is executed automatically when the webpage is downloaded
- Javascript, Microsoft Active-X controls, etc.
- Can do damage if computer has vulnerability

Social Engineering in Malware
- Social engineering is attempting to trick users into doing something that goes against security policies
  - Several types of malware use social engineering
  - Spam (unsolicited commercial e-mail)
  - Phishing (authentic-looking e-mail and websites)
  - Spear phishing (aimed at individuals or specific groups)
  - Hoaxes

FIGURE 1-9 Other Malware Attacks (Study Figure)

DOWNLOADERS Some Trojan horses are **downloaders** (sometimes called **droppers**). They usually are fairly small programs, which makes detection difficult. After they are installed, however, they download a much larger Trojan horse capable of doing much more damage.

SPYWARE The term ***spyware*** refers to a broad spectrum of Trojan horse programs that gather information about you and make it available to an attacker.[45] There are several types of spyware.[46]

- **Cookies** are small text strings stored on your PC by websites. The next time you go to the website, the website can retrieve the cookie. Cookies have many benefits, such as remembering your password each time you visit. Cookies can also remember what happened last in a series of screens leading to purchases. However, when cookies record too much sensitive information about you, they become spyware. (Cookies are not Trojan horses per se, but we include them with other types of spyware.)
- **Keystroke loggers,** also known as keyloggers, capture all of your keystrokes. Your keystrokes can then be searched for usernames, passwords, social security numbers, credit card numbers, and other sensitive information. They can send this information to an attacker. Some keyloggers can record the websites you visit, the programs you run, and even take screenshots at specific intervals.
- **Password-stealing spyware** tells you that you have been logged out of the server you are visiting and asks you to retype your username and password. If you do, the spyware sends your username and password to the attacker.
- **Data mining spyware** searches through your disk drives for the same types of information sought by keystroke loggers. It also sends this information to the adversary.

[45] Although the biggest problem with spyware is the theft of information, spyware also tends to make computers run sluggishly.
[46] One new form of spyware is *camera spyware*, which spies on the victim visually by turning on a computer's camera and perhaps its microphone also.

ROOTKITS Trojan horses replace legitimate programs. A deeper threat is a set of programs called rootkits. In Unix computers, the **root** account is a super user account that has complete power over the computer. Although this super user account is called Administrator on Windows computer, super user accounts are referred to generically as root accounts. **Rootkits** take over the root account and use its privileges to hide themselves. They do this primarily by preventing their operating system's file-viewing methods from detecting their presence. Rootkits are seldom caught by ordinary antivirus programs, and rootkit detection programs often are specific to particular rootkits.

IN THE NEWS

In 2005, Sony BMG downloaded a rootkit onto the PCs of people playing Sony BMG media disks. The now-infamous discovery of this digital rights management rootkit generated extreme negative publicity. This negative publicity increased when it was learned that the rootkit left the PC open to attack by anyone.[47]

TEST YOUR UNDERSTANDING

5. **a.** How can nonmobile malware be delivered to computers?
   b. What is a Trojan horse?
   c. What is a RAT?
   d. What is a downloader?
   e. What is spyware?
   f. Why can cookies be dangerous?
   g. Distinguish between keystroke loggers, password-stealing spyware, and data mining spyware.
   h. Distinguish between Trojan horses and rootkits.
   i. Why are rootkits especially dangerous?

Mobile Code

When you download a webpage, it may contain executable code as well as text, images, sounds, and video. This is called **mobile code** because it executes on whatever machine downloads the webpage. Javascript is a popular language for writing mobile code. Microsoft Active X controls are also popular. In most cases, mobile code is innocent and often is necessary if a user wishes to use a website's functionality. However, if (and only if) the computer has the vulnerability used by a particular piece of mobile code, hostile mobile code will be able to exploit this vulnerability.

Social Engineering in Malware

Social engineering attacks take advantage of flawed human judgment by convincing the victim to take actions that are counter to security policies. For instance, if an employee receives an e-mail message warning about a mass layoff being imminent, he or she may open an attachment and therefore download a virus, worm, or Trojan horse. Although technology can provide many protections, it is very difficult for companies to protect against human misjudgment.

---

[47] Robert Lemos, "Hidden DRM Code's Legitimacy Questioned," *SecurityFocus*, November 2, 2005. http://www.securityfocus.com/news/11352.

Social engineering attacks take advantage of flawed human judgment by convincing the victim to take actions that are counter to security policies.

SPAM The bane of all e-mail users is **spam**, which is defined as unsolicited commercial e-mail. Although ISP, corporate, and personal spam filters have reduced the volume of spam greatly, people are still bombarded constantly by spam. In addition to being annoying, spam messages often are fraudulent or advertise dangerous products. Spam has become a common vehicle for distributing viruses, worms, Trojan horses, and many other types of malware. As mentioned earlier, MessageLabs reported that 92 percent of all e-mail messages were spam in September 2010. Some hosting providers have seen rates at 96 percent or higher.

Even the load on networks caused by simply transmitting and storing spam can be significant. This is especially true because many spammers now send spam that has image bodies instead of text bodies as a way to avoid detection from spam scanning programs. Image spam messages are much larger than traditional text spam messages.

PHISHING In **phishing attacks**, victims receive e-mail messages that appear to come from a bank or another firm with which the victim does business. The message may even direct the victim to an authentic-looking website. The official appearance of the message and website often fool the victim into giving out sensitive information. A small but significant fraction of all people who receive phishing messages respond to them because these messages seem so authentic. A Gartner survey in 2007 indicated that U.S. consumers were scammed out of $3.2 billion through phishing that year. More recently, EMC estimated phishing losses at $1.5 billion for 2012.[48] Phishing also causes many expensive help-desk calls within firms.

Security @ Work

Going Phishing

Phishing scams are used by criminals to fraudulently extract confidential information from users. These scams are creative, complex, and well organized. Criminals, typically located outside the United States, use a compromised server to host a fake website that gathers and automatically transmits information harvested from users. The example below shows how a typical phishing scam works.

The Scam

A phishing scam was sent to one of the authors (Randy.Boyle@utah.edu) on 5/12/2010 at 1:09 AM located in Salt Lake City, Utah. The "To" line read "info@helpdesk.org" not the author's e-mail address. The e-mail address listed for the sender of the e-mail was from a county health care administrator in Scottsville, Kentucky. The scam indicated that the user's mailbox was over its limit and they needed to log in and "validate" their quota.

