Information Technology Engineering

Mohammad Hossein Manshaei

manshaei@gmail.com

1401

Module B.1

CyberAttacks and CyberSecurity

Reference:

Ethics in Information Technology

6th Edition

George W. Reynolds

Chapter 3: Cyberattacks and Cybersecurity

Contents

- IT Security Incidents: A Major Concern
  - Why Computer Incidents are so Prevalent?
  - Types of Exploits
  - Types of Perpetrators
  - Federal Laws for Prosecuting Computer Attacks

IT Security Incidents: A Major Concern

- Security of information technology is of utmost importance
  - Protect confidential data
    - Safeguard private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Must be balanced against other business needs and issues
- Number of IT-related security incidents is increasing around the world

Most Common Security Incidents

Type of security incident	2004	2005	2006	2007	2008
Virus	78%	74%	65%	52%	50%
Insider abuse	59%	48%	42%	59%	44%
Laptop theft	49%	48%	47%	50%	42%
Unauthorized access	37%	32%	32%	25%	29%
Denial of service	39%	32%	25%	25%	21%
Instant messaging abuse				25%	21%
Bots				21%	20%

Source: "2008 CSI Computer Crime and Security Survey."

53% of organization ➔ Spend 5% or less of their overall IT Budget on Information Security

Most Common Security Incidents

Type of incident	Percent of organizations that experienced this type of incident		
	2008	2009	2010
Malware infection	50%	64%	67%
Being fraudulently represented as the sender of email messages requesting personal information	31%	34%	39%
Laptop or mobile hardware loss	42%	42%	34%
Employee abuse of Internet access or email (e.g., accessing pornography or use of pirated software)	44%	30%	25%

Source Line: "2010/11 Computer Security Institute Computer Crime & Security Survey," courtesy of the Computer Security Institute.

Ethical Decisions For IT Security

1. Should they pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform their affected customers, or take some other action?
2. How much effort and money should be spent to safeguard against computer crime?
3. If the firm produces software with defects that allow hackers to attack customer data and computers, what actions should they take?
4. What should be done if recommended computer security safeguards make life more difficult for customers and employees, resulting in lost sales and increased costs?

IT Security Incidents: A Worsening Problem

- Computer Emergency Response Team/ Coordination Center (CERT/ CC)
  - Established in 1988 at the Software Engineering Institute (SEI)
  - Charged with
    - Coordinating communication among experts during computer security emergencies
    - Helping to prevent future incidents

Contents

- IT Security Incidents: A Major Concern
  - Why Computer Incidents are so Prevalent?
  - Types of Exploits
  - Types of Perpetrators
  - Federal Laws for Prosecuting Computer Attacks

Why Computer Incidents are so Prevalent?

Countries with highest rate of infected computers		Countries with lowest rate of infected computers	
Country	**Rate**	**Country**	**Rate**
Sudan	70%	Japan	6%
Bangladesh	64%	Germany	9%
Iraq	62%	Switzerland	10%
Rwanda	57%	Luxembourg	10%
Nepal	56%	Denmark	11%

Source Line: Stefan Tanase, "Q1/2011 Malware Report," Kaspersky Lab, May 17, 2011.

Why Computer Incidents are so Prevalent?

- Computing environment is enormously complex
  1. Increasing Complexity Increases Vulnerability
  2. Higher Computer User Expectation
  3. Expanding and Changing Systems Introduce New Risks
  4. Increased Reliance on Commercial Software with Known Vulnerabilities

1. Increasing Complexity Increases Vulnerability

- **Computing environment is enormously complex**
  - Continues to increase in complexity
  - Number of possible entry points to a network expands continuously

1. Increasing Complexity Increases Vulnerability (Cloud and Virtualization Example)

Question	Yes	No
Are the interfaces between the cloud service and users secure, with appropriate levels of access control?		
Is data encrypted as it travels over the Internet?		
Does the service provide secure storage and access control over data stored in the cloud?		
Does the service provide backup capabilities in the event that a human-caused or natural disaster renders the primary service unusable?		
Is the cloud service provider reputable and financially viable?		

