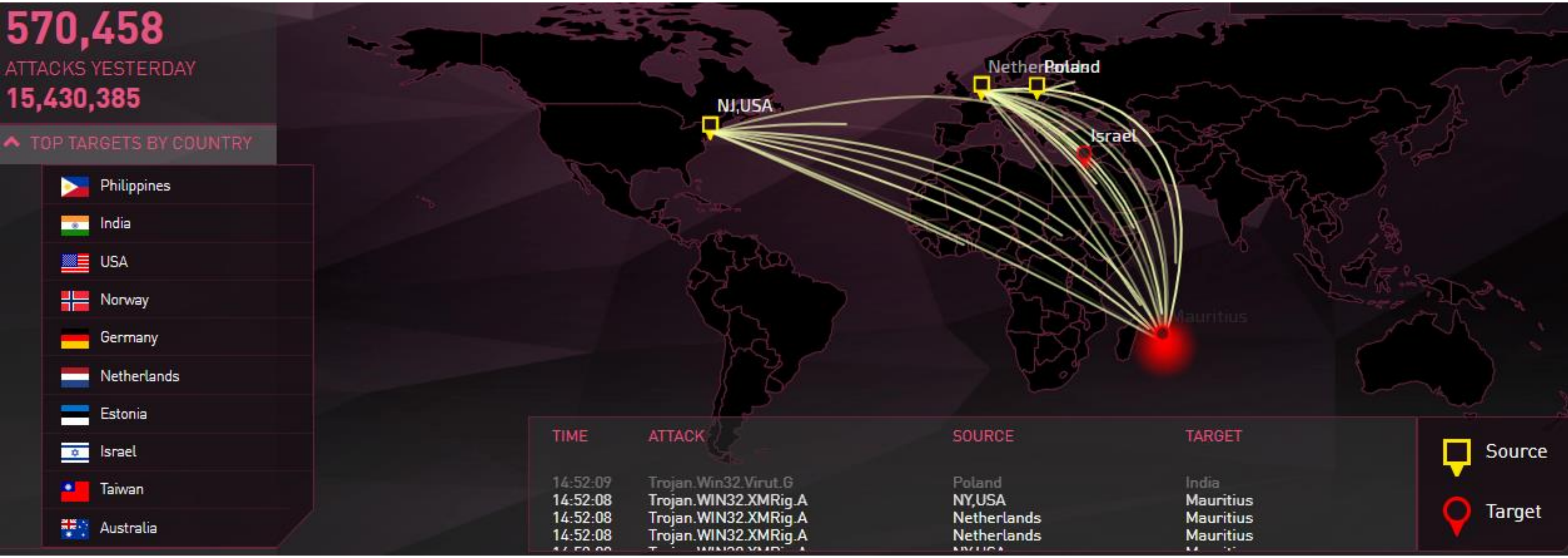
Examining Network Security Fundamentals

Networks Are Targets



570,458

ATTACKS YESTERDAY

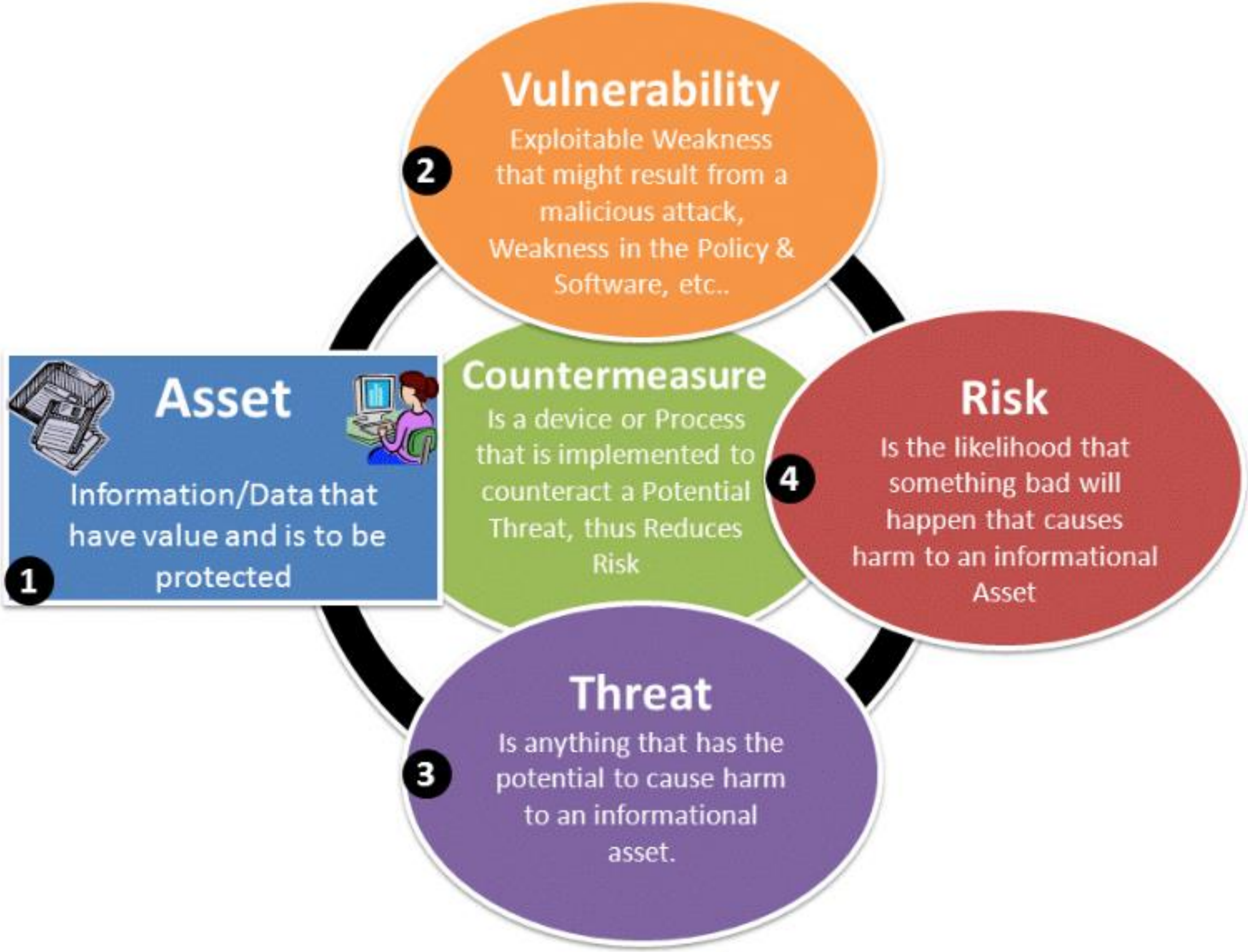
15,430,385

TOP TARGETS BY COUNTRY

- Philippines
- India
- USA
- Norway
- Germany
- Netherlands
- Estonia
- Israel
- Taiwan
- Australia

TIME	ATTACK	SOURCE	TARGET
14:52:09	Trojan.Win32.Virut.G	Poland	India
14:52:08	Trojan.WIN32.XMRig.A	NY,USA	Mauritius
14:52:08	Trojan.WIN32.XMRig.A	Netherlands	Mauritius
14:52:08	Trojan.WIN32.XMRig.A	Netherlands	Mauritius

Security Terms



1 **Asset**

Information/Data that have value and is to be protected

2 **Vulnerability**

Exploitable Weakness that might result from a malicious attack, Weakness in the Policy & Software, etc..

3 **Threat**

Is anything that has the potential to cause harm to an informational asset.

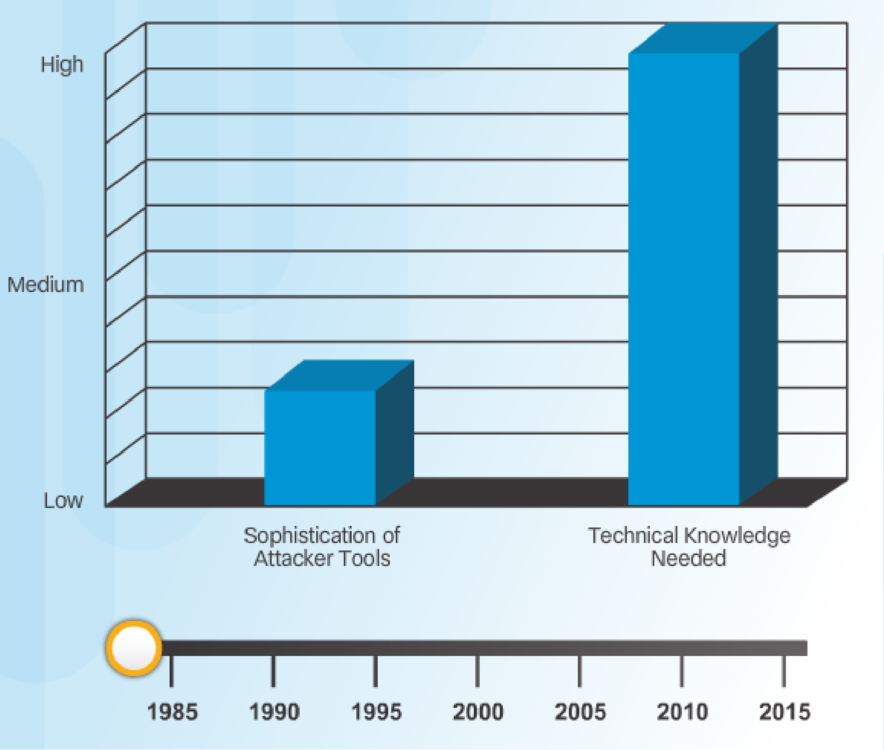
4 **Risk**

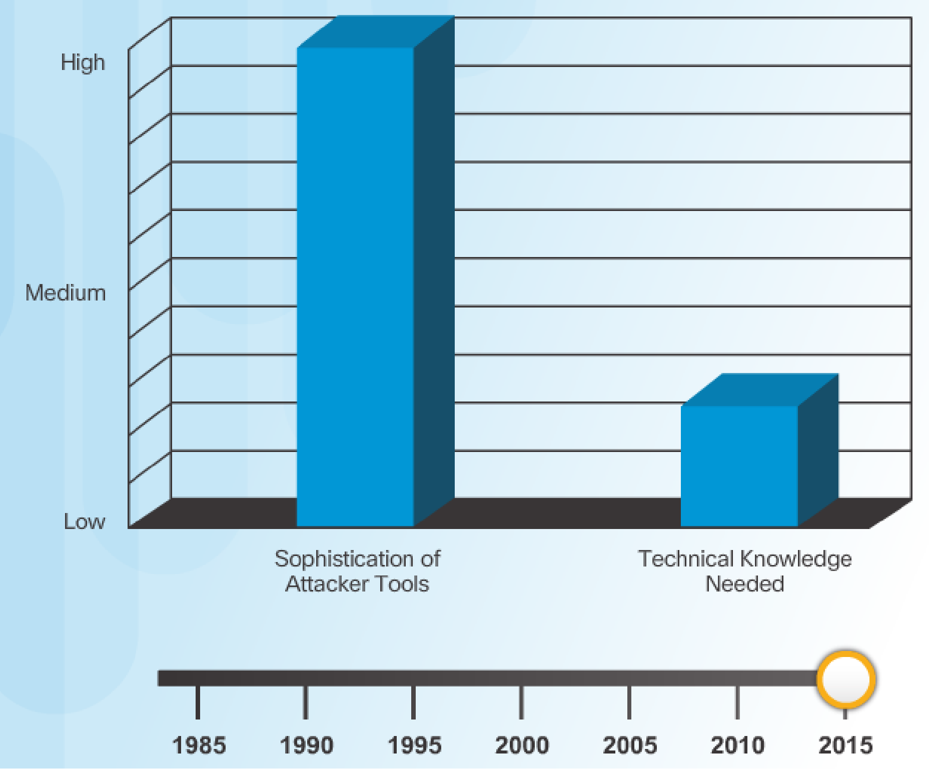
Is the likelihood that something bad will happen that causes harm to an informational Asset

