ACS-1803
Introduction to Information Systems

Instructor: Kerry Augustine

Security/ Auditing & Controls of Information Systems

Lecture 11

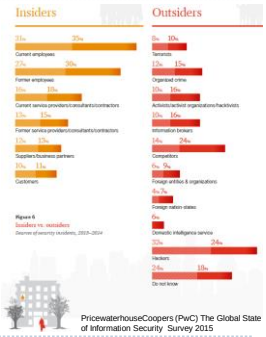
Information Technology (IT) Security

General IT Security

- Businesses must protect against the unknown.
- New methods of attacking networks and Web sites and new network security holes are being constantly discovered or invented.
- An organization cannot expect to achieve perfect security for its network and Web site
  - How is the data protected once it is delivered to the Business?
  - How are credit card transactions authenticated and authorized?
- The biggest potential security problem in an organization is of human, rather than electronic, origin.
  - The weakest link in any security system is the user.

Insider Attacks

- Employees are the most-cited culprits of incidents
- Percentage of respondents that point the finger at current employees jumped over 10% in one year (2014-15)



PricewaterhouseCoopers (PwC) The Global State of Information Security Survey 2015

Why Computer Incidents Are So Prevalent

- Increasing Complexity Increases Vulnerability
  - Cloud computing, networks, computers, mobile devices, virtualization, OS applications, Web sites, switches, routers, and gateways are interconnected and driven by millions of lines of code
- Higher Computer User Expectations
  - Computer help desks are under intense pressure to respond very quickly to users' questions
- Expanding and Changing Systems Introduce New Risks
  - It is difficult for IT organizations to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them

Why Computer Incidents Are So Prevalent

- Increased Prevalence of Bring Your Own Device Policies
  - Bring your own device (BYOD): a business policy that permits (encourages) employees to use their own mobile devices to access company computing resources and applications
  - BYOD makes it difficult for IT organizations to adequately safeguard additional portable devices with various OSs and applications
- Growing Reliance on Commercial Software with Known Vulnerabilities
  - An exploit is an attack on an information system that takes advantage of a particular system vulnerability
    - Often this attack is due to poor system design or implementation
  - Users should download and install patches for known fixes to software vulnerabilities
    - Any delay in doing so exposes the user to a potential security breach

Goals of information Security

- **Confidentiality**: This means that information is only being seen or used by people who are authorized to access it.
- **Integrity:** This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- **Availability:** This means that the information is accessible when authorized users need it.

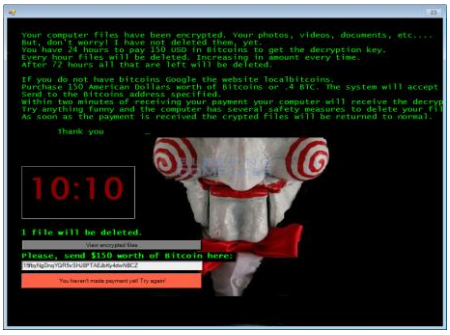
Types of Exploits

- Viruses
  - A piece of programming code (usually disguised as something else) that causes a computer to behave in an unexpected and undesirable manner
  - Spread to other machines when a computer user shares an infected file or sends an email with a virus-infected attachment
- Worms
  - A harmful program that resides in the active memory of the computer and duplicates itself
  - Can propagate without human intervention

Ransomware

- **Ransomware** is a denial-of-access attack that prevents computer users from accessing files.
- Utilizes malware that installs covertly on a victim's computer, executes a cryptovirology attack that is intractable to decrypt the files without the decryption key.
- Attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file.
- Attackers demands a ransom payment to decrypt the files – or to not publish the data.
- Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it.
- More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.
- Ransomware - Anatomy of an Attack

Ransomware – Jigsaw 2016



Types of Exploits

- Trojan Horses
  - A seemingly harmless program in which malicious code is hidden
  - A victim on the receiving end is usually tricked into opening it because it appears to be useful software from a legitimate source
    - The program's harmful payload might be designed to enable the attacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or spy on users
  - Often creates a "backdoor" on a computer that enables an attacker to gain future access
  - Logic bomb
    - A type of Trojan horse that executes when it is triggered by a specific event