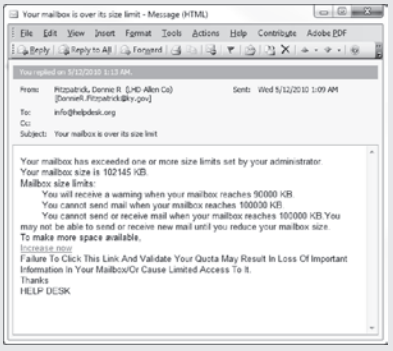
This phishing scam may or may not have originated from the e-mail server in Kentucky. However, it is likely that the e-mail server for the county health care organization was compromised. A trace of the e-mail showed that it came from a nearby e-mail server in Frankfort, Kentucky. However, the e-mail address could

[48] EMC Corporation, "The Year in Phishing," January 2013. http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf.

have been spoofed and the e-mails could have come from an entirely different e-mail server. Without more information from the administrators of those systems, it's difficult to say for sure.

The phishing scam itself was running within a website for a company in Jamestown, North Dakota, that makes tombstones. Yes, tombstones. The server associated with this IP address had several ports open including 21 (FTP), 53 (DNS), 80 (HTTP), 143 (IMAP), 443 (HTTPS), 587 (Sendmail), and 3306 (MySQL). Some of these services were likely being used legitimately by the tombstone company and others may have been initiated by the scammers.

The website that was compromised was being hosted by a hosting company in Tampa, Florida. The administrator for that hosting company was e-mailed within 10 minutes of getting the phishing scam. They were told that one of their machines was hosting an illegal phishing scam within a legitimate website. They never responded and the phishing scam remained up for several hours (or more).

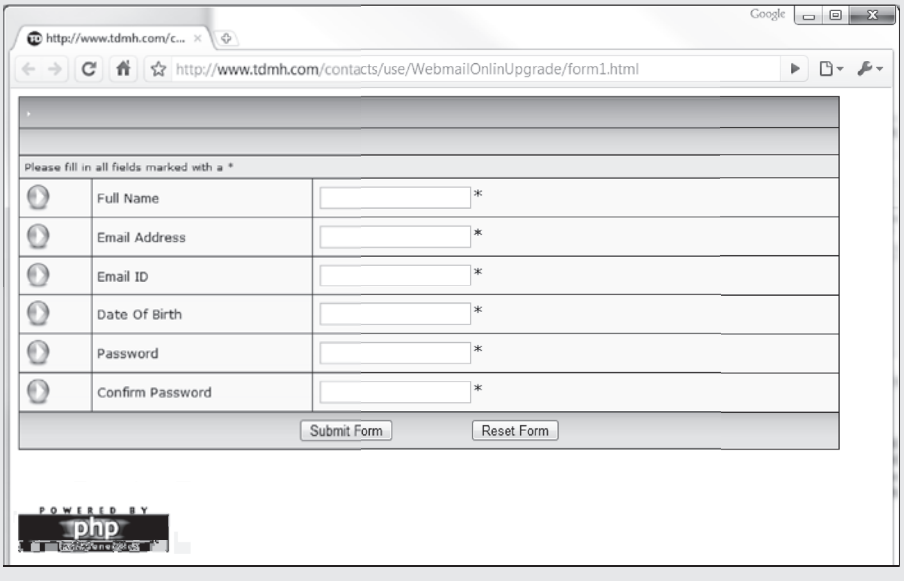


Phishing Scam E-Mail

Scam Part 2

A week later, on 5/20/2010, the same phishing scam was again sent. The "To" line read "admin@helpdesk.org." The sender's e-mail address was actually an e-mail address of a professor of clinical surgery (Oncology) at a large university in the western United States. An e-mail trace showed that the e-mail originated from a mail server on the same university network. The new scam website was modified to include fields for Full Name, E-mail ID, and Date of Birth. The first scam might have been very effective and the scammers decided to ask for more detailed information.

On the second attempt, the phishing scam was part of a compromised website for a commercial trucking company in Alpharetta,



Information Sought in Phishing Scam

(*continued*)

Georgia. The website was hosted by a hosting company in Philadelphia, Pennsylvania. The administrator for that hosting company was sent an e-mail within 10 minutes of receiving the phishing scam. The administrator for that hosting company responded almost immediately and said they had quarantined the site. This was an excellent response.

Phishing scams typically use webservers, e-mail servers, and compromised hosts in multiple states and countries. Phishing scams are a profitable criminal enterprise and will likely continue for some time.

There are several things users can do to protect themselves from phishing scams.

- Do not click on links within e-mails from people you don't know.
- Do not click on links within e-mails if you are not the intended recipient.
- Make sure the URL within the e-mail is linked to a legitimate site.
- Make sure the URL within the e-mail is not modified.
- Do not open attachments unless you were already expecting them.
- Administrators don't need your password, so don't give it to them.
- Report phishing scams to your systems administrator immediately.

Locations of Hosts Used in the Phishing Scam

SPEAR PHISHING Normal phishing attacks tend to appeal broadly to many people so that they can dupe as many victims as possible. By contrast, spear phishing attacks are aimed at single individuals or small groups of individuals. For instance, if an attacker's goal is to get the CEO of a corporation to download a Trojan horse, the attacker may craft an e-mail message that deals with a pressing issue for the CEO, appears to come from a trusted person, and contains specific details that only the trusted person is likely to know.

IN THE NEWS

In one case, a number of CEOs received a message disguising itself as a court order. The message directed the CEO to a website, uscourts.com. There, the CEO could find court documents could be downloaded, along with a plug-in to read the documents. The plug-in, of course, was spyware that searched the CEO's valuable computer.[49]

HOAXES Some e-mail messages contain hoaxes. In some cases, these hoaxes simply make the victim feel stupid when they tell other people what they "learned." In other cases, the hoaxes try to persuade the victim to damage their own system by deleting critical system files.

TEST YOUR UNDERSTANDING

6. **a.** What is mobile code?
   b. What is social engineering?
   c. What is spam?
   d. What is phishing?
   e. Distinguish between normal phishing and spear phishing.
   f. Why are hoaxes bad?