Countermeasure

Is a device or Process that is implemented to counteract a Potential Threat, thus Reduces Risk

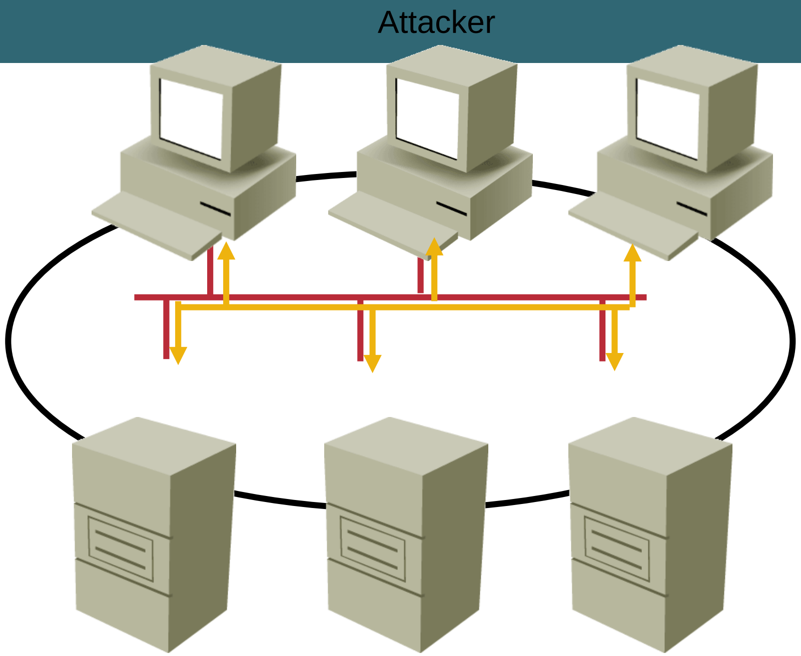
Introduction of Attack Tools



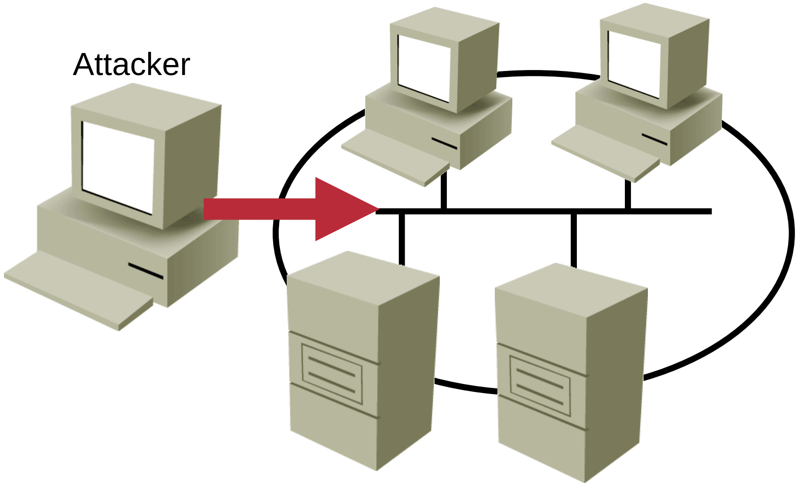


Threats to Security

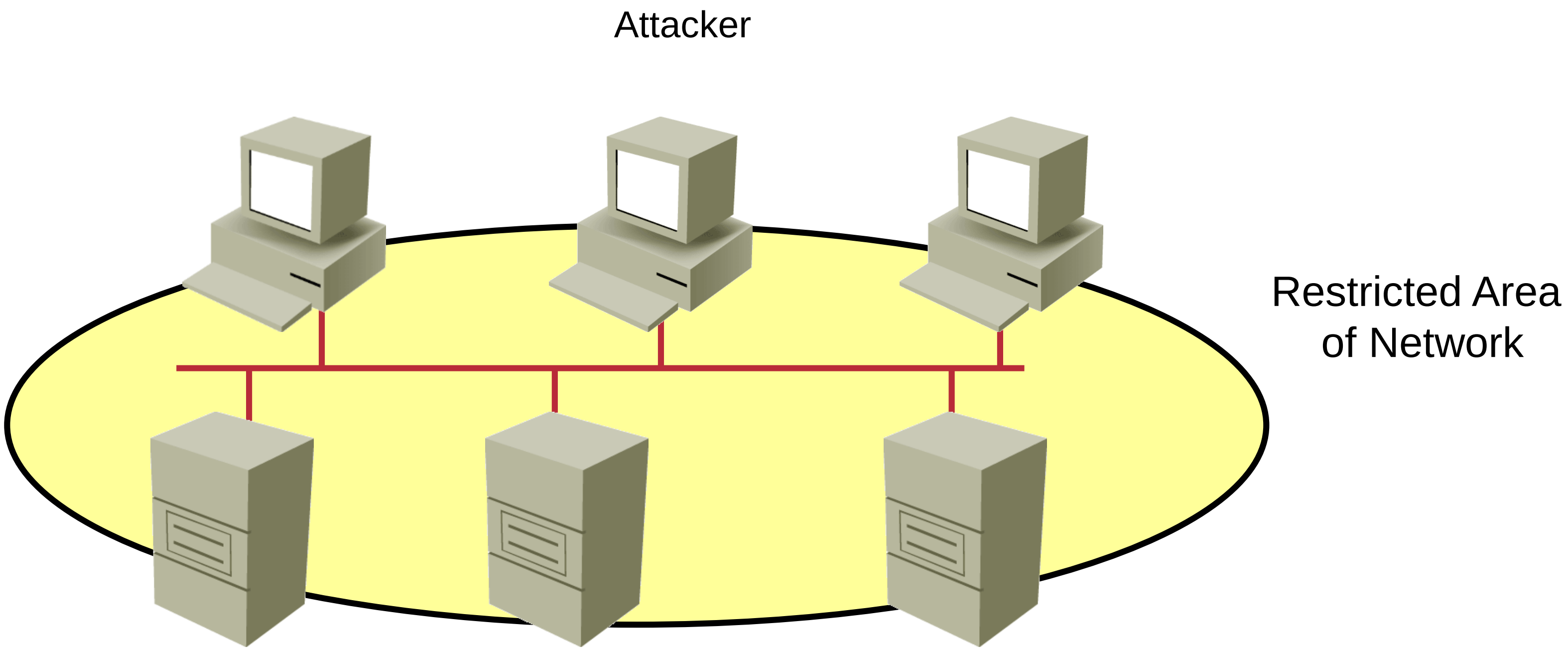
Internal threats, such as unauthorized access or network misuse



