Database Security

ITMS 428-528
Hosea Lee
IIT

Objectives

- Define the nature of database and information systems security
- Identify the three main security objectives when protecting information systems
- Identify security threats
- Define and identify the characteristics of viruses and how they infiltrate systems
- Identify specific types of operational security and describe how to implement them

Objectives (cont'd.)

- Describe the information security life cycle
- Describe the multilayered nature of security architecture

Why Database Security?

- Most databases provide access spanning several networks and across the world
- Most online transactions involve a database
- Water supplies, electricity grids, and gas and oil production depend on a computer network to thrive
  - Breach could have disastrous impact
- Network intruders are well trained and growing more sophisticated

HACK OF THE CENTURY (SONY)

HACK OF THE CENTURY (SONY)

--Warninig--

We continue till our request be met.
We¡¯ve obtained all your internal data including your secrets and top secrets.
If you don¡¯t obey us, we¡¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,
and we¡¯ll contact the email address.
¡°Thanks a lot to God¡¯sApstls contributing your great effort to peace of the world.¡±
And even if you just try to seek out who we are, all of your data will be released at once.
Data Link :

HACK OF THE CENTURY (SONY)

- Wiping out half of Sony's network
- Erased everything stored on 3,262 of the company's 6,797 PCs
- Erased everything stored on 837 of its 1,555 servers
- The studio was reduced to use fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.
- 47,000 SSN stolen

Heartland Payment Systems

- March 2008
- Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.

Sony's PlayStation Network

- April 2011
- Impact: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.
- About 10 million accounts have credit card numbers associated with them, but Sony said it had no evidence those numbers were stolen. The credit card numbers, unlike the personal information, are stored in an encrypted database, although Sony has not said what encryption system was used.

ESTsoft

- July-August 2011
- Impact: The personal information of 35 million South Koreans was exposed after hackers breached the security of a popular software provider.
- South Korean news outlets reported that attackers with Chinese IP addresses uploaded malware to a server used to update ESTsoft's ALZip compression application.

Google and IT companies

- Mid 2009
- In an act of industrial espionage, the Chinese government launched a massive and unprecedented attack on Google, Yahoo, and dozens of other Silicon Valley companies.
- The Chinese hackers exploited a weakness in an old version of Internet Explorer to gain access to Google's internal network. It was first announced that China was trying to gather information on Chinese human rights activists. It's not known exactly what data was stolen from the American companies, but Google admitted that some of its intellectual property had been stolen and that it would soon cease operations in China.
- For users, the urgent message is that those who haven't recently updated their web browser should do so immediately.

Verisign

- Through 2010
- Security experts are unanimous in saying that the most troubling thing about the VeriSign breach, or breaches, in which hackers gained access to privileged systems and information, is the way the company handled it -- poorly.
- VeriSign never announced the attacks. The incidents did not become public until 2011, through a new SEC-mandated filing. "How many times were they breached?" asks eIQnetworks' John Linkous. "What attack vectors were used? The short answer is: we don't know. And the response to that is simply: we should." "Nearly everyone will be hacked eventually," says Jon Callas, CTO for Entrust, in a post earlier this month on Help Net Security. "The measure of a company is how they respond."

Card Systems Solutions

- June 2005
- 40 million credit card accounts exposed. CSS, one of the top payment processors for Visa, MasterCard, American Express is ultimately forced into acquisition.
- Hackers broke into CardSystems' database using an SQL Trojan attack, which inserted code into the database via the browser page every four days, placing data into a zip file and sending it back through an FTP. Since the company never encrypted users' personal information, hackers gained access to names, accounts numbers, and verification codes to more than 40 million card holders.

AOL

- August 6, 2006
- Data on more than 20 million web inquiries, from more than 650,000 users, including shopping and banking data were posted publicly on a web site.
- Michael Arrington, a lawyer and founder of the blog site TechCrunch, posted a comment on his blog saying, "The utter stupidity of this is staggering." AOL Research, headed by Dr. Abdur Chowdhury, released a compressed text file on one of its websites containing 20 million search keywords for more than 650,000 users over a three-month period. While it was intended for research purposes, it was mistakenly posted publicly.

Target Stores

- December 2013
- Credit/debit card information and/or contact information of up to 110 million people were compromised.
- The breach actually began before Thanksgiving, but was not discovered until several weeks later. The retail giant initially announced that hackers had gained access through a third party to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers.
- By January 2014, however, the company upped that estimate, reporting that contact information of 70 million of its customers had been compromised. Target's CIO resigned in March 2014, and its CEO resigned in May. The company recently estimated the cost of the breach at $162 million.

Home Depot

- September 2014
- Theft of credit/debit card information of 56 million customers.
- The hardware and building supply retailer announced in September what had been suspected for some weeks – that beginning in April or May, its POS systems had been infected with malware. The company later said an investigation concluded that a "unique, custom-built" malware had been used, which posed as anti-virus software.
- The company reported in February that the breach had cost it $33 million.

A Secure Data Environment

- Multiple layers of security
  - Most effective approach to minimizing risk of data breach
- Example of multiple security layers to protect against malicious e-mail attachments
  - User awareness training
  - Filter on exchange server to remove known malicious attachments
  - Firewall configured to deny certain types of traffic

A Secure Data Environment (cont'd.)

- Database security
  - Set of established procedures, standards, policies, and tools
  - Protects against theft, misuse, and attacks
  - Deals with permission and access to the data structure
- Common vendor features for database security
  - Database-level access control
  - Database-level authentication
  - Data storage encryption

A Secure Data Environment (cont'd.)