1.4 HACKERS AND ATTACKS

In the 1970s, malware writers were joined by external hackers, who began to break into corporate computers that were connected to modems. Today, nearly every firm is connected to the Internet, which harbors millions of external hackers. Hackers are able to break into corporate networks, steal confidential data, or do damage to critical infrastructure from thousands of miles away.

Traditional Motives

Most traditional external hackers did not cause extensive damage or commit theft for money. They were motivated primarily by the thrill of break-ins, by the validation of their skills, and by a sense of power. In addition, external hackers often communicated with one another. By demonstrating their ability to break into well-defended hosts, hackers could increase their reputations among their peers.[50] This type of attacker still exists.

Often, traditional hackers focused on embarrassing the victim. In 2009, for example, vandals broke into a computerized road sign in Austin, Texas, and changed its message to read, "The end is near! Caution! Zombies ahead!"[51] However, many traditional external hackers do engage in some direct theft, extortion, and other damage to support their "hobby."

---

[49] Robert McMillan, "Criminals Hack CEOs with Fake Subpoenas," *PC World*, April 14, 2008. http://www.pcworld.com/article/144548/article.html.

[50] Others have weirder motivations. British hacker Gary McKinnon reportedly broke into 73,000 U.S. government computers looking for evidence of extraterrestrial contacts. Ian Grant, "Garry McKinnon Broke into 73,000 U.S. Government Computers, Lords Told," *ComputerWeekly.com*, June 16, 2008. No longer available online.

[51] Dan X. McGraw, "Austin Road Sign Warns Motorists of Zombies," *The Dallas Morning News*, January 29, 2009. http://www.dallasnews.com/sharedcontent/dws/news/localnews/transportation/stories/013009dnmetzombies.1595f453.html.

Traditional Hackers
- Motivated by thrill, validation of skills, and sense of power
- Motivated to increase reputation among other hackers
- Often do damage as a by-product
- Often engage in petty crime

Anatomy of a Hack
- Reconnaissance probes
  - IP address scans to identify possible victims
  - Port scans to learn which services are open on each potential victim host
- The exploit
  - The specific attack method that the attacker uses to break into the computer is called the attacker's exploit
  - The act of implementing the exploit is called exploiting the host

IP Address Spoofing
- Attackers often use IP address spoofing to conceal their identities
- Putting false source IP addresses in reconnaissance and exploit packets
- Hiding the attacker's identity
- However, the attacker cannot receive replies sent by the victims to the false IP address

Chain of Attack Computers
- The attacker attacks through a chain of victim computers
- Probe and exploit packets contain the source IP address of the last computer in the chain
- The final attack computer receives replies and passes them back to the attacker
- Often, the victim can trace the attack back to the final attack computer
- But the attack usually can only be traced back a few computers more

FIGURE 1-10 Traditional External Attackers: Hackers (Study Figure)

TEST YOUR UNDERSTANDING

7. a. What were the motivations of traditional external hackers?
b. Did traditional external hackers engage in theft?

Anatomy of a Hack

Although there are many different ways to hack a computer, there is a general broad process that attackers often follow when they are attempting to hack a company's computers. It is similar to what a thief would do if he wanted to physically steal a company's computers.

TARGET SELECTION A hacker can randomly search all possible companies for a potential target or look up a specific company by name. A company's domain name can be resolved using a simple WHOIS lookup (www.whois.net). Corporations typically have blocks of contiguous IP addresses that they allocate to internal computers. Once the hacker knows the target IP address range, he can start probing the network for vulnerable hosts.

RECONNAISSANCE PROBES Before a thief breaks into a home, he or she often "cases" the neighborhood to look for vulnerable houses. The attacker then gathers information about potential victim houses to decide which ones to break into. Hackers also tend to do reconnaissance before breaking into a computer.[52] As Figure 1-11 shows, the attacker often sends probe packets into a network.[53] These probe packets are designed to elicit replies from internal hosts and routers. If internal hosts or routers respond to these probe packets, their responses can tell the attacker a great deal about the network.

IP Address Scanning The first round of probe packets is designed to find hosts that are active. The attacker sends **IP address scanning** probes to all IP addresses in target range. These probes often use the Internet Control Message Protocol (ICMP) Echo and Echo reply messages discussed in Module A. When a host receives an ICMP Echo message, it should send back an ICMP Echo reply message. When the attacker receives an ICMP Echo reply message from an IP address, it knows that there is a live host at that IP address.

Port Scanning Once the attacker knows the IP addresses of live hosts, he needs to know what programs the identified hosts are running because most attacks rely on vulnerabilities in specific programs. On server hosts, applications correspond to port numbers. Using the "home" metaphor, a port would be the equivalent of a door on a house.

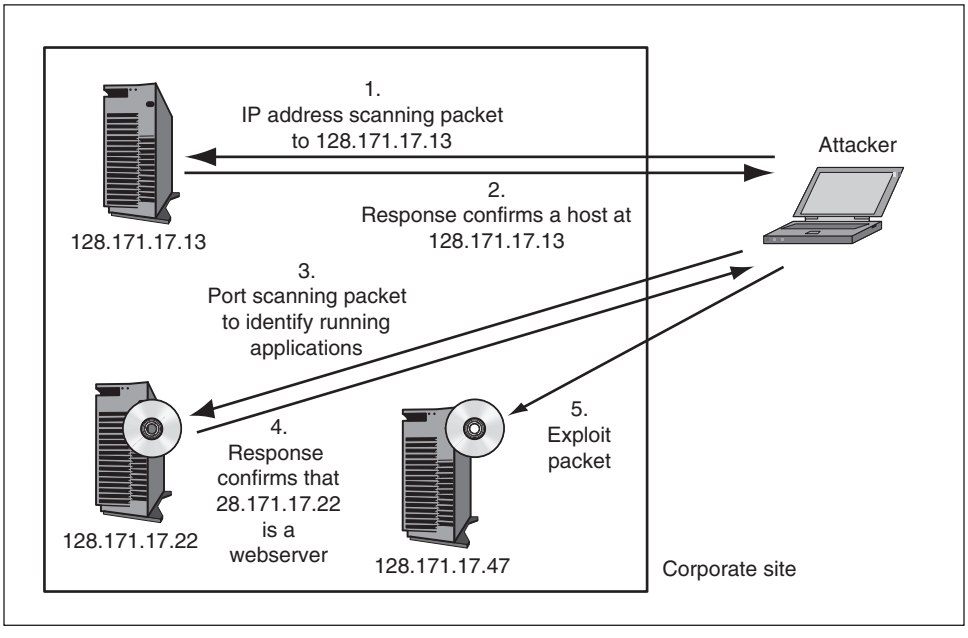


FIGURE 1-11 Probe and Exploit Attack Packets

[52] In one study in 2005, only about half of all attacks were preceded by scans, but if scans were done, the probability of a follow-on attack was high. Jaikumar Vijayan, "Port Scans Don't Always Precede Hacks," *Techworld*, December 13, 2005. http://www.techworld.com/security/news/index.cfm?NewsID=4991. Last accessed December 15, 2005.