External threats, such as social engineering or viruses



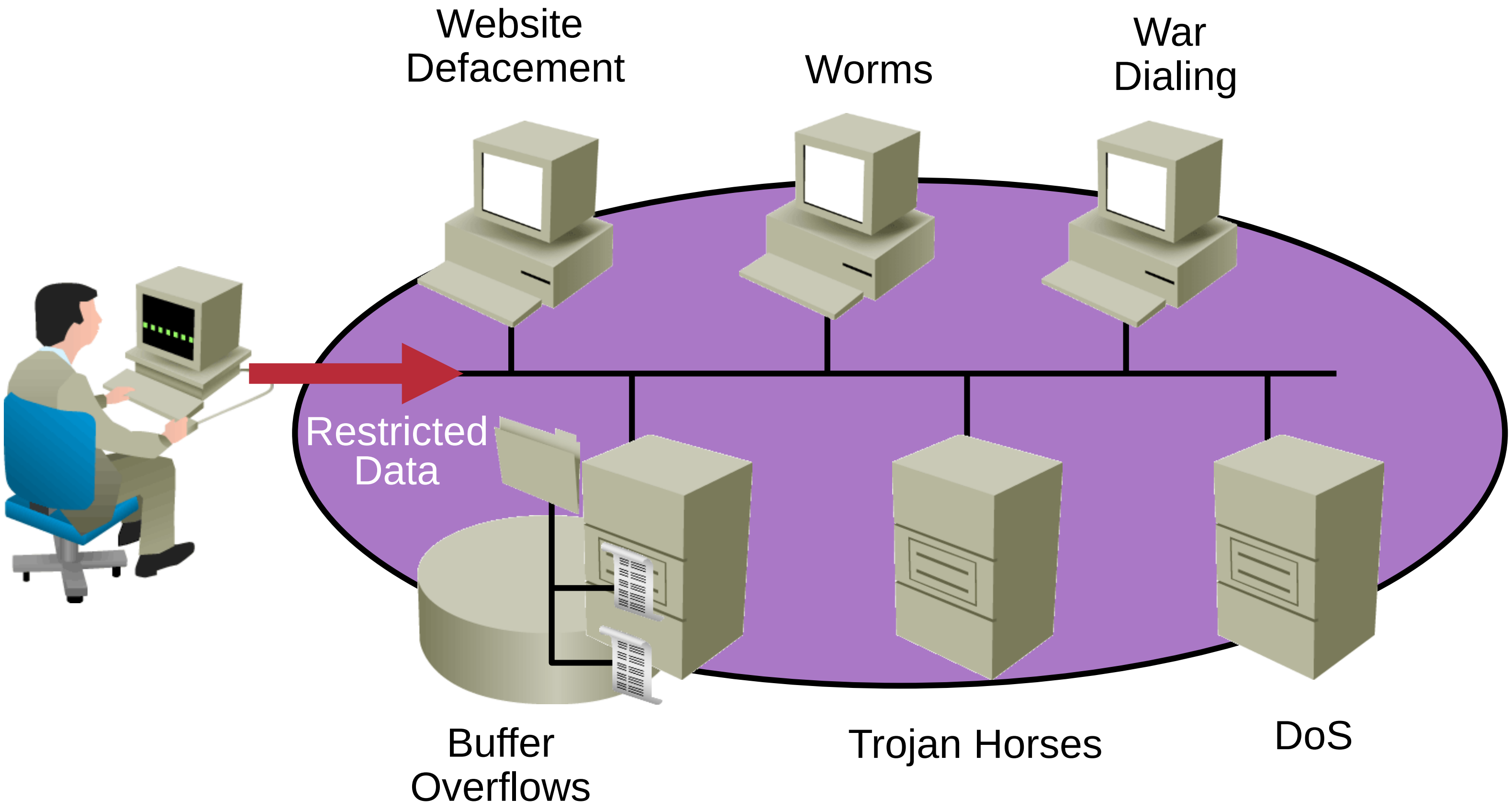
Addressing Internal Threats



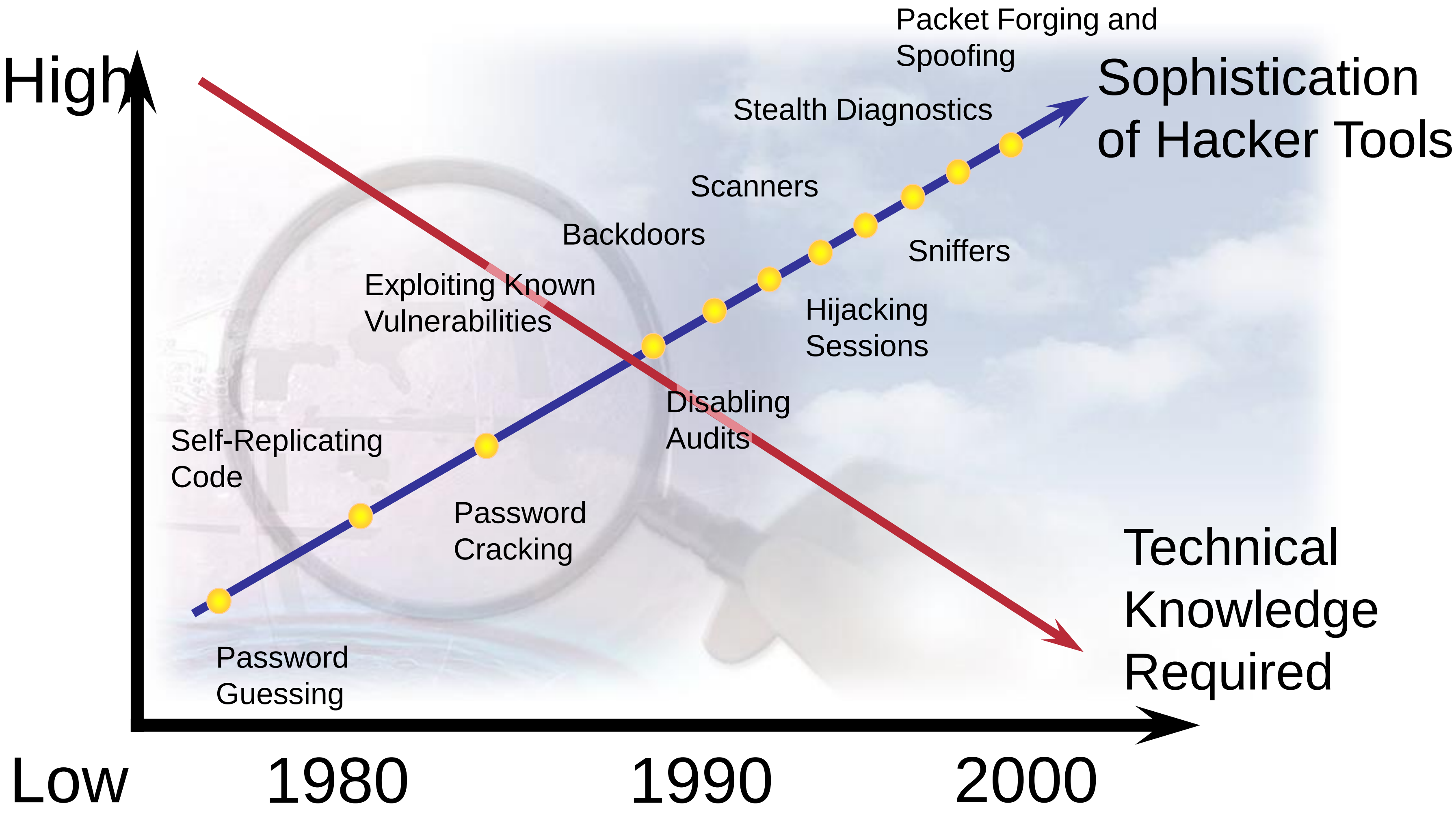
Internal threats occur because

- The recommended best practices of a vendor are not followed
- Blank or default passwords are used
- In-house developers use insecure programming practices

External Threats

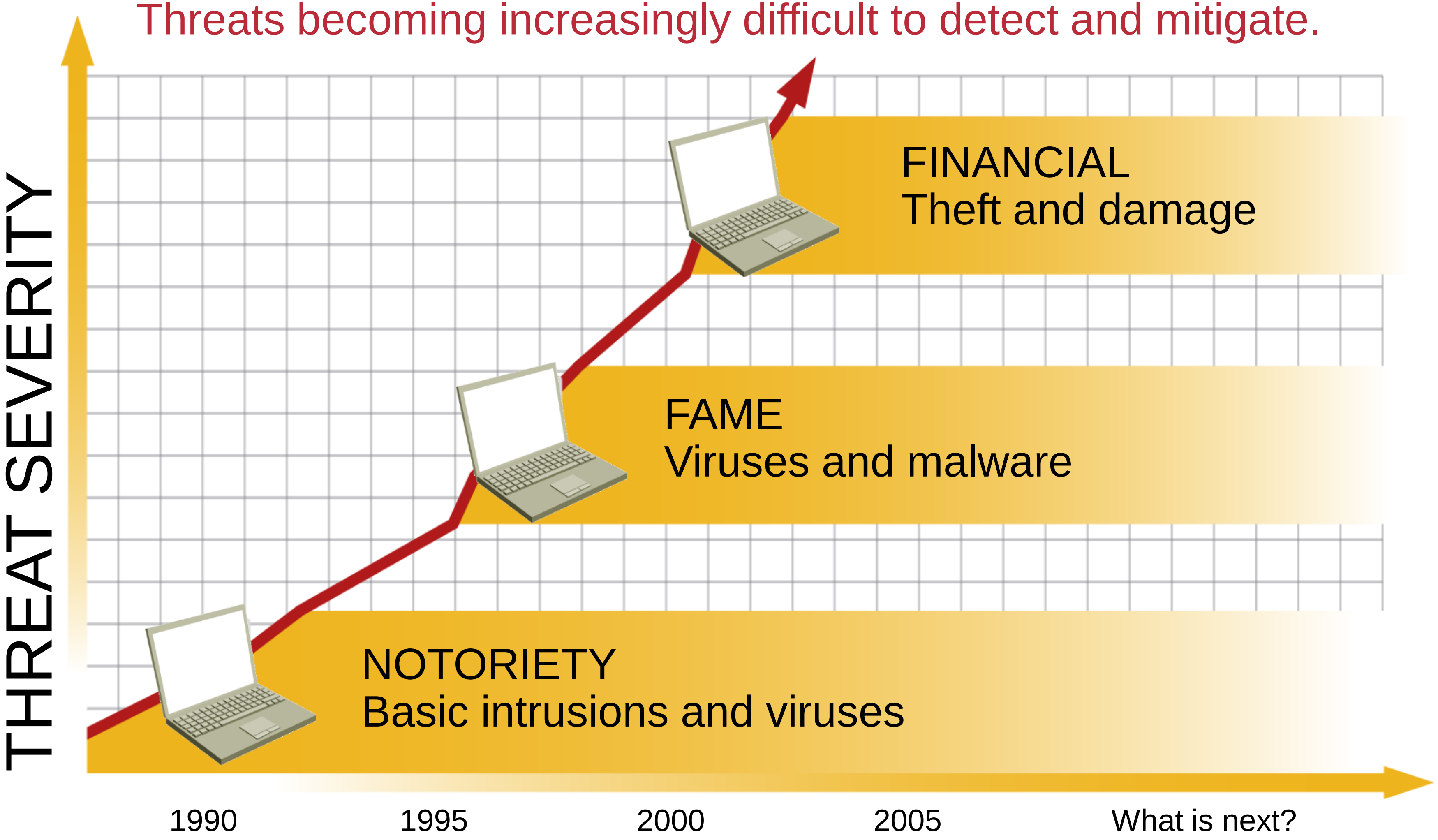


Threat Capabilities—More Dangerous and Easier to Use



The Evolution of Intent

Threats becoming increasingly difficult to detect and mitigate.



Vulnerable Custom Applications

Focus of attacks moves to the application layer

75% of Attacks Focused Here

No Signatures or Patches

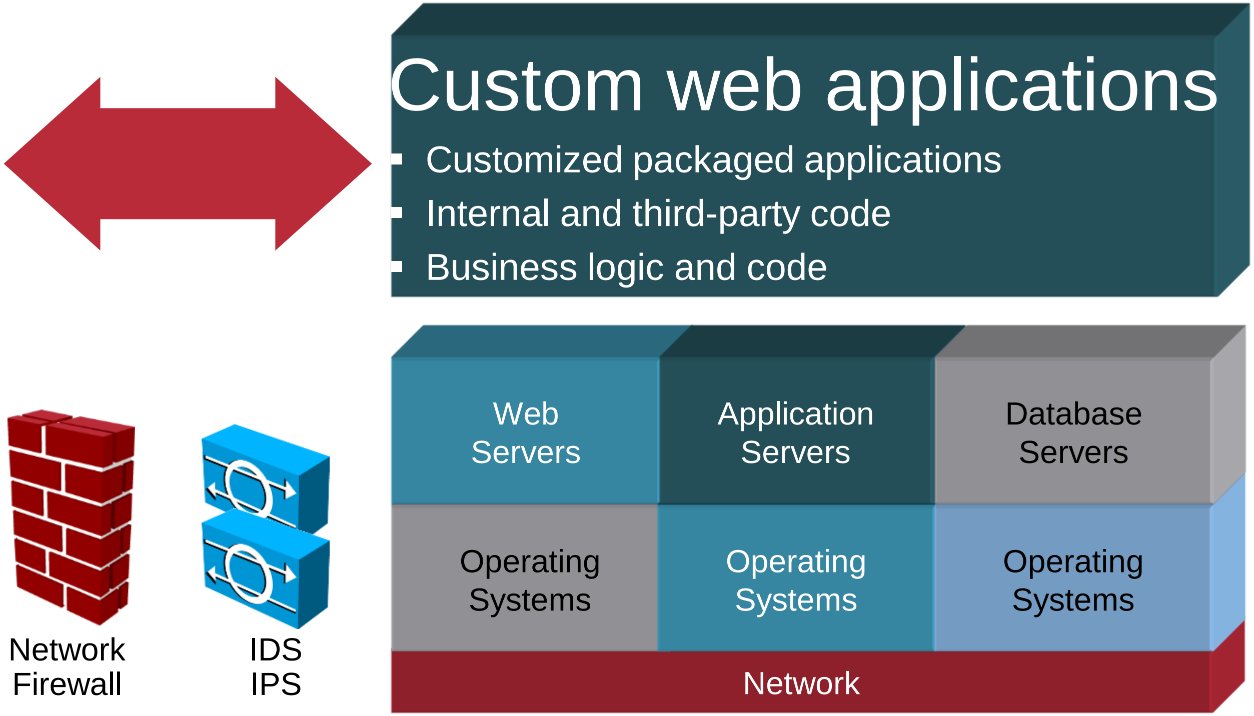
Oracle Applications Login - Microsoft Internet Explorer provided by Cisco Systems, Inc

Welcome to Oracle 11i

You must have an Oracle account to access this application.
Internal employees: Use your CEC username & password to login.
External users: Use your EMCO username & password to login.
Note: As of 12:30am PT 9/5/2005 your 11i password is now kept in sync with your CEC or EMCO password at all times. Please use your current CEC or EMCO password as appropriate to login.

Username
Password
Connect
Change Password | Synchronize Password

Login Problems:
If you know your CEC or EMCO password and your Oracle 11i password is not working, select Synchronize Password. This resets your Oracle 11i password to match your current CEC or EMCO password.

