Chapter 7: Computer and Network Security

Ethics for the Information Age
Fifth Edition

by
Michael J. Quinn

PEARSON

ALWAYS LEARNING

Chapter Overview

- Introduction
- Hacking
- Malware
- Cyber crime and cyber attacks
- Online voting

7.1 Introduction

- Computers getting faster and less expensive
- Utility of networked computers increasing
  - Shopping and banking
  - Managing personal information
  - Controlling industrial processes
- Increasing use of computers $\rightarrow$ growing importance of computer security

7.2 Hacking

Hackers, Past and Present

- Original meaning of hacker: explorer, risk taker, system innovator
  - MIT's Tech Model Railroad Club in 1950s
- Modern meaning of hacker: someone who gains unauthorized access to computers and computer networks

Computer Fraud and Abuse Act

- Criminalizes wide variety of hacker-related activities
  - Transmitting code that damages a computer
  - Accessing any Internet-connected computer without authorization
  - Transmitting classified government information
  - Trafficking in computer passwords
  - Computer fraud
- Maximum penalty: 20 years in prison and $250,000 fine

Sidejacking

- Sidejacking: hijacking of an open Web session by capturing a user's cookie
- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"
- Internet security community complained about sidejacking vulnerability for years, but ecommerce sites did not change practices

Case Study: Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser
- Firesheep made it possible for ordinary computer users to easily sidejack Web sessions
- More than 500,000 downloads in first week
- Attracted great deal of media attention
- Early 2011: Facebook and Twitter announced options to use their sites securely

Utilitarian Analysis

- Release of Firesheep led media to focus on security problem
- Benefits were high: a few months later Facebook and Twitter made their sites more secure
- Harms were minimal: no evidence that release of Firesheep caused big increase in identity theft or malicious pranks
- Conclusion: Release of Firesheep was good

Kantian Analysis

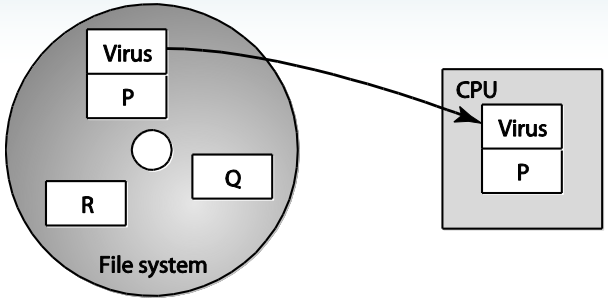
- Accessing someone else's user account is an invasion of their privacy and is wrong
- Butler provided a tool that made it much simpler for people to do something that is wrong, so he has some moral accountability for their misdeeds
- Butler was willing to tolerate short-term increase in privacy violations in hope that media pressure would force Web retailers to add security
- He treated victims of Firesheep as a means to his end
- It was wrong for Butler to release Firesheep

7.3 Malware

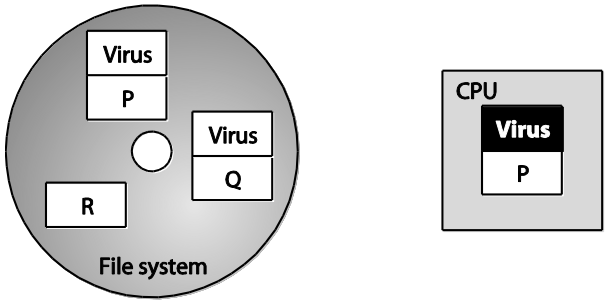
Viruses

- Virus: Piece of self-replicating code embedded within another program (host)
- Viruses associated with program files
  - Hard disks, floppy disks, CD-ROMS
  - Email attachments
- How viruses spread
  - Diskettes or CDs
  - Email
  - Files downloaded from Internet

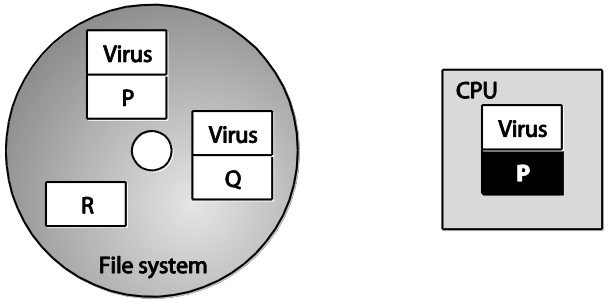
How a Virus Replicates



(a)