- Computer security
  - Necessary element of database security
  - Typically defined by the operating system
- Common computer security features
  - Operating system-level access control
  - Operating system-level authentication
  - Application security
  - Hardware and software monitors and logs

A Secure Data Environment (cont'd.)

- Network security
  - Outermost layer of the database
  - Arguably biggest security concern
  - Set of established procedures, standards, policies, and tools
  - Goal: protect network from theft, misuse, and attacks
- Hardware and software devices used to secure a network
  - Firewalls, antivirus programs, network monitors, intrusion detections systems, proxy servers, and authentication servers

Database Security Objectives

- Security measures
  - Keep information private from outside viewing
  - Maintain consistency of data
  - Ensure resources remain at a high degree of availability
- Key to achieving effective data security architecture
  - Organization must maintain confidentiality, integrity, and availability of its environment

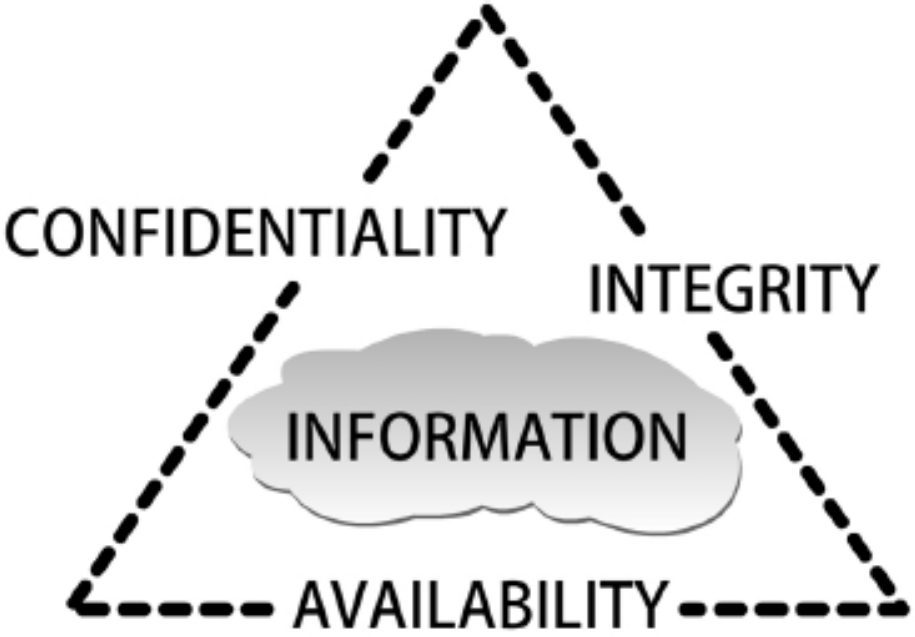


Figure 1-1 C.I.A. triangle

Courtesy Course Technology/Cengage Learning

Database Security Objectives (cont'd.)

- Confidentiality requirements
  - Ensure information remains private by limiting authorized access to resources
  - Block unauthorized access to resources
- Confidentiality protected using authentication and access controls
  - State and federal laws may apply to these measures
- Breaches in confidentiality could result in:
  - Stolen identity
  - Exposed business trade secrets

Database Security Objectives (cont'd.)

- Integrity
  - Reliable, accurate, and consistent data stored in and retrieved from the database
  - Protected by preventing accidental or deliberate modifications
  - Most difficult item to measure
- Auditing used to compare data with older, backed-up versions of the data
- Results of integrity breaches
  - Unreliable data, flawed programs, system failures

Database Security Objectives (cont'd.)

- Availability
  - Maintaining accessible network or database resources
  - Business cannot operate without it
- Must identify potential threats to availability
  - Assess threat level
  - Plan appropriate intervention
  - Example of threats: technical failures, natural disasters, intrusions, user-caused harm

Who Are We Securing Ourselves Against?

- Must understand what poses a threat
  - More threats exist on the inside of a network than on the outside
- Overly restrictive databases are as ineffective as those that give too much access
  - Healthy balance is needed

Hackers

Hackers

- Hacker
  - Person who has mastered firmware and software of modern computer systems
  - Person who enjoys exploration and analysis of network security without intent to cause harm
- Cracker
  - Person who breaks into a network to destroy or steal information

Intruder type:	Definition:	Example:
White hat	Ethical hacker: a hacker that uses extensive experience and knowledge to test systems and provide security consultation to others; white hats pose no threat to our network systems	A security consultant hired by an organization to use different methodology to attempt to hack into their system with the intention of testing the security of that environment
Grey hat	An individual or groups of individuals that waver between the classification of a hacker and a cracker; grey hats sometimes act in goodwill and other times in malice	An individual breaks into the *Wall Street Journal*'s network and leaves notes within the system's database to alert the network team of the vulnerabilities that exist; on a different occasion, this same individual breaks into *The Boston Globe*'s human resource system to obtain sensitive employee information for personal gain
Black hat	Someone who breaks into computer networks without authorization and with malicious intent; black hats are responsible for the theft and destruction that affect our systems	An individual breaks into Walmart's point of sales system to obtain credit card information from consumers in hopes of financial gain
Hactivist	Refers to hackers and crackers who use their extensive experience and skill to use networks to share their ideologies regarding controversial social, political, and economic topics; hactivism can be malicious in nature due to the methods by which hactivists attempt to place further attention and emphasis on their cause	A group of political extremists use their computer know-how to hijack MSNBC's Web site, altering the site to display messages that disparage mainstream media
Script kiddie	Refers to an amateur cracker that uses programs and scripts written by other people to infringe upon a computer network system's integrity; script kiddies are especially inexperienced, and attacks are often experimental in nature	An individual searches for and downloads a cracking tool found online and uses it to haphazardly gain access into an organization's network and steals information

