SE 4352
Software Architecture and Design

Fall 2018

Module 9

Importance of Information Security

- The internet allows an attacker to attack from anywhere on the planet.
- Security is Everyone's Responsibility.
- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and companies)
  - Termination if company policies are not followed
- According to www.SANS.org , the top vulnerabilities available for a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights

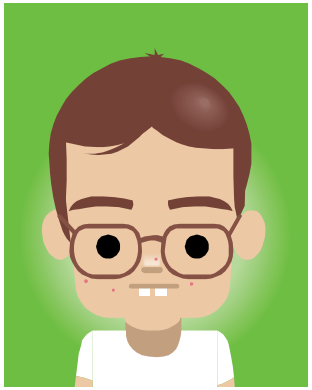
Security vs Safety

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.

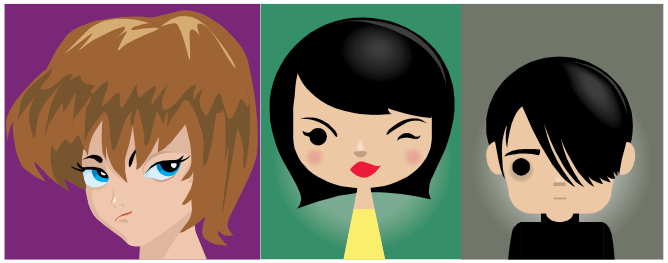
User Awareness

Computer Criminals



Cracker:
Computer-savvy programmer creates attack software

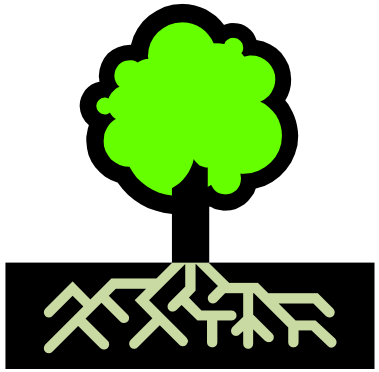
Script Kiddies:
Unsophisticated computer users who know how to execute programs



Criminals:
Create & sell bots -> spam
Sell credit card numbers,…

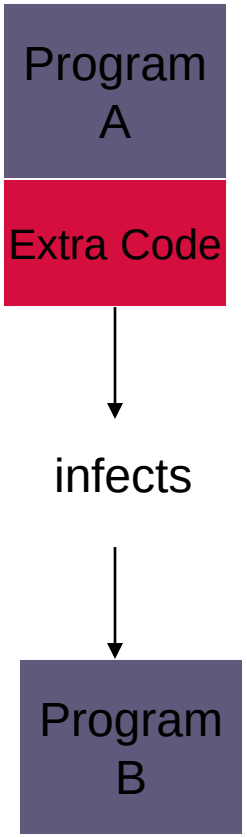
Leading Threats

- Virus
- Worm
- Trojan Horse / Logic Bomb
- Social Engineering
- Rootkits
- Botnets / Zombies



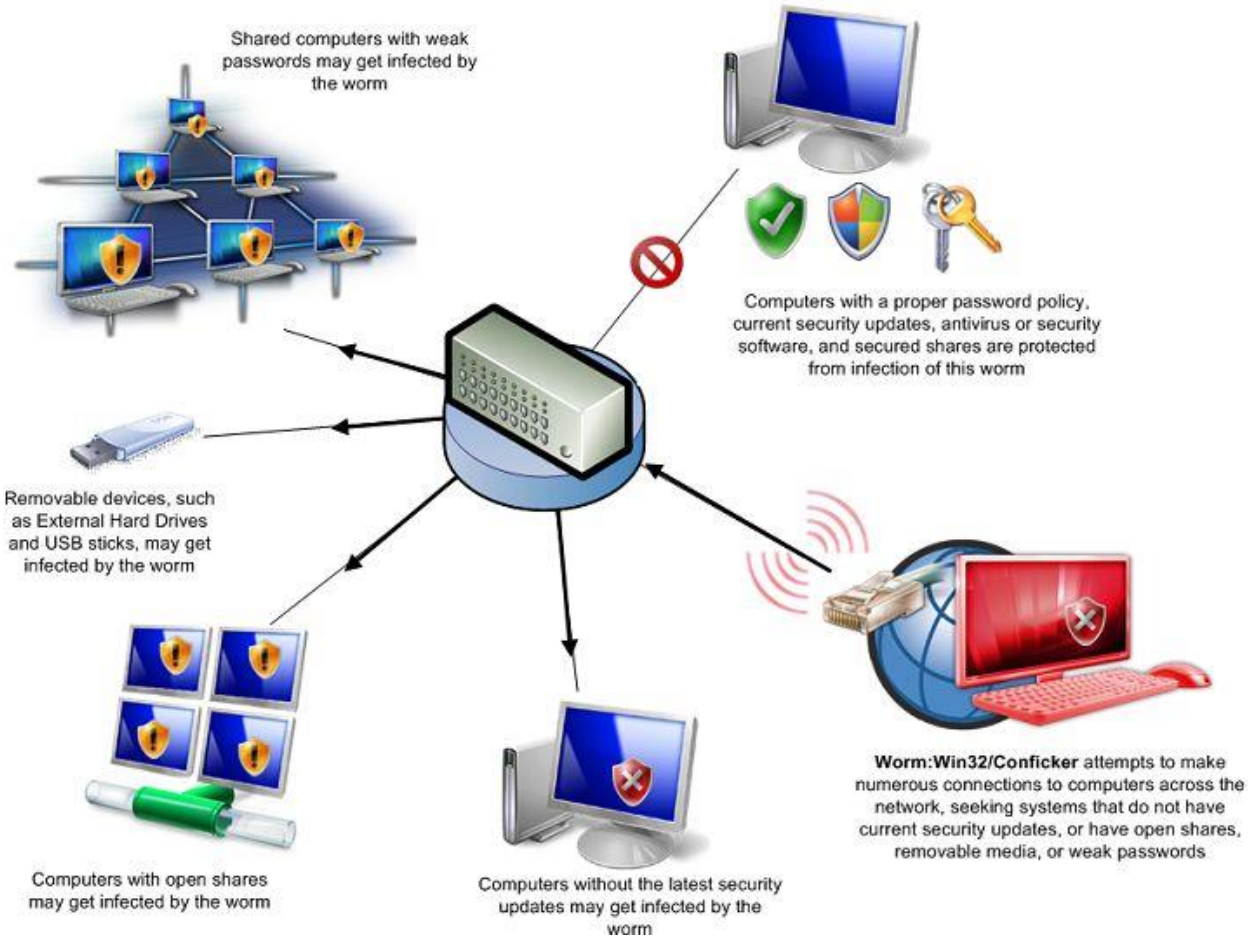
Virus

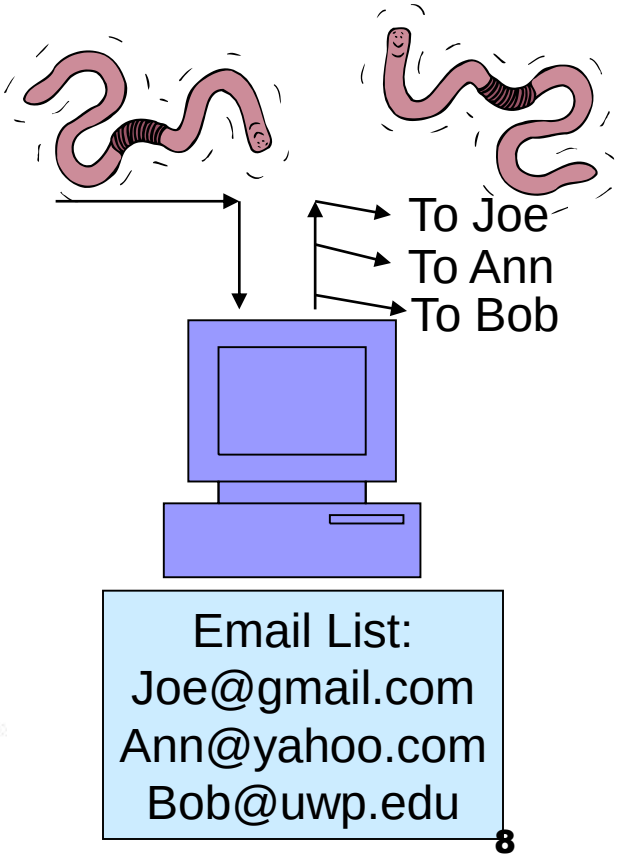
- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus activates and replicates itself
- The virus may be benign or malignant but executes its payload at some point (often upon contact)
  - Viruses result in crashing of computers and loss of data.



Worm

- Independent program which replicates itself and sends copies from computer to computer across network connections. Upon arrival the worm may be activated to replicate.

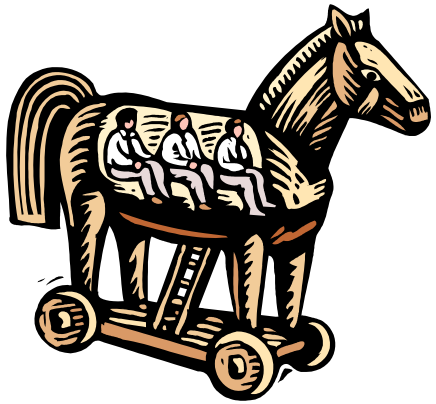




Logic Bomb/Trojan Horse

- **Logic Bomb:** Malware logic executes upon certain conditions. Program is often used for legitimate reasons.
  - Employee triggers a database erase when he is fired.

- **Trojan Horse:** Masquerades as beneficial program while quietly destroying data or damaging your system.
  - Download a game: Might be fun but has hidden part that emails your password file without you knowing.



Social Engineering

- Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phone Call: This is John, the System Admin. What is your password?

Email: ABC Bank has noticed a problem with your account…

In Person: What ethnicity are you? Your mother's maiden name?

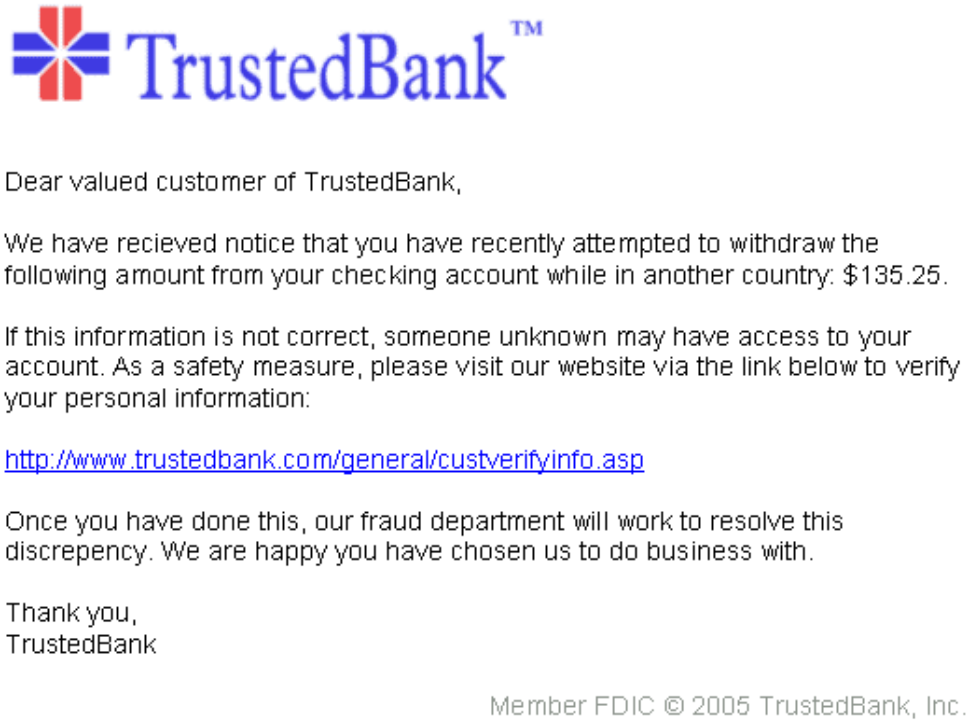
I have come to repair your machine…

and have some software patches

Phishing = Fake Email

- **Phishing**: a 'trustworthy entity' asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.