Types of Exploits

- Blended Threat
  - A sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload
  - Might use server and Internet vulnerabilities to initiate and then transmit and spread an attack using EXE files, HTML files, and registry keys
- Spam
  - The use of email systems to send unsolicited email to large numbers of people
  - Also an inexpensive method of marketing used by many legitimate organizations
  - Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act states that it is legal to spam, provided the messages meet a few basic requirements
    - Spammers cannot disguise their identity by using a false return address
    - The email must include a label specifying that it is an ad or a solicitation
    - The email must include a way for recipients to opt out of future mass mailings

Types of Exploits

- Distributed Denial-of-Service (DDoS) Attacks
  - An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks
  - Keeps target so busy responding to requests that legitimate users cannot get in
  - Botnet
    - A large group of computers, controlled from one or more remote locations by hackers, without the consent of their owners
    - Sometimes called zombies
    - Frequently used to distribute spam and malicious code

Types of Exploits

- Rootkit
  - A set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
  - Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration
  - Symptoms of rootkit infections:
    - Computer locks up or fails to respond to input from the keyboard
    - Screen saver changes without any action on the part of the user
    - Taskbar disappears
    - Network activities function extremely slow

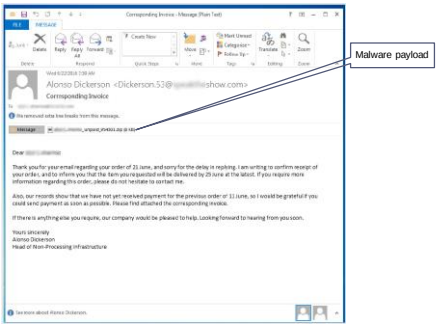
Types of Exploits

- Advanced Persistent Threat
  - APT is a network attack in which an intruder gains access to a network and stays undetected with the intention of stealing data over a long period of time
  - An APT attack advances through the following five phases:
    - Reconnaissance
    - Incursion
    - Discovery
    - Capture
    - Export
  - Detecting anomalies in outbound data is the best way for administrators to discover that the network has been the target of an APT attack

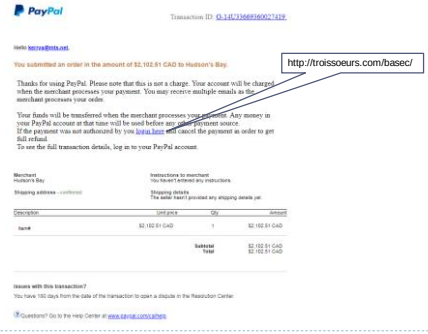
Phishing

- Like "fishing" for information
- Deceptive online attempt by third party to get confidential information for financial gain
- No malware involved
- Uses straight forward misrepresentation and fraud
- Analogous to a con artist, who tricks people into voluntarily giving what is requested
- E.g., email scams, account verifications, quota exceeded
- Offers to give you something as long as you respond with certain information

Example of Phishing



Example of Phishing



Spoofing

- Misrepresent oneself via fake emails or use of fake name
  - "Watch This Hacker Break into my Cell Phone Account in 2 Minutes"
- **Pharming** = spoofing a website
  - E.g., link to a fake site
  - Can harm businesses (e.g., steal customers, create bad reputation)
  - Can harm customers (e.g., lose money)
- **Spam/junk websites** = sites that promise some product or service but are simply collection of ads
  - Often contains malware
- **Splogs** = spam blogs
  - Created to raise search engine rankings of affiliated sites

Types of Exploits

- Smishing and Vishing
  - Smishing is a variation of phishing that involves the use of texting
  - Vishing is similar to smishing except the victims receive a voice mail message telling them to call a phone number or access a Web site
- Identity Theft
  - The theft of personal information and then used without their permission
  - Data breach is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals
    - Often results in identity theft
  - Most e-commerce Web sites use some form of encryption technology to protect information as it comes from the consumer

Examples of Cyber Crime

While it Isn't Always About The **MONEY…**

- **It often is!!!**
- **Organized crime generates significant revenue from cybercrime!**
- **Estimated to exceed the drug trade!**

Examples of Cyber Crime

- While some illegal marketplaces are viewable on the public Internet, news coverage around underground sites has increased this year, forcing many scammers to move to darker parts of the Internet. For example, some forums are now hosted on the anonymous Tor network as hidden services.
- Other markets are only accessible with an invitation and require a buy-in, which could involve money or goods—like 100 freshly stolen credit cards. Other markets are run on private chat rooms and have rigid vetting procedures for new users. In these closed circles, prices are usually much lower and the traded amount of goods or services is higher.