[53] In 2003, it was estimated that 45–55 percent of all suspicious activity found by intrusion detection systems was hackers scanning for targets. Christine Burns, "Danger Zone," *Network World*, August 25, 2003. http://www.nwfusion.com/techinsider/2003/0825techinsiderintro.html.

For example, 80 is the well-known port number for HTTP webservers. If Port 80 is open, then the computer is probably a webserver. There are many well-known port numbers between 0 and 1023. Each indicates the presence of a particular type of application.

The attacker sends **port scanning** probes to each identified host in order to determine which applications the host is running. Typically, a port scanning program requests a connection to a program on a particular port number.[54] If the target sends back an agreement to proceed, the attacker knows that the target host is running a program on that port number.

THE EXPLOIT Once potential victim hosts and ports are identified, the attack can begin. In this case, the attacker sends exploit packets to victim hosts, instead of probe packets. The specific attack method that the attacker uses to break into the computer is called the attacker's **exploit**, and the act of implementing the exploit is called **exploiting** the host. If the exploit succeeds, the attacker "owns" at least an account and may "own" the computer itself. Owning a computer allows the attacker to do anything that he or she wishes.

SPOOFING Each packet carries a source IP address, which is like the return address on an envelope. The source IP address is dangerous for hackers because it allows corporations to locate the attackers. As Figure 1-12 shows, attackers can frustrate efforts to find them by **spoofing** the source IP address, that is, placing a different IP address in the source IP address field. This way, the victim cannot learn the attacker's true IP address.

Not all packets can be spoofed. For instance, the attacker usually must be able to read replies to probe packets. Victim replies are always sent to the host whose IP address is in the probe's source IP address field. If the attacker spoofs the IP address in probe packets, it will not receive the replies. Many exploits also need to receive replies in order to be successful.

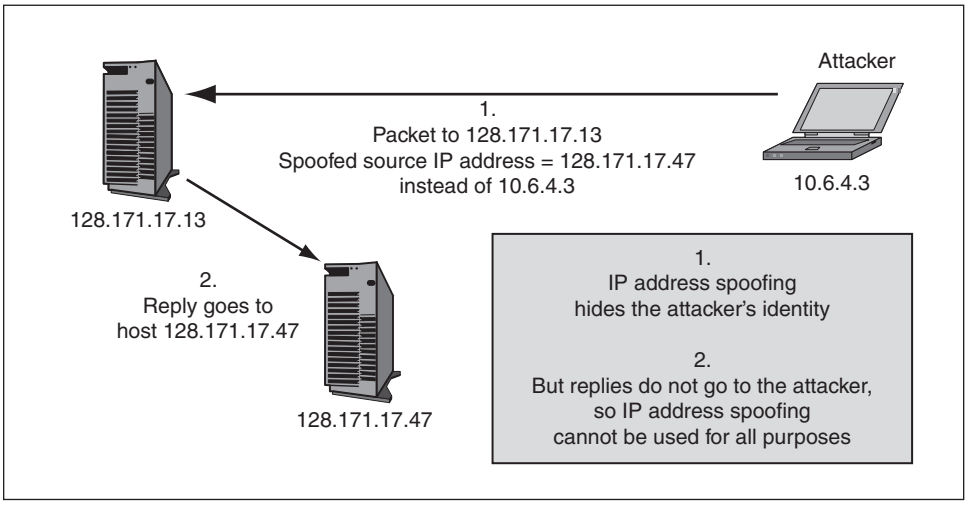


FIGURE 1-12 Source IP Address Spoofing

[54] If the program uses TCP at the transport layer, TCP segments requesting connections have their SYN bits set. Replies indicating a willingness to proceed set both the SYN and ACK bits.

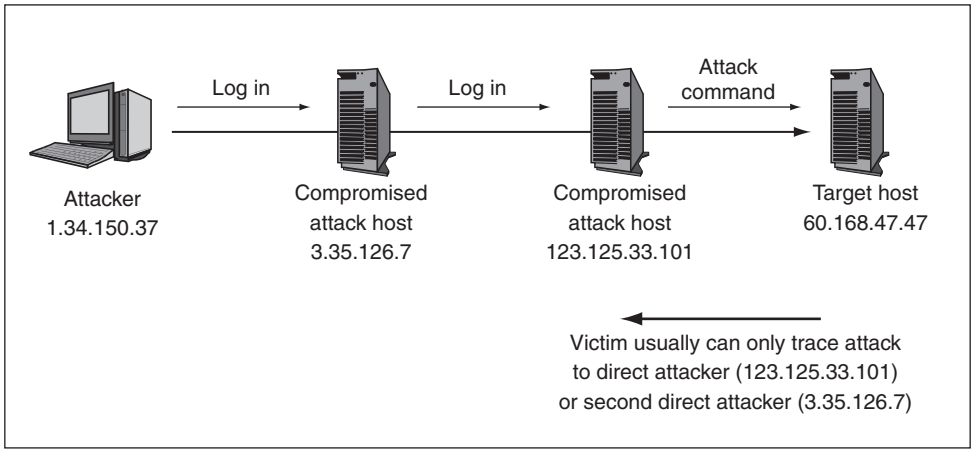


FIGURE 1-13 Chain of Attack Computers

Figure 1-13 shows that attackers who need to receive replies often work through a **chain of attack computers** previously compromised by the attacker.[55] Commands are passed through the chain to the final computer, which sends the probe or attack packets. Replies are also passed through the chain back to the attacker. The victim usually will be able to trace the attack back to the last computer in the chain and perhaps to one or two more hosts in the chain. Rarely can the victim trace the attack all the way back to the attacker's host because the chain of computers goes through multiple companies, states, and countries.