Table 1-1 Types of online intruders

Social Engineers

- People who manipulate others to gain access to systems, unauthorized areas, or confidential information
  - Often build trust with authorized user
  - Use deception and trickery to convince people to break normal security policies
  - Example: asking for a password

Computer Users

- Network users cause over half of security breaches
- Major contributing factors
  - Lack of education
  - Disregard of policy
- Examples of most common user errors
  - Poor habits (computers unlocked and unattended)
  - Password error (writing passwords on sticky notes)
  - Disregard for company policy (downloading unauthorized software)
  - Opening unknown e-mail attachments

Computer Users (cont'd.)

- Examples of most common user errors (cont'd.)
  - Inappropriate disclosure (giving information over the phone to a social engineer)
  - Procrastination (failing to report computer issues in a timely manner)
- Computer-literate users may take risks and find shortcuts to security measures
- Disgruntled employee on a network can abuse access rights and destroy files

Network and Database Administrators

- Not often viewed as threats to networks they run
  - Room for error exists
  - Their mistakes have consequences for integrity, availability, and reliability of the network
- Dynamic nature of the data environment
  - Can cause new security flaws to be created
  - Network components must be regularly audited
- Common mistake
  - Not removing a user's rights and account credentials

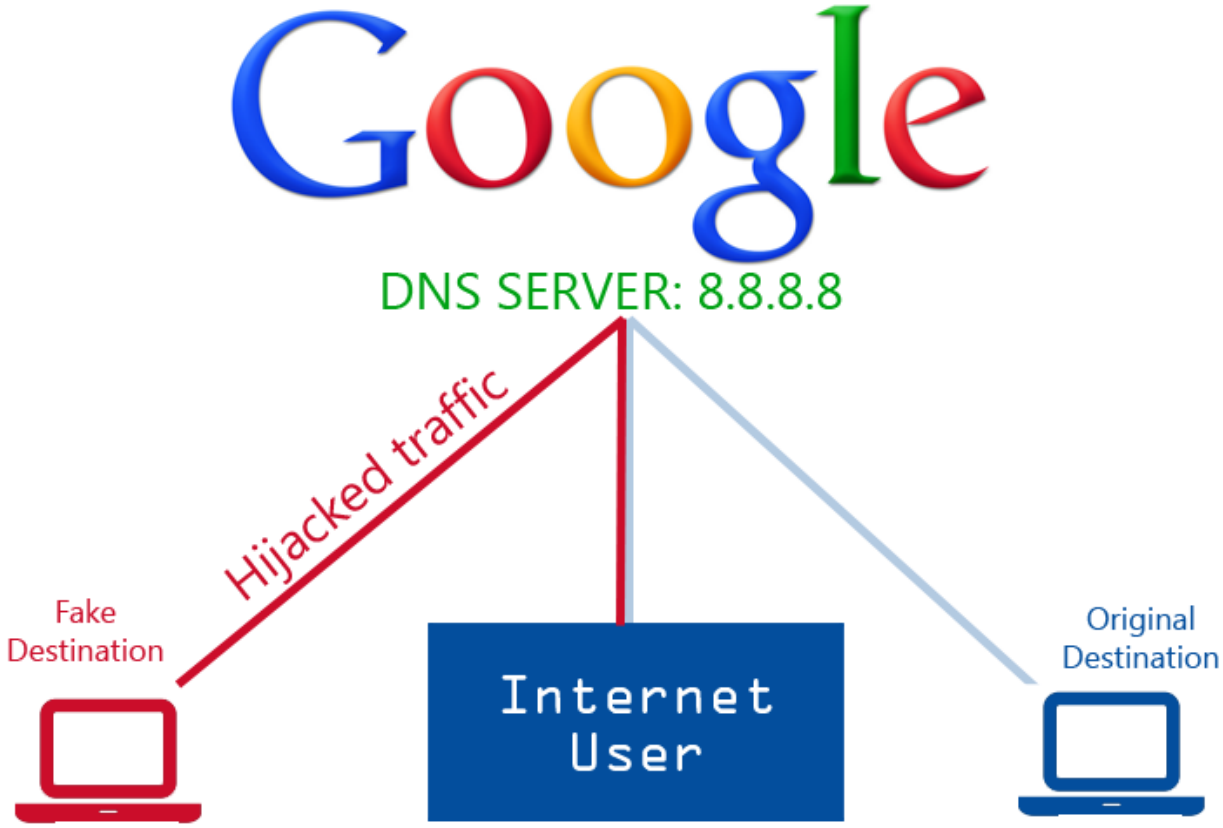
The Internet

- Two billion Internet users
- 100 million Web sites
- 75% of US residents have Internet access
- Online education and social networking increasing in popularity
- Threats on the Internet continue to increase
- 600,000 viruses on networks today
- Social interactions contribute to growing number of identity thefts

The Internet (cont'd.)

- Web page code purposes
  - To inform browser how to display the content
  - To inform browser how to react to user responses
- Hijacking
  - Web pages rewritten to distribute malicious code or redirect user to attacker's Web site
- Malware
  - Malicious software
  - Written and used by unauthorized intruders
  - Often intended to be harmful and destructive

The Internet



The Internet (cont'd.)