Source Line: Course Technology/Cengage Learning.

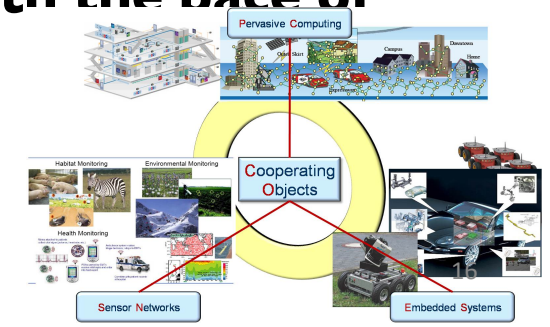
Questions to ask when evaluating cloud services

2. Higher Computer User Expectations

- Computer help desks
  - Under intense pressure to provide fast responses to users' questions
  - Sometimes forget to
    - Verify users' identities
    - Check whether users are authorized to perform the requested action
- Computer users share login IDs and passwords

3. Expanding and Changing Systems Introduce New Risks

- **Network era**
  - **Personal computers connect to networks with millions of other computers**
  - **All capable of sharing information**
- **Information technology**
  - **Ubiquitous**
  - **Necessary tool for organizations to achieve goals**
  - **Increasingly difficult to keep up with the pace of technological change**



4. Increased Reliance on Commercial Software with Known Vulnerabilities

- **Exploit**
  - Attack on information system
  - Takes advantage of a particular system vulnerability
  - Due to poor system design or implementation
- **Patch**
  - "Fix" to eliminate the problem
  - Users are responsible for obtaining and installing patches
  - Delays in installing patches expose users to security breaches

Increased Reliance on Commercial Software with Known Vulnerabilities

- **Zero-day attack**
  - Takes place before a vulnerability is discovered or fixed
- U.S. companies rely on commercial software with known vulnerabilities

Organizations Behaving Badly: Zero-day Exploit

- A **zero-day exploit** is a cyberattack that takes place before the security community and/or software developers become aware of and fix a security vulnerability.
- Information about one zero-day vulnerability in Apple's iOS was reportedly sold for $500,000.
- Packages of zero-day exploits have reportedly been sold to U.S. government contractors for $2.5 million a year
- **Vulnerability Equities Process (VEP)**