TEST YOUR UNDERSTANDING

8. a. Distinguish between IP address scanning and port scanning.
b. What is an exploit?
c. What does "owning" a computer mean?
d. What is IP address spoofing?
e. Why is IP address spoofing done?
f. When can an attacker not use IP address spoofing?
g. When attackers must use valid IP source addresses in probe or exploit packets, how do they conceal their identities?

Social Engineering in an Attack

Many external (and internal) attacks use social engineering, which, as we saw earlier, is attempting to trick users into doing something that goes against the interests of security. Compared to technical protections, human gullibility often is far easier to exploit. For example, a hacker calls a secretary claiming to be working with the secretary's boss. The hacker then asks for sensitive information, such as a password or even a restricted file.

[55] For example, the attacker may use Telnet to get from one computer to another. In the end, the attacker will be able to type commands that go directly to the final computer. To the attacker, it is not even apparent during operation that there are multiple computers between the attacker and the final computer.

IN THE NEWS

In a 2005 study, U.S. Treasury Department inspectors posing as computer technicians called 100 Internal Revenue Service employees and managers. The treasury agents asked each target for his or her username and asked the user to change his or her password to a specific password chosen by the "technician." This was a clear violation of policy, yet 35 percent fell for the ruse. As bad as this was, it was an improvement over 2001, when 71 percent changed their passwords.[56]

Other examples of social engineering include following someone through a secure door without entering a pass code (this is called **piggybacking**) and looking over someone's shoulder when he or she types a password (this is called **shoulder surfing**). In **pretexting**, the attacker calls claiming to be a certain customer in order to get private information about that customer.

Social Engineering
- Social engineering is often used in hacking
  - Call and ask for passwords and other confidential information
  - E-mail attack messages with attractive subjects
  - Piggybacking (walking through a door opened by another who has access credentials)
  - Shoulder surfing (watching someone type his or her password)
  - Pretexting (pretending to be someone and asking for information about that person)
  - Etc.
- Often successful because it focuses on human weaknesses instead of technological weaknesses

Denial-of-Service (DoS) Attacks
- Make a server or entire network unavailable to legitimate users
- Typically send a flood of attack messages to the victim
- Distributed DoS (DDoS) attacks
  - Bots flood the victim with attack packets
  - Attacker controls the bot

Skill Levels
- Expert attackers are characterized by strong technical skills and dogged persistence
- Expert attackers create hacker scripts to automate some of their work
- Scripts are also available for writing viruses and other malicious software
- Script kiddies use these scripts to make attacks
- Script kiddies have low technical skills
- Script kiddies are dangerous because of their large numbers

FIGURE 1-14 Attackers and Attacks (Study Figure)

[56] Marcia Savage, "Audit: IRS Employees Susceptible to Social Engineering," *SC Magazine*, March 18, 2005. http://www.scmagazine.com/audit-irs-employees-susceptible-to-social-engineering/article/31923/.

IN THE NEWS

In 2006, senior executives at Hewlett-Packard (HP) attempted to find the source of an information leak that must have come from someone on the board. A firm hired by HP allegedly used pretexting to get telephone call records about suspected leakers from the telephone company by pretending to be the suspected leakers.[57] Although the leaker was found, the revelation of pretexting used against board members sparked a fury. The board's chairperson, Patricia Dunn, and several other executives were forced to resign, and HP had to pay a $14.6 million fine to the state of California.[58]

TEST YOUR UNDERSTANDING

9. a. How can social engineering be used to get access to a sensitive file?
b. What is piggybacking?
c. What is shoulder surfing?
d. What is pretexting?

Denial-of-Service Attacks

Another type of external attack is the **denial-of-service (DoS) attack**. A DoS attack attempts to make a server or network unavailable to legitimate users. In terms of the CIA security goal taxonomy discussed earlier, DoS attacks are attacks on availability.

A denial-of-service (DoS) attack attempts to make a server or network unavailable to serve legitimate users by flooding it with attack packets.

Figure 1-15 illustrates the most common type of DoS attack, a **distributed denial-of-service (DDoS) attack**. In this exploit, the attacker first places programs called **bots** on many

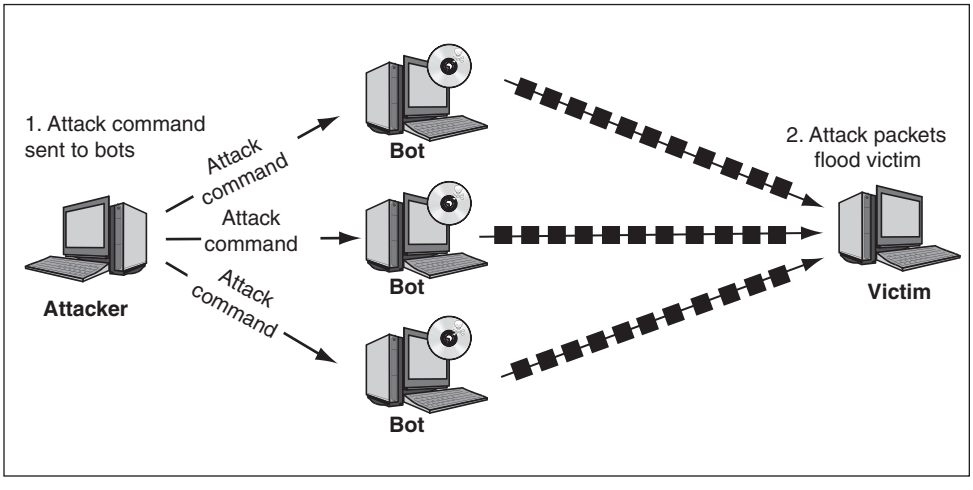


FIGURE 1-15 Distributed Denial-of-Service (DDoS) Flooding Attack

[57] Robert Lemos, "HP's Pretext to Spy," *Security Focus*, September 6, 2006. http://www.securityfocus.com/brief/296.
[58] Kelly Martin, "HP Pretexting Scandal Comes to Partial Close," *Security Focus*, December 8, 2006.

Internet hosts (clients, servers, or both). Later, when it is time to begin the DoS attack, the **botmaster** (or handler) sends a message to all of the bots. The bots then begin to flood the server or network listed in the attack message with attack packets. Soon, overloaded servers and networks cannot serve their legitimate users.