Pharming = Fake Web Pages



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

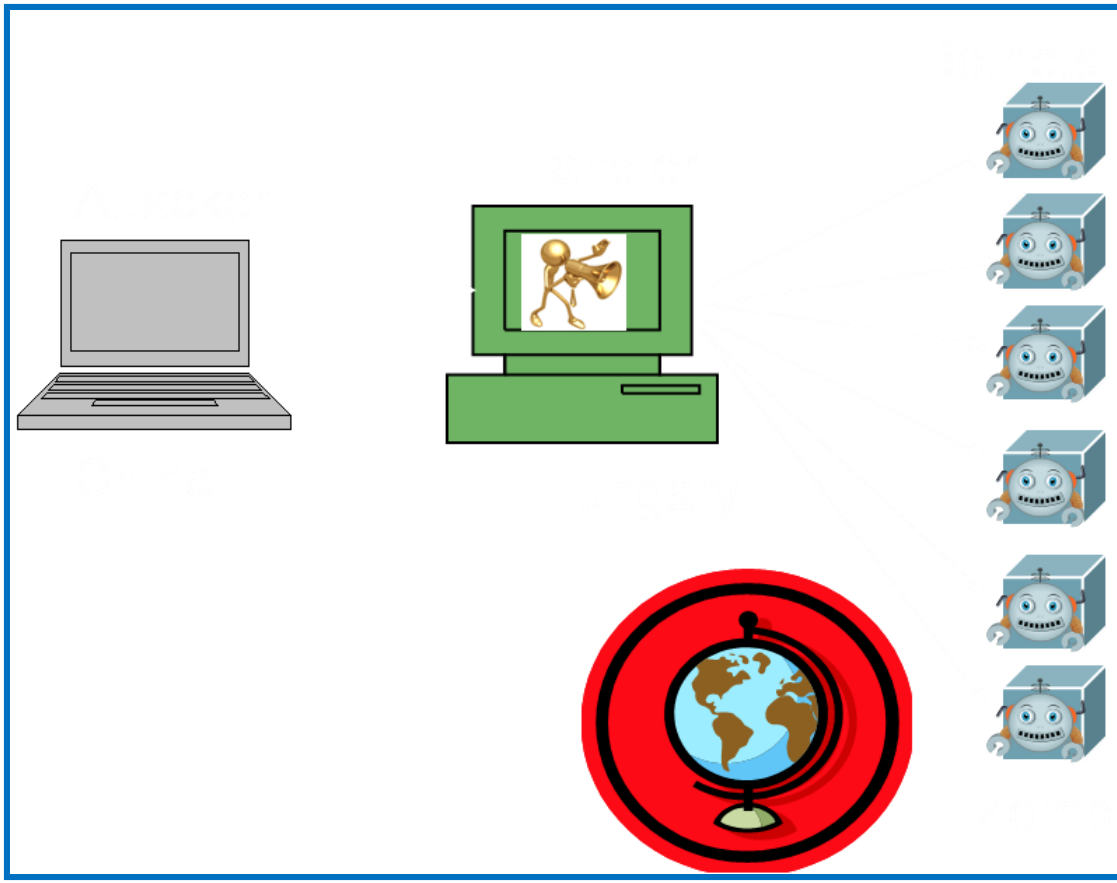
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

- The link provided in the e-mail leads to a fake webpage which collects important information and submits it to the owner.
- The fake web page looks like the real thing
  - Extracts account information

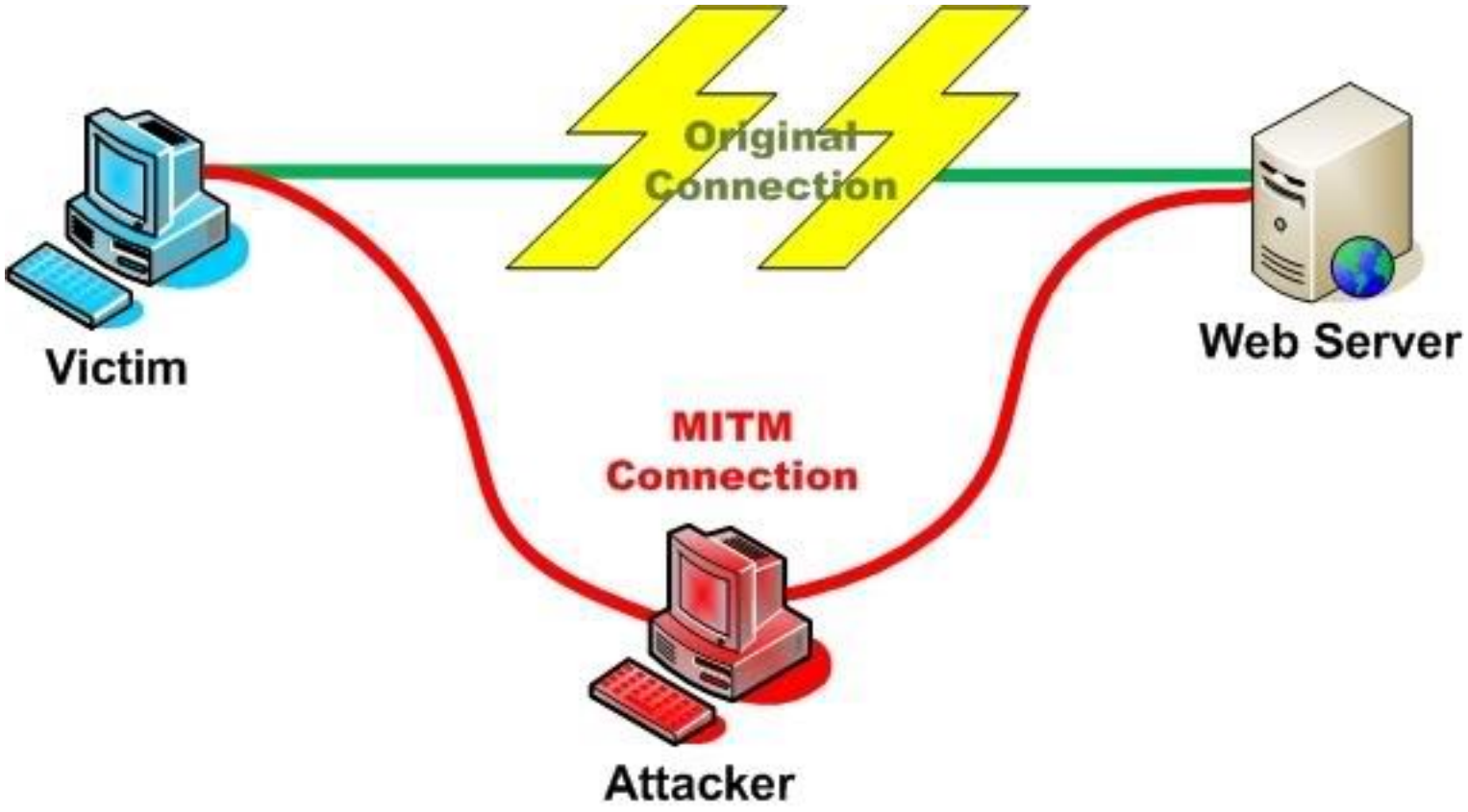
BotNet

- A **botnet** is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called **zombies**



Man In The Middle Attack

- An attacker pretends to be your final destination on the network. If a person tries to connect to a specific WLAN access point or web server, an attacker can mislead him to his computer, pretending to be that access point or server.



RootKit

- Upon penetrating a computer, a hacker installs a collection of programs, called a **rootkit**.
- May enable:
  - Easy access for the hacker (and others)
  - Keystroke logger
- Eliminates evidence of break-in
- Modifies the operating system

Password Cracking: Dictionary Attack & Brute Force

Pattern	Calculation	Time to Guess
Personal Info: interests, relatives		Manual 5 minutes
Social Engineering		Manual 2 minutes
American Dictionary		< 1 second
4 chars: lower case alpha	26^4	
8 chars: lower case alpha	26^8	
8 chars: alpha	52^8	
8 chars: alphanumeric	62^8	3.4 min.
8 chars alphanumeric +10	72^8	12 min.
8 chars: all keyboard	95^8	2 hours
12 chars: alphanumeric	62^{12}	96 years
12 chars: alphanumeric + 10	72^{12}	500 years
12 chars: all keyboard	95^{12}	
16 chars: alphanumeric	62^{16}	

Data Breach Notification Law

- Restricted data includes:
  - Social Security Number
  - Driver's license # or state ID #
  - Financial account number (credit/debit) and access code/password
  - DNA profile (Statute 939.74)
  - Biometric data
- In US, HIPAA protects:
  - Health status, treatment, or payment

Break-In Detection

- Symptoms:
  - Antivirus software detects a problem
  - Pop-ups suddenly appear (may sell security software)
  - Disk space disappears
  - Files or transactions appear that should not be there
  - System slows down to a crawl
  - Unusual messages, sounds, or displays on your monitor
  - Stolen laptop (1 in 10 stolen in laptop lifetime)
  - Your mouse moves by itself
  - Your computer shuts down and powers off by itself
  - Often not recognized

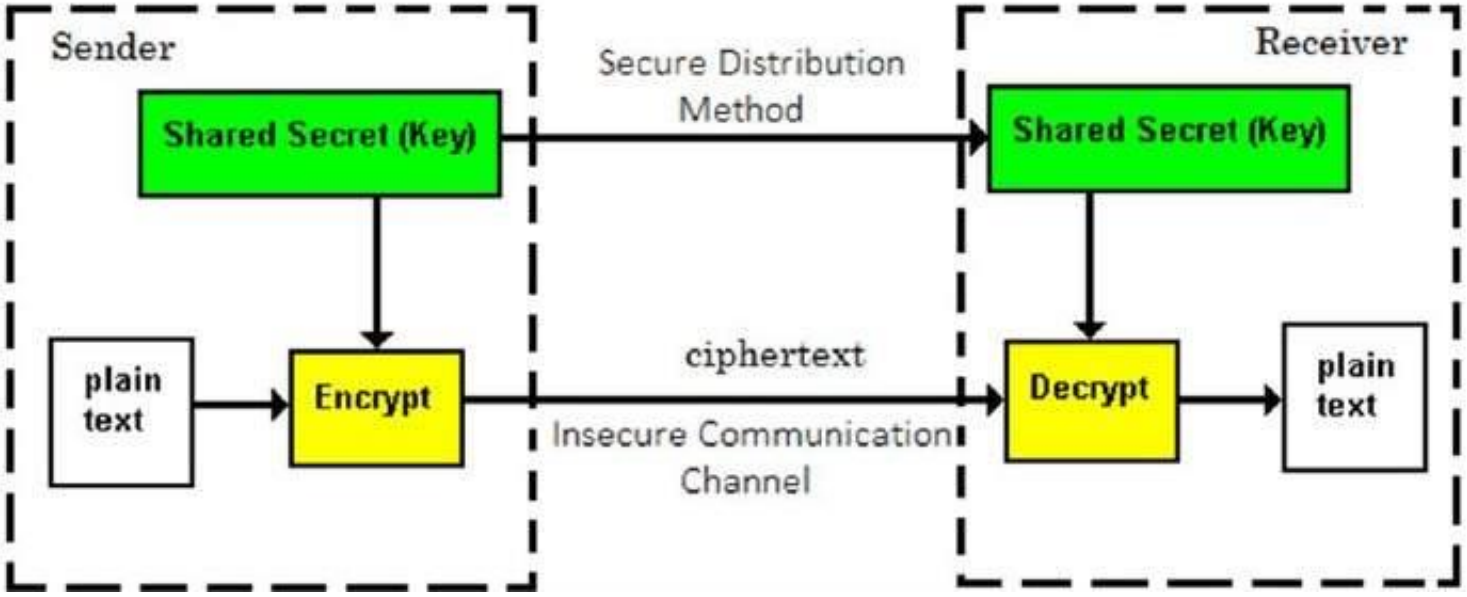
Malware Detection

- Spyware symptoms:
  - Change to your browser homepage/start page
  - Ending up on a strange site when conducting a search
  - System-based firewall is turned off automatically
  - Lots of network activity while not particularly active
  - Excessive pop-up windows
  - New icons, programs, favorites which you did not add
  - Frequent firewall alerts about unknown programs trying to access the Internet
  - Bad/slow system performance

Safe & Secure User Practices

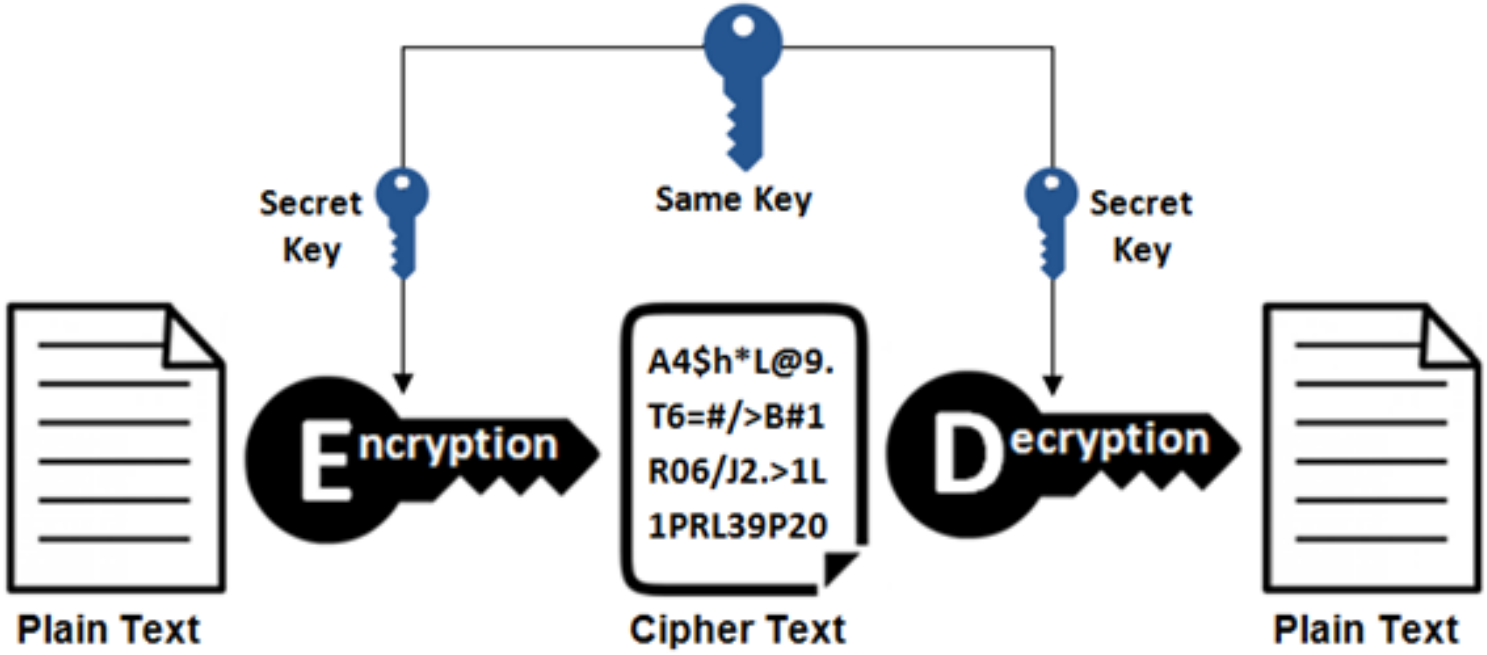
Secure Message Transfer

- The ability to reliability exchange messages between sender and receiver while hiding its contents from third parties.
- Encryption / Decryption in the security of local computers.
- Encrypted messages (cipher text) is transmitted across insecure channels i.e. the internet.