Number of Vulnerabilities Reported to CERT/CC

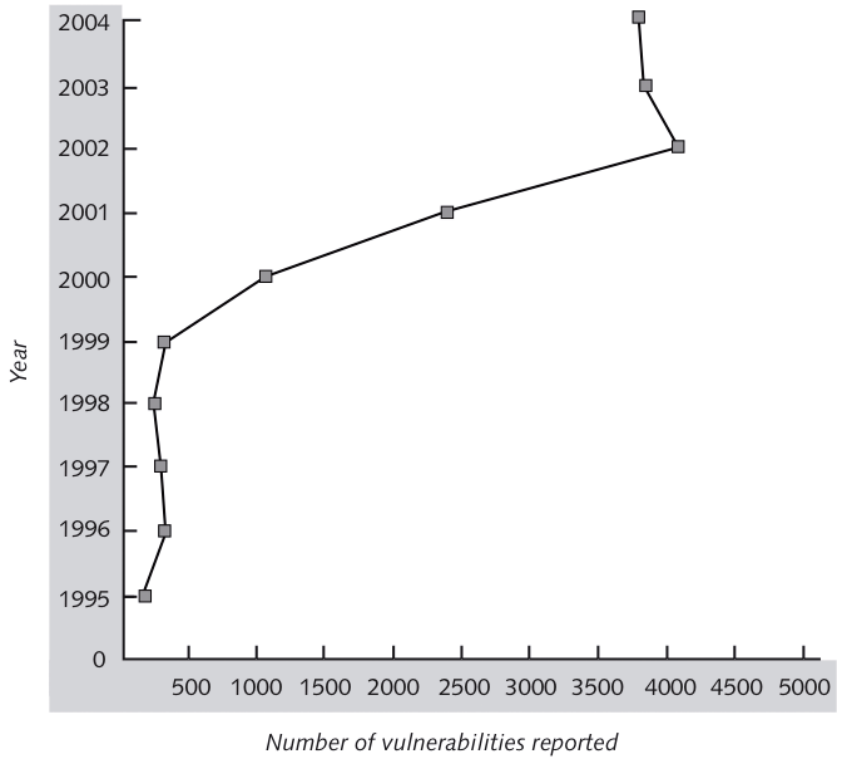
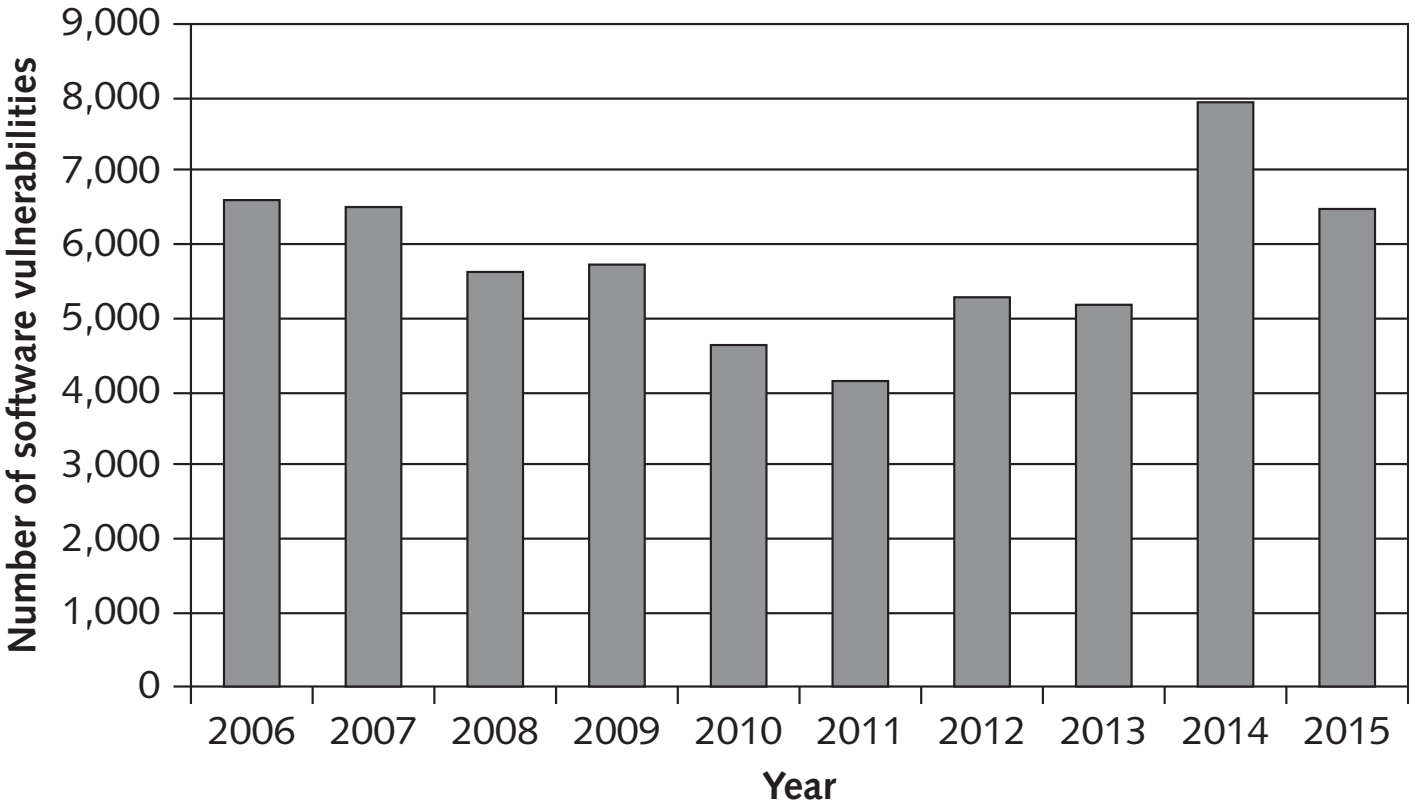