IN THE NEWS

Starting on July 4, 2009, dozens of websites in the United States and South Korea were attacked using a DDoS attack. The attack lasted several days and targeted, among others, the White House, the State Department, the Department of Homeland Security, and several South Korean government websites. It was estimated that 50,000+ bots were used in the coordinated attack.[59] The origin of the attackers is still unknown. A similar attack occurred again on March 20, 2013. This second attack took banks, TV stations, and insurance firms offline for several days.[60]

To attack a server, for instance, the bots might flood the server with TCP (Transmission Control Protocol) connection–opening requests (TCP SYN segments). A server reserves a certain amount of capacity each time it receives a SYN segment. By flooding a computer with SYN segments, the attacker can cause the server to run out of resources and therefore crash or be unable to respond to further connection-opening attempts from legitimate users. If the attack stream is especially heavy, the victim corporation's entire network will be unable to communicate over the Internet.

There are other ways of executing a DoS attack. Chapter 4 will look at additional DoS attack methods and ways of mitigating their effects. It will also look at other types of network attacks, such as ARP (Address Resolution Protocol) Poisoning and how to secure networks against external attacks.

IN THE NEWS

Jeanson Ancheta was indicted for crimes involving a large botnet. Ancheta was charged with creating the botnet and installing adware programs, which constantly pop up advertisements on these computers for a fee. He also was charged with renting parts of his botnet to other criminals for spam and denial-of-service attacks.[61] Ancheta pled guilty to four felony counts and was sentenced to 60 months in prison.

---

[59] Lolita Baldor, "US Largely Ruling Out NKorea in 2009 Cyberattacks," *Associated Press,* July 3, 2010. http://abcnews.go.com/Business/wireStory?id=11079735.

[60] John Leyden, "South Korean TV and Banks Paralysed in Disk-Wipe Cyber-Blitz," *The Register*, March 20, 2013. http://www.theregister.co.uk/2013/03/20/south_korea_cyberattack.

[61] Department of Justice, Central District of California, "Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers," November 3, 2005. http://www.cybercrime.gov/anchetaArrest.htm.

TEST YOUR UNDERSTANDING

10. a. What is a DoS attack?
b. Describe a DDoS attack.
c. Describe a SYN flooding attack in some detail.
d. Why do many botnets have multiple owners over time?

Skill Levels

Hollywood movies often portray hackers as geniuses who can break into tightly protected servers in a few seconds. In reality, *highly* skilled **hackers** usually need days or even months of hard work to break into a well-protected system—if they succeed at all. During this time, they will try many different attacks. In other words, skilled hackers are characterized by both high technical expertise and dogged persistence.

To automate some aspects of their attacks, hackers often write programs called **hacker scripts**. The term *script* traditionally has denoted a fairly crude program written in a simple language. Today's hacker scripts, however, often have easy-to-use graphical user interfaces and look like commercial software products.

In addition, automated hacker scripts and software are readily available on the Internet. These easy-to-use hacker scripts have created a new type of hacker—the **script kiddie**. This is a derogatory term that skilled hackers give to relatively unskilled hackers who use these pre-made scripts. Although individual script kiddies are much less likely to succeed in breaking into a computer than skilled hackers, there are far more script kiddies than skilled hackers. This makes script kiddies as a community extremely dangerous.

Furthermore, the large number of script kiddie attacks makes it difficult for corporations to identify the small number of highly dangerous attacks that companies face from very skilled attackers and that need special attention. In July 2002, Riptech (now owned by Symantec Corp.) examined data from 400 of its customers in detail. It noted that only about 1 percent of attacks were sophisticated aggressive attacks. However, when sophisticated aggressive attacks did appear, they were 26 times more likely to do severe damage than even moderately sophisticated aggressive attacks.

IN THE NEWS

In 2012, a 16-year-old Dutch teenager took control of more than 20,000 Twitter profiles. Damien Reijnaers gained control over the profiles by tricking users into signing up for a profile comparison tool called "Do you match with me." The illicit application was then used to post updates to the victim's profiles ridiculing them for poor security practices.[62]

Today, tools are available for creating all types of exploits. One of the most important is the Metasploit Framework, which makes it easy to take a new exploitation method and rapidly turns it into a full attack program. Metasploit is used both by attackers to launch attacks and by security professionals to test the vulnerability of their systems to specific exploits.

[62] John Leyden, "Dutch Script Kiddie Owns 20,000 Twitter Profiles," *The Register*, December 14, 2012. http://www.theregister.co.uk/2012/12/14/twitter_hijack_prank.

TEST YOUR UNDERSTANDING

11. a. What are the two primary characteristics of skilled hackers?
b. Why are script kiddies dangerous? (Give two reasons.)
c. Why are malware and exploit toolkits expanding the danger of script kiddies?

1.5 THE CRIMINAL ERA

Dominance by Career Criminals

Prior to about 2003, most external attackers were employees, ex-employees, or traditional external attackers interested only in fame and a feeling of power. Today, however, *most* external attackers are **career criminals**, who attack to make money illegally. They have traditional career criminal motives and many of their attack strategies are computer adaptations of traditional crimes.

Today, most external attackers are career criminals.

Contrary to popular belief, criminals are not slow to take advantage of new technologies. In 1888, Inspector John Bonfield of the Chicago police said, "It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class." During the 1930s, John Dillinger and many other criminals took advantage of newly affordable automobiles to rob banks and disappear before the police could apprehend them. License plates were introduced primarily to help police and to reduce the advantages of mobile criminals.

In addition, criminals do not make strong distinctions between various types of crimes. In 2003, for example, VeriSign examined IP addresses from which attacks came. It found a high correlation between the IP addresses used in hacking and those used in fraud.[63] To give another example, police who searched locations used in identity theft found meth pipes and other material indicating that the criminals were meth addicts using online identity theft to support their meth addictions. They were stealing information and selling it to other criminal groups.[64]

CYBERCRIME **Cybercrime**—the execution of crimes on the Internet—has become an extremely large problem in a very short period of time. According to the U.S. Treasury Department, cybercrime proceedings surpassed those from illegal drug sales in 2005.[65] In 2004, Internet crimes accounted for only 1.3 percent of all recorded crimes in Germany but accounted for 57 percent of the material damage caused by crimes.[66] In 2009, the FBI received 336,655 complaints of Internet-related crimes with reported losses totaling $559.7 million.[67] Cybercrime is not *becoming* an important problem for Internet security. It *has already become* the dominant problem.