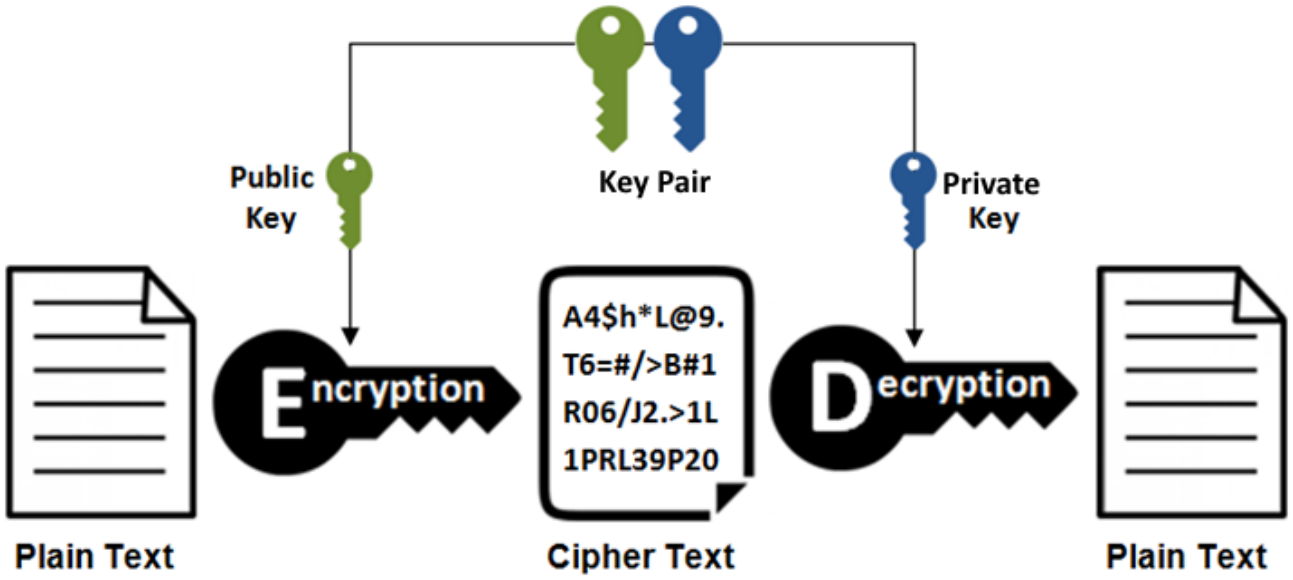
Single Shared Key Symmetric Encryption

- A single key, shared between sender and receiver, is used to encrypt and decrypt the message to be securely transmitted between two parties.



Public / Private Key Encryption

- A party wishing to receive secure messages generates two keys (a key-pair) using a key-pair generator:
  - Public Key: Is provided to anyone wishing to send a secure message and is used to encrypt the message into cypher text.
  - Private Key: Is used to decrypt cypher text messages encrypted with the public key.



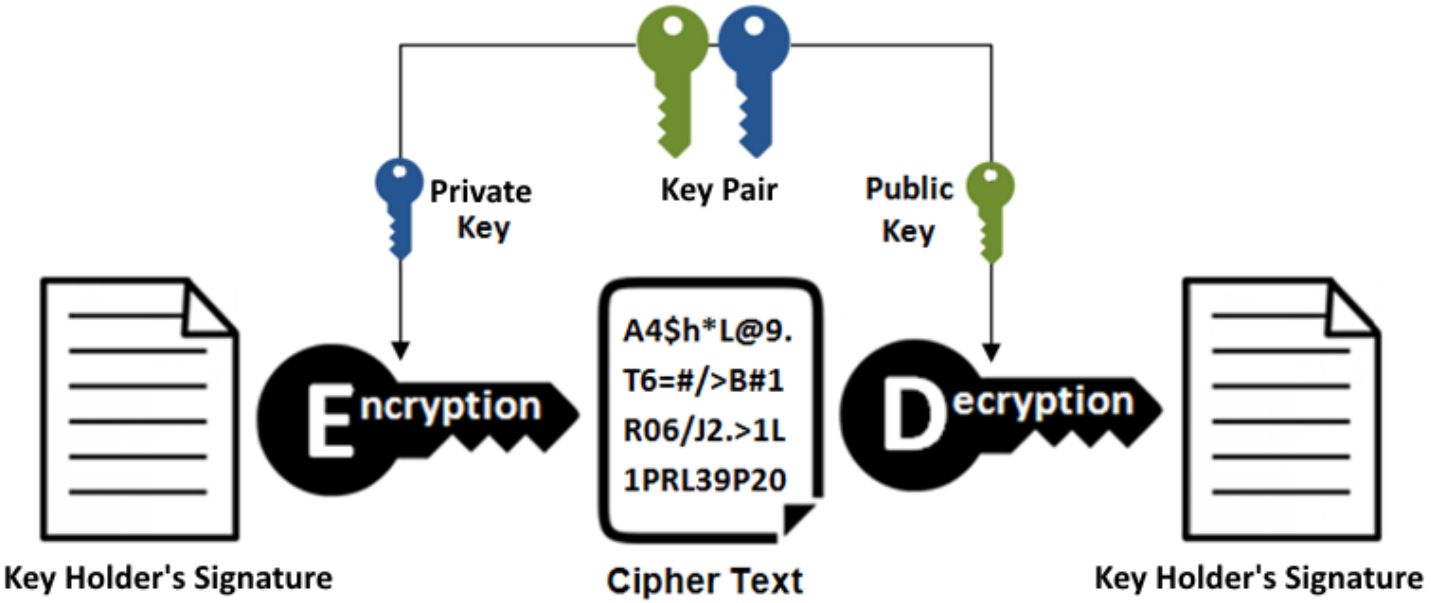
Public / Private Key Encryption

- The public key can be “sent in the open”.
  - Solving the problem of symmetric key distribution.
- The private key is held in secret.
  - The assumption is that only the key pair’s owner has access to their private key.

- This is asymmetric encryption in that a message can be encrypted / decrypted in only one direction.
  - A message encrypted with the public key can only be decrypted using the private key.
  - A message encrypted with the private key can only be decrypted using the public key.

Public / Private Key Authentication

- Using a private key to *sign* a document for the purpose of verifying the identity of the document originator.
  - To send signed legal documents.
  - To authenticate identity to remote servers e.g. AWS SSH.



Message Authentication

- The signer's private key is used to generate a signature that can only be 'opened' by the signer's public key.
- The document's signature can be verified by anyone with the signer's public key.
  - Because the public key is not secret, a signed document can be verified by anyone.
- How can either party be certain that the document was not modified in transit?
  - A hash of the document can be generated and encrypted using the sender's private key.

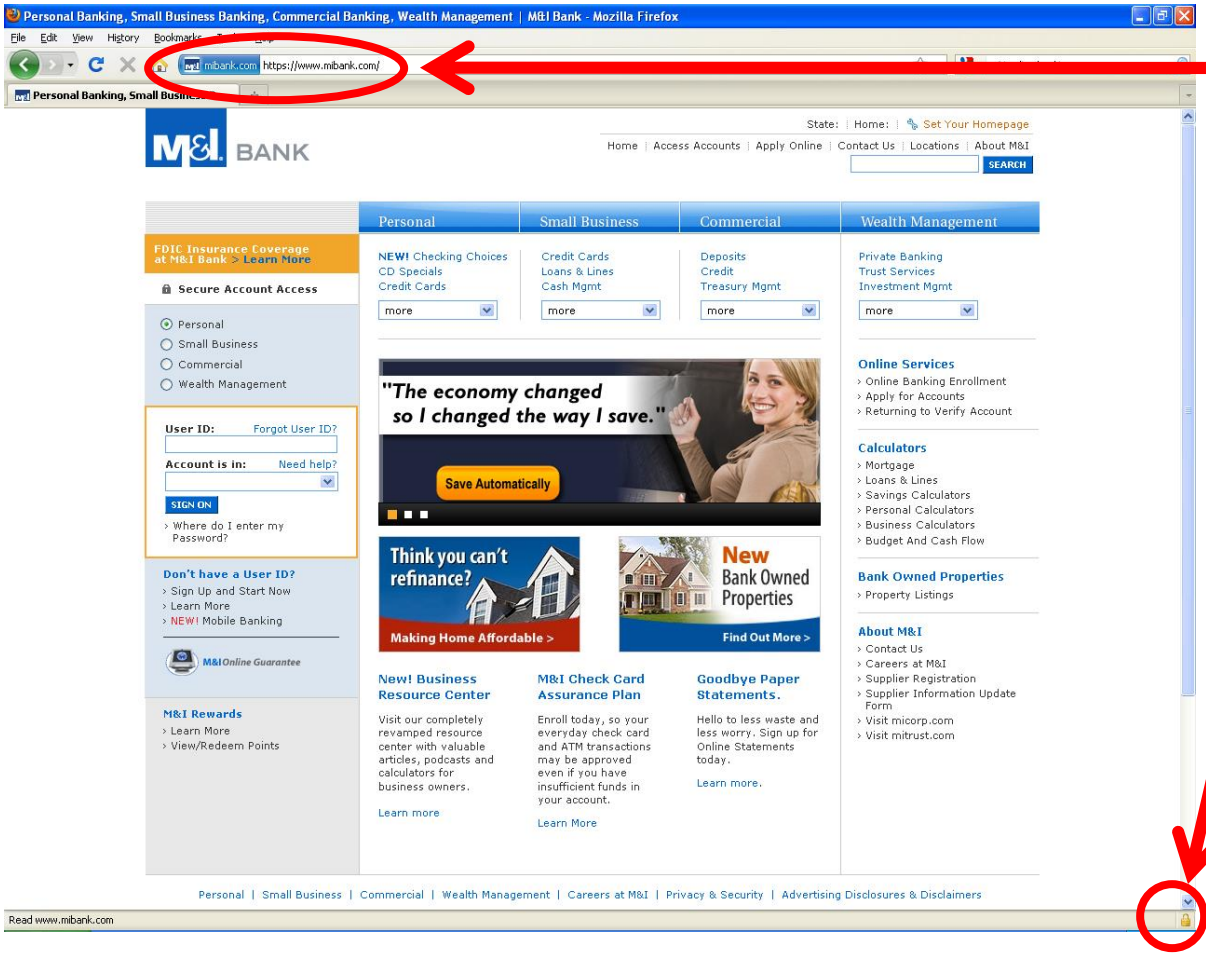
Hashing Functions

- A hashing function takes input data (e.g. a document) and generates a hash value that is unique to the data.

- If the document is hashed by the originator, and the hash value is securely sent with the document, its hash can verified by the receiver.
  - Even slight changes to the document during transit will generate a different hash value at the receiver.

Secure Online Banking & Business

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.



https://

Symbol showing enhanced security

Secure Web Communication using SSL

- Secure Socket Layer (SSL) creates an encrypted two-way channel between the client and server.
  - Third parties are unable to read the contents of the channel.
- When an SSL channels is used by a browser it is referred as the HTTPS protocol.
- SSL uses a combination of Public-Private Key and Symmetric Encryption.
  - Symmetric algorithms are orders of magnitude faster than PPK.

The Process of Establishing a SSL Connection

- The client requests the server to start an SSL connection.
  - Services using SSL are generally located at port 443.
- The server sends the client its public key in a certificate.
- The client generates a one-time shared key to be used to encrypt the traffic between client and server. The key is encrypted using the server's PK and sent to the server.
- Having securely exchanged the shared key, the client and server can now use a faster asymmetric algorithm to encrypt the data transmitted over the "Secured Socket".