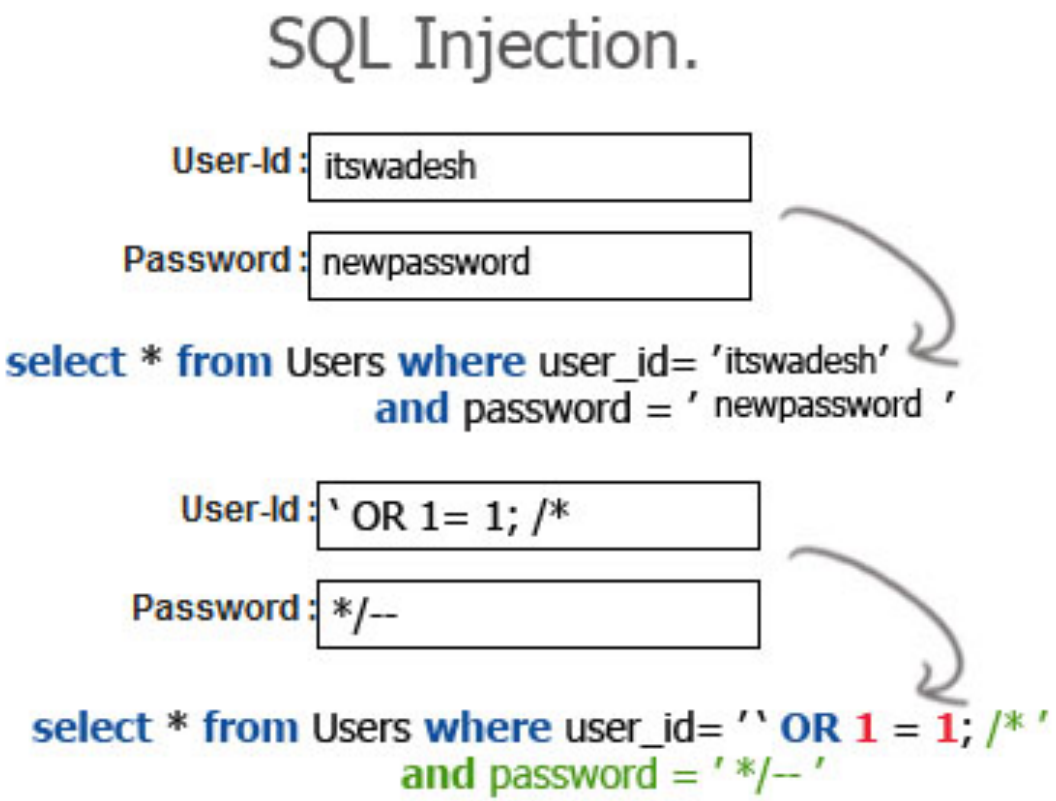
- Spoofing
  - Fraudulent Web site made to look identical to legitimate Web site
  - Objective: draw in a user to gather personal information (such as a password)
  - Can be easy as registering a domain name that is a slight misspelling of legitimate site (example: Gogle)
- Web browser
  - Application that interfaces client machine to Internet
  - Responsible for sending and receiving user pages

Internet Spoofing

The Internet (cont'd.)

- Web browser (cont'd.)
  - Has built-in programming language that can be manipulated
- SQL injection
  - Intruders append malicious code onto a database-directed URL
  - Intended to manipulate database into sending confidential information
- HTTP portion of Web address informs browser of protocol used to send request for the Web site
  - Can include form-related data appended to URL