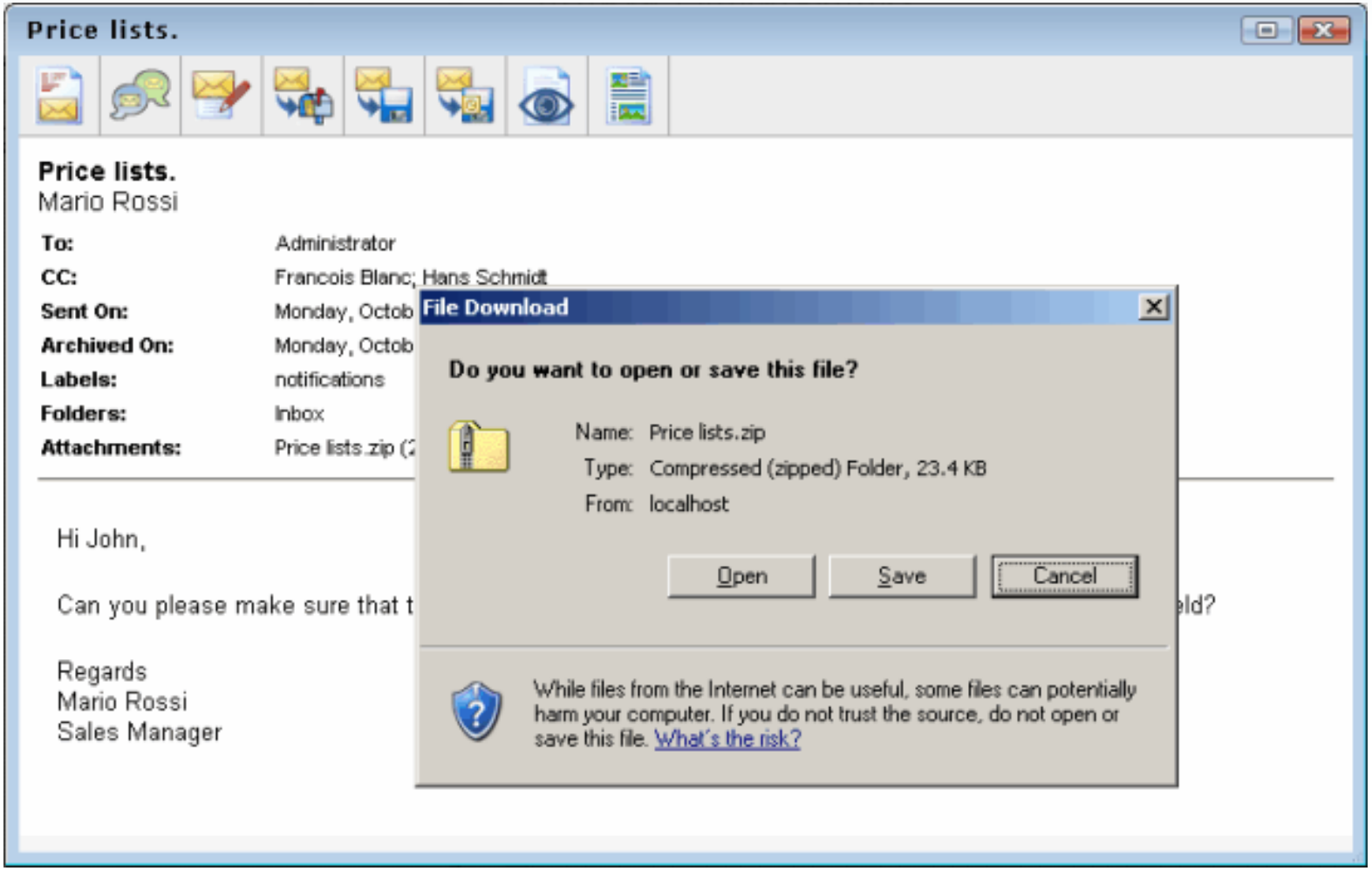


(b)