The Process of Establishing a SSL Connection

Network Services

- Network services are provided by applications (process) installed on a server (machine) at an address & port number.
- Clients access a service by first connecting to the application.
  - Machines have internet (IP) addresses.
  - Applications are installed *at ports* on the machine.
- For example, HTTP services is an application (e.g. Apache) running on a publically-accessible machine at port 80.
  - Port 80 is the default port for HTTP services.
  - Browsers (clients) open a connection (socket) to the HTTP service using the machine's address and port 80.

Public and Private Networks & Addresses

- An Internet Protocol Address (IPv4) is made up of four groups of 8-bit numbers (xx.xx.xx.xx).
  - IPv6 defines an address using eight groups of 16-bit numbers.

- Networks are classified as either Public or Private.
- The Internet standards committee has set aside certain ranges of addresses for private networks.
  - One such range is the Class C address 192.168.xx.xx.
  - Machines inside the enterprise (or home) network are on a private network e.g. 192.168.0.12 .

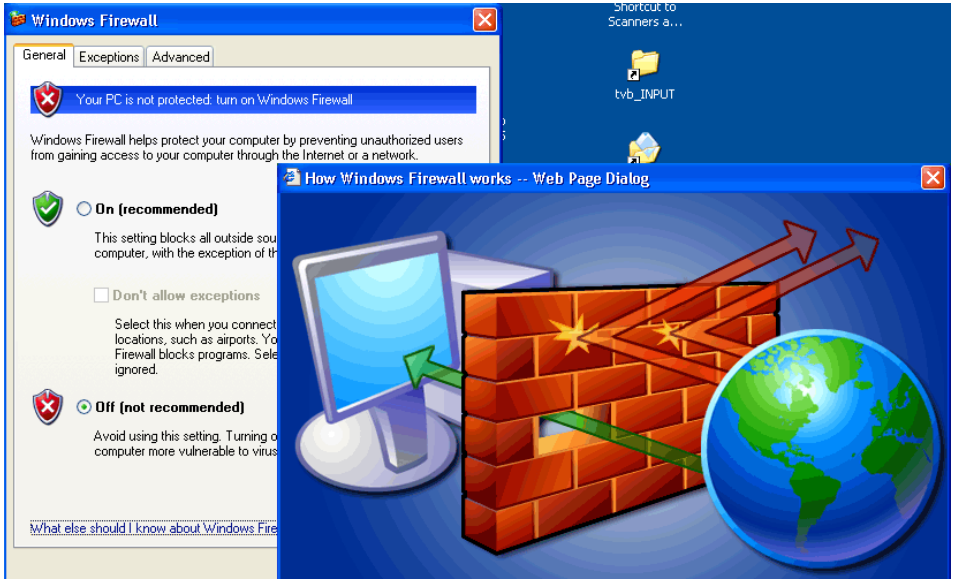
- The internet's routers will not pass packets addressed to private networks.

Restricting Network Access to Services

- Many network services run on a typical machine (server).
  - Some services are intended for public access.
  - Some services should only be accessible from within the enterprise
- Secure Shell (SSH) is an example of a restricted service.
  - SSH provides machine-level access for the enterprise's operators allowing them to perform maintenance on the server.
  - SSH could also provide a channel through which 'hackers' can break into a server, steal information, disrupt services, etc.
- A mechanism is needed that allows external access to public services but denies external access to restricted service.

Firewall

- A firewall acts as a wall between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents hacker connections from entering your computer.
- Filters packets that enter or leave your computer

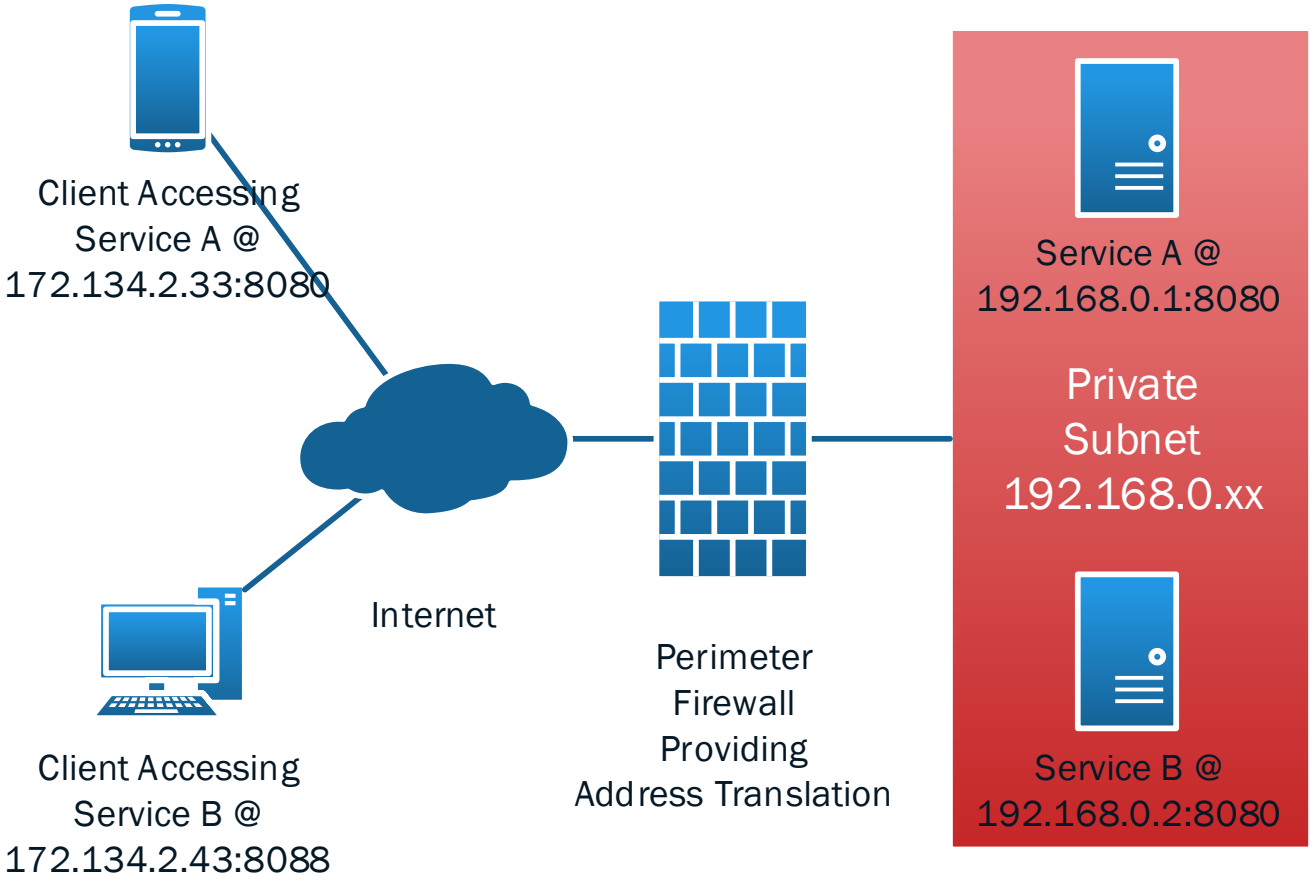


Security Tactic: Firewalls

- A Firewall is a machine / server that acts as a *gate keeper* between the public internet and machines running in the enterprise's private networks.
  - A Firewall / Router provides several network management services

  A Firewall can be:
  - Purchased as a standalone network appliance from vendors such as Cisco. This is the best but more expensive alternative.
  - Installed and configured on machines running general-purpose operating systems such as BSD or Linux.

Firewall Providing Address Translation from Public Internet to Private Enterprise Networks



Translating Public Addresses into Private Network Addresses

- Services accessible from the public internet are made available at public addresses.
  - The firewall is installed at those public internet addresses.
  - Servers are installed behind the firewall at private addresses.
- The Firewall translates public addresses to private addresses hosted in the enterprise's private network.
  - According to the firewall's configuration, a network packet addressed to the firewall's public address will be forwarded to a private address (machine) running in the enterprise's private network.

How Does a Firewall Secure the Private Network?

- Traffic in the private network is restricted to only the network.
  - Private Class C addresses (192.168.xx.xx) will by rejected by the internet's infrastructure (routers).
  - So public clients cannot directly address the servers in the private network.

- The firewall will filter (reject) any IP packets whose destination address in not in its translation configuration.
  - The firewall will reject a packet from the public network addressed to 172.134.2.33:22 (SSH) because no public to private translation has been configured.

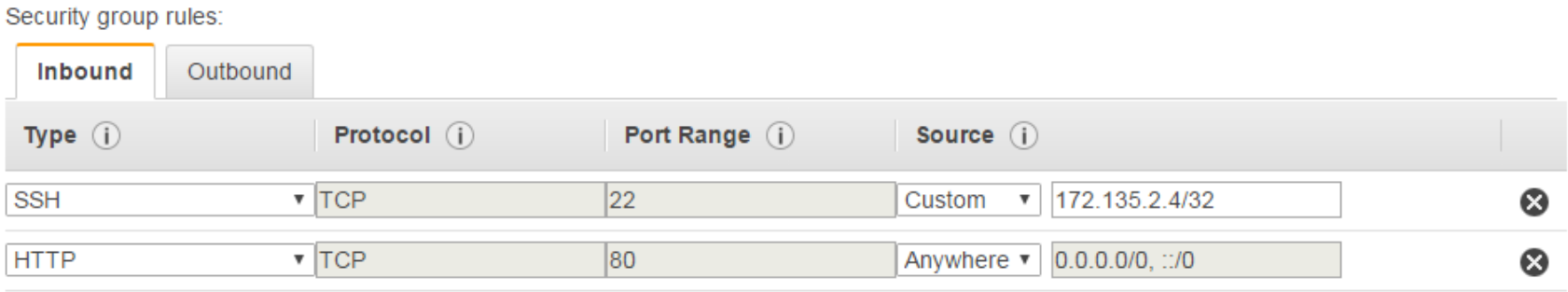
Firewall Configuration

- A firewall is configured by:

  1. Initially blocking all traffic from the public internet.

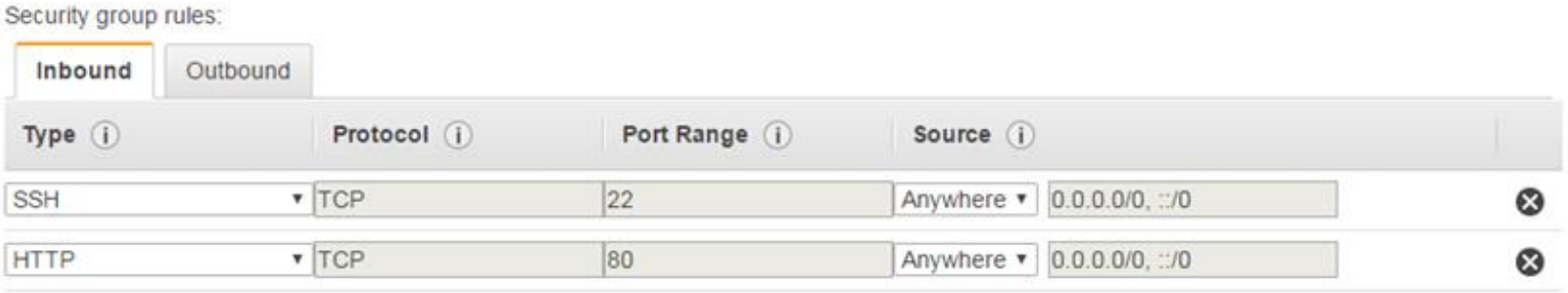
  2. Selectively allowing address / port combinations though.

- AWS Security Groups are Firewall Rules for associated EC2 servers.
  - Every EC2 server maintains its own firewall.

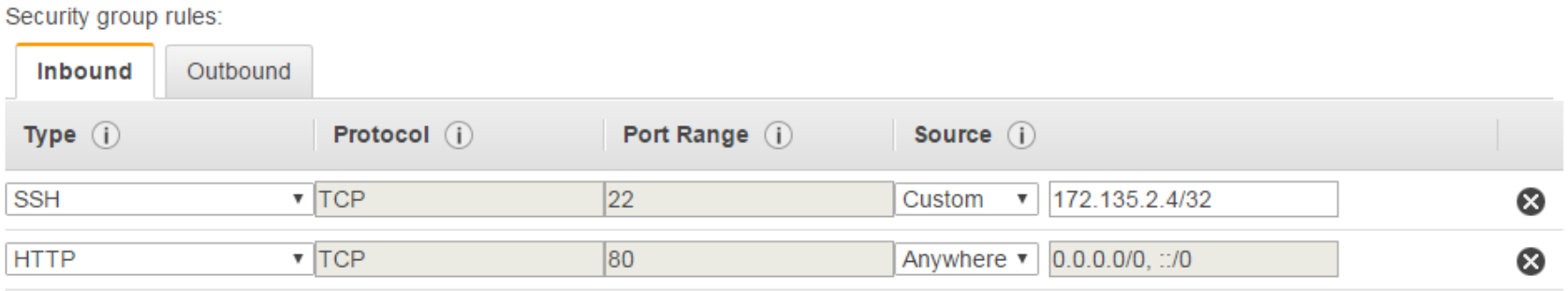


Example AWS Security Groups

- Allows both HTTP and SSH traffic from anywhere (Bad Idea).