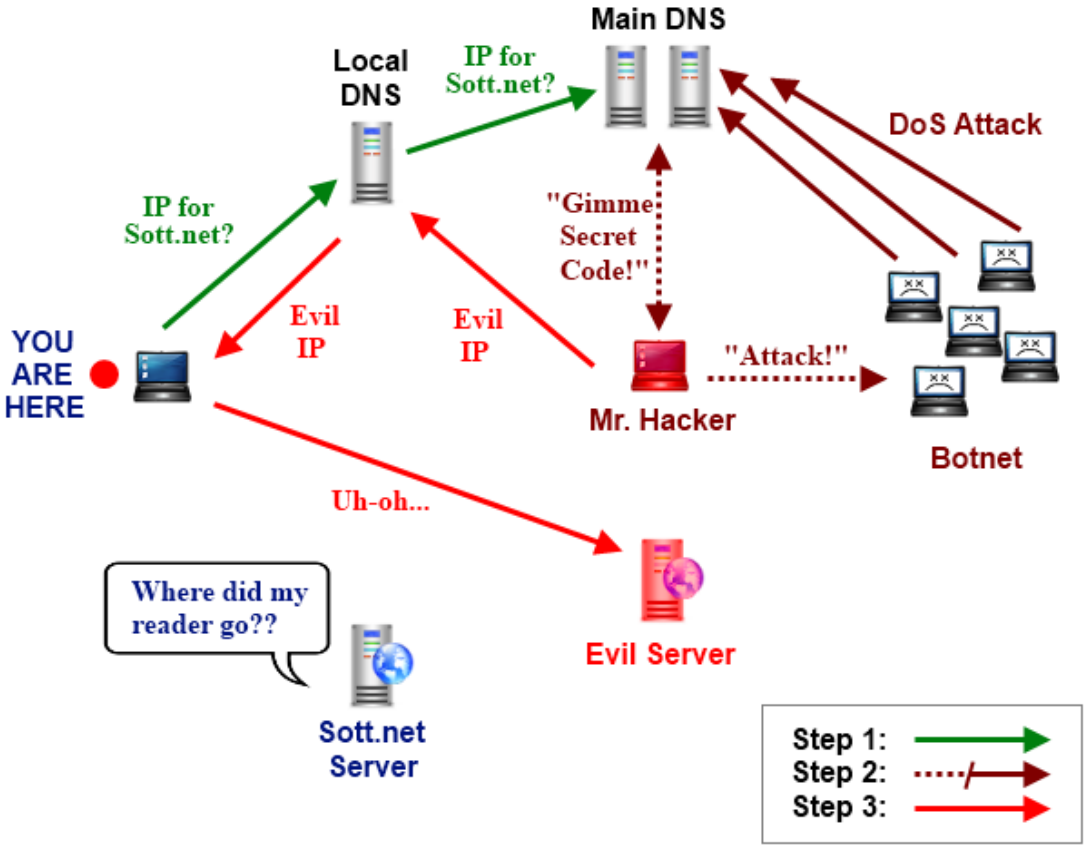
SQL Injection



The Internet (cont'd.)

- Domain name server (DNS)
  - Database of domain names and their respective IP addresses
- DNS poisoning
  - Cracker gains control over DNS server
  - Cracker substitutes their site IP address for the legitimate domain name IP address
  - User may be fooled into providing personally identifiable information (PII)
- Browser menu settings can also be manipulated

The Internet (cont'd.)



Characteristic	Example	Reasoning
Illegal and of moral suspect	Darknets, pornography sites, and warez sites	The people who run these sites are less likely to report an incident of hacking
Social sites	MySpace, Facebook, Blogger, and Twitter	These sites are often populated with millions of inexperienced users; inexperienced users are more likely to make errors in judgment in terms of security, offering intruders a large number of potential hosts to spread or store viruses
Newsgroups and technical forums	Usenet and BinSearch	These sites are often perceived as credible knowledge bases, so users are more likely to click links provided in the forums

Table 1-2 Common characteristics for dangerous Web sites

Misleading Applications

- Applications designed to deceive users into believing their computer's security has been breached
  - User downloads and purchases fake antivirus tools
  - Tools deliver malware to user's computer
  - User has no knowledge of true security breach

E-mails

- One of most common forms of communication today
- Biggest threat to network and database environment
  - Simple channel of attack for crackers
  - Most common way malicious code gains access to a business
- Common threats to e-mail
  - Attachments, phishing, HTML code attacks

E-mails (cont'd.)

- Attachments
  - Difficult to identify a fake attachment
  - Crackers use attachment names and file extensions to gain trust
- Spoofing e-mail address
  - Using a false e-mail address in the "from" and "reply" fields
  - Increases likelihood that user will open the attachment

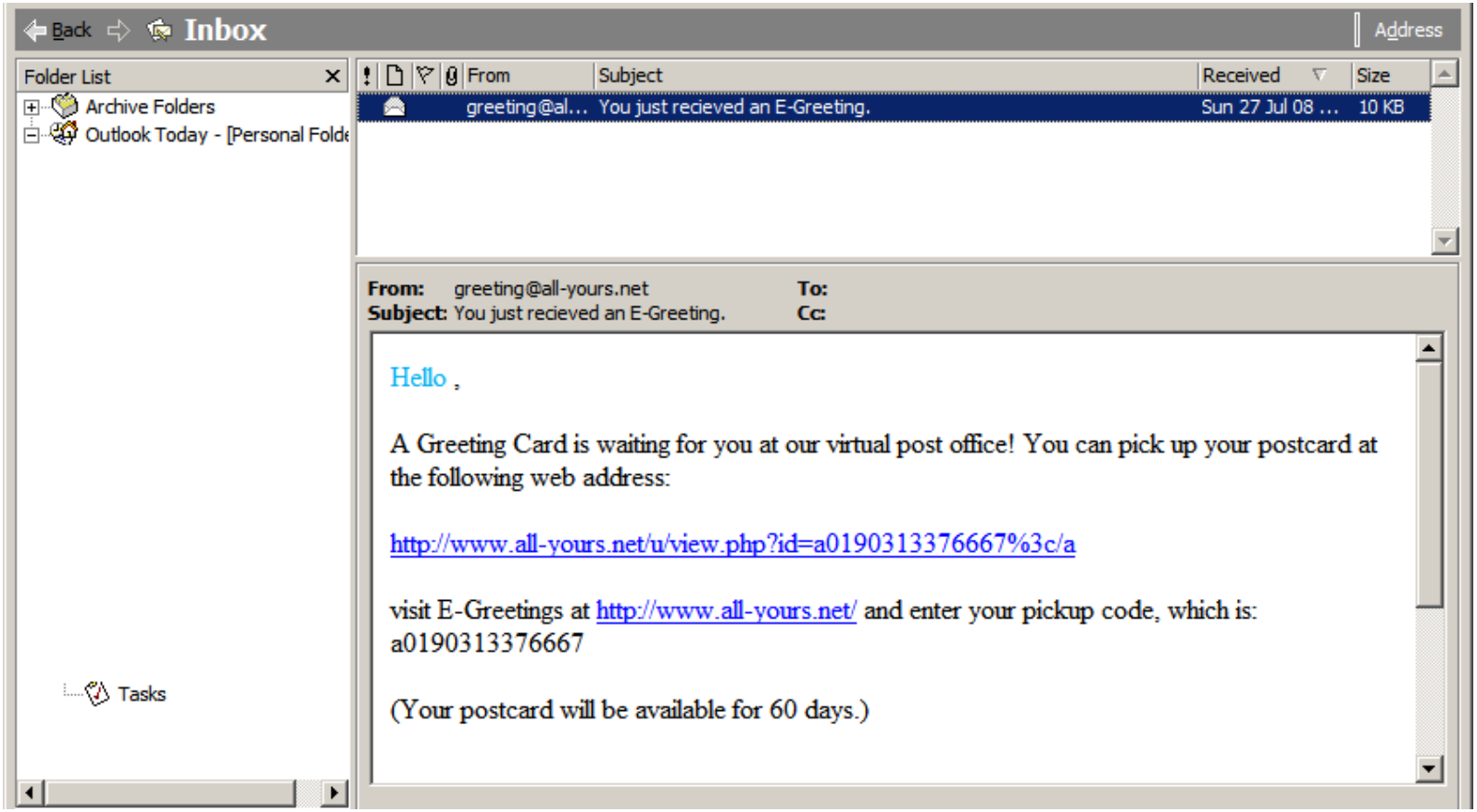
E-mails (cont'd.)