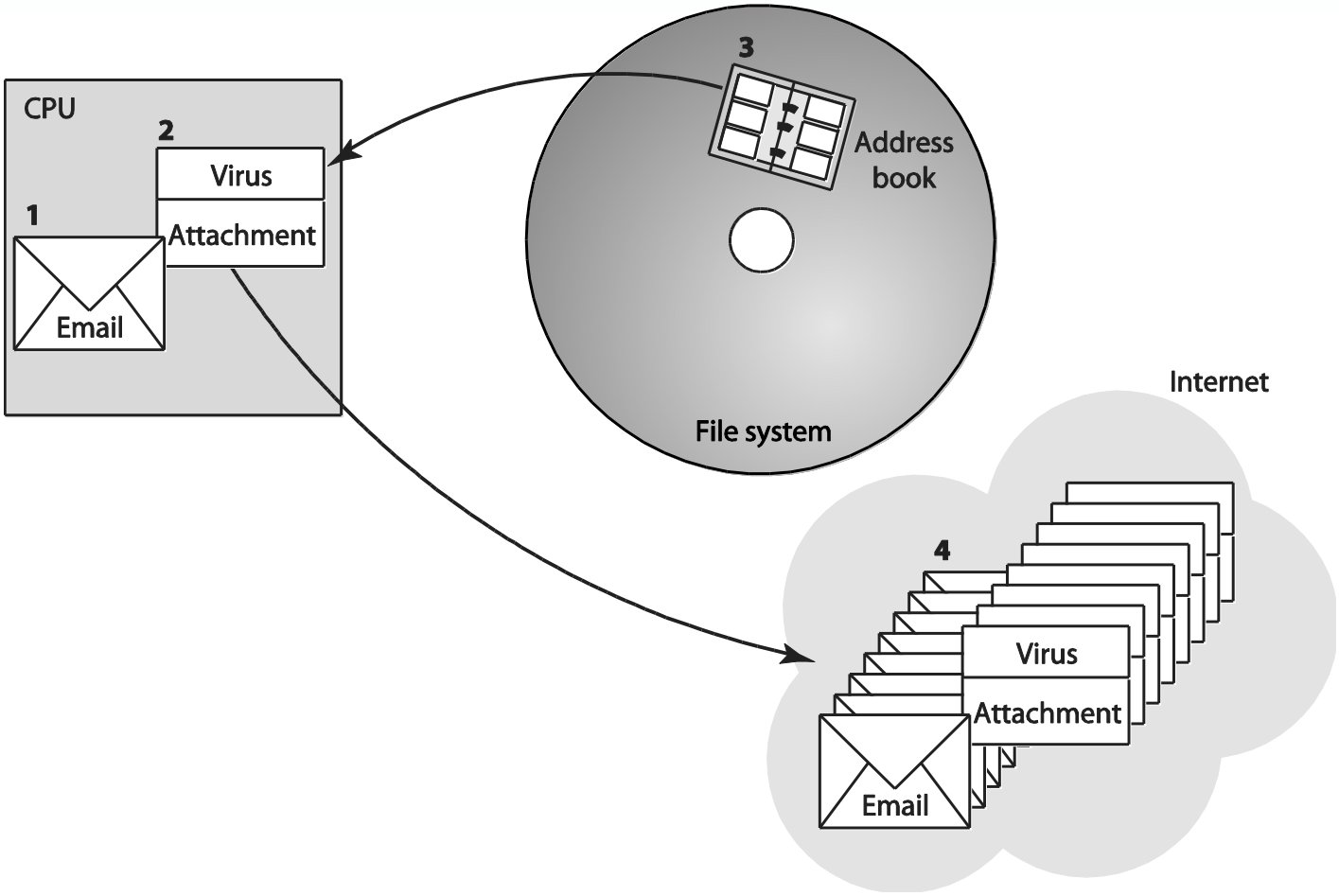


(c)