- Allows HTTP from anywhere but restricts SSH to a specific public address used by the site operators.



With this level of protection, how are intrusions into private networks (hacks) accomplished?

- By exploiting bugs or incorrect configurations of the firewall.
- By the installation of intrusion software from within the enterprise.
  - Typically by an employee or someone with access to the internal network.

- To make hacks of critical information more difficult to accomplish, what can be done?

With this level of protection, how are intrusions into private networks (hacks) accomplished?

- By exploiting bugs or incorrect configurations of the firewall.
- By the installation of intrusion software from within the enterprise.
  - Typically by an employee or someone with access to the internal network.

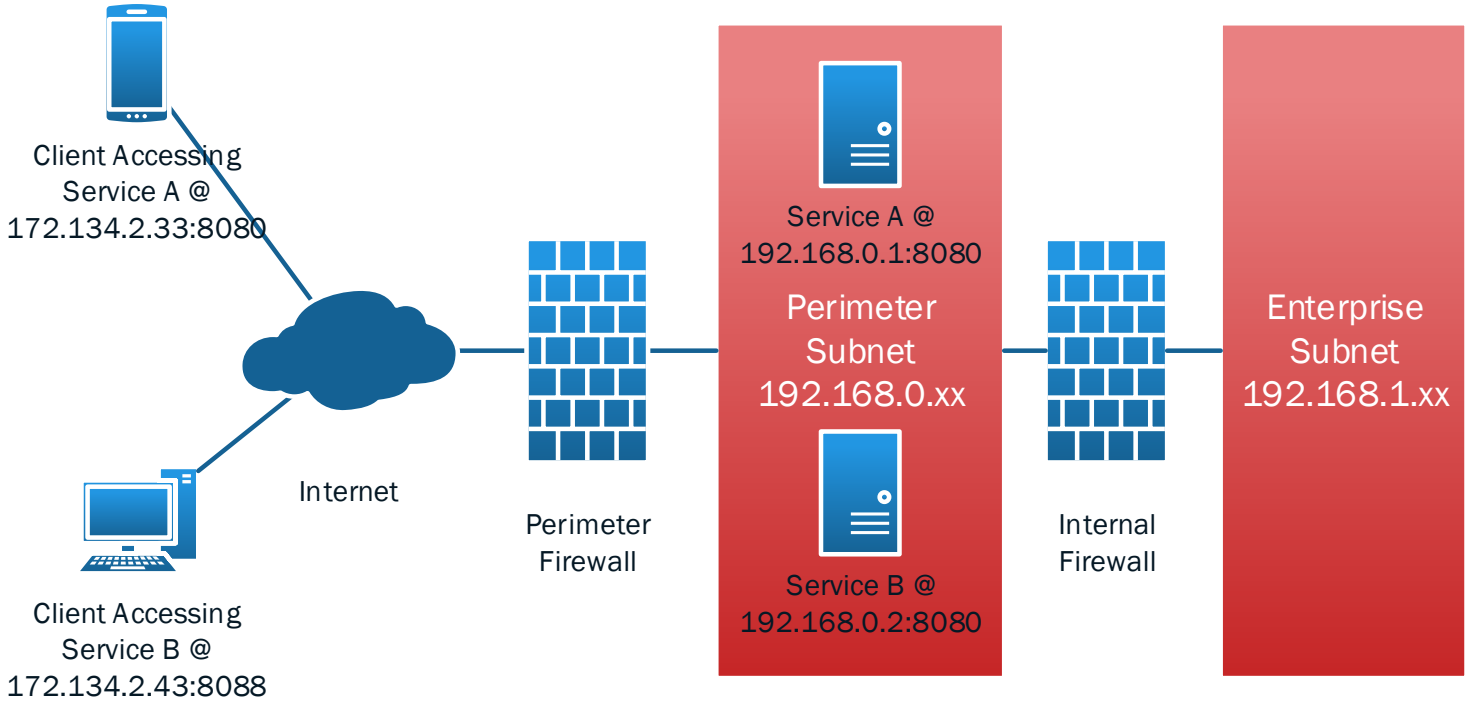
- To make hacks of critical information more difficult to accomplish, two levels of firewall protection are placed in the private network.
  - A Perimeter Firewall between the public network and the machines hosting the services.
  - A Internal Firewalls between the public-facing machines and enterprise's private network.

The Perimeter Network or DMZ

- Two firewalls allow the creation of a *Perimeter Network* that contains the machines exposed to the public internet.

- The perimeter network lies between the perimeter firewall that faces the public network and internal firewalls that protect the enterprise's private network.

The addition of a Perimeter Sub-Network



Advantages of a Perimeter Subnet (DMZ)

- If intruders gain access to the DMZ though the perimeter firewall, they are blocked from access the enterprise network by the internal firewall.

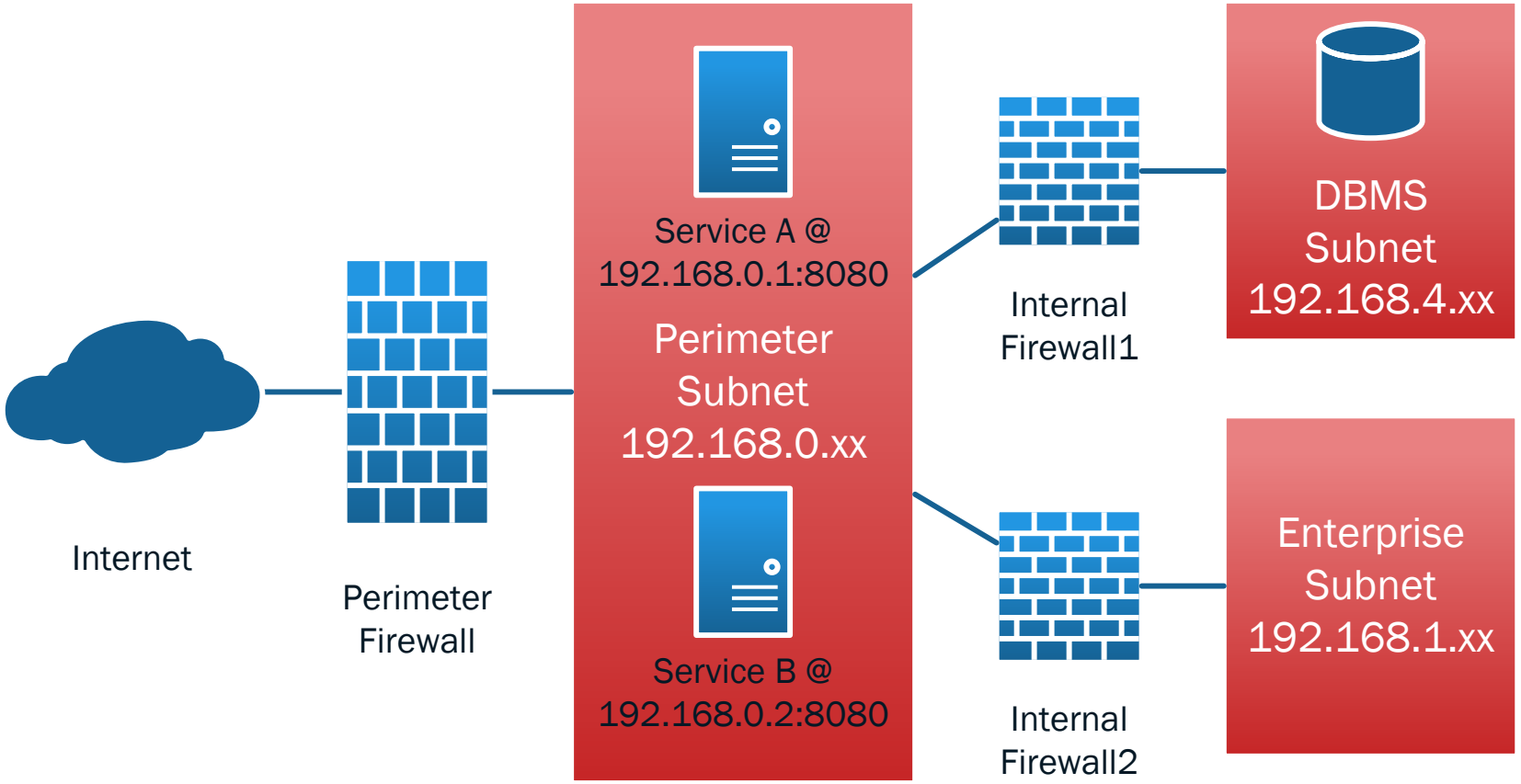
- Rules in the internal firewall can deny access to the perimeter servers from inside the enterprise network.
  - This help to protect those servers from attacks from inside the enterprise.

Protecting Sensitive Information From Intrusions Within the Enterprise

- Assume a DBMS containing critical data e.g. credit cards.
- It is common to place these servers in a separate private network (subnet) inside the enterprise.

- In this example, the use of multiple firewalls allows the creation of a subnet containing the Credit Card DBMS that can only be accessed from inside the perimeter subnet.
  - Machines on the enterprise network cannot access the protected DBMS Subnet.

The Addition of Protected Subnetworks



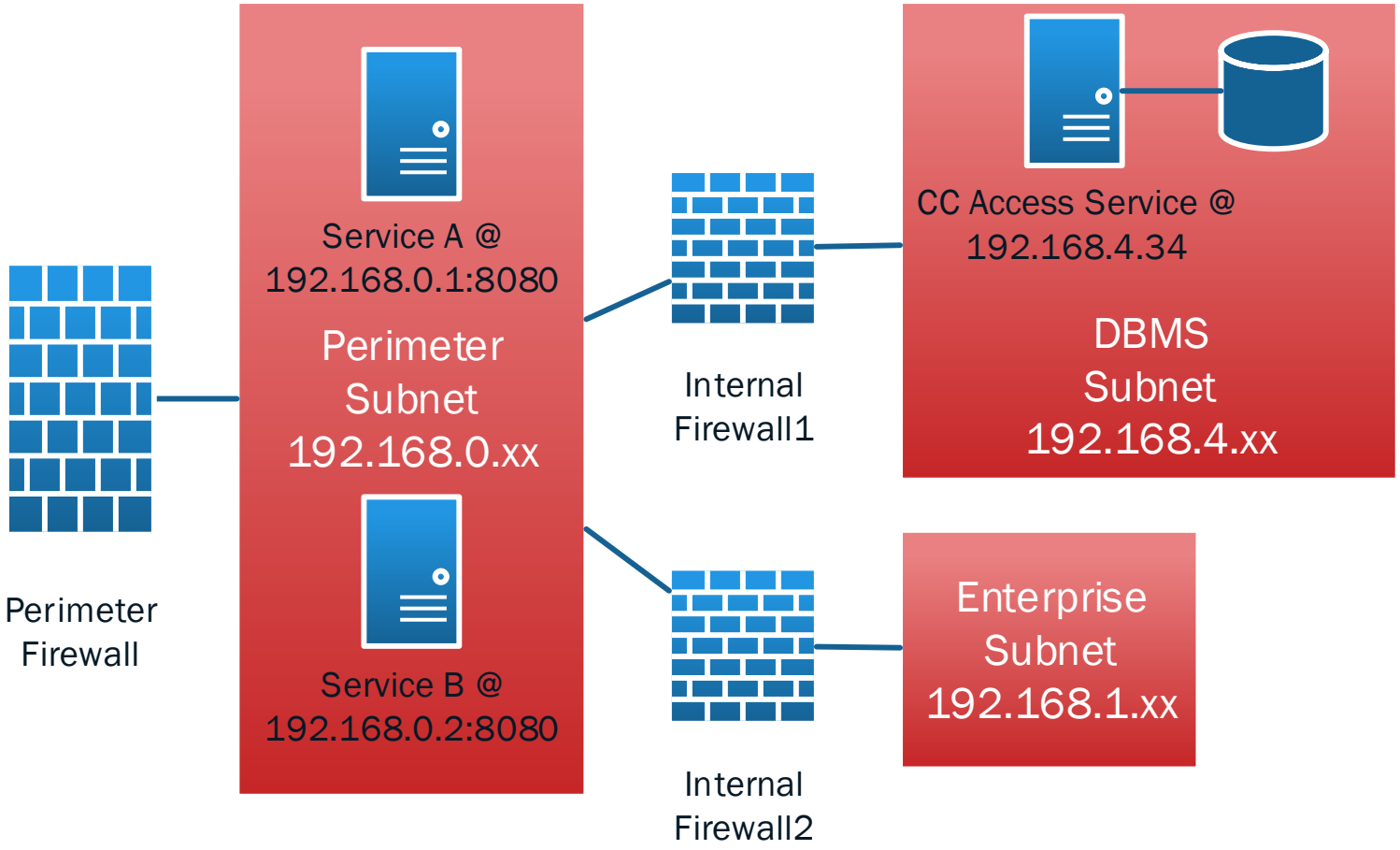
Advantages of Protected Subnets

- If intruders gain access to the DMZ though the perimeter firewall, they are blocked from accessing the protected subnet.
  - The protected subnet's firewall rules can be more specific in terms of the servers allowed to access the DBMS.
- Affords the protected subnet (DBMS) an even better level of protection from attacks from inside the enterprise network.