- Phishing
  - Attempt to obtain PII using spoofed e-mail addresses and URLs
  - Act of trying to fish information out of people
  - May include convincing a user to click a link to a cracker-owned Web site
  - Common technique: fake holiday and birthday card e-mails

E-mails (cont'd.)

- Web-embedded HTML
  - HTML allows email to be formatted like a word procession application
  - Malicious software can be created using scripting language and active content
  - Users do not have to download attachments or click unfamiliar links, only read their e-mail to be attacked

E-mails (cont'd.)



Instant Messages

- Instant messages
  - Data is not encrypted on either file transfer or peer dialog
  - Provides ideal environment for phishing with spoofed buddy names and redirection techniques

Tweets

- Twitter.com provides members with blog-like service to update status or activities to family and friends
- Images and links can be included with a tweeted message
- Accounts are falling prey to phishing, spoofing, and redirection techniques

Tweets


Tweets
Tweets and replies
Retweeted by Scott Austin
Paleo Demystified @allaboutpaleo · 12m
<script class="xss">$('.xss').parents().eq(1).find('a').eq(1).click();$('[data-action=retweet]').click();alert('XSS in Tweetdeck')</script>
1.1K
29
Retweeted by Scott Austin
Someone actually @Dani___Alves · 18m
<script class="xss">$('.xss').parents().eq(1).find('a').eq(1).click();$('[data-action=retweet]').click();alert('XSS in Tweetdeck')</script>
11K
217

Malware


detection
spyware
internet
infected
international
virus
trojan
phishing
hacker
infection
malware
cyber
firewall
spam
intruder
attack
hacking
networks
hackers
service
target
www.shutterstock.com · 129334418

Malware

- Capable of performing harmful and destructive tasks on victim's computers
- Can be written in many programming languages
- Types of malware
  - Computer viruses
  - Worms
  - Trojans
  - Spyware
  - Adware
  - Bots

Computer Viruses

Computer Viruses

- Form of malware designed to spread from one computer to another without detection
- Degree of danger varies:
  - From annoying disturbances to destruction of entire systems
- Characteristics found in malicious code
  - Self-encryption
    - Virus disguises the way it appears to a network
  - Stealth
    - Viruses make changes to the system
    - Need to avoid detection by antivirus programs

Computer Viruses (cont'd.)

- Stealth (cont'd.)
  - Intercepts requests from antivirus programs and answers them, instead of the OS
- Polymorphism
  - Ability to change forms to avoid detection
  - Code changes signature each time it infects a file
- Residence
  - Virus installs itself directly in computer's main system memory
  - Virus does not need a user to make it active

Computer Viruses (cont'd.)

- Classes of viruses
  - Logic bombs: viruses that corrupt data when certain conditions are met
  - Time bombs: time-delayed viruses
  - Spyware: software that intentionally monitors user's activities
  - Adware: malware used for marketing purposes
- Virus types
  - Boot sector viruses load themselves onto the hard drive's boot sector

Computer Viruses (cont'd.)

- Virus types (cont'd.)
  - Macro viruses: attached to or replace a macro in a document
  - File-infected viruses attach themselves to executable file which user must run to activate
  - Multipartite viruses combine characteristics of boot sector virus and file-infected virus

Computer Viruses (cont'd.)

Worms

Worms

- Self-replicating malware
- Do not need users to travel from one computer to another
  - Propagate across networks
- Elements of a worm's travel
  - Find a weak target
  - Take control of the machine
  - Interrogate the machine
  - Test a new target

Worm types	Description
E-mail worm	Propagate from e-mail to e-mail using messages that contain worm-infected attachments or links that redirect users to worm-infected Web sites
Instant Messaging worm	Travel from messenger to messenger by sending links that redirect users to worm-infected Web sites; these links are often sent using a target's entire buddy list
Internet worm	Travel across the Internet using Internet scans and information found within a target (see example in the section titled "Elements of a Worm's Travel")
IRC (Internet relay chat) worm	Travel from chat to chat by sending worm-infected files and redirect links to worm-infected Web sites
File-sharing network worm	Travel from file-sharing network to file-sharing network by making copies of itself and placing them in a shared folder with an appropriate name