Email Attachment with Possible Virus



How an Email Virus Spreads



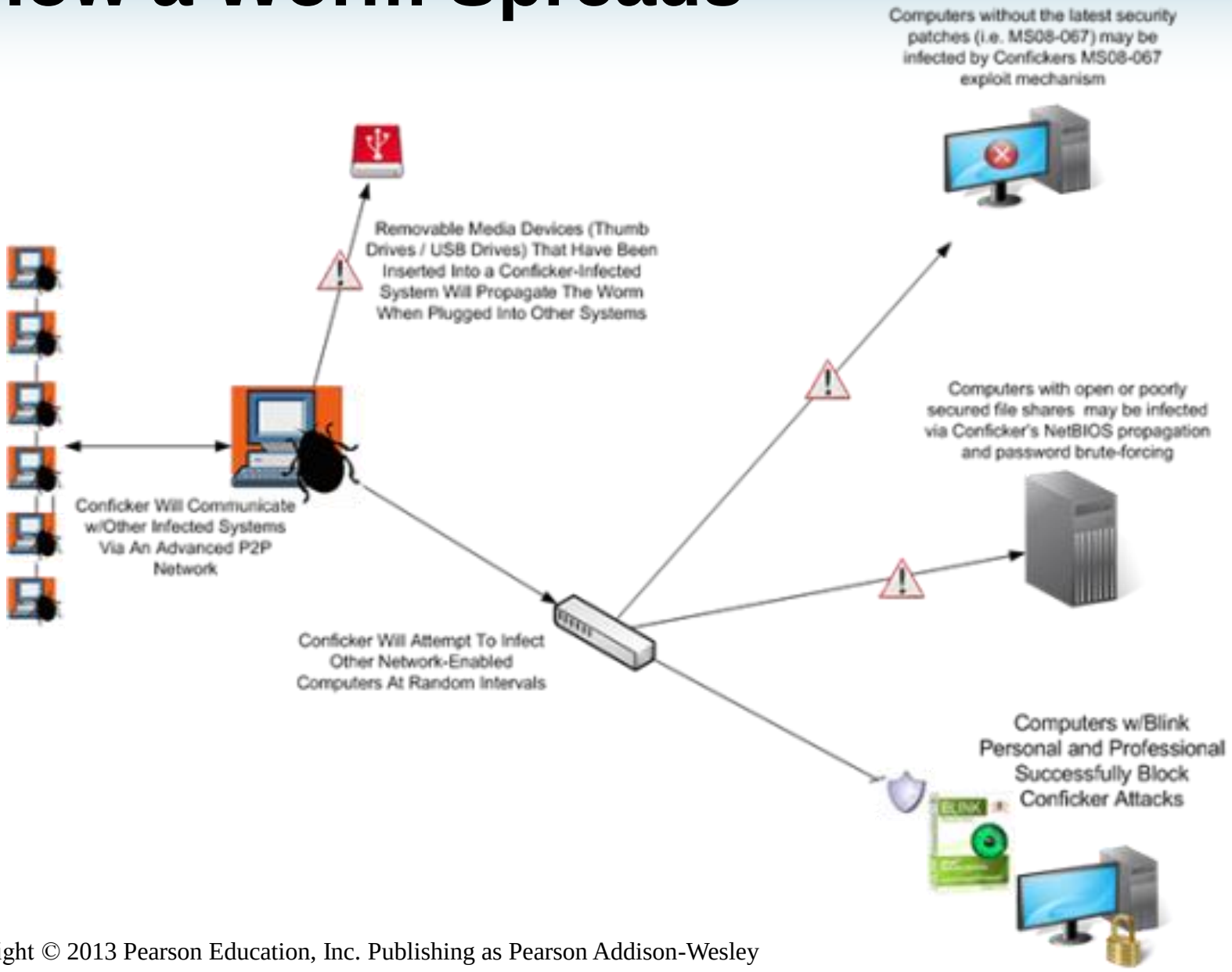
Antivirus Software Packages

- Allow computer users to detect and destroy viruses
- Must be kept up-to-date to be most effective
- Many people do not keep their antivirus software packages up-to-date
- Consumers need to beware of fake antivirus applications