Providing Access to Sensitive Information

- Some access to sensitive information is required to provide the system's required services.
  - The Customer Service Rep requires access to a customer's credit card information to manage the customer's relationship.
- The previous design allows unrestricted access to the DBMS from within the Perimeter Subnet.
  - Making it vulnerable to access from hacks within the perimeter.
- System services can be designed to provide limited access to sensitive information.
  - The next slide shows a Credit Card Access Service that provides limited access to CC information.

The Addition of Protected Services



Application Security Tactics

- Application Security Tactics are concerned with protecting sensitive information hosted by services from access by unauthorized applications and personnel.

- Access to sensitive services (e.g. CC Service) is restricted to specific roles assigned to client / users.
  - For example, a customer service representative logs into an internal web application.
  - Their ID is associated with a role that allows the client access to the sensitive services.

Role-Based Security

- The process of gaining access to a protected service is defined in two steps:
- Authentication
  - The use of IDs and Passwords to authenticate the user's identity i.e. determine that the user (client) is who they claim to be.
- Authorization
  - Assign roles to users that determine the services / information they are permitted to access.
  - Roles are maintained by the same services that authenticated the user's identity.

Multiple layers of Service Protection

- A system can maintain as many roles as needed to protect access to several sensitive services.
- For example, a ecommerce site may have these roles:
  - CSClerk has limited access a Customer's name and purchase history.
  - CSSupervisor can access CSClerk data plus the Customer's personal information i.e. credit cards, drivers license number, etc.
  - ProductMngt role provides access to services that manage the products and categories maintained by the site.

- The use of multiple roles allows architects to design services that provide targeted access to sensitive information
  - Providing a user / client access to only the information needed to perform a given role / responsibility in the system.

Role-based Access to Services

- Access to a server is allowed / denied to a user or client based on the roles assigned by the system administrators.
- The authorization process works something like:
  - 1. The user / client connects to an application and invokes a specific service hosted by the application.
  - 2. The application accesses the roles assigned to the client to determine whether the request should be executed.
  - 3. If the client has the needed role, the request is executed.
  - 4. Else if the client does not have the needed role, the client's service request is denied with an error (exception).

Implementing Role-based Access with Application Containers

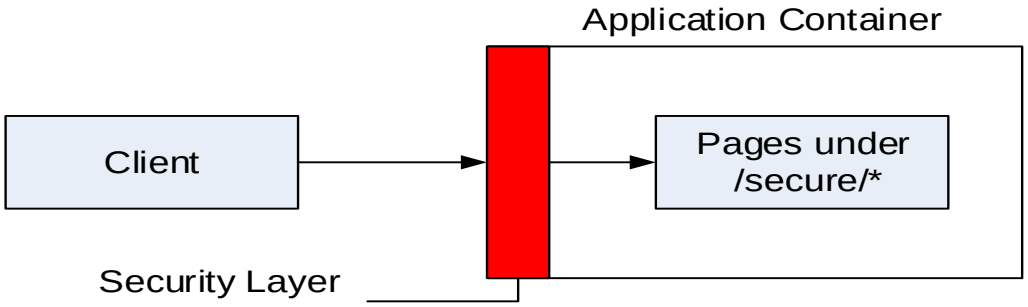
- Application Container is an enterprise service installed and run on a machine.
  - Tomcat is an example of a popular container for Java apps.
- Web services are deployed in Application Containers.
  - The resources that make up the web service is bundled into a single deployment unit i.e. .war files.
  - Access to individual resources contained in the application can be restricted based on the role assigned to the user making the request.