---

[63] Carolyn Duffy Marsan, "VeriSign Correlates Hacker, Fraud Activity," *NetworkWorldFusion*, November 19, 2003. http://www.nwfusion.com/newsletters/isp/2003/1117isp2.html.
[64] Byron Acohido and Jon Schwartz, "'Meth Addicts' Other Habit: Online Theft," *USA Today*, December 15, 2005. http://www.usatoday.com/tech/news/internetprivacy/2005-12-14-meth-online-theft_x.htm.
[65] *Money.cnn.com*, "Record Bad Year for Computer Security," December 29, 2005. http://money.cnn.com/2005/12/29/technology/computer_security/index.htm.
[66] *Associated Press*, "Europe Council Looks to Fight Cybercrime: Group Pushes Ratification of International Treaty," September 15, 2004.
[67] Internet Crime Complaint Center, "2009 Internet Crime Report," October 4, 2010. http://www.ic3.gov/media/annualreports.aspx.

The Criminal Era

- Today, most attackers are career criminals with traditional criminal motives
- Adapt traditional criminal attack strategies to IT attacks (fraud, etc.)
- Many cybercrime gangs are international
  - Makes prosecution difficult
  - Dupe citizens of a country into being transshippers of fraudulently purchased goods to the attacker in another country
- Cybercriminals use black market forums
  - Credit card numbers and identity information
  - Vulnerabilities
  - Exploit software (often with update contracts)

Fraud, Theft, and Extortion

Fraud

- In fraud, the attacker deceives the victim into doing something against the victim's financial self-interest
- Criminals are learning to conduct traditional frauds and new frauds over networks
- Also, new types of fraud, such as click fraud

Financial and Intellectual Property Theft

- Steal money or intellectual property they can sell to other criminals or to competitors

Extortion

- Threaten a DoS attack or threaten to release stolen information unless the victim pays the attacker

Stealing Sensitive Data about Customers and Employees

- Carding (credit card number theft)
- Bank account theft
- Online stock account theft
- Identity theft
  - Steal enough identity information to represent the victim in large transactions, such as buying a car or even a house

Corporate Identity Theft

- Theft of a corporation's identity

FIGURE 1-16 The Criminal Era (Study Figure)

INTERNATIONAL GANGS Due to the interconnected nature of the Internet, national borders and passports are irrelevant. As a result, criminal enterprises are able to freely commit a variety of cybercrimes without worrying about foreign countries prosecuting them for crimes committed against victims within their borders. When prosecution does result, it typically is only because of creativity on the part of prosecutors.

IN THE NEWS

Russian hacker Vasiliy Gorshkov stole credit card numbers and other personal information from numerous computers in the United States. He received a job offer from a U.S. recruiting firm, Invita. He was required to demonstrate hacking skills against a test network before coming to the United States. At a job interview with Invita in Seattle, he discussed hacking freely. When asked about his concerns with the FBI, he said that the FBI was no problem because the FBI could not get him in Russia. Yes, you guessed it. Invita was an FBI front. Gorshkov was tried and convicted.[68]

One problem that international gangs have is that many online sellers will not ship to addresses outside of the United States. To get around this problem, criminal gangs engage **transshippers** in the United States. These people receive shipped goods at U.S. offices and then ship them to the criminal gang in another country. Transshippers are paid a fee for each package they transship. Often, the transshippers are solicited over the Internet and never realize that they are doing anything to help criminals. Similarly, international gangs use **money mules** to transfer money (in return for a small percentage fee paid to the money mule). Often, transshippers and money mules are recruited through online job sites.

BLACK MARKETS AND MARKET SPECIALIZATION Traditional criminals have always worked cooperatively. For example, fences buy stolen goods from thieves at a discount and then resell the stolen goods at apparently legitimate outlets where the origin of the goods will not be obvious.

Internationally, there are many **black market websites** for stolen consumer information.[69] There are even going rates for credit card numbers, with price being determined by how well the credit card numbers have been validated, for instance, by making a small purchase with each card number to ensure that the number is "live."[70]

IN THE NEWS

Researcher Dan Clements of CardCops (http://www.cardcops.com) posted fake credit card information on a website.[71] He leaked information about the website to a few chat rooms frequented by hackers. Within 15 minutes, the website had been visited by 74 carders from 31 different countries. By the end of the weekend, 1,600 carders had visited the site.

In 2008, the Symantec Corporation (http://www.symantec.com) reported typical prices in hacker forums. U.S. credit cards with the card verification value went for between $0.50 and $12 per card. Full identity theft information (U.S. bank account with password, credit card information, date of birth, etc.) went for between $0.90 and $25. Bank account credentials went for $10 to $1,000, depending on the balance. E-mail accounts with passwords went for between $4 and $30.

---

[68] U.S. Department of Justice, "Russian Computer Hacker Convicted by Jury," October 10, 2001. www.cybercrime.gov/gorshkovconvict.htm.
[69] Byron Acohido and Jon Schwartz, "Cybercrime Flourishes in Online Hacker Forums," *USA Today*, October 11, 2006.
[70] Carders and identity thieves also prey on one another. One practice is ripping—selling credit card numbers that are known to be invalid.
[71] Bob Sullivan, "Net Thieves Caught in Action," www.MSNBC.com, March 15, 2002. http://www.cardcops.com/msnbc/msnbc5.htm.

Most black markets deal in credit card and identity information. However, there are also black markets for malware, botnets, and newly discovered vulnerabilities. When an analyst discovers a security vulnerability in a piece of software, he or she usually notifies the software company, which credits the analyst when a patch is released. However, software companies rarely pay vulnerability discoverers. As a consequence, a growing number of analysts sell vulnerability discoveries on one of several vulnerability black market.

Other programmers write exploitation software and sell it on black markets. In most cases today, exploitation software is sold with a provision for online support and free updates. After purchase, payments may even be held in escrow until the buyer has tested the exploitation software.

In many ways, cybercrime is maturing like many traditional markets. At the beginning, all-in-one companies usually dominate in a new market. Later, vertical and horizontal specialization appear. In cybercrime, some criminals search for exploits, others develop toolkits, others specialize in distribution and botnet management, others run markets for identity theft and credit card numbers, and others create shared codes and libraries. Over time, new market niches continue to appear rapidly.