FIGURE 3-1 Number of vulnerabilities reported to CERT/CC

Number of New Software Vulnerabilities



Contents

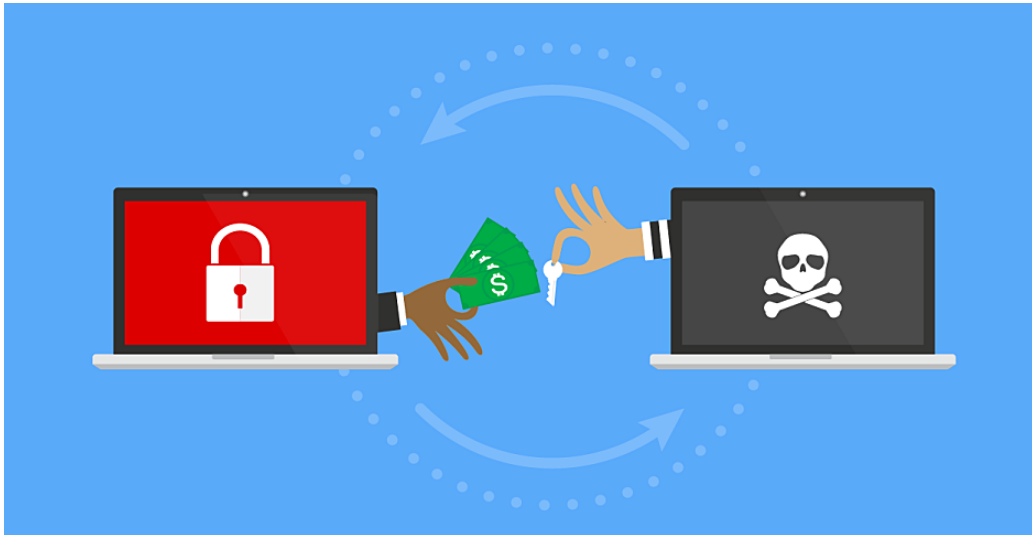
- IT Security Incidents: A Major Concern
  - Why Computer Incidents are so Prevalent?
  - Types of Exploits
  - Types of Perpetrators
  - Federal Laws for Prosecuting Computer Attacks

Types of Attacks (Exploits)

- Most frequent attack is on a networked computer from an outside source
- Types of attacks
  1. Ransomware
  2. Virus
  3. Worm
  4. Trojan horse
  5. Blended Threats
  6. Spam
  7. Distributed Denial-of-Service (DDoS)
  8. Rootkit
  9. Advanced Persistent Threat (APT)
  10. Phishing
  11. Smishing and vishing
  12. Cyberespionage
  13. Cyberterrorism

1. Ransomware

- A malware that stops you from using your computer or accessing your data until you meet certain demands, such as paying a ransom or sending photos to the attacker.
- Spread with email attachment, USB drive, or text messages
- Case: February 2016, Hollywood Presbyterian Medical Center



2. Viruses

- Pieces of programming code
- Usually disguised as something else
- Cause unexpected and usually undesirable events
- Often attached to files
- Deliver a "payload"
- Programmed to display a certain message on the computer's display screen, delete or modify a certain document, or reformat the hard drive.