2010/2011 Pricing

Service	Description	Prices Encountered	
DDoS service	Prices are falling. One year ago prices were generally $20 for one hour and between $100 and $200 for 24hours.	10 minutes for $1	1 hour for $10
		2 hours for $15	5 hours for $25
		1 day for $50	
Botnet rental (for DDoS)	For this price, your botnet includes 2000 machines.	1 month for $50	1 year for $175
		Unlimited: $275	
Install software	If you have malware, they have the vulnerable computers! They install your malware for you. The price is for 1000 installs.	Asia: 9$	Mix: 18$
		Europe: 32$	USA: 110$
		GB: 180$	IT: 120$
		DE: 120$	PL: 100$
		BR: 30$	CA: 130$

Value of Stolen Information

- Sell stolen info to underground economy servers

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

- Goal is not always money; could be vandalism, disruption to website, damage organization's reputation

Types of Exploits

- Cyberespionage
  - Involves the development of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms
  - Mostly targeted toward high-value data such as the following:
    - Sales, marketing, and new product development plans, schedules, and budgets
    - Details about product designs and innovative processes
    - Employee personal information
    - Customer and client data
    - Sensitive information about partners and partner agreements

Types of Exploits

- Cyberterrorism
  - The intimidation of government of civilian population by using information technology to disable critical national infrastructure to achieve political, religious, or ideological goals
  - Department of Homeland Security (DHS) provides a link that enables users to report cyber incidents
    - Incident reports go to the U.S. Computer Emergency Readiness Team (US-CERT)
  - Cyberterrorists try daily to gain unauthorized access to a number of important and sensitive sites

Hacking and Cyber Vandalism

- **Hacker** = individual who intends to gain unauthorized access to a computer
  - **Cracker** = hacker with criminal intent
  - Typically excited by thrill of breaking into corporate/govt sites
- Definitions taken from: *Perrin, Chad (2009). Hacker Vs. Cracker.* http://www.techrepublic.com/blog/security/hacker-vs-cracker/1400
- **Cyber vandalism** = methods used to intentionally disrupt, deface, or destroy a site
- **White hats** = good hackers hired to help locate/fix security flaws by hacking into site externally
- **Black hats** = hackers who act with intention of causing harm
  - E.g., reveal confidential or proprietary information due to belief that the info should be free
- **Grey hats** = hackers who believe they are pursuing greater cause by breaking in and revealing system flaws
  - Reward: prestige of discovery of security flaws; recognition i.e. Anonymous

This is NOT Ethical Hacking!

Individuals appearing in public as Anonymous, wearing Guy Fawkes masks.

A member holding an Anonymous flier at Occupy Wall Street, a protest that the group actively supported, September 17, 2011

Management Controls of IT

Management Controls of IT

- As Information Technology (IT) is a Strategic Asset, controls need to be set up to ensure the information managed is always secure
- Any policy, procedure, process, or practice designed to provide reasonable assurance that an organization's objectives will be achieved.
  - assets are safeguarded against theft & misuse
  - operations are efficient and effective
  - financial reporting is reliable and complete
  - compliance with applicable laws & regulations

Access Controls

- Based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties.
  - Physical Access Controls
  - Electronic Controls
- Examples:
  - Deny access to systems by undefined users or anonymous accounts.
  - Suspend or delay access capability after a specific number of unsuccessful logon attempts.
  - Remove obsolete user accounts and suspend inactive ones
  - Disable unneeded system features, services, and ports.
  - Replace default password settings on accounts.
  - Ensure that logon IDs are nondescriptive of job function.
  - Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
  - Audit system and user events and actions and review reports periodically. Protect audit logs.