WAR File Deployment Descriptor

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="2.5">
  <security-role>
    <role-name>manager</role-name>
  </security-role>
  <security-constraint>
    <web-resource-collection>
       <web-resource-name>management pages</web-resource-name>
            <url-pattern>/secure/*</url-pattern>
            <url-pattern>/mixed/secure3.jsp</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <role-name>manager</role-name>
        </auth-constraint>
    </security-constraint>
</web-app>
```

Container-Based Authorization

- Application are deployed into containers with information that includes the roles that are allowed access specific services.
  - When the service is accessed, the container verifies that the client's authentication includes the roles required by the service configuration and denies access to the service if the user roles are not found.



- Container-based protection is provided by the container and requires no explicate code to enforce role-based security.

Application-Based Authorization

- While container-based authorization is simple to deploy and maintain, it lack fine-grain control over how clients are given access to services.
- The application architects may decide to incorporate security checks directly into their application.
  - If the container's security is not specific enough to implement the needed features.
  - If the application is not deployed in a container.
- For example, requirements may call for access to be allowed during specific times or restrictions on what can be requested of a service.

Implementing Authorization in the Application

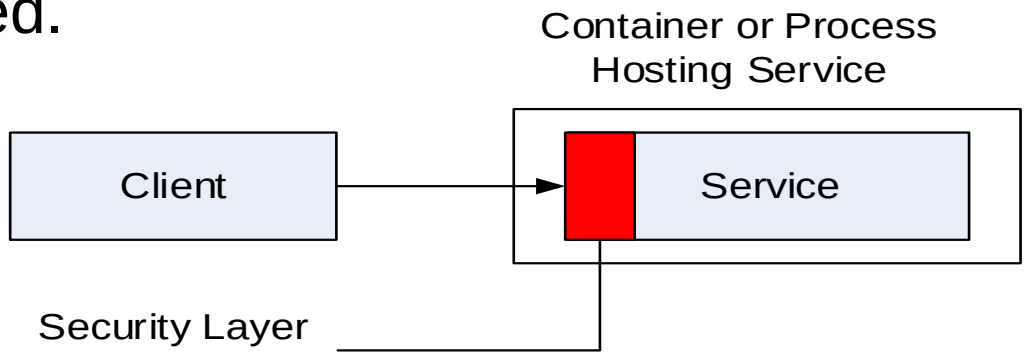
- Authorization checks are coded directly into the service implementation.
  - Role-based access checks are embedded directly into the application code…
  - and combined with other information (time of day) to determine whether to provide access.

- Developers use libraries that provide access to the clients authentication information including assigned roles.
  - This technique is far more complex to implement but provides increased flexibility enforcing access rules.

Application-Based Authorization

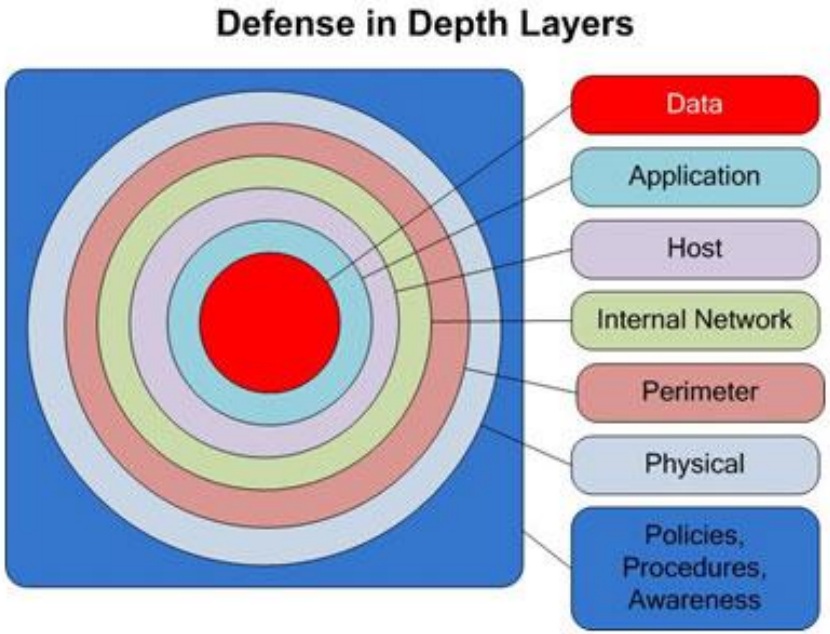
- Application-based security is implemented with libraries and services integrated into the application's design and code.
  - See the Java Apache Shiro project.

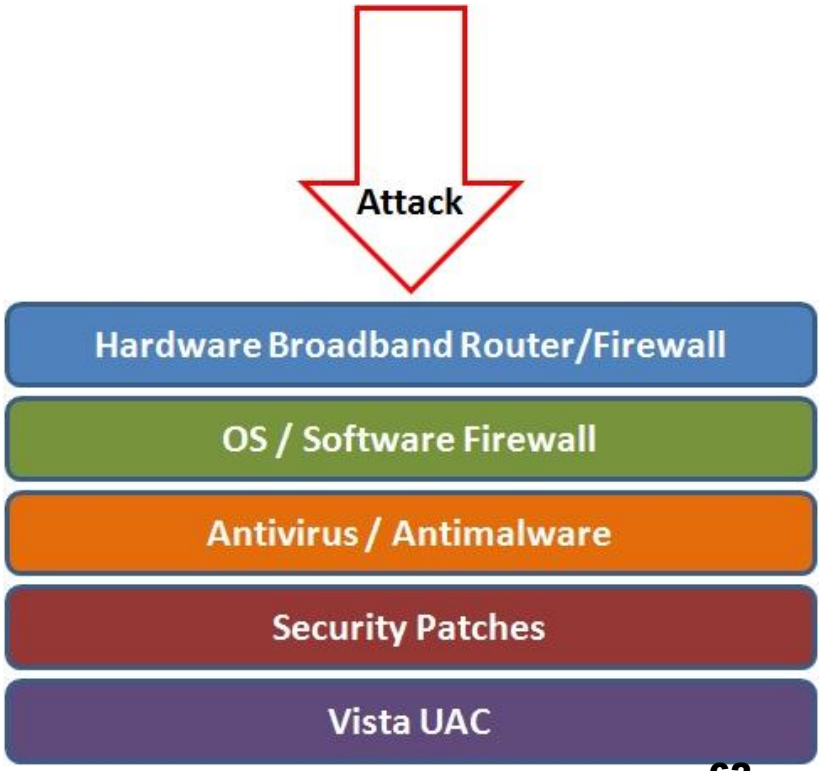
- Gives the architect full control over how services are accessed.



Security: Defense In Depth

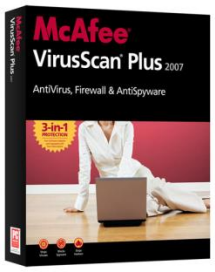
Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.

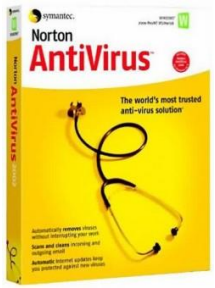




Anti-Virus & Anti-Spyware

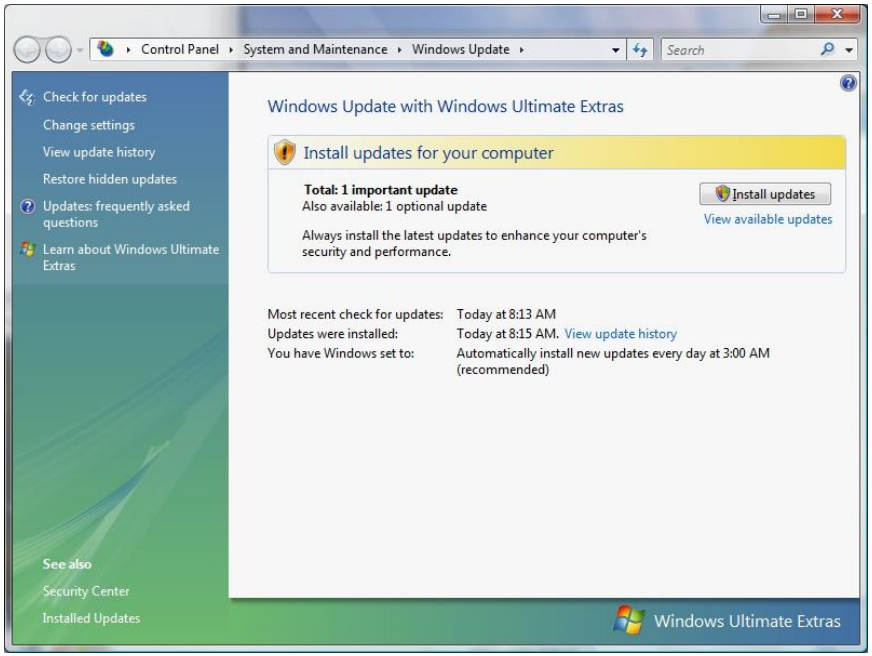
- Anti-virus software detects malware and can destroy it before any damage is done
- Install and maintain anti-virus and anti-spyware software
- Be sure to keep anti-virus software updated
- Many free and pay options exist

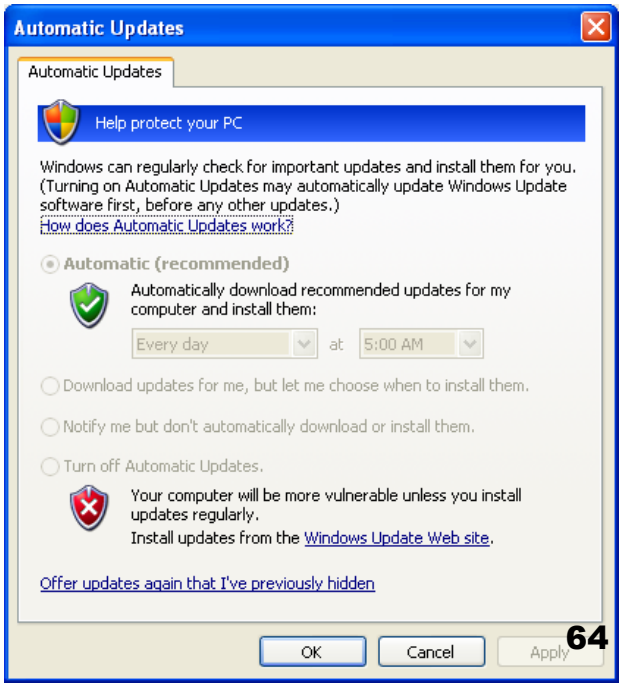




Protect Your Operating System

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator





Creating A Good Password

Combine 2 unrelated words	Mail + phone = m@!lf0n3
Abbreviate a phrase	My favorite color is blue= Mfciblue
Music lyric	Happy birthday to you, happy birthday to you, happy birthday dear John, happy birthday to you. hb2uhb2uhbdJhb2u

Password Recommendations

- Never use ‘admin’ or ‘root’ or ‘administrator’ as a login for the admin

- A good password is:
  - **private**: it is used and known by one person only
  - **secret**: it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal
  - **easily remembered**: so there is no need to write it down
  - **at least 8 characters, complex**: a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation
  - **not guessable** by any program in a reasonable time, for instance less than one week.
  - **changed regularly**: a good change policy is every 3 months

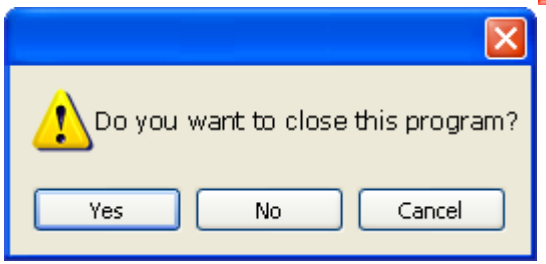
- Beware that someone may see you typing it. If you accidentally type your password instead of your login name, it may appear in system log files

Avoid Social Engineering & Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.

Other Hacker Tricks To Avoid

- Be sure to have a good firewall or pop-up blocker installed
- Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the ‘X’ in the upper corner.
- Never click “yes,” “accept” or even “cancel”



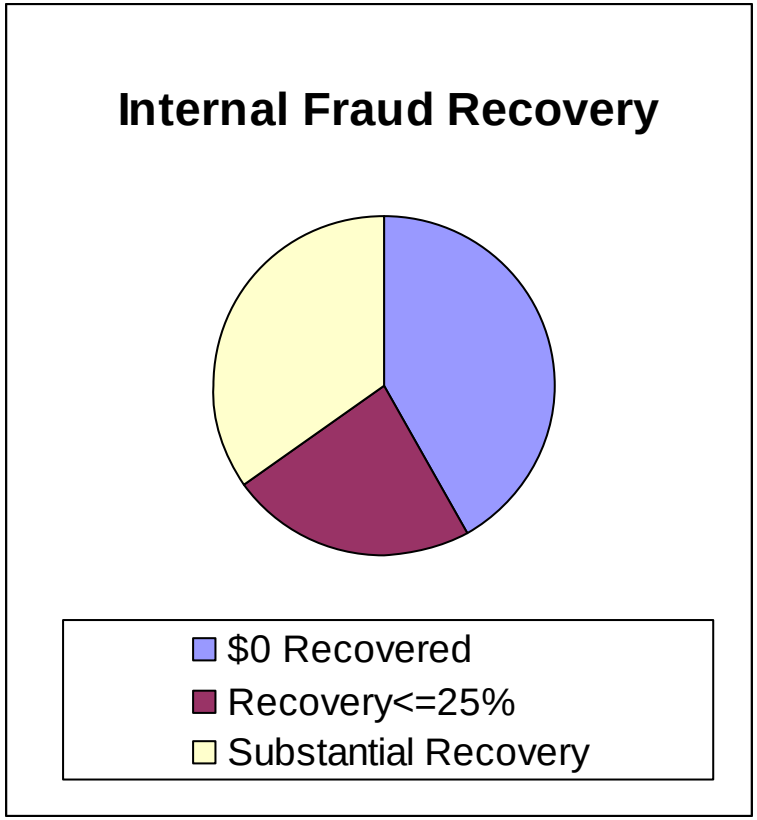
- Infected USB drives are often left unattended by hackers in public places.

Back-up Important Information

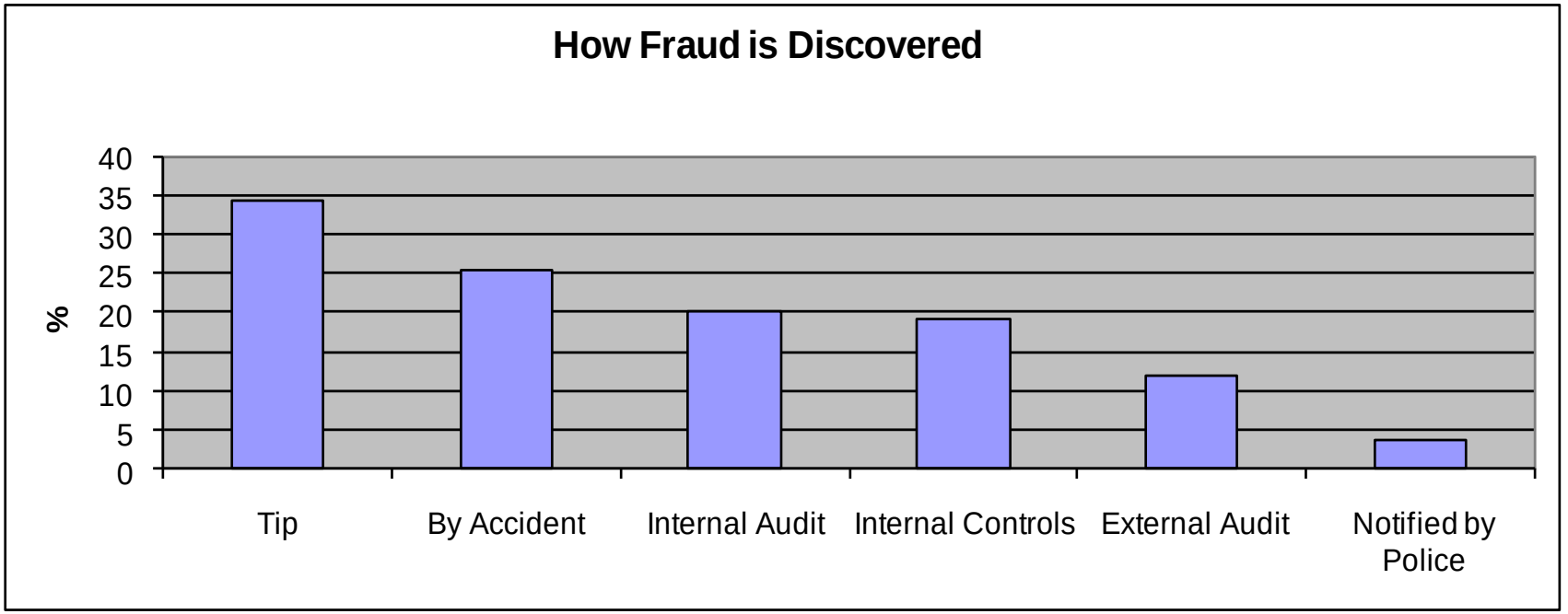
- No security measure is 100%
- What information is important to you?

The Fraud Problem

- Organizations lose 5-6% of revenue annually due to internal fraud = $652 Billion in U.S. (2006)
- Average scheme lasts 18 months, costs $159,000
- 25% costs exceed $1M
- Smaller companies suffer greater average $ losses than large companies



How Is Fraud Discovered?



Tips are most common way fraud is discovered.

Tips come from:

- Employee/Coworkers 64%,
- Anonymous 18%,
- Customer 11%,
- Vendor 7%

Put these Practices to Work

- These are best practices involving Information Security.
  - Most of these practices are from the National Institute of Standards and Technology.
- Use these practices at home and at work to keep safe and secure.
- Employers have policies and procedures regarding secure practices. Be sure to understand them and adhere to them. It will protect you, your employer and your customers.

Software Security

Overview

- What is software security ?
  - Understanding the role that software plays
    - in providing security
    - as source of insecurity
- Principles, methods & technologies to make software more secure
  - Practical experience with some of these
- Typical threats & vulnerabilities in software, and how to avoid them

Overview

- Software plays a major role in providing security, and is a major source of security problems
- Software security does not get much attention
  - In programming courses
    - Many future programmers have little training on software security
  - In software company's goal

Overview

- We focus on software security, but don't forget that security is about many things:
  - people
    - human computer interaction, HCI
    - Attackers, users, employees, sys-admins, programmers
  - access control, passwords, biometrics
  - cryptology, protocols
  - Monitoring, auditing, risk management
  - Policy, legislation
  - public relations, public perception
  - ….

- Security Concepts and Goals

Software and Security

- Security is about *regulating access to assets*
  - E.g., information or functionality
- Software provides *functionality*
  - E.g., on-line exam results
- This functionality comes with certain *risks*
  - E.g., what are risks of on-line exam results?
    - Privacy (score leakage); Modification
- Software security is about *managing these risks*

Software and Security

- Security is always a secondary concern
  - Primary goal of software is to provide functionalities or services
  - Managing associated risks is a derived/secondary concern
- There is often a trade-off/conflict between
  - security
  - functionality & convenience
- Security achievement is hard to evaluate when nothing bad happens

Starting Point for Ensuring Security

- Any discussion of security should start with an inventory of