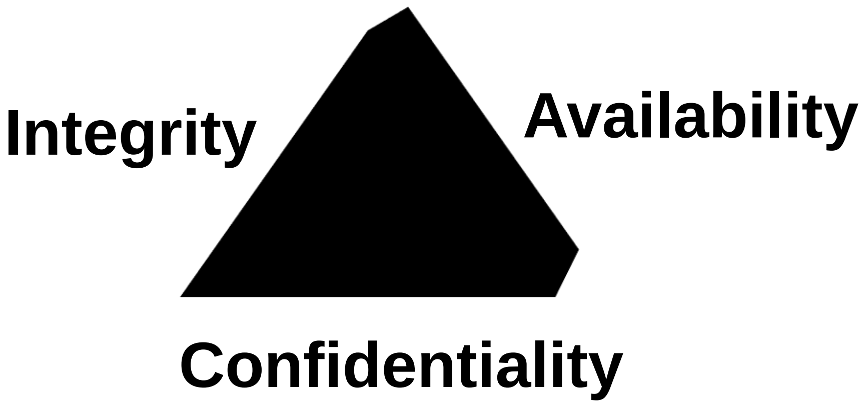


Custom web applications

- Customized packaged applications
- Internal and third-party code
- Business logic and code

Network Security Objectives

- Networking exposes computing resources to a vast audience of users and potential attackers.
- Computer systems are complex and therefore vulnerable.
- Network security aims to provide three key services to manage risk:
  - Data confidentiality
  - Data integrity
  - Data and system availability



Confidentiality

- Data confidentiality allows only authorized users to read sensitive data.
- Confidentiality mechanisms provide separation of data from users.
  - Physical separation
  - Logical separation, such as access controls and encryption

Integrity

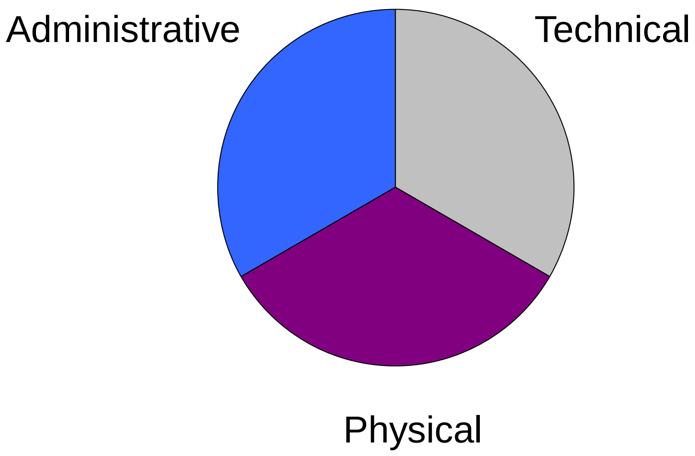
- Data integrity ensures that only authorized subjects can change sensitive data.
  - This can also be referred to as data authenticity (freshness, authentic source, or both, plus integrity)
- Integrity technologies provide some level of assurance that
  - Data does not change without authorization
  - Unauthorized changes can be detected

Availability

- Availability refers to providing uninterrupted access to computing resources.
  - Prevents accidental disruptions
  - Prevents deliberate disruptions such as DoS attacks
- This is quickly becoming one of the most important security services.
- Availability is possibly the most difficult service to provide considering modern threats and system complexity.
- DoS attacks are usually a consequence of two things:
  - A host or application fails to handle an unexpected condition
  - A network, host, or application is unable to handle an enormous quantity of data

Security Controls

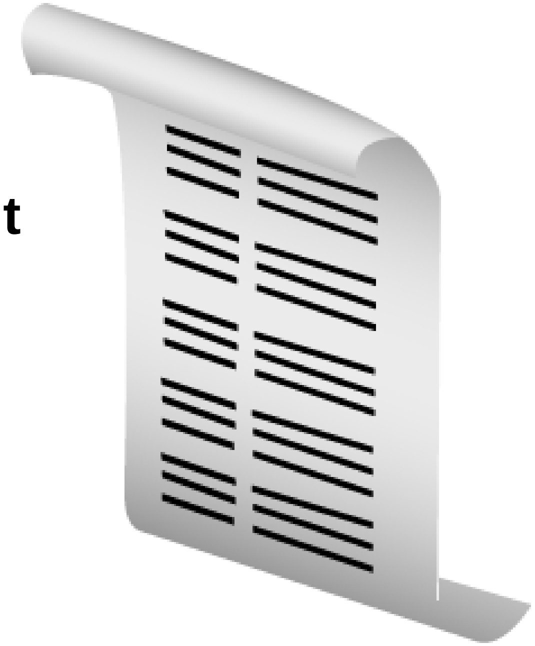
- **Security controls minimize the effects of security threats on an organization to a level that is tolerable.**
- **There are three categories of controls:**
  - **Administrative**
  - **Technical**
  - **Physical**



Administrative Controls

Administrative controls include

- **Security awareness training**
- **Policies and standards**
- **Change and configuration management**
- **System activity audits**
- **Good hiring procedures**
- **Background checks**



Technical Controls

- Network devices
  - Firewall
  - IPS
  - VPN
- Methods to identify the users
  - TACACS+
  - RADIUS
  - OTP
- Security devices
  - Smart cards
  - Biometrics
  - NAC systems
- Logical access control mechanisms

Physical Controls

- Monitoring equipment
  - Intruder detection systems
- Physical security devices
  - Door locks
  - Safes
  - Racks
- Environmental controls
  - UPS
  - Fire suppression system
  - Air flow system
- Security guards

Examining Network Attack Methodologies

Data Loss

Vectors of data loss:

- Email/Webmail
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control

Main Vulnerability Categories

Today the main vulnerabilities of systems can usually be categorized as

- **Design errors**
- **Protocol weaknesses**
- **Software vulnerabilities**
- **Misconfiguration**
- **Hostile code**
- **Human factor**

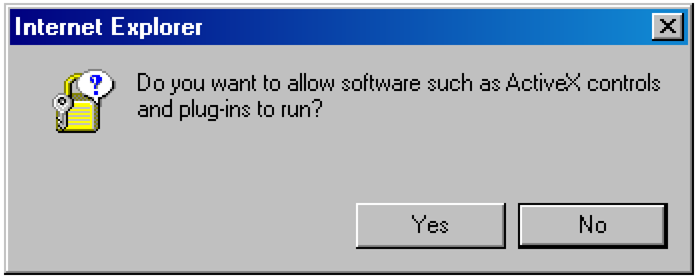
The Human Vulnerability Factor

- People are often too helpful, making social engineering one of the easiest methods to compromise computer systems.
  - It is necessary to train end users to promote security consciousness.
- Most security incidents are caused by insiders, so
  - Strong internal controls on security are required.
  - Special organization practices (operations security) are required.

The Human Vulnerability Factor (Cont.)

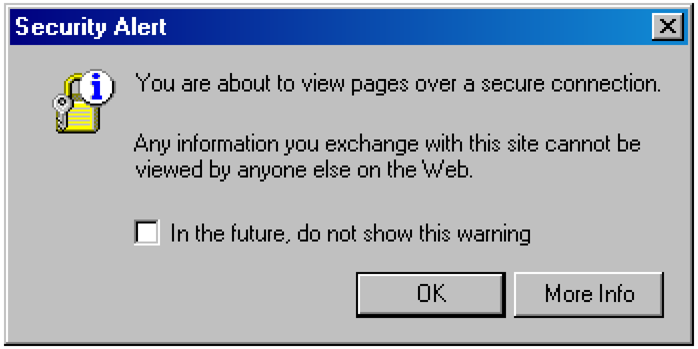
Security is often difficult to understand:

- Users prefer “whatever” functionality to no functionality.
- Software does not make decisions simple for end users.



Internet Explorer

Do you want to allow software such as ActiveX controls and plug-ins to run?

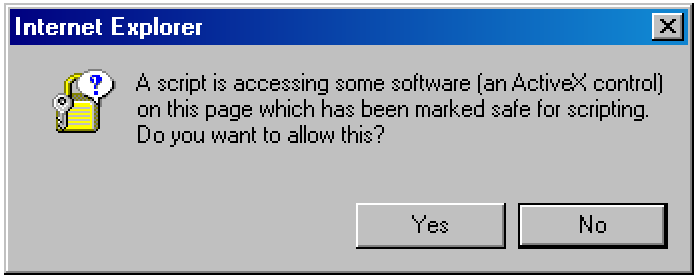


Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

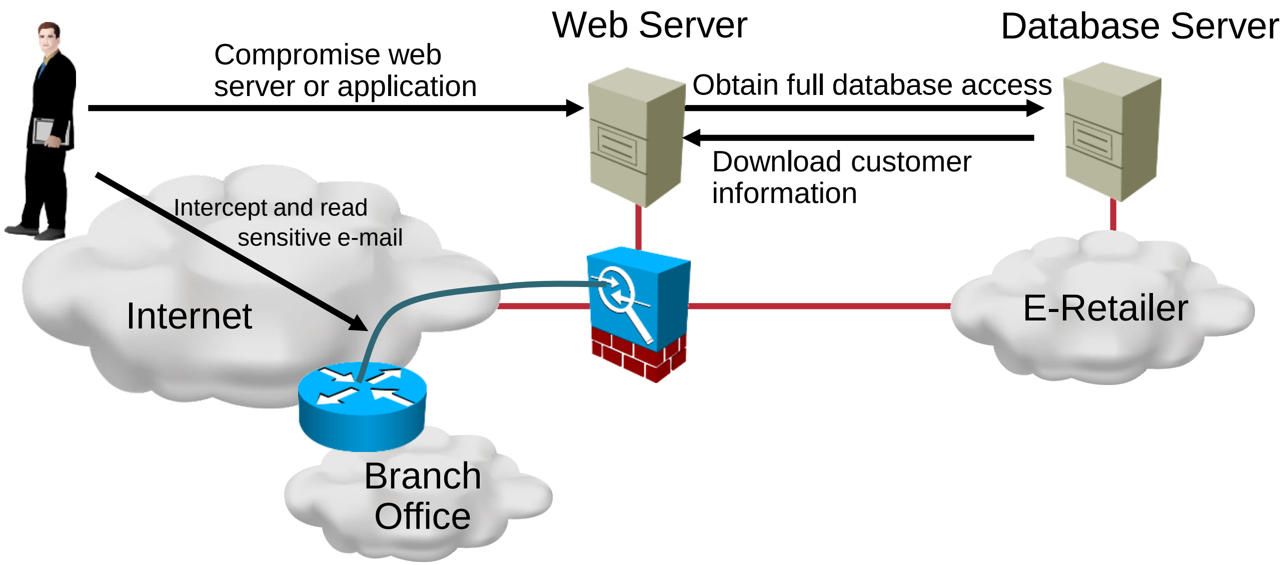
□ In the future, do not show this warning



Internet Explorer

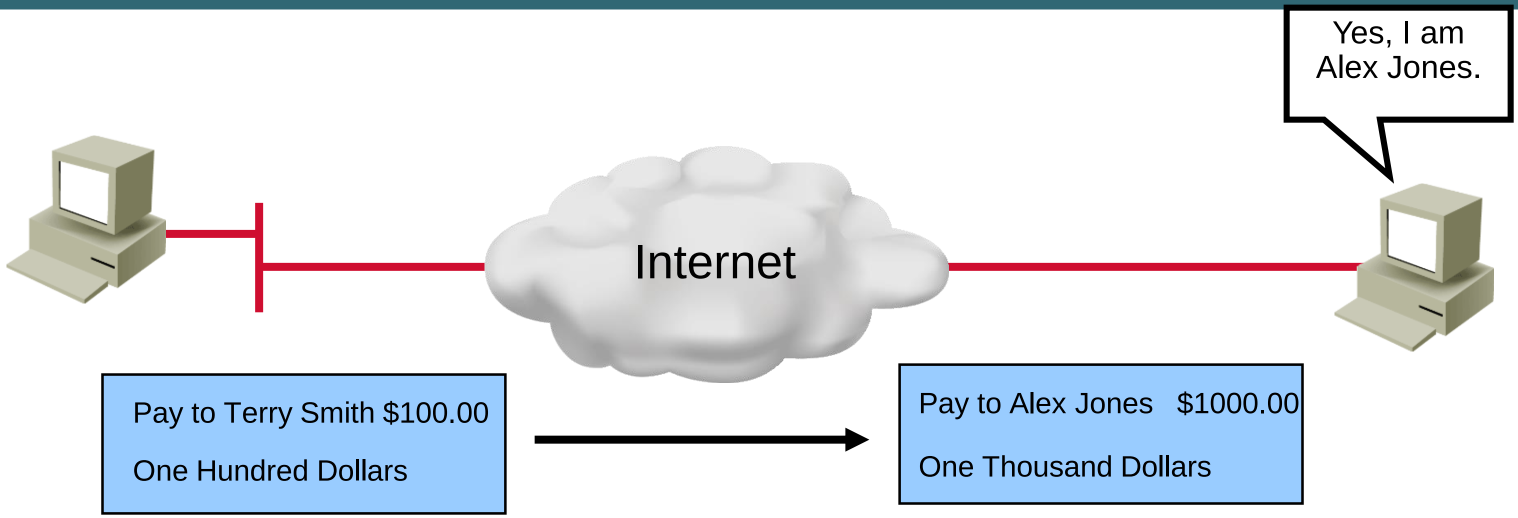
A script is accessing some software (an ActiveX control) on this page which has been marked safe for scripting. Do you want to allow this?