Application System Controls

- **Administrative:** Laws, regulations, policies, practices and guidelines that govern the overall requirements and controls for an Information Security or other operational risk program.
- **Logical:** virtual, application and technical controls (systems and software), such as firewalls, anti virus software, encryption and maker/checker application routines.
- **Physical:** video surveillance systems, gates and barricades, the use of guards or other personnel to govern access to an office

Types of Controls

- **Preventive**: Controls that prevent the loss or harm from occurring
- **Detective**: controls monitor activity to identify instances where practices or procedures were not followed (e.g. Reconciling accounting records)
- **Corrective**: Corrective controls restore the system or process back to the state prior to a harmful event

Corrective Control: Backups and Disaster Recovery

- **Backups** – taking periodic snapshots of critical systems data and storing in a safe place or system (e.g. backup tape)
- **Disaster Recovery Plans** – spell out detailed procedures to be used by the organization to restore access to critical business systems (e.g. viruses or fire)
- **Disaster Recovery** – executing Disaster Recovery procedures using backups to restore the system to the last backup if it was totally lost

Preventive Control: Trust Services

- WebTrust is a seal awarded to web sites that consistently adhere to certain business standards established by the Canadian Institute of Chartered Accountants (CICA.ca) and the American Institute of Chartered Public Accountants (AICPA).
- Grown considerably in recent years, due in large part to the advent and growth of e-commerce and the overall e-business environment
- developed to addresses consumer and business concerns over privacy and security.
- WebTrust is an Internet seal that can give web-goers true confidence that certain businesses can be trusted with consumers' (and business') most important asset and prized possession: their private information.

34

Trust Services

- Can you trust a business on the Web and in what areas, to what degree?
- See Access Controls and Web Trust

35

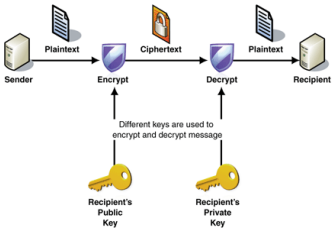
Web Trust Services

- There are six WebTrust Seals:
- **Privacy** - adhering to the strictest rules for collecting, storing and using client/customer information
- **Security** - following the most appropriate and current safety measures, technologies and procedures.
- **Business** Practices/Transaction Integrity - reducing fears that information can be stolen during an online transaction, and that the transaction will be completed successfully.
- **Availability** - maintaining the service levels outlined in your agreements with customers and clients.
- **Confidentiality** - demonstrating the ability to protect business-to-business information.
- **Non-Repudiation** - confirming customers' identity and ability to pay for their online purchases.

36

Preventive Controls: Data Transmission

- Encryption: process of transforming plain text (data) into cipher text that is only understood by sender and receiver
- Key = method of transforming a message – aka "Cypher"



37

Preventive Control: Data Transmission

- Firewalls
  - Prevent specific types of information from moving between the outside, untrusted network (e.g., Internet) and the inside or trusted network
  - There are ~ 5 main types and combinations that fall into two major categories:
    1. **Network layer firewalls** generally make their decisions based on the source address, destination address and ports in individual IP packets.
       - A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from.
    2. **Application layer firewalls** defined, are hosts running proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them.
       - E.g., packet filter: a router that inspects incoming data packets and if it finds a packet that matches a restriction programmed into it will prevent packet's entry.

38

IS Audit

- An audit involves practices to ensure that those controls work properly to ensure security in Information systems
- It involves regular activities to test specific areas of IT in the organization including:
  - IT Security Planning
  - IT Security Strategy and Governance
  - IT Security Monitoring
  - IT Security Risk Management
  - IT Security Roles and Training
  - System Configuration
  - IT Security Management
  - Incident and problem management

39

IS Audit

- Obtained evidence determines if the information systems in the organization are *safeguarding assets, maintaining data integrity, and operating effectively* to achieve the organization's goals or objectives.
  - Ensure data accuracy
  - Ensure data Security
  - Ensure data integrity
- The main job of an auditor is to assess and report on the existence and proper functioning of controls in an organization