Security @ Work

Zeus

On October 1, 2010, the FBI announced that it had identified an international criminal organization that was using a Trojan horse named "Zeus" to steal over $260 million.[72] Zeus had infected approximately 4 million hosts in almost 200 countries. Criminals had purchased Zeus for $700–$4,000 and then infected target computers through phishing scams or infected downloads.

Zeus would use a keylogger to record login information for banks, social networks, e-mail accounts, and so on.[73] Criminals would then remotely retrieve the login information from the compromised computer. They would use this login information to access the victim's bank account and transfer funds to money mules.

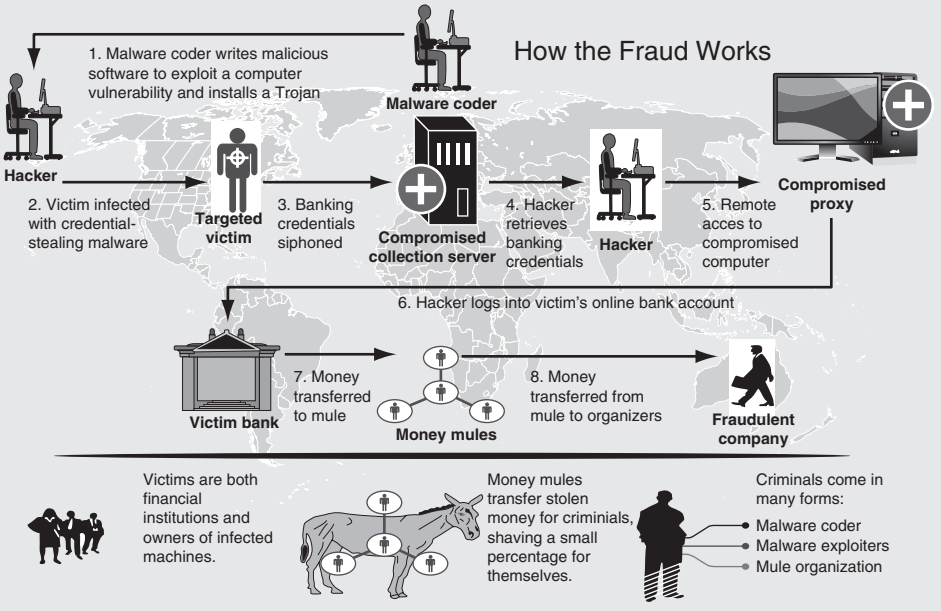
The money mules would take a percentage and then transfer the rest of the funds to overseas accounts in Europe. The below figure, released by the FBI, shows how the criminal gang used Zeus to infect target computers and receive the stolen funds.

The FBI has arrested more than 100 suspects, including 90 within the United States. In addition to transferring stolen funds, these suspects are accused of using fake passports and documentation to open numerous bank accounts.

In the press release about the arrests, FBI Director Robert Mueller said, "No one country, no one company, and no one agency can stop cybercrime. The only way to do that is by standing together. For ultimately, we all face the same threat. Together, the FBI and its international partners can and will find better ways to safeguard our systems, minimize these attacks, and stop those who would do us harm."[74]

(*continued*)

[72] Jeremy Kirk, "Zeus Botnet Thriving Despite Arrests in the US, UK," *CIO.com*, October 2, 2010. http://www.cio.com.au/article/363041/zeus_botnet_thriving_despite_arrests_us_uk.
[73] FBI National Press Office, "International Cooperation Disrupts Multi-Country Cyber Theft Ring," *FBI.gov*, October 1, 2010. http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud.
[74] Robert S. Mueller, III, "International Cooperation Disrupts Multi-Country Cyber Theft Ring," *FBI.gov*, October 1, 2010. http://www.fbi.gov/pressrel/pressrel10/tridentbreach100110.htm.



How Zeus Is Used

Suspects Sought For Involvement In Theft Ring

Source: http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud

TEST YOUR UNDERSTANDING

12. a. What is the dominant type of attacker today?
b. Is cybercrime negligible today compared to noncomputer crime?
c. Why are international gangs difficult to prosecute?
d. Why do international gangs use transshippers?
e. How do they use transshippers?
f. How do they use money mules?

Fraud, Theft, and Extortion

Fraud, theft, and extortion are traditional criminal attacks. Today, criminals have learned to execute these crimes over networks.

FRAUD Criminals attempt to get money illicitly in a number of ways. We will list just a few in this chapter. One characteristic of many of these criminal attacks is that they involve fraud. In **fraud**, the attacker deceives the victim into doing something against the victim's financial self-interest. For example, in the T-Data example given later in this chapter, the attacker defrauded a company into giving him equipment by pretending to be a real company that would pay.

In fraud, the attacker deceives the victim into doing something against the victim's financial self-interest.

There is nothing new about fraud. In the physical world, fraud has been perpetrated since the beginning of humankind. Cyber criminals are simply learning how to conduct classical fraud schemes over computer networks. Most spam messages, for example, use classic fraud methods and have classic fraud goals.

In other cases, criminals are creating new network-specific frauds. For instance, many websites get paid by advertisers on a per-click basis. Every time a website visitor clicks on an advertising link at the website the advertiser pays the original website a small fee. In **click fraud**, a criminal website owner creates a program to click on the link repeatedly. Each of these bogus clicks takes money from the advertiser without generating potential customers.

FINANCIAL AND INTELLECTUAL PROPERTY THEFT Just as career criminals have long burgled homes and robbed banks, career criminals on the Internet engage in financial theft.

In other cases, career criminals steal a firm's intellectual property for sale to other criminals or to corporate competitors. As noted earlier in the chapter, intellectual property (IP) consists of formally protected information such as patents and other information and trade secrets, which are sensitive pieces of information that the company acts to protect, such as corporate plans and even price lists.

In a recent report by the Commission on the Theft of American Intellectual Property, it was estimated that IP theft is costing the United States $300 billion a year. The report notes that the majority of the theft is done through cyber espionage.[75]

[75] Emma Woollacott, "US Should Get Tough on Chinese IP Theft, Committee Warns," *Forbes*, May 23, 2013. http://www.forbes.com/sites/emmawoollacott/2013/05/23/us-should-get-tough-on-chinese-ip-theft-committee-warns/.