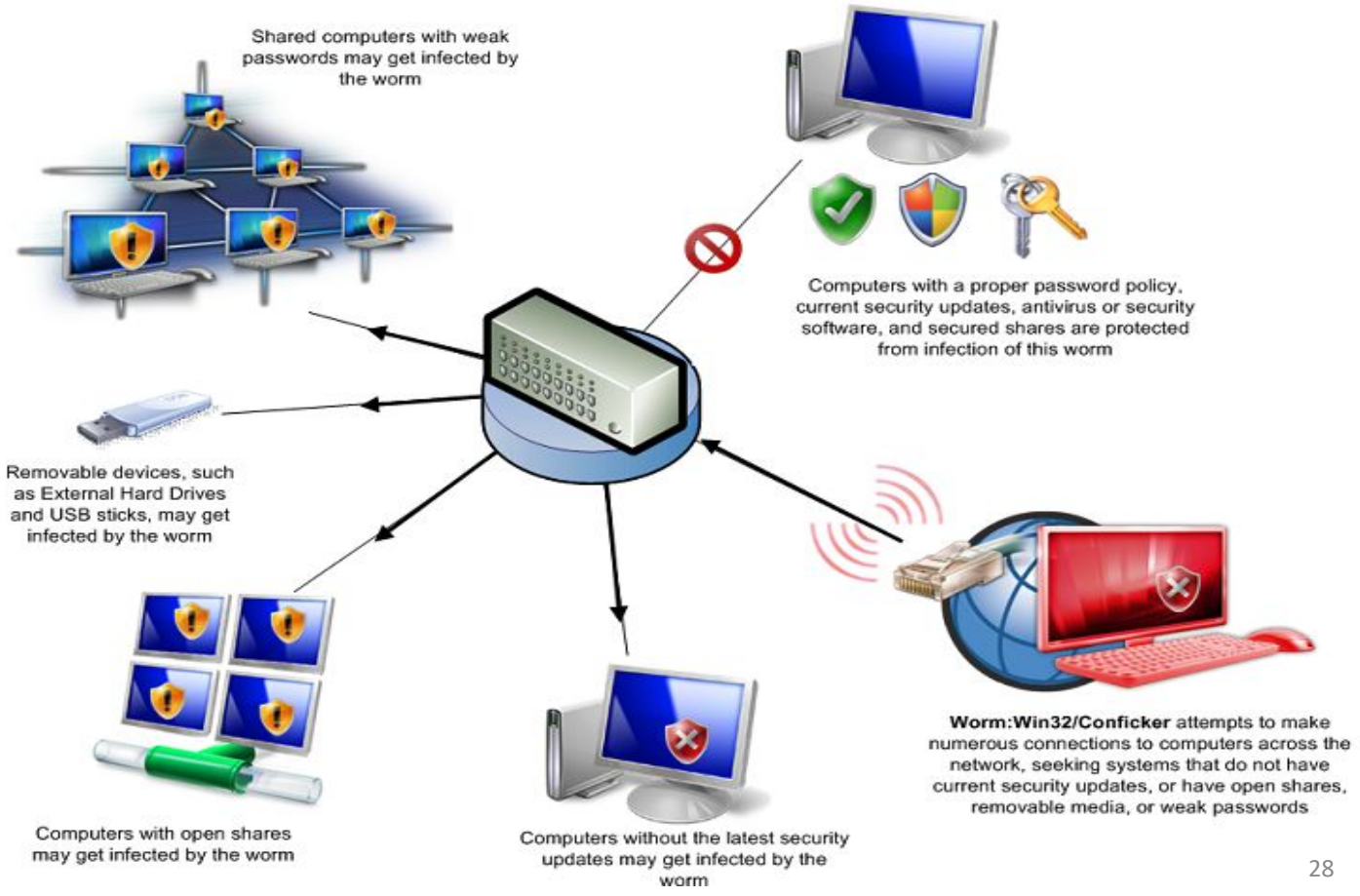
Viruses Types and Spread

- **Does not spread itself from computer to computer**
  - Must be passed on to other users through
    - Infected e-mail document attachments
    - Programs on diskettes
    - Shared files
- **Macro viruses**
  - Most common and easily created viruses
  - Created in an application macro language
  - Infect documents and templates