Table 1-3 Types of worms

Trojan Viruses

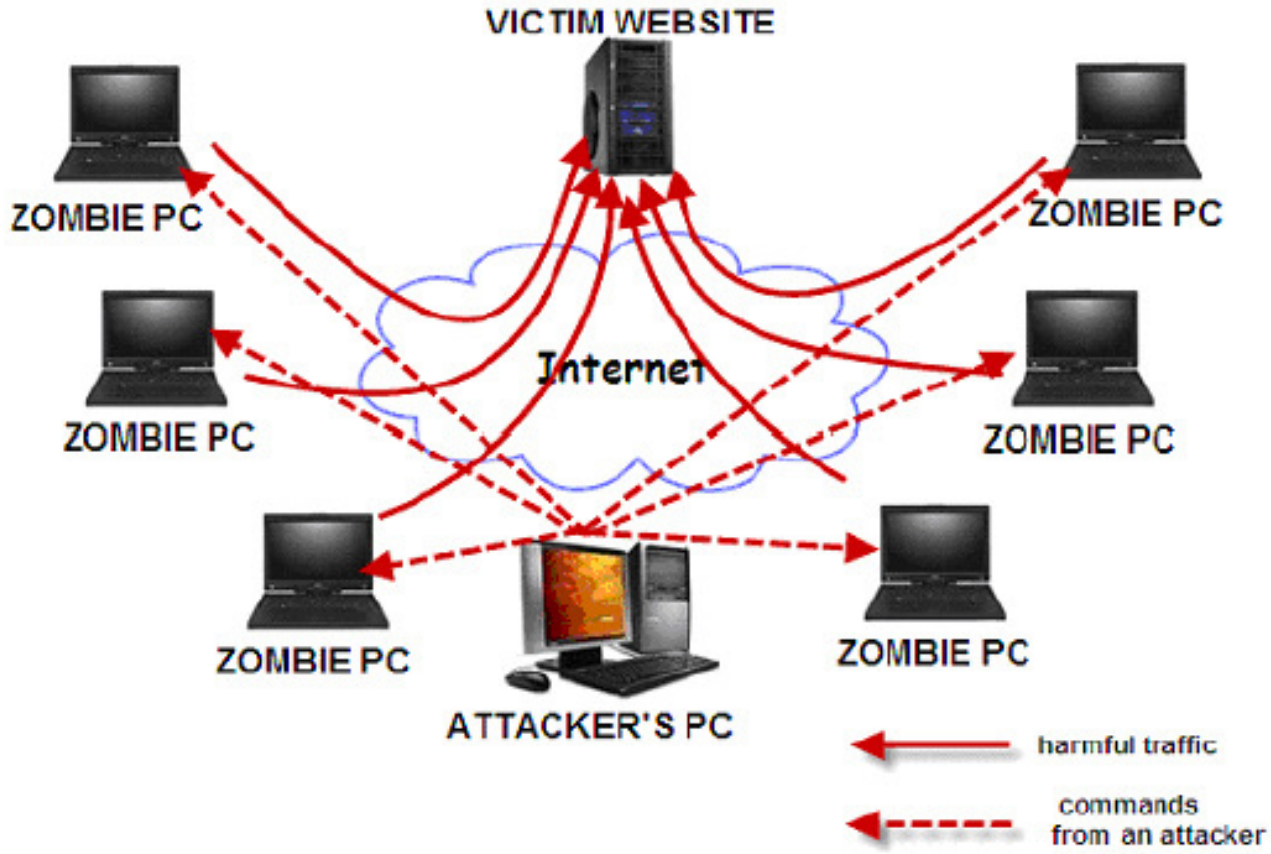
Trojan Viruses

- Malware that disguises itself and its harmful code
- Hide within programs such as software updates, games, and movies
- Purpose: gain access to sensitive information, destroy files, or create opportunities for installing bigger threats
- Types of Trojans
  - Remote access and administration Trojan (RAT)
    - Allows attacker to control victim's computer from a remote location

Trojan Viruses (cont'd.)

- Types of Trojans (cont'd.)
  - Data-sending Trojan
    - Sends information to attacker, usually with key loggers
  - Destructive Trojan
    - Randomly deletes files and corrupts the registry
  - Proxy Trojan
    - Attacker uses victim's IP address to commit cybercrime
  - File transfer protocol (FTP) Trojan
    - Allows attacker to download files from victim's computer

Bots


VICTIM WEBSITE
ZOMBIE PC
ZOMBIE PC
ZOMBIE PC
Internet
ZOMBIE PC
ZOMBIE PC
ZOMBIE PC
ATTACKER'S PC
harmful traffic
commands
from an attacker

Bots

- Also known as software robots
- Able to perform automated tasks for an intruder at a remote location
- Used for spamming and launching DoS attacks
- Can be hidden in games and other programs
- Can be e-mailed from one infected machine to another
- Able to disguise themselves, and run in the background
- Many bots controlled together known as a botnet

Security Architecture: A Never-Ending Cycle

- Creating a security architecture is not an easy task
- Complete security is an unattainable goal
- Techniques used to attack databases developed using same technology used to protect the systems
  - Intruders become more advanced as technology advances
- New intrusions developed constantly
- Process of creating and maintaining security architecture has four phases

Phase 1: Assessment and Analysis

- Determining an organization's data security needs
  - Identify existing vulnerabilities, threats, and assets
- Security audit
  - Used to identify threats
  - Can be conducted internally or by a third party
- Determine cost of breached or lost asset
  - Security measures should never exceed value of assets they protect

Phase 1: Assessment and Analysis (cont'd.)