Worm

- Self-contained program
- Spreads through a computer network
- Exploits security holes in networked computers

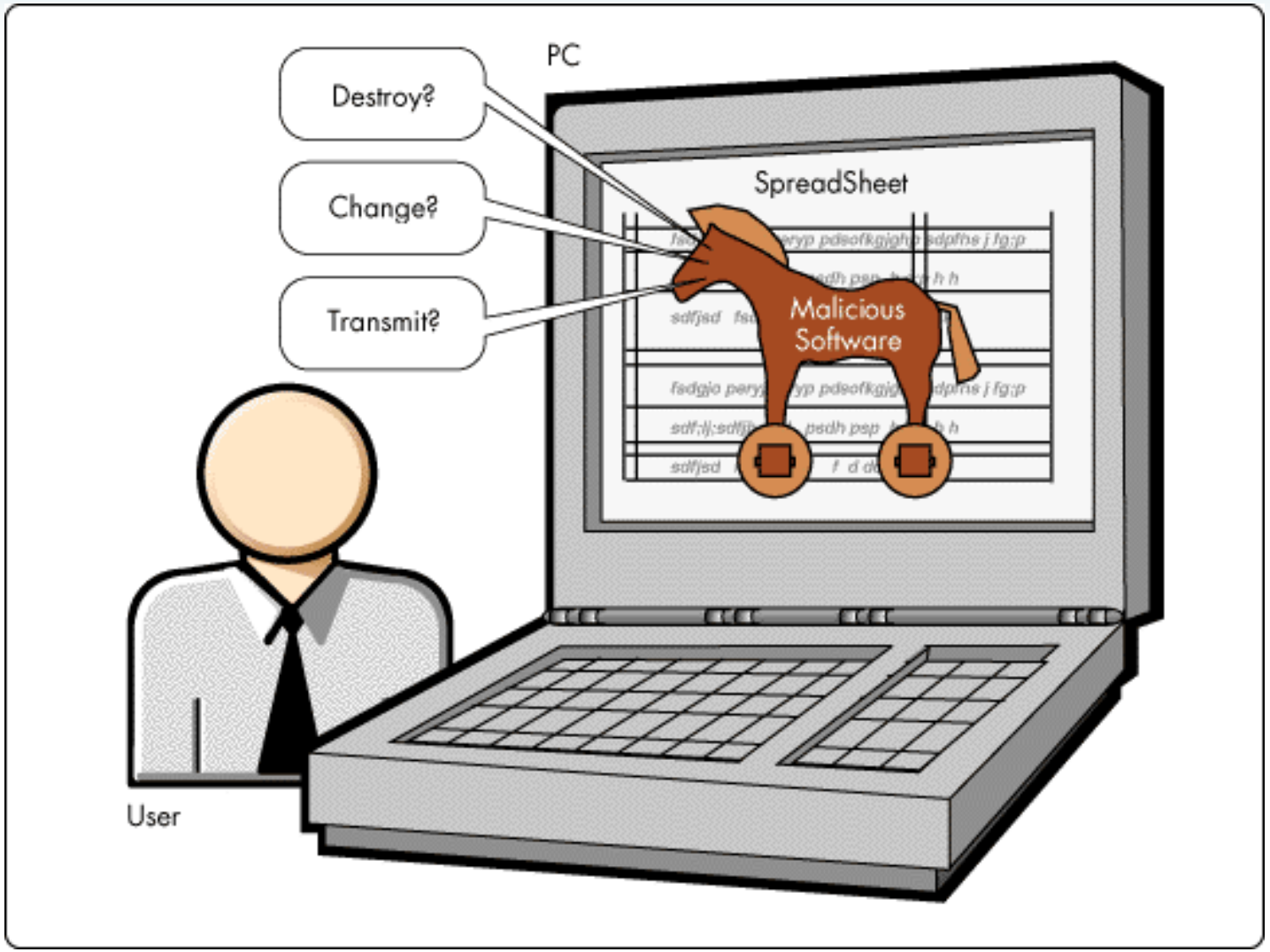
How a Worm Spreads



Ethical Evaluation

- Kantian evaluation
  - Morris used others by gaining access to their computers without permission
- Social contract theory evaluation
  - Morris violated property rights of organizations
- Utilitarian evaluation
  - Benefits: Organizations learned of security flaws
  - Harms: Time spent by those fighting worm, unavailable computers, disrupted network traffic, Morris's punishments
- Morris was wrong to have released the Internet worm