Confidentiality Violations


Web Server
Database Server
Compromise web server or application
Obtain full database access
Download customer information
Intercept and read sensitive e-mail
Internet
E-Retailer
Branch Office

- **Confidentiality violations occur when the attacker can read sensitive data.**
- **Confidentiality violations can be caused by**
  - **Failure of access control (network, operating system, application)**
  - **Failure to protect data in transit over an untrusted network**

Integrity Violations



Yes, I am Alex Jones.

Internet

Pay to Terry Smith $100.00

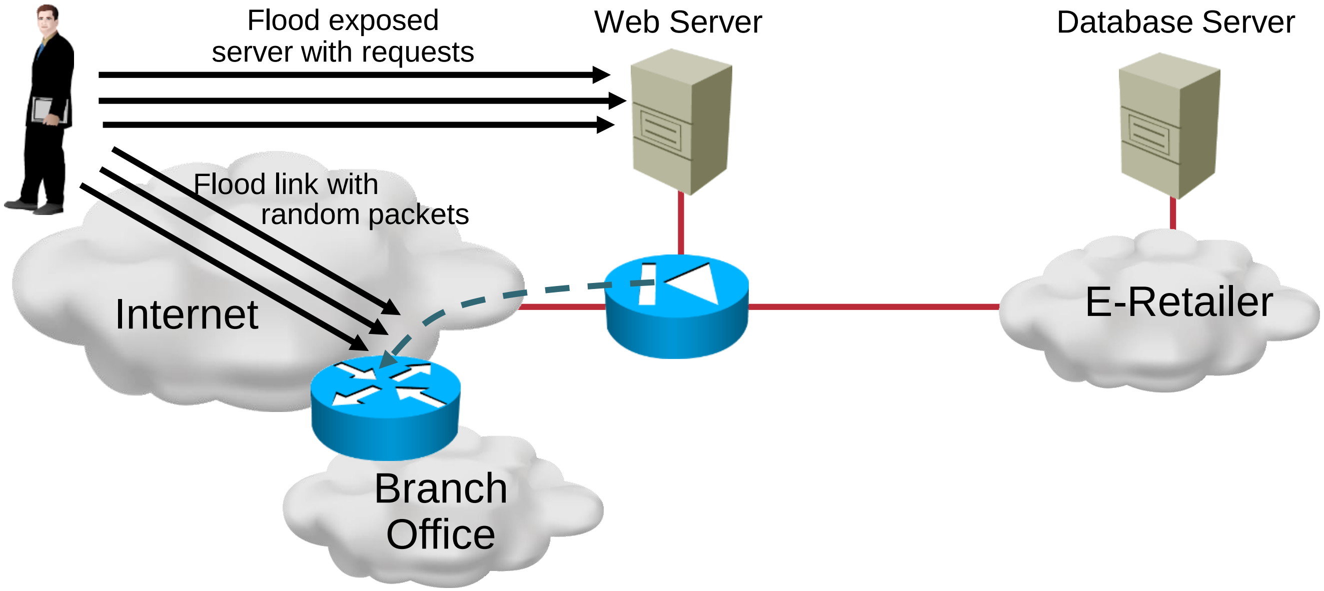
One Hundred Dollars

Pay to Alex Jones $1000.00

One Thousand Dollars

- **Integrity violations occur when the attacker can change sensitive data.**
- **This type of attack is caused by**
  - **Failure of access control (network, operating system, application)**
  - **Failure to protect data in transit over an untrusted network**

Availability Violations

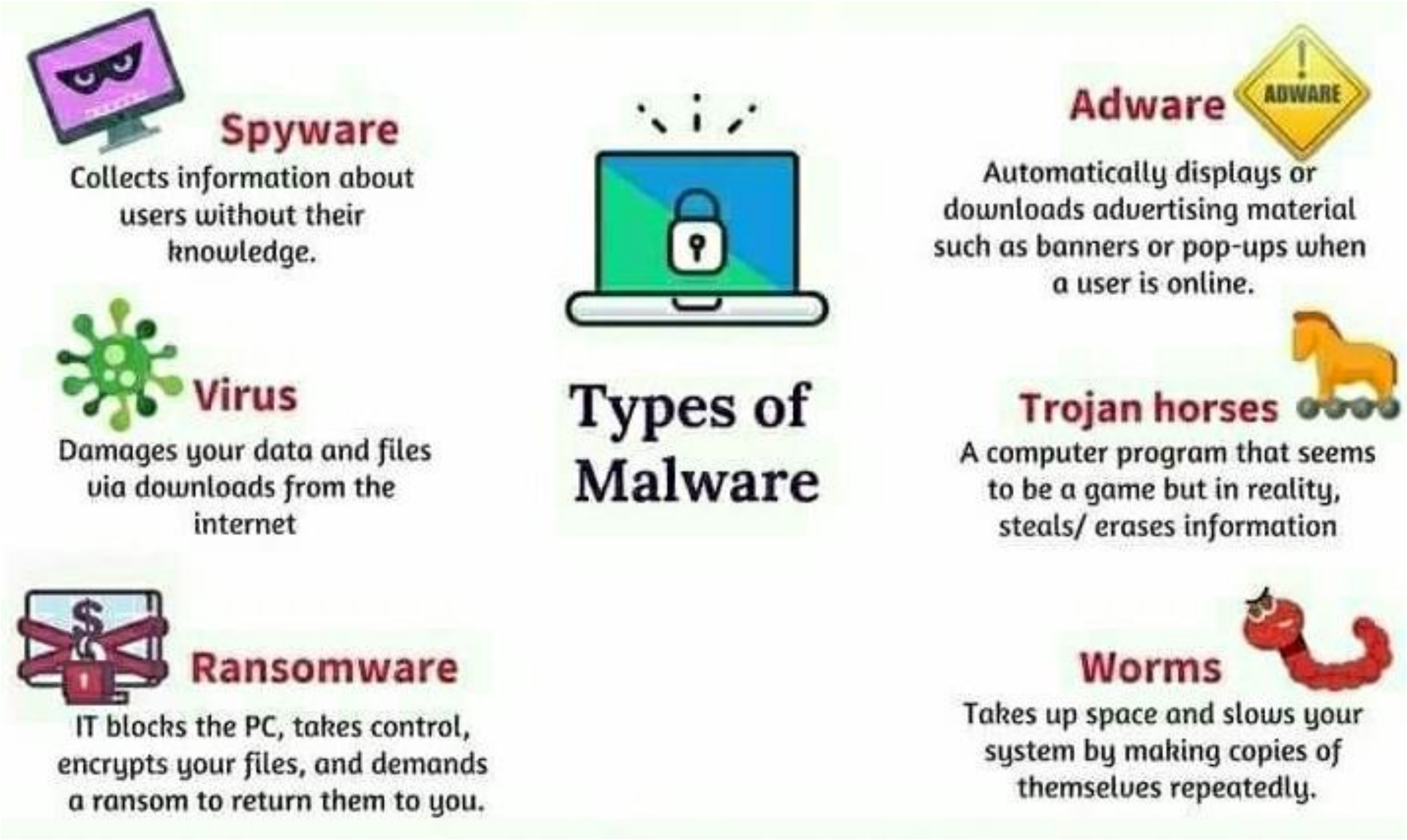


- **Availability is compromised with DoS attacks.**
- **These attack are the result of**
  - **Failure of a system to handle exceptional conditions**
  - **Failure of a system to handle vast quantities of data**

What Is Malware?

- **Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software."**
- **Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.**

Types of Malware



Types of Malware

Spyware

Collects information about users without their knowledge.

Virus

Damages your data and files via downloads from the internet

Ransomware

IT blocks the PC, takes control, encrypts your files, and demands a ransom to return them to you.

Adware

Automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

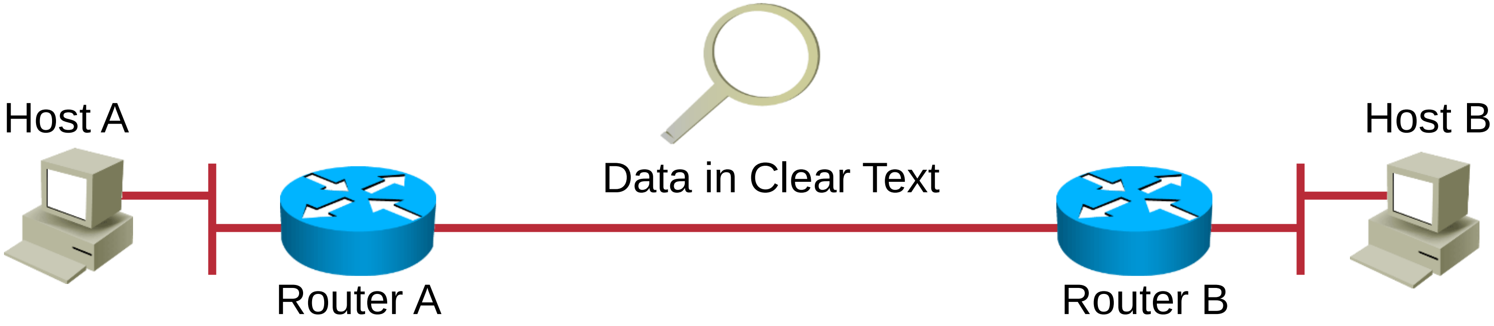
Trojan horses

A computer program that seems to be a game but in reality, steals/ erases information

Worms

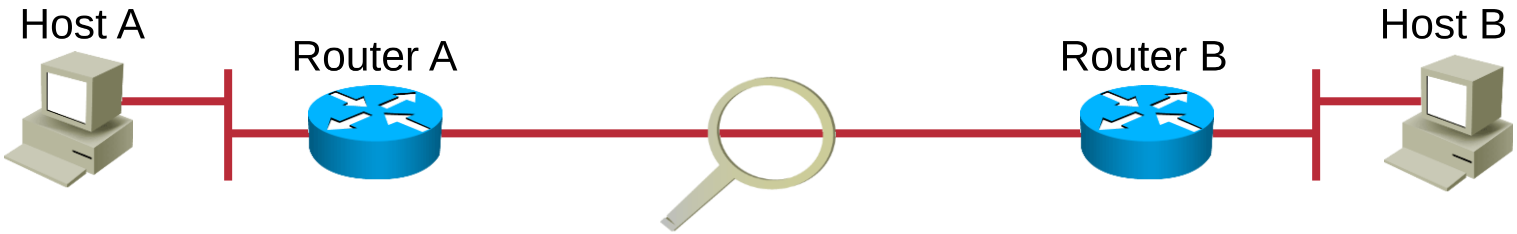
Takes up space and slows your system by making copies of themselves repeatedly.