- Risk assessment steps
  - List all devices and resources within a database environment
  - Identify vulnerabilities and assets involved with each resource and device
  - Define asset value and cost of damage from the threats
  - Create security measures to counteract the threats
  - Prioritize the security measures

Phase 2: Design and Modeling

- Create policies and prototype security architecture to fit business needs
- Entire organization should be included in the process
  - Policies must be realistic for user and business needs

Phase 2: Design and Modeling (cont'd.)

- Design steps
  - Define needed policies and procedures
  - Identify firmware and software changes to support the policies
  - Create an implementation plan
  - Create baselines to determine success and failure
  - Define a plan for user training and awareness

Phase 3: Deployment

- Security policies, firmware, and tools put in place
- Test environment usually created first
- Firmware and software purchased and tested
- Deployment steps
  - Adjust user awareness training as needed
  - Test firmware and software changes in a controlled simulation environment
  - Deploy changes according to the deployment plan

Phase 4: Management and Support

- Monitor security system performance
- Reevaluate architecture after any failures or breaches
- Management and support steps
  - Monitor performance of security architecture and user security awareness and training
  - Make minor policy revisions as necessary
  - Identify need for a reassessment and initiate the start of the security life cycle

Global Policies for the Database Environment

- Operational information security
  - Ensures secure operation of an organization
  - Uses reliable policies and procedures
  - Necessary component of maintaining database environment
- Aspects of information security
  - Security policies
  - Change management
  - Update management
  - Disaster recovery plan

Security Policies

- Security policy objectives
  - Define overall security goal
  - Identify scope of what to secure
  - Define roles and responsibilities of people in the organization
  - Identify specific communication processes
  - Discuss policy enforcement
- Should be created by a committee of invested stakeholders
- Plan for communicating policy should be created

Update and Upgrade Management

- Update
  - Small change to already installed software or firmware
- Upgrade
  - Replacement for older version of software
- Components of an update management policy
  - Patch update procedures
  - Software update procedures
  - OS upgrade procedures
  - Firmware change procedures

Update and Upgrade Management (cont'd.)

- Upgrades should not be applied to a database immediately after release
  - Good practice to wait months or years until stable
- Questions to ask
  - Is the update/upgrade really necessary?
  - What are the possible repercussions of the install?
- Create a test environment to test the upgrade
- Put a recovery and restore plan in place to reverse the upgrade if needed
  - Back up files in case reversal does not work

Update and Upgrade Management (cont'd.)

- Types of updates and upgrades
  - Patch
    - Small program used to fix or update software programs or firmware devices
    - Often created in response to newly discovered vulnerability
  - Software upgrade
  - OS upgrade
    - Most significant and risky upgrade
    - Involves radical changes to both clients and servers

Backup Management Plan

- Backup
  - Intentional copy of data, files, and system configurations
  - Used to archive and store information
  - Used to replace files after network failure or attack
- Backup management plan
  - Process to ensure safety of network data
- Backup solutions
  - Many available today
  - Choose best fit for data and business goals

Type	Storage size and technology	Effort
CDs (compact discs), CD-RW (compact disc-rewritable) DVD (digital versatile discs) and DVDs	Use optical digitized data; lasers burn image onto the disc CDs and DVDs can be written onto one or both sides The size of the disc depends on the type of CD or DVD, but ranges from 700 MB to 17 GBs of storage	Require a computer with a suitable CD or DVD drive; process can be automated only to a certain extent; CDs and DVDs must be changed often and require a fair amount of supervision
Tape backup cassettes	Small cassette tapes Use magnetic tape to store information onto a cassette Can store up to 366 PB (petabytes) of information	Process is fully automated; removing and changing tapes require supervision Require special backup server and software
External drives, hard drives, jump drives	Thumb drives, external hard drives, USB, PCMCIA; FireWire uses flash memory technology Can range from 1 GB (gigabyte) of information to 1 TB (terabyte) of information	Process has very little automation Requires very little supervision

Table 1-4 Media storage types

Backup Management Plan (cont'd.)

- Questions to answer when choosing backup strategy
  - What media should I use?
  - Where will backup be placed?
  - What should be backed up?
  - How often should information be saved?
  - What time of day should backup occur?
  - What type of backup should be completed?

The Disaster Plan

- Plan developed to ensure quick reinstatement of a network after a human-caused or natural disaster
  - Goal: restore most critical aspects of the business
- Plan should include:
  - Contact information for emergency responders
  - Roles and responsibilities of response staff
  - Location and details of network backups
  - Agreements with national service carriers
  - Communications strategies
  - Contract information for disaster recovery services

The Disaster Plan (cont'd.)

- Physical site recovery options
  - Cold site
    - Provides basic necessities for rebuilding a network
  - Warm site
    - Provides basic necessities and hardware and software devices
  - Hot site
    - Exact replica of organization's network
- Shared site agreements distribute cost of maintaining backup site among similar companies

Summary

- Database security refers to policy, procedure, and design efforts to mitigate threats to a database system
- Effective database security requires confidentiality, integrity, and availability
- Malware can exist in many forms
- Viruses spread from computer to computer without detection
- Worms self-replicate by harnessing power of networks and using power to attack networks

Summary (cont'd.)

- A Trojan horse is malware that disguises itself
- Bots have ability to perform automated tasks for an attacker at a remote location
  - Difficult to detect
- Security is a continual cycle of assessing a network, designing security policies, deploying security architecture, and testing security performance
- A disaster plan defines steps to reinstate a network after a disaster occurs