3. Worms

- **Harmful programs**
  - Reside in active memory of a computer
- **Duplicate themselves**
  - Can propagate without human intervention
- **Negative impact of virus or worm attack**
  - Lost data and programs
  - Lost productivity
  - Effort for IT workers

Worm


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

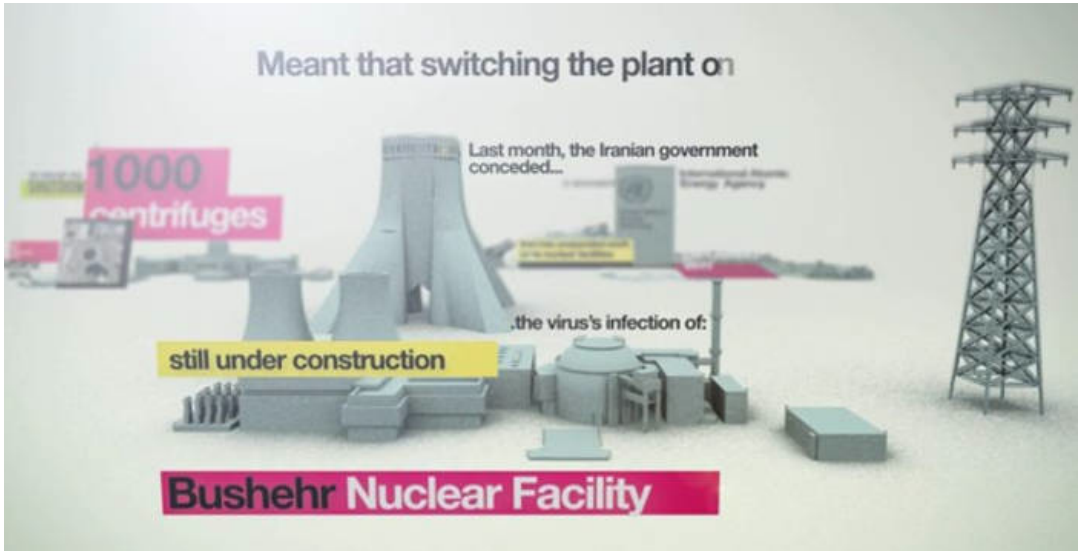
Cost Impact of Worms

Name	Year released	Worldwide economic impact
Storm	2007	> $10 billion (est.)
ILOVEYOU	2000	$8.75 billion
Code Red	2001	$2.62 billion
SirCam	2001	$1.15 billion
Melissa	1999	$1.10 billion