  - the stakeholders (owners, companies…)
  - their assets (data, service, customer info…)
  - the threats to these assets (erase, steal…)
  - Attackers
    - employees, clients, script kiddies, criminals
- Any discussion of security without understanding these issues is meaningless

Security Concepts

- Security is about imposing countermeasures to reduce risks to assets to acceptable levels
  - “Perfect security” is not necessary and costly
- A security policy is a specification of what security requirements/goals the countermeasures are intended to achieve
  - secure against what and from whom ?
- Security mechanisms to enforce the policy
  - What actions we should take under an attack?

Security Objectives: CIA

- Confidentiality (or secrecy)
  - unauthorized users cannot read information
- Integrity
  - unauthorized users cannot alter information
- Availability
  - authorized users can always access information

Security Goals

- The well-known trio
  - confidentiality, integrity, avaliability (CIA)
- There are more “concrete” goals
  - traceability and auditing (forensics)
  - monitoring (real-time auditing)
  - multi-level security
  - privacy & anonymity
  - ...

How to Realize Security Objectives? AAAA

- Authentication
  - who are you?
- Access control/Authorization
  - control who is allowed to do what
  - this requires a specification of who is allowed to do what
- Auditing
  - check if anything went wrong
- Action
  - if so, take action

How to Realize Security Objectives?

- Other names for the last three A's
  - Prevention
    - measures to stop breaches of security goals
  - Detection
    - measures to detect breaches of security goals
  - Reaction
    - measures to recover assets, repair damage, and persecute (and deter) offenders

Threats vs Security Requirements

- information disclosure
  - confidentiality
- tampering with information
  - integrity
- denial-of-service (DoS)
  - availability
- spoofing
  - authentication
- unauthorized access
  - access control

Countermeasures

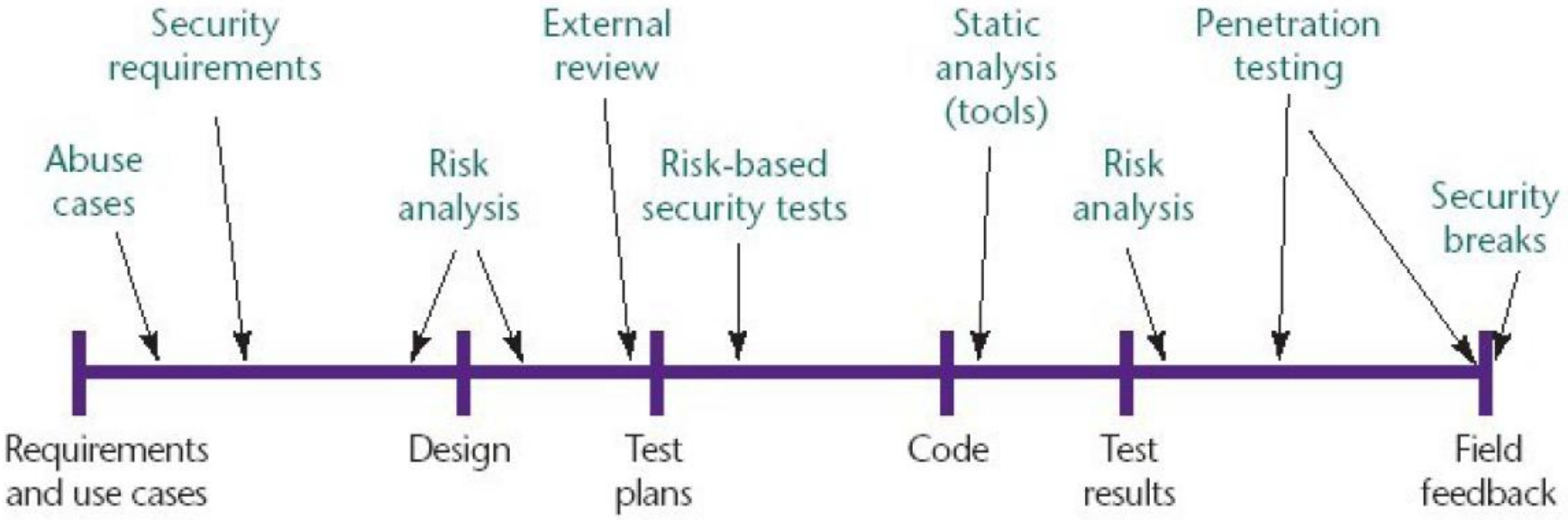
- Countermeasures can be non-IT related
  - physical security of building
  - screening of personnel
  - legal framework to deter criminals
  - training employee

Software Security

Two Sides to Software Security

- What are the methods and technologies, available to us if we want to provide security?
  - security in the software development lifecycle
  - engineering & design principles
  - security technologies
- What are the methods and technologies available to the enemy who wants to break security ?
  - What are the threats and vulnerabilities we're up against?
  - What are the resources and tools available to attackers?

Security in Software Development Life Cycle



- Source: Gary McGraw, Software security, Security & Privacy Magazine, IEEE, Vol 2, No. 2, pp. 80-83, 2004.

Example Security Technologies

- Cryptography
  - for threats related to insecure communication and storage
- Access control
  - for threats related to misbehaving users
  - E.g., role-based access control
- Language-based security
  - for threats related to misbehaving programs
    - typing, memory-safety
    - sandboxing
  - E.g., Java, .NET/C#

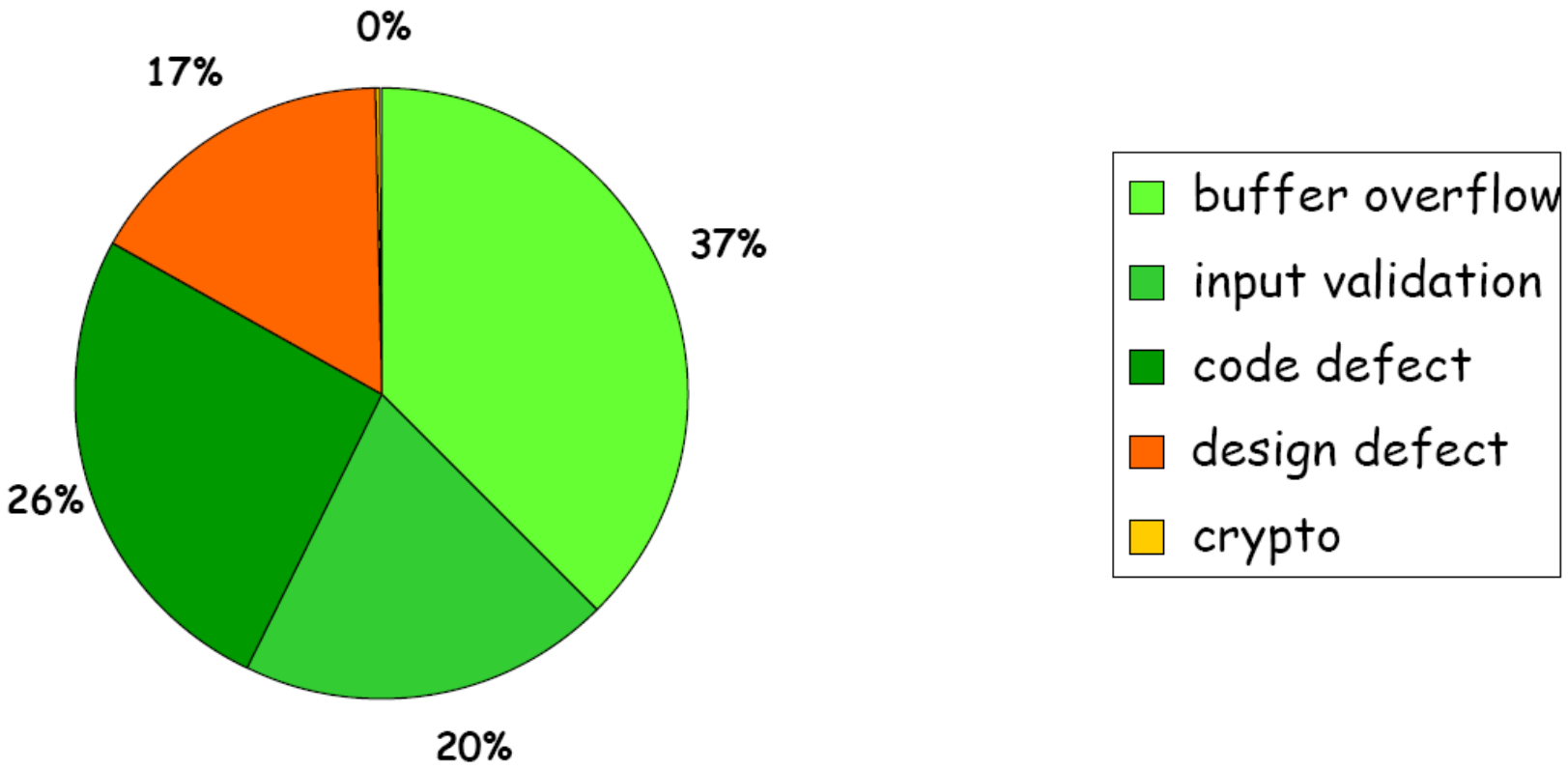
Example Security Technologies

- These technologies may be provided by the infrastructure/platform an application builds on,
  - networking infrastructure
    - which may e.g. use SSL
  - operating system or database system
    - providing e.g. access control
  - programming platform
    - for instance Java or .NET sandboxing
- Of course, software in such infrastructures implementing security has to be secure

Software Infrastructure

- Applications are built on top of "infrastructure" consisting of
  - operating system
  - programming language/platform/middleware
    - programming language itself
      - interface to CPU & RAM
    - libraries and APIs
      - interface to peripherals (socket, interrupt…)
      - provider of building blocks
  - other applications & utilities
    - E.g., database
- This infrastructure provides security mechanisms, but is also a source of insecurity

Typical Software Security Vulnerabilities



Security bugs found in Microsoft bug fix month (2002)

Functionality vs Security

Lost battles?

- operating systems
- programming languages
- Web browsers
- email clients

Functionality vs Security

Lost battles?

- operating systems
  - huge OS, with huge attack surface (API),
- programming languages
  - buffer overflows, format strings, ... in C
  - public fields in Java
  - lots of things in PHP
- Web browsers
  - plug-ins for various formats, javascript, VBscript, ...
- email clients

Threat Modeling

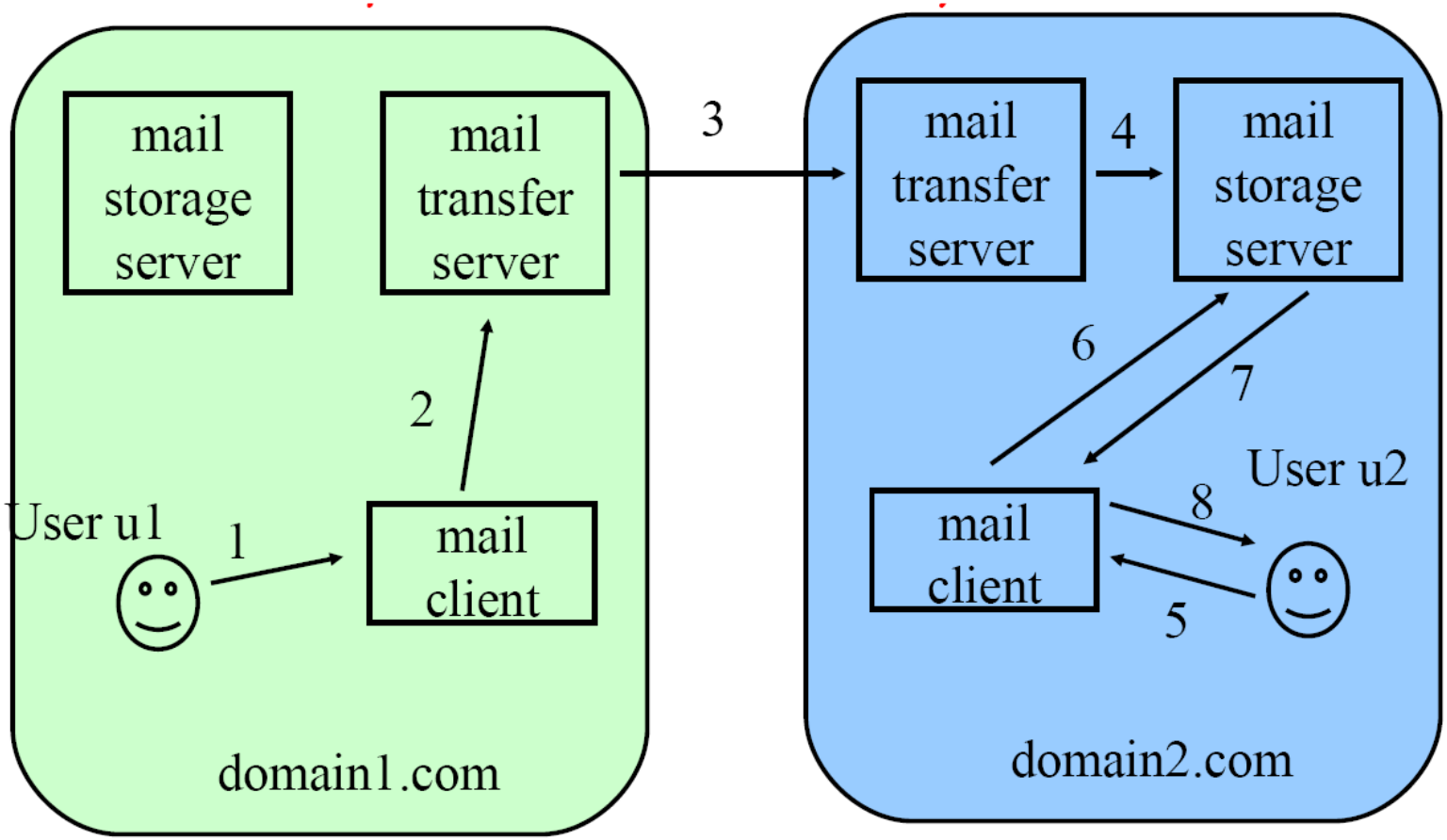
Threat Modeling

- Aka security/risk/requirements analysis
- A first step, not just for software
  - Identify assets & stakeholders
  - Consider architecture of application & its environment
  - Brainstorm about known threats
  - Define security assumptions
  - Rank threats by risk
    - ≈ impact x likelihood
  - Decide which threats to respond to
  - Decide how to mitigate these threats
    - which techniques & technologies

Example Techniques to Mitigate Threats

- Spoofing Identity
  - authentication, protect keys & passwords, ...
- Tampering with Data
  - access control, hashes, digital signatures, MACs (message authentication codes), write-once storage...
- Repudiation
  - logging, audit trails, digital signatures, ...
- Information Disclosure
  - access control, encryption, not storing secrets, ...
- Denial of Service
  - graceful degradation, filtering, increase server resources
- Elevation of Privilege
  - access control, sandboxing, ...

Example: Email System



Potential threats to the e-mail system

- Eavesdropping on e-mail
  - Communication over the Internet is relatively easy to eavesdrop
  - Hence, content of e-mail is by no means confidential
  - Critical information can be encrypted in email attachment
- Modifying e-mail
  - Interception of the communication (e.g. between the two MTS's) allows an attacker to modify the e-mail
  - Hence, integrity of the e-mail is not guaranteed
- Spoofing e-mail
  - MTS blindly believes other MTS about who the sender of the e-mail is
  - Hence, no guarantee about the identity of the sender
- Attacks against the mail servers
  - Server is a "trusted software layer", making a limited functionality (sending/receiving mail) available to all clients
- Email as an attack dispersion channel

Possible Defenses

- Eavesdropping and modification
  - Can be countered by cryptographic techniques
- Spoofing
  - Can be countered by strong authentication protocols
- Attacks against servers
  - Can be countered by
    - Careful software coding
    - Clear access control model
    - Strong authentication
- Many other threats
  - Privacy threat: detecting when an e-mail is read
  - Repudiation of sending: sender can deny having sent a message
  - Repudiation of receiving: receiver can deny having ever received a particular message

Group Exercise

- For the below scenarios:

  i) As head of the TSA, you set the rules for screening passengers at airport checkpoints.

  ii) You own a local Panera restaurant franchise.

  - What assets do you need to protect?
  - What threats will you defend against?
  - What countermeasures can you justify, in terms of costs and benefits?