The Four "R's" of Audit & Controls for Information Systems

Risk

Reputation

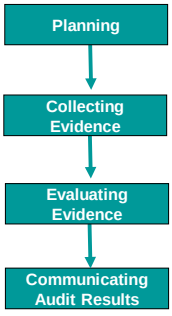
Regulation

Revenue

Two Types of Auditors

- **External auditor**: The primary mission of the external auditors is to provide an independent opinion on the organization's financial statements, annually. They are from outside the organization.
- **Internal auditor**:
  - works inside an organization
  - Have a broader mandate:
  - Is the organization fulfilling its mission?
    - Review the reliability and integrity of operating and financial information
    - Are org systems intended to comply with policies, plans and regulations being followed?
    - How are assets safeguarded?
    - Is operational efficiency being promoted?

The Nature of Auditing

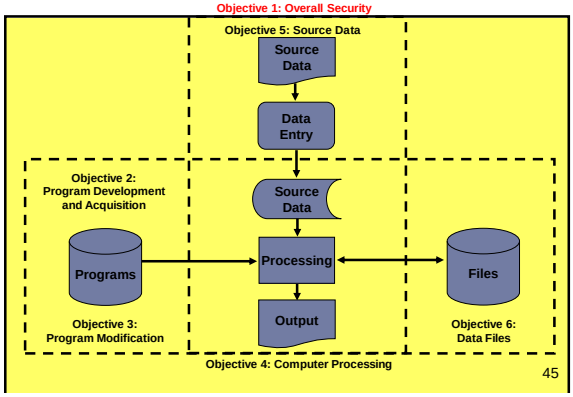


- **An overview of the auditing process**
- All audits follow a similar sequence of activities and may be divided into four stages:
  - Planning
  - Collecting evidence
  - Evaluating evidence
  - **Communicating audit results**

IS Audit

- At all stages of the audit, findings and conclusions are carefully documented in working papers.
- Documentation is critical at the evaluation stage, when final conclusions must be reached and supported.
- The purpose of an information systems audit is to review and evaluate the internal controls that are part of the information system, that are intended to protect the system.

IS Components and Audit Locations



Six Areas of Risk

- There are **six areas of risk** in an organization's information systems as identified here:
  - 1. Overall (General)
  - 2. System development, acquisition
  - 3. System Modification
  - 4. The working of the programs in the system (processing)
  - 5. The capture and input of data into the system (source data)
  - 6. The storage of data that has been input (data files)
- For each area of risk an auditor would look into:
  - A) What are some actual threats?
  - B) What are some controls to counteract such risk?

Objective 1: Overall Security

OBJECTIVE 1: Overall Security

1A. General Risks:

- Break-in to facilities where computer is housed and destruction of data
- Theft of data as it is transmitted
- Virus infection of system
- Computer breakdown

OBJECTIVE 1: Overall Security Evaluate General Controls

- **1B. Control procedures to minimize general risks:**
  - Developing an information security/protection plan.
  - Restricting physical and logical access.
  - Encrypting data.
  - Protecting against viruses.
  - Implementing firewalls.
  - Instituting data transmission controls.
  - Preventing and recovering from system failures or disasters, including:
    - Designing fault-tolerant systems.
    - Preventive maintenance.
    - Backup and recovery procedures.
    - Disaster recovery plans.
    - Adequate insurance.

Objective 2: Program Development & Acquisition

OBJECTIVE 2: Program Development and Acquisition

2A. Risks: Types of errors and fraud

- Two things can go wrong in program development:
  - Inadvertent errors due to careless programming or misunderstanding specifications; or
  - Deliberate insertion of unauthorized instructions into the programs.

OBJECTIVE 2: Program Development and Acquisition

2B. Control procedures:

- The preceding problems can be controlled by requiring:
  - Management and user authorization and approval
  - Thorough testing
  - Proper documentation
- Thorough step-by-step documentation in acquisition of canned software systems

Objective 3: Program Modification

OBJECTIVE 3: Program Modification

3A. Risks: Errors and fraud

- program change implemented incorrectly
  - program change introduces new errors into existing system
- program change not implemented
- program change not documented

OBJECTIVE 3: Program Modification

3B. Control procedures

- When a program change is submitted for approval, a list of all required updates should be compiled by management and program users.
- Changes should be thoroughly tested and documented.
- During the change process, the developmental version of the program must be kept separate from the production version.
- When the amended program has received final approval, it should replace the production version.