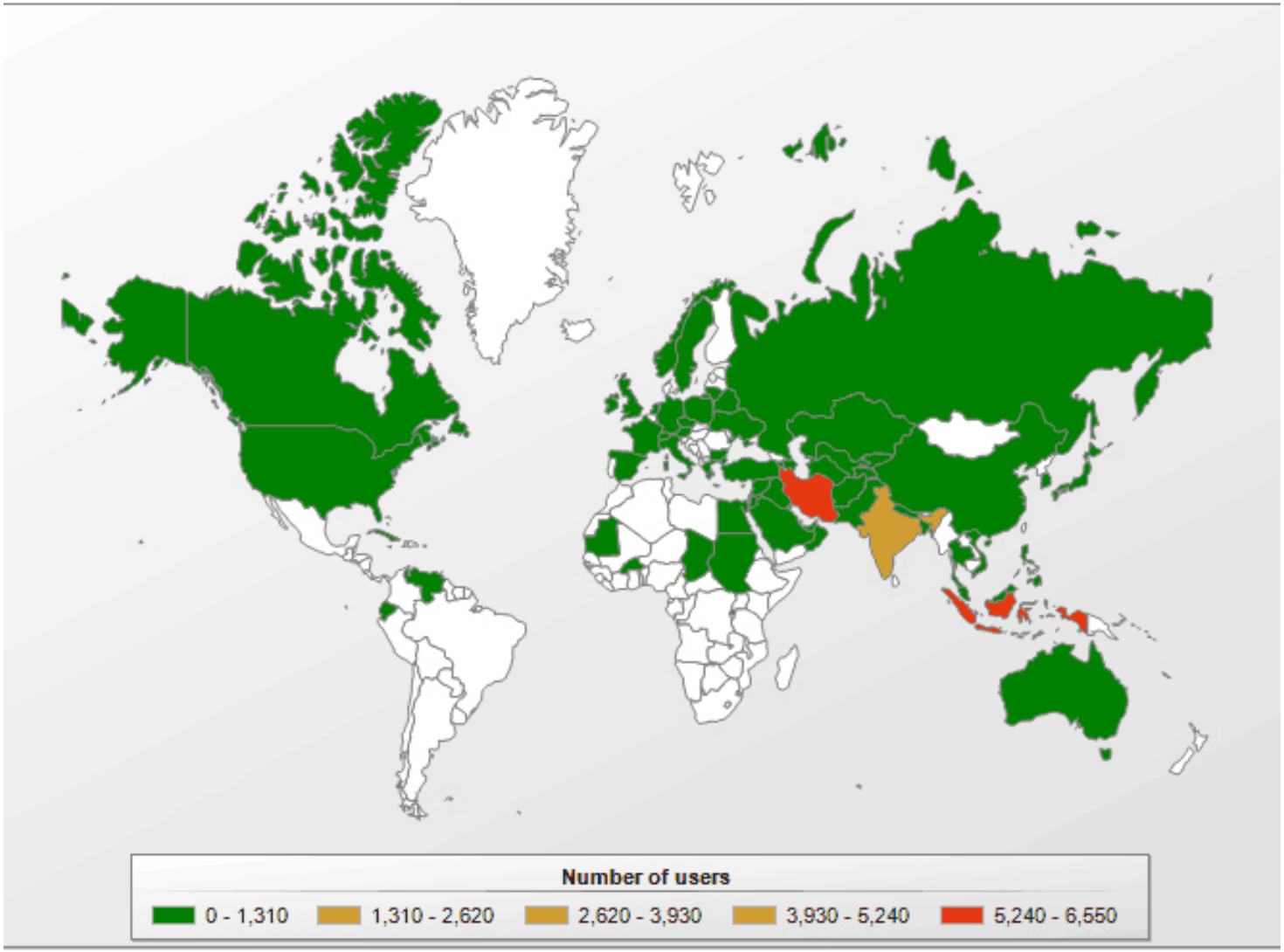
Source: Pelin Aksoy and Laura Denardis, *Information Technology in Theory* (Boston: Cengage Learning, 2007), 299–301.

Case Study: Stuxnet

- **Stuxnet** is a **computer worm** discovered in June 2010 that is believed to have been created by the United States and Israel to attack Iran's nuclear facilities.



Rootkit.Win32.Stuxnet geography



4. Trojan Horses

- Program that a hacker secretly installs
- Users are tricked into installing it
- **Logic bomb**
  - Executes under specific conditions

Trojan Horse: Case Study

Some pirated copies of iWork (Apple) contain a Trojan horse, iServices.a, which launches when the user begins installation of the pirated software. When installed, the Trojan horse "phones home" to the hacker's server to confirm the Mac is infected and awaits further instructions

5. Blended Threat

A blended threat is a sophisticated threat that combines the features of a **virus**, **worm**, **Trojan horse**, and other malicious code into a single payload.

Rather than launching a narrowly focused attack on specific EXE files, a blended threat might attack multiple EXE files, HTML files, and registry keys simultaneously.