Trojan Horses



Trojan Horses and Backdoor Trojans

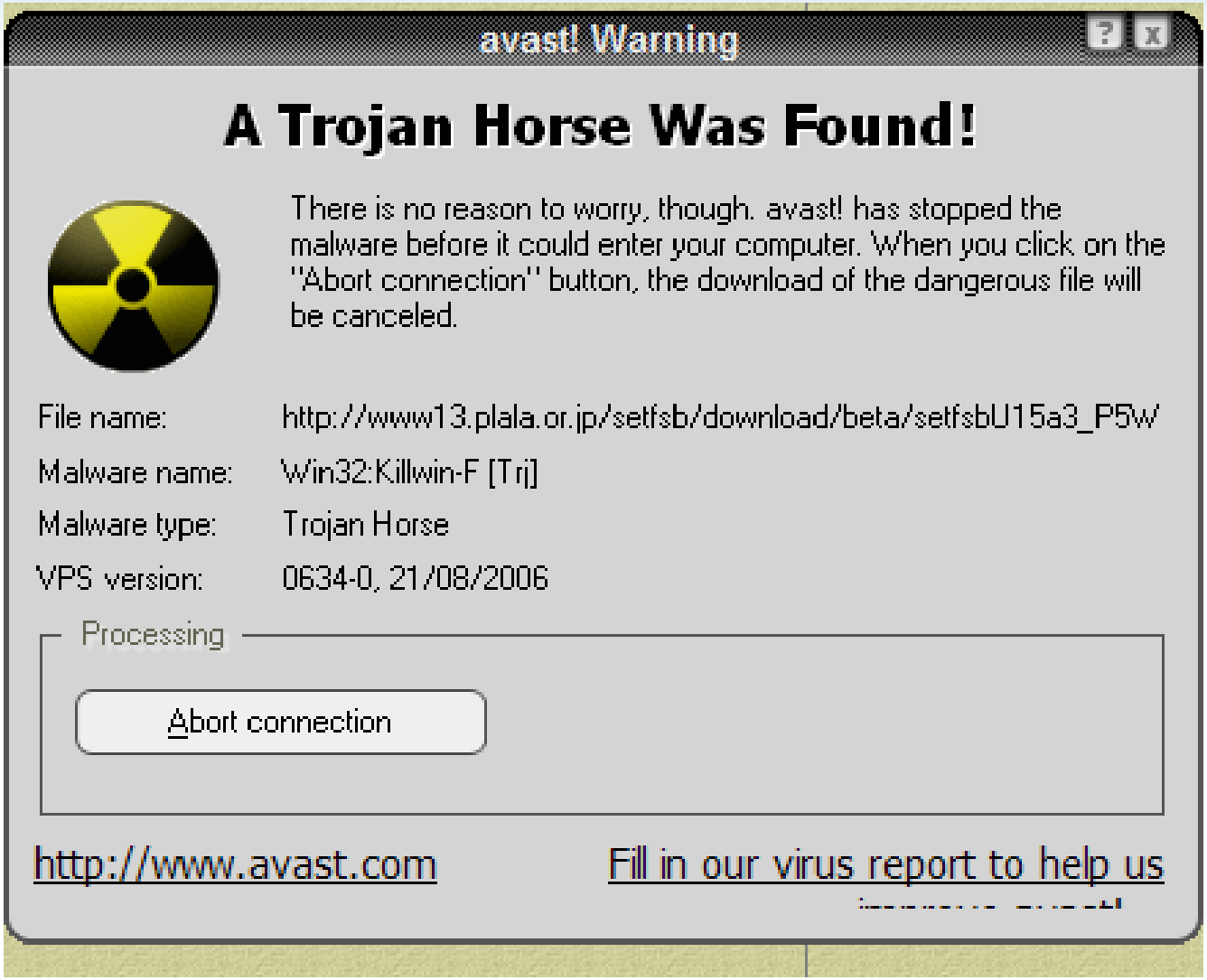
- Trojan horse: Program with benign capability that masks a sinister purpose
- Backdoor Trojan: Trojan horse that gives attack access to victim's computer