Objective 4: Computer Processing

OBJECTIVE 4: Computer Processing

4A. Types of errors and fraud

- During computer processing, the system may:
  - Fail to detect erroneous input.
  - Improperly correct input errors.
  - Process erroneous input.
  - Improperly distribute or disclose output.

OBJECTIVE 4: Computer Processing

4B. Control procedures

- Computer data editing routines.
- Reconciliation of batch totals.
- Effective error correction procedures.
- Effective handling of data input and output by data control personnel..
- Maintenance of proper environmental conditions in computer facility.

Objective 5: Source Data - Input

OBJECTIVE 5: Source Data – Input

5A. Types of errors and fraud

- Inaccurate source data
- Unauthorized source data

OBJECTIVE 5: Source Data

5B. Control procedures

- Effective handling of source data [input documents] input by data entry dept personnel
- User authorization of source data input
- Logging of the receipt, movement, and disposition of source data input
- Effective procedures for correcting and resubmitting erroneous data

Objective 6: Data Files

OBJECTIVE 6: Data Files

6A1. The sixth objective concerns the accuracy, integrity, and security of **data stored in machine-readable files (including relational tables in a database**) after this data has been entered

- Data storage risks include:
  - Unauthorized modification of data
  - Destruction of data
  - Disclosure of data
- If file controls are seriously deficient, especially with respect to access or backup and recovery, the auditor should strongly recommend they be rectified.

OBJECTIVE 6: Data Files

6A2. Types of errors and fraud

- Destruction of stored data due to:
  - Inadvertent errors
  - Hardware or software malfunctions
  - Intentional acts of sabotage or vandalism
- Unauthorized modification or disclosure of stored data

OBJECTIVE 6: Data Files

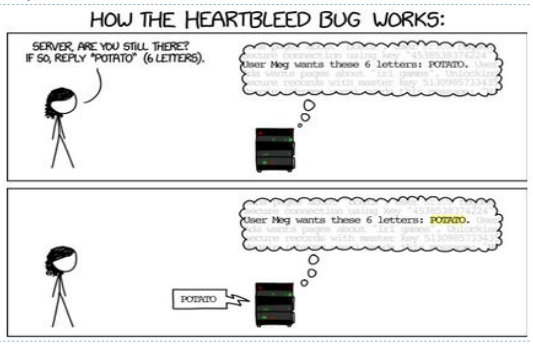
6B. Control procedures

- Restrictions on physical access to data files
- Logical access (access by program) controls using passwords
- Encryption of highly confidential data
- Use of virus protection software
- Maintenance of backup copies of all data files in an off-site location

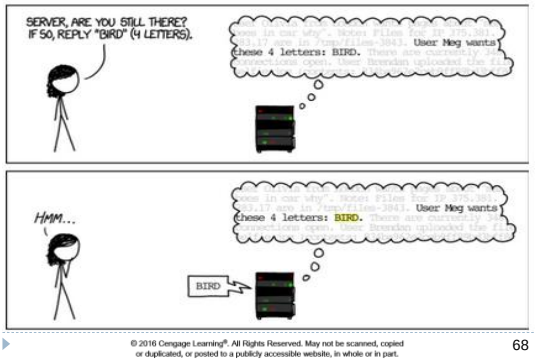
Open SSL & Heartbleed

- **Heartbleed** is a security bug in the OpenSSL cryptography library. OpenSSL is a widely used implementation of the Transport Layer Security (TLS) protocol.
- Heartbleed may be exploited whether the party using a vulnerable OpenSSL instance for TLS is a server or a client.
- On April 7, 2014, some 17 percent (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords.
- On April 8, 2014, the Canada Revenue Agency reported the theft of Social Insurance Numbers belonging to 900 taxpayers, and stated that they were accessed through an exploit of the bug during a 6-hour period.

Open SSL & Heartbleed



Open SSL & Heartbleed



Open SSL & Heartbleed