Man-in-the-Middle Attacks



- **A man-in-the-middle attack requires that the hacker have access to network packets that come across a network.**
- **A man-in-the-middle attack is implemented using the following:**
  - **Network packet sniffers (nonblind attack)**
  - **Routing and transport protocols (blind attack)**

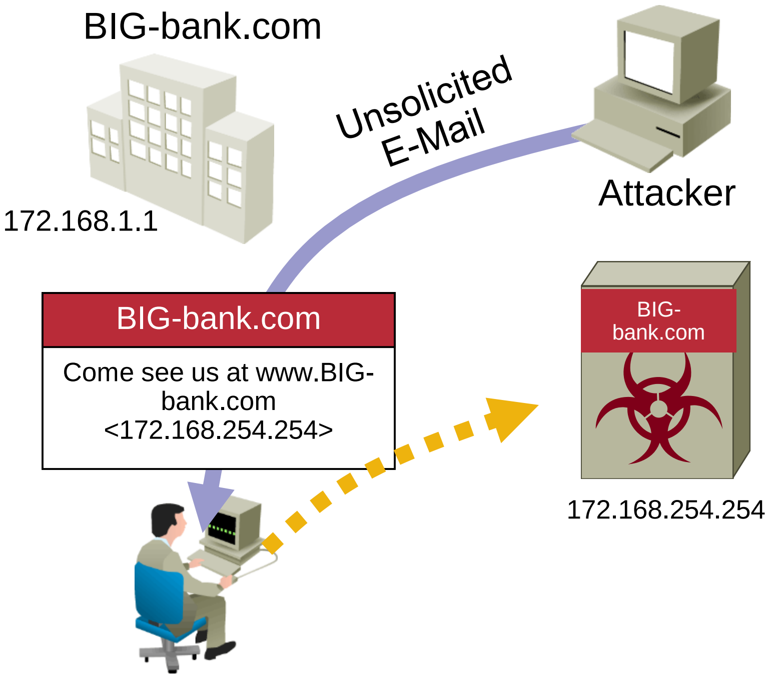
Packet Sniffers



- **A packet sniffer is a software application that uses a NIC in promiscuous mode to capture all network packets.**
- **Packet sniffers exploit information passed in plaintext. Protocols that pass information in plaintext include**
  - **Telnet**
  - **FTP**
  - **SNMP**
  - **POP**
  - **HTTP**
- **Packet sniffers must be on the same collision domain.**
- **Packet sniffers can be general purpose or can be designed specifically for attack.**

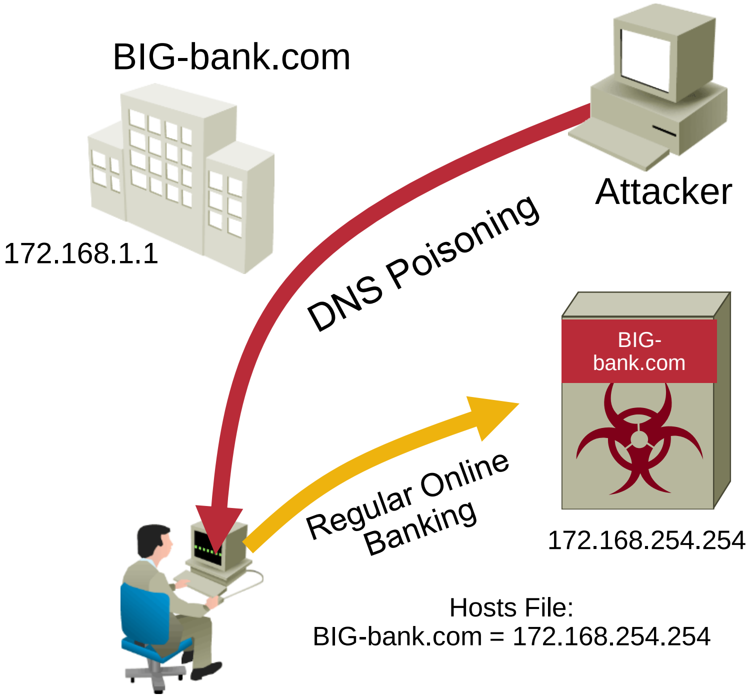
Phishing, Pharming, and Identity Theft

Phishing



- Identity theft continues to be a problem.
- Phishing scams are more sophisticated every day.
- You must protect your users. Implement technology and educate users.

Pharming



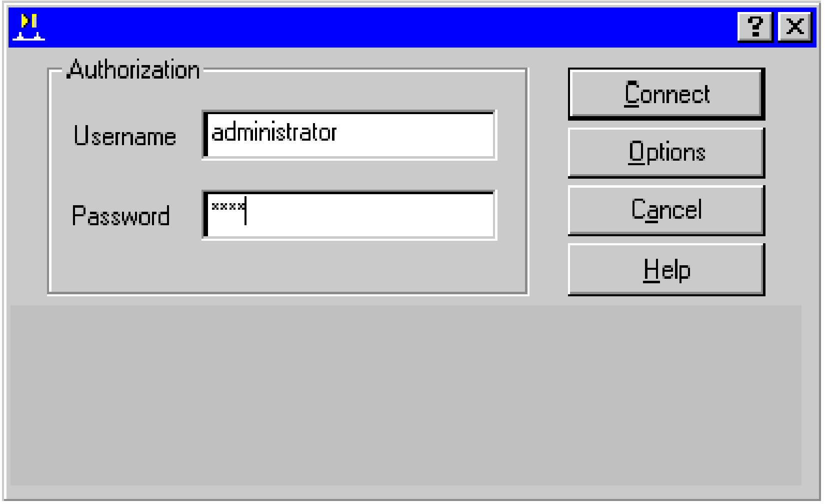
If you are a target

- Consider “personalization” technologies (e.g., user-chosen images on a web page)
- Support identified e-mail initiatives

Password Attacks

Hackers can implement password attacks using several methods:

- **Brute-force attacks**
- **Trojan horse programs**
- **Keyloggers**
- **Packet sniffers**



Authorization

Username administrator

Password ****

Botnets

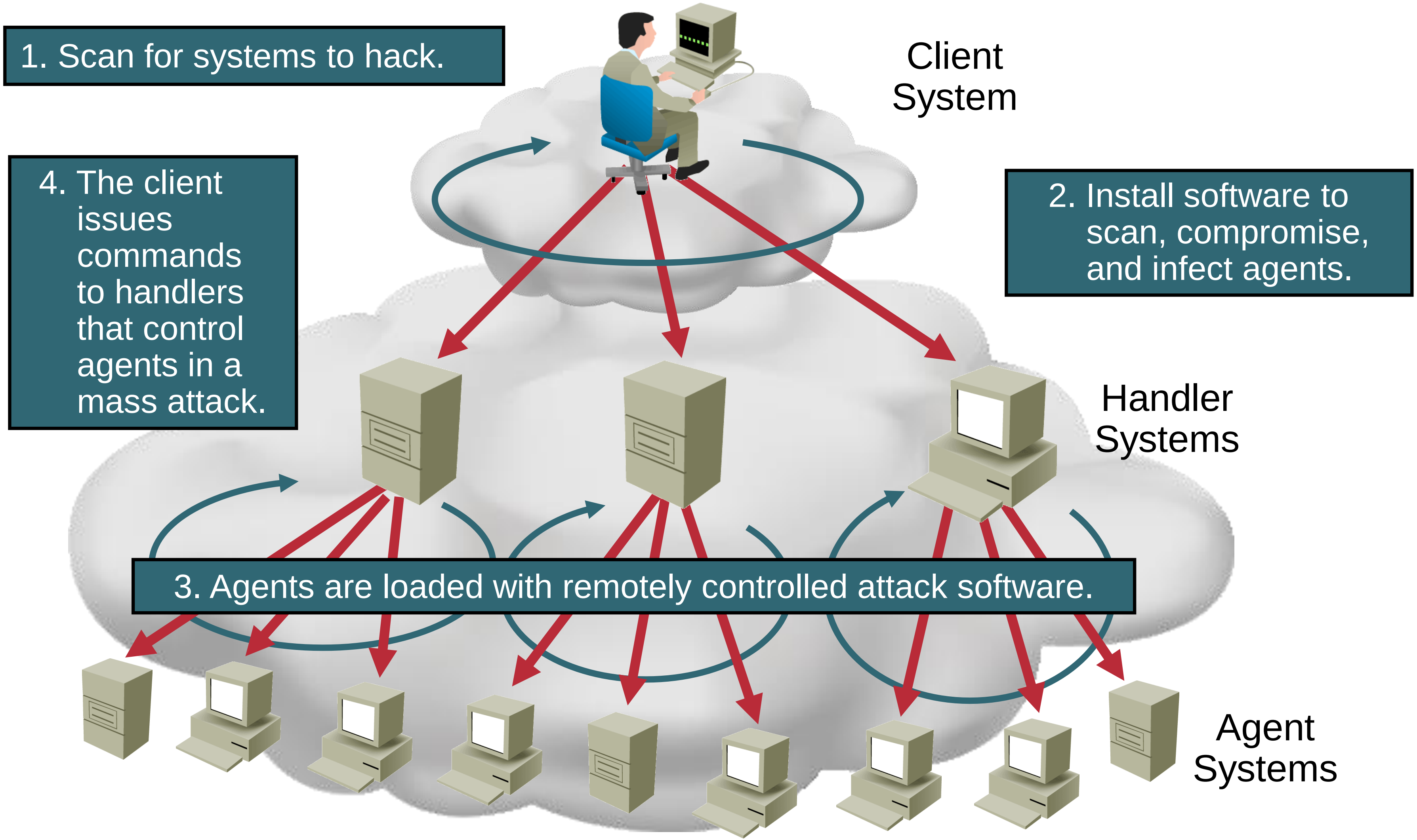
- A collection of compromised machines running programs under a common command and control infrastructure
- Building a botnet
  - Viruses, worms, infected spam, drive-by downloads, or other exploitation methods are used to send a Trojan program or back door to infect a computer.
  - A spammer can purchase access to the botnet from the controller. Spam levels jumped 30% in September and October 2006 largely due to botnets.
- Controlling a botnet
  - A covert channel, typically an IRC, is used to control the botnet.
  - Historically, free DNS hosting services have been used to point bots to the IRC server.
  - It is becoming more common for control services to be placed on compromised high-speed machines, such as in academic institutions.