Spyware and Adware

- Spyware: Program that communicates over an Internet connection without user's knowledge or consent
  - Monitor Web surfing
  - Log keystrokes
  - Take snapshots of computer screen
  - Send reports back to host computer
- Adware: Type of spyware that displays pop-up advertisements related to user's activity
- Backdoor Trojans often used to deliver spyware and adware

Defensive Measures

- Security patches: Code updates to remove security vulnerabilities
- Anti-malware tools: Software to scan hard drives, detect files that contain viruses or spyware, and delete these files
- Firewall: A software application installed on a single computer that can selectively block network traffic to and from that computer



7.4 Cyber Crime and Cyber Attacks

Phishing and Spear-phishing

- Phishing: Large-scale effort to gain sensitive information from gullible computer users
  - At least 67,000 phishing attacks globally in second half of 2010
  - New development: phishing attacks on Chinese e-commerce sites
- Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients

Denial-of-service and Distributed Denial-of-service Attacks

- Denial-of-service attack: Intentional action designed to prevent legitimate users from making use of a computer service
- Aim of a DoS attack is not to steal information but to disrupt a server's ability to respond to its clients
- Distributed denial-of-service attack: DoS attack launched from many computers, such as a botnet

Cyber Crime

- Criminal organizations making significant amounts of money form malware

Attacks on Twitter and Other Social Networking Sites

- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009
- Three other sites attacked at same time: Facebook, LiveJournal, and Google
- All sites used by a political blogger from the Republic of Georgia
- Attacks occurred on first anniversary of war between Georgia and Russia over South Ossetia

Fourth of July Attacks

- 4th of July weekend in 2009: DDoS attack on governmental agencies and commercial Web sites in United States and South Korea
- Attack may have been launched by North Korea in retaliation for United Nations sanctions

Supervisory Control and Data Acquisition (SCADA) Systems

- Industrial processes require constant monitoring
- Computers allow automation and centralization of monitoring
- Today, SCADA systems are open systems based on Internet Protocol
  - Less expensive than proprietary systems
  - Easier to maintain than proprietary systems
  - Allow remote diagnostics
- Allowing remote diagnostics creates security risk

SCADA Systems Carry Security Risks

© p77/ZUMA Press/Newscom

Stuxnet Worm (2009)

- Attacked SCADA systems running Siemens software
- Targeted five industrial facilities in Iran that were using centrifuges to enrich uranium
- Caused temporary shutdown of Iran's nuclear program
- Worm may have been created by Israeli Defense Forces

7.5 Online Voting

Benefits of Online Voting

- More people would vote
- Votes would be counted more quickly
- No ambiguity with electronic votes
- Cost less money
- Eliminate ballot box tampering
- Software can prevent accidental over-voting
- Software can prevent under-voting

Risks of Online Voting

- Gives unfair advantage to those with home computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to vote-changing virus or RAT
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

Utilitarian Analysis

- Suppose online voting replaced traditional voting
- Benefit: Time savings
  - Assume 50% of adults actually vote
  - Suppose voter saves 1 hour by voting online
  - Average pay in U.S. is $18.00 / hour
  - Time savings worth $9 per adult American
- Harm of DDoS attack difficult to determine
  - What is probability of a DDoS attack?
  - What is the probability an attack would succeed?
  - What is the probability a successful attack would change the outcome of the election?

Kantian Analysis

- The will of each voter should be reflected in that voter's ballot
- The integrity of each ballot is paramount
- Ability to do a recount necessary to guarantee integrity of each ballot
- There should be a paper record of every vote
- Eliminating paper records to save time and/or money is wrong

Conclusions

- Existing systems are highly localized
- Widespread tainting more possible with online system
- No paper records with online system
- Evidence of tampering with online elections
- Relying on security of home computers means system vulnerable to fraud
- Strong case for not allowing online voting