6. Spam

The abuse of e-mail systems to send unsolicited e-mail to large numbers of people.

- Low-cost commercial advertising
- May also be used to deliver harmful worms or other malware

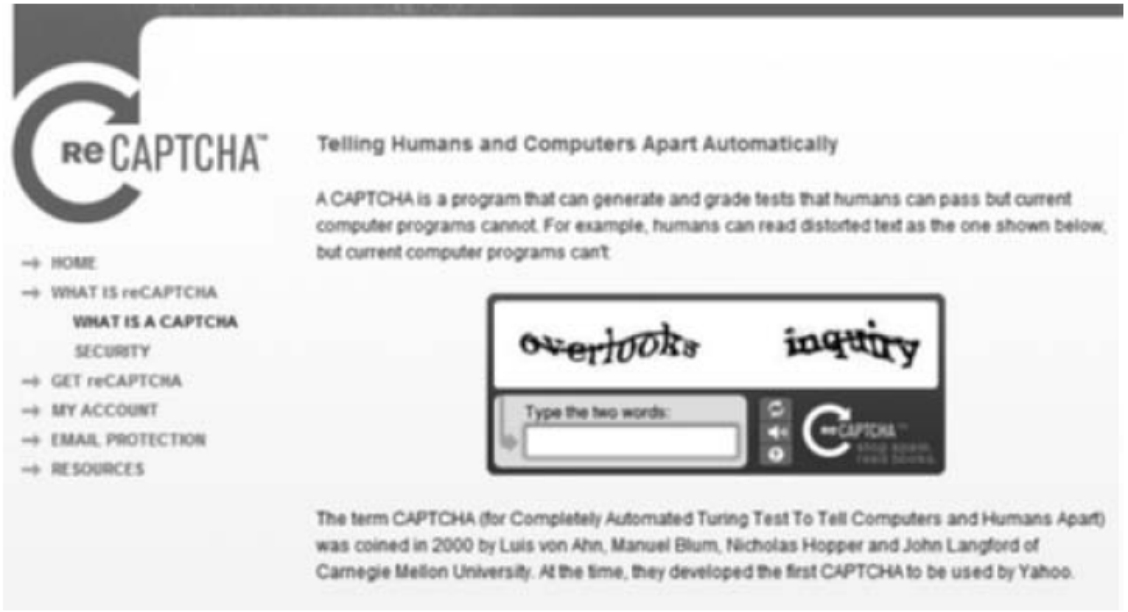
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)

- In January 2004
- It is legal to spam, provided the messages meet a few basic requirements
  1. Spammers cannot disguise their identity by using false return addresses
  2. There must be a label in the message specifying that it is an ad or a solicitation
  3. Such e-mails must include a way for recipients to indicate that they do not want future mass mailings.
- From 2005 to 2008, the average global proportion of spam in e-mail traffic shrunk from 92 percent to 81 percent

Free Email Service for Spams

- Microsoft, Yahoo!, and Google offer free e-mail
- Spammers seek to use e-mail accounts from such major, free, and reputable Web-based e-mail service providers.
- In 2008, about 6.5-12 percent of spam was sent from such accounts.
- Spammers can defeat the registration process of the free e-mail services by launching a coordinated bot attack that can sign up for thousands of e-mail accounts.
- A third of the world's spam is generated from compromised computers in North America (21%), Russia (8%), and China (4%).

Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)



Source: Permission needed from http://recaptcha.net/captcha.html

Spam: Case Study

- Edward Davidson (1972-2008)
- He managed a large network of computers that sent hundreds of thousands of spam e-mails
- The sale of watches, perfume, and other items for nearly two dozen companies.
- Header information that concealed the actual sender
- In April 2008, Edward Davidson was sentenced to:
  - Serve 21 months in federal prison for violation of the CAN-SPAM Act.
  - Pay $714,139 in restitution to the IRS for taxes