DoS and DDoS Attacks

DoS attacks focus on making a service unavailable for normal use. They have the following characteristics:

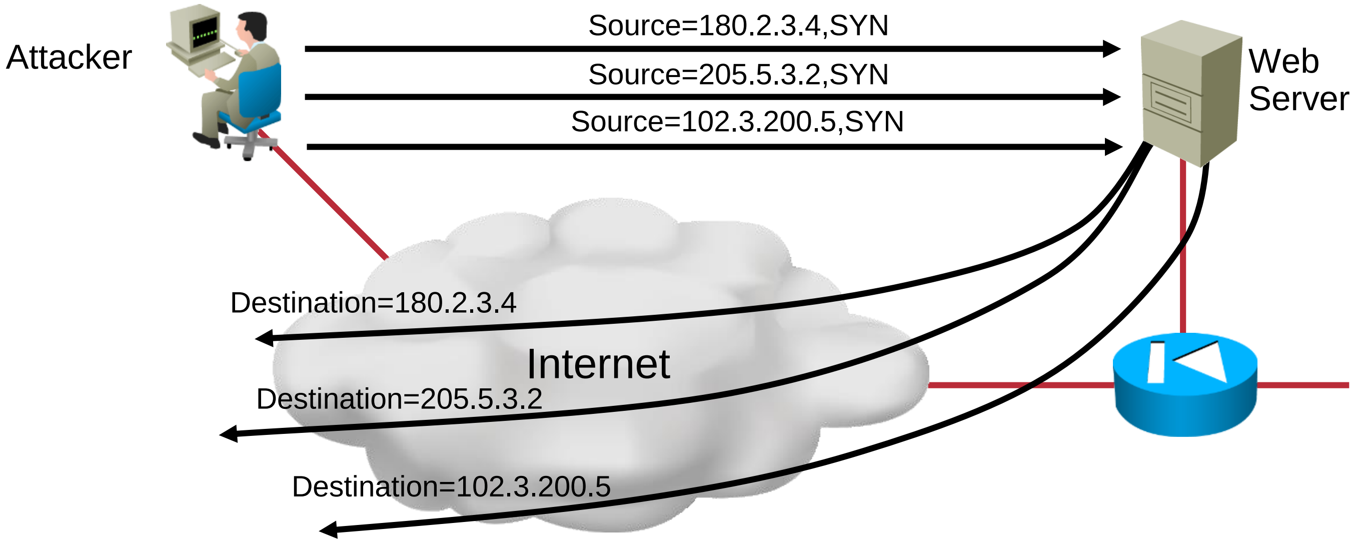
- **They are different from most attacks because they do not typically try to gain access to your network or the information on your network.**
- **They require very little effort to execute.**
- **They are among the most difficult attacks to completely eliminate.**

DDoS Example



1. Scan for systems to hack.
Client System
4. The client issues commands to handlers that control agents in a mass attack.
2. Install software to scan, compromise, and infect agents.
Handler Systems
3. Agents are loaded with remotely controlled attack software.
Agent Systems

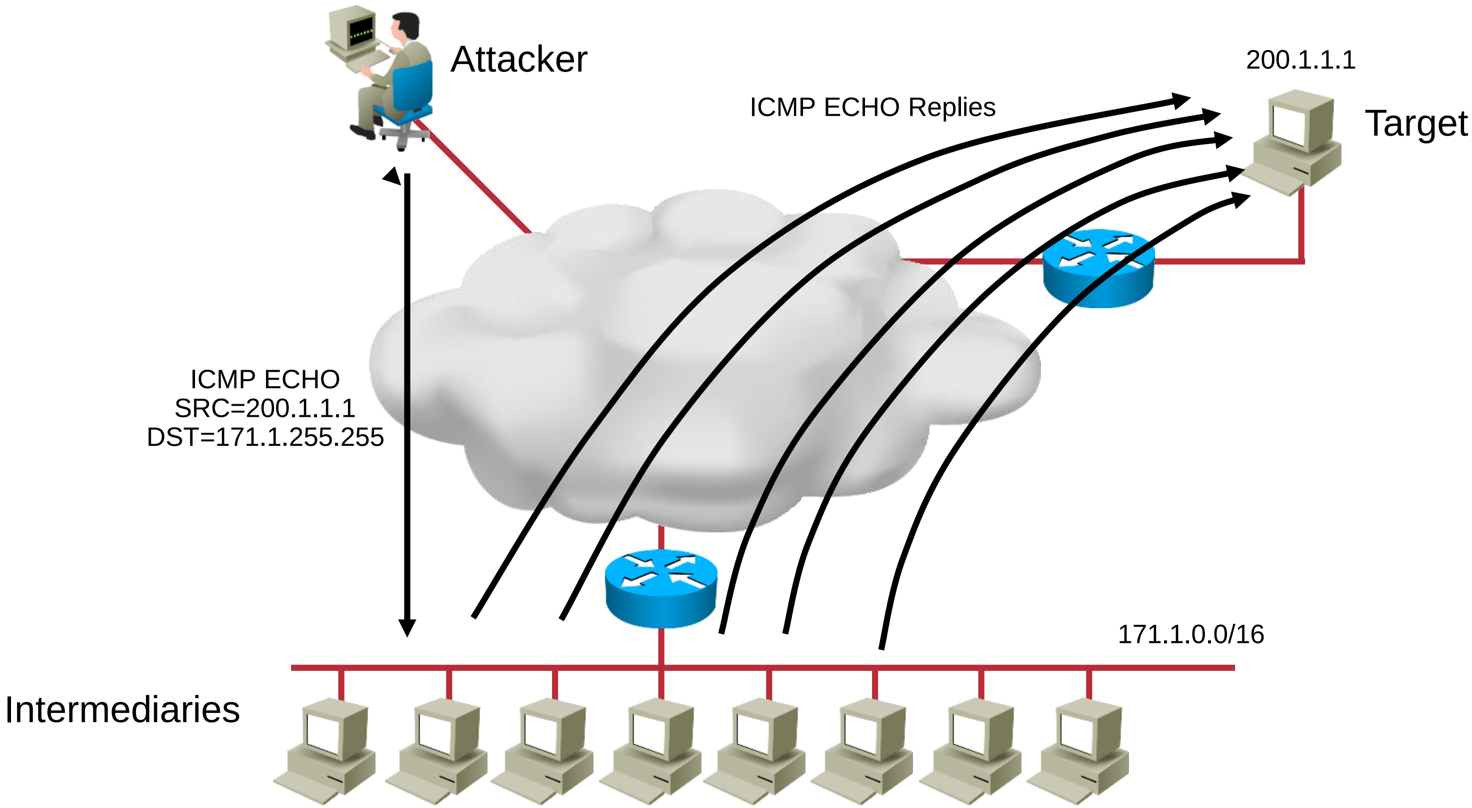
TCP SYN Flooding



An attacker sends a flood of SYN segments to a target server and never completes the handshake:

- **Servers have a limited number of half-open connections and stop accepting new connections.**
- **The source address is usually forged, using a nonresponsive part of the address space to prevent RSTs.**

Smurf Attack



ICMP flooding attacks are popular due to amplification techniques:

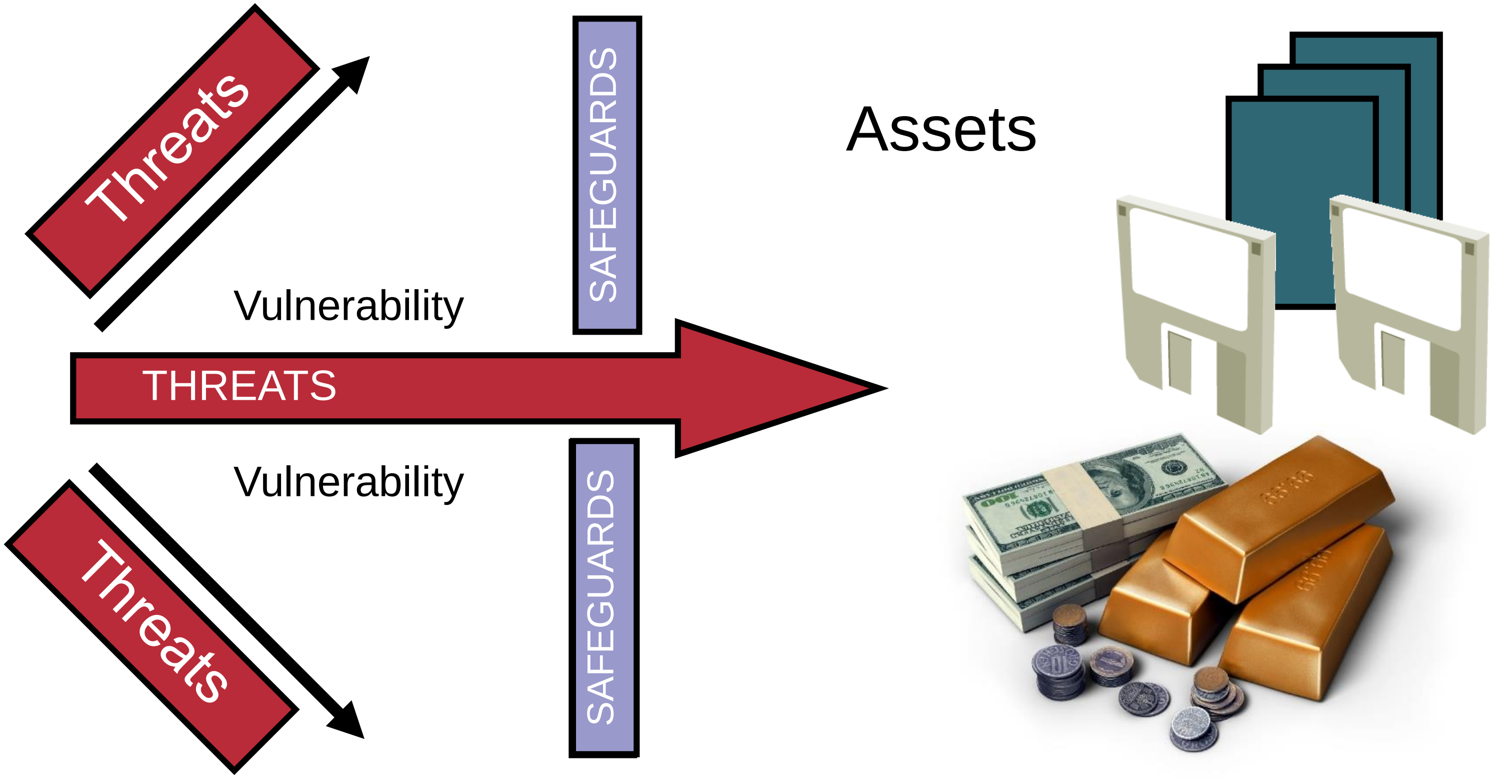
- **Smurf attacks use a spoofed broadcast ping to elicit a large number of responses to the target.**

Best Practices to Defeat Hackers

- Keep patches up to date.
- Shut down unnecessary services and ports.
- Use strong passwords and change them often.
- Control physical access to systems.
- Curtail unexpected and unnecessary input.
- Perform system backups and test them on a regular basis.
- Warn everybody about social engineering.
- Encrypt and password-protect sensitive data.
- Use appropriate security hardware and software.
- Develop a written security policy for the company.

Understanding and Developing a Comprehensive Network Security Policy

Figure Out What You Are Protecting



- **Things you have that others want**
- **Critical processes, data, or information systems**
- **Anything that will bring your business to a halt**

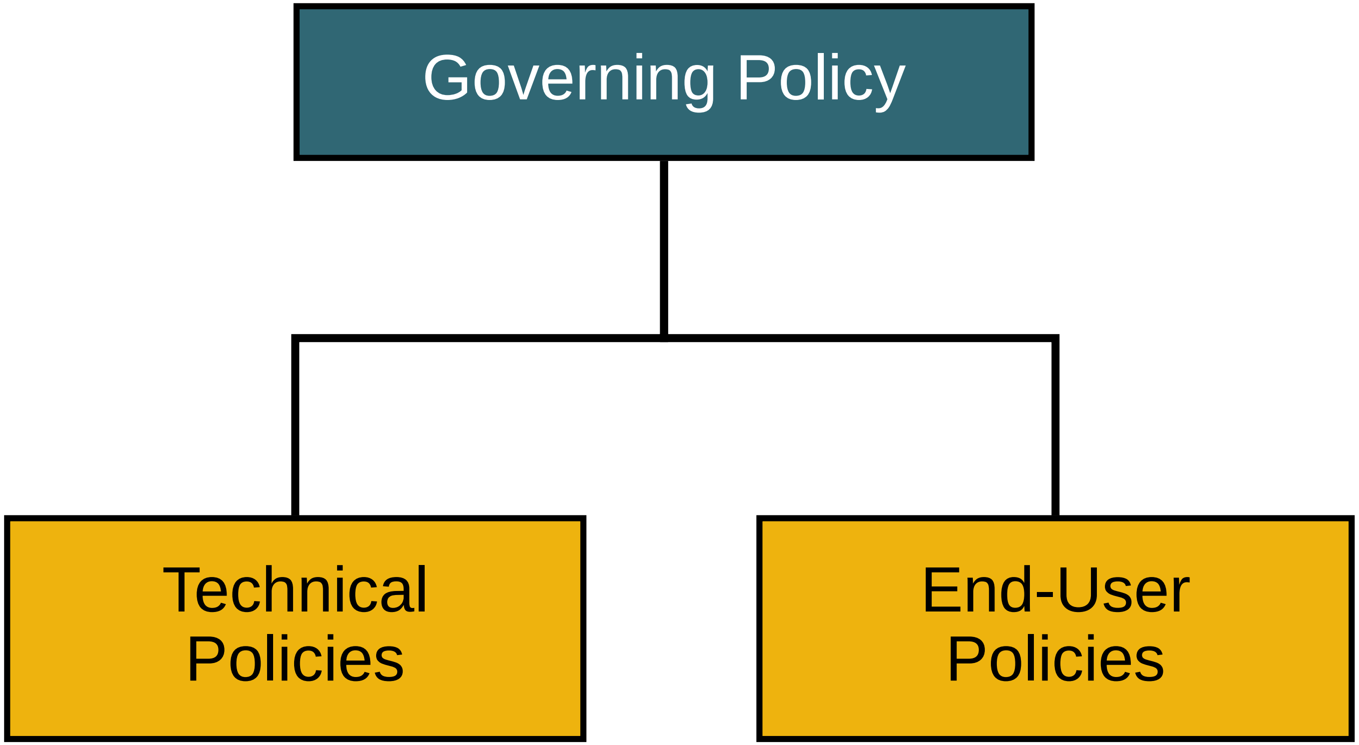
Why Do You Need a Security Policy?

- Three reasons for a security policy
  - To inform users, staff, and managers
  - To specify mechanisms for security
  - To provide a baseline
- A comprehensive security policy does the following:
  - Protects people and information
  - Sets the rules for expected behavior
  - Authorizes staff to monitor, probe, and investigate
  - Defines the consequences of violations
- AUP is the most common element of a security policy

Who Uses the Security Policy?

- Internal audiences
  - Managers and executives
  - Departments and business units
  - Technical staff
  - End users
- External audiences
  - Partners
  - Customers
  - Suppliers
  - Consultants and contractors

Components of a Comprehensive Security Policy



Governing Policy

Technical Policies

End-User Policies

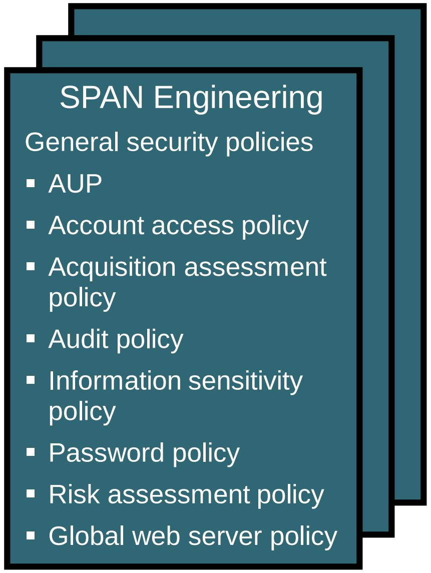
Governing Policy Comes from the Top

A governing policy includes these key components

- **A statement of the issue that the policy addresses**
- **A statement about your position on the policy**
- **How the policy applies in the environment**
- **The roles and responsibilities of those affected by the policy**
- **What level of compliance to the policy is necessary**
- **Which actions, activities, and processes are allowed and which are not**
- **The consequences of noncompliance**

Technical and End-User Policies

- **Technical policies describe the duties of the security staff in specified technical areas:**
  - **General policies**
  - **E-mail policies**
  - **Remote-access policies**
  - **Telephony policies**
  - **Application policies**
  - **Network policies**
  - **Wireless policies**



SPAN Engineering

General security policies

- AUP
- Account access policy
- Acquisition assessment policy
- Audit policy
- Information sensitivity policy
- Password policy
- Risk assessment policy
- Global web server policy

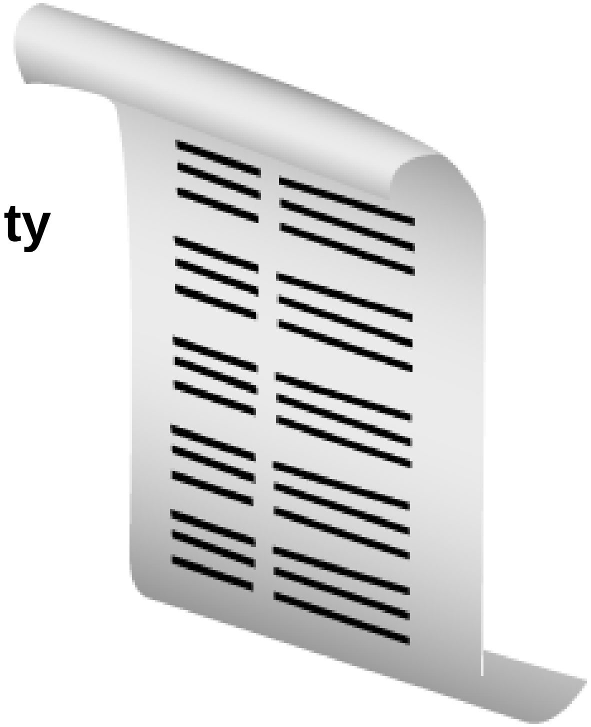
- **End-user policies detail specific duties and responsibilities for end users.**

Standards, Guidelines, and Procedures

- **Standards, guidelines, and procedures are the next level down from policies.**
- **They contain the actual details for the items defined in the policies.**
- **Standards, guidelines, and procedures are separate yet related.**
- **They should be separate documents despite the temptation to combine them into one.**
  - **Each document serves a different function with usually a different audience.**
  - **The security controls for each document may differ.**
  - **It is easier to update and maintain documents if they are separate.**

Standards

- **Specify the use of specific technologies in a uniform way**
- **Improve efficiency**
- **Are easier to secure**
- **Are usually mandatory**
- **Accomplish consistency and uniformity**



Guidelines

- Are similar to standards
- Are not usually mandatory
- Are more flexible than standards
- Can be used to define how standards should be developed
- Can be used to guarantee adherence to general security policies
- Some widely available guidelines include
  - NIST Computer Security Resource Center
  - NSA Security Configuration Guides
  - The Common Criteria standard
  - Rainbow Series

Procedures

- Are usually required
- Are the lowest level of the policy chain
- Provide detailed steps used to perform specific tasks
- Provide the steps required to implement the policies, standards, and guidelines
- Are also known as practices

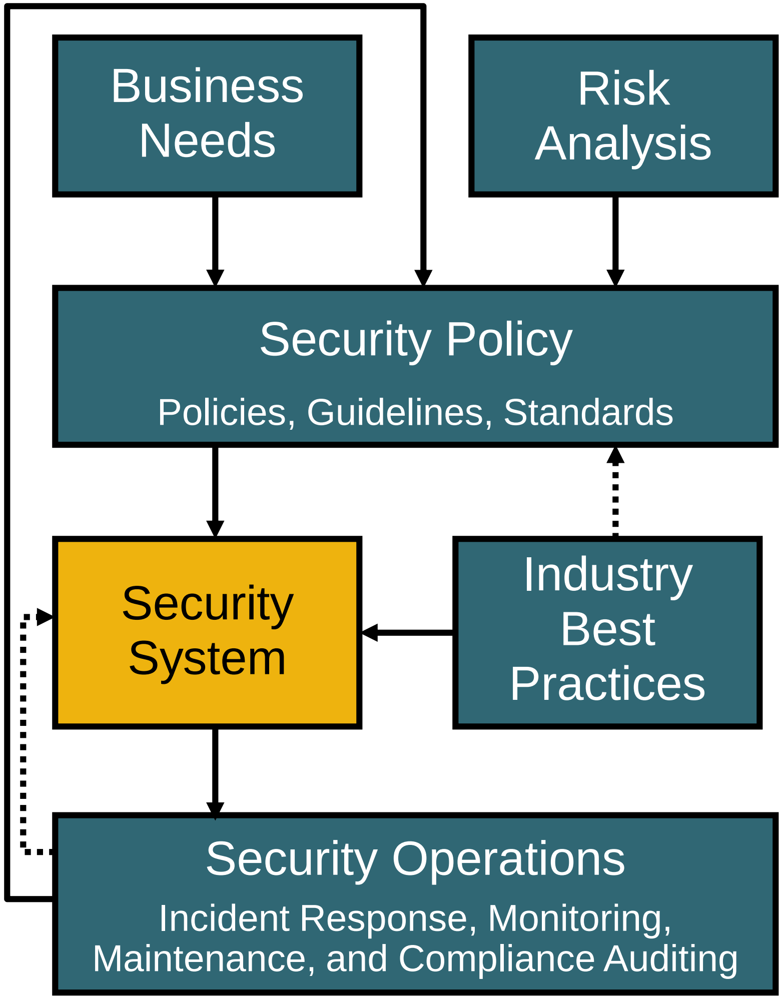
Responsibilities for the Security Policy

- Senior management (CEO)
  - Ultimately responsible
- Senior security—IT management (CSO, CIO, CISO)
  - Responsible for security policy
- Senior security—IT staff
  - Has input on security policy
  - Possibly drafts parts of security policy
- Security—IT staff
  - Responsible for implementing security policy
- End users
  - Responsible for complying with security policy

Secure Network Design Factors

Many factors affect the design of a secure network:

- Business needs
- Risk analysis
- Security policy
- Industry best practices
- Security operations



Least Privilege Concept

- A subject should have the minimal necessary privileges to perform a task.
  - This applies to users, programs, hosts, and so on.
  - This is perhaps the most important concept in a secure system design.
- This concept enhances simplicity because it narrows down the window of vulnerability.
- It limits possible unwanted interaction of system components.
- This concept is often not followed because it can make a system cumbersome to use.

Design and Implementation Simplicity

- **Complexity makes parts of the system interact in unpredictable ways.**
  - **The system can be hard or impossible to analyze.**
  - **Complexity is often considered the biggest enemy of security design.**
- **You should make design and implementation simple and straightforward.**
- **You should use multiple simple security features instead of one complex one, as long as they are comparable in protection strength.**
- **Make sure that the user of the system understands it well enough to use it properly.**

Simplicity Example

End-user responsibilities

All end users will participate in risk mitigation by enforcing discretionary access control on file system objects in such way as to prevent external subjects from violating the integrity of the properties or contents of an object.

VS.

End-user responsibilities

When changing file permissions, ensure that only Cisco employees will have “write” access to that file.

Simplicity in protection policy makes it easier to implement.

Security Awareness

- There are three pillars of a successful security awareness program.
  - Awareness
  - Education
  - Training
- An effective security awareness and training program require
  - Proper planning
  - Proper implementation
  - Maintenance
  - Periodic evaluation

Awareness

- This is often an overlooked part of the security practitioner job.
- It can be overdone; moderation is a good thing with awareness.
- Some ways to increase awareness:
  - Lectures, videos, and computer-based training
  - Posters, newsletter articles, and bulletins
  - Awards for good security practices
  - Reminders such as login banners, mouse pads, coffee cups, and notepads

Education and Training

- Security training for end users
- Awareness training for groups
  with sensitive positions
- Technical security training for the IT staff
- Advanced INFOSEC training for the security practitioners
- Specialized training for senior management

CISCO