



# **Business Continuity and Disaster Recovery Planning**

---

**CSC 3570  
IT Security  
Fall 2021**

## **Slide Source:**

**CISSP Guide to Security Essentials, Gregory, Peter, Chapter 4  
Fundamentals to Information Systems Security, Kim and Solomon, Chapter 4**

---



# Objectives

---

- ❑ Business continuity plan (BCP) and disaster recovery plan (DRP)
    - Develop
    - Test
    - Maintain
-



# What Is a Disaster

---

- ❑ Any natural or man-made event that disrupts the operations of a business in such a significant way that a considerable and coordinated effort is required to achieve a recovery.



# Natural Disasters

---

- Health:**
    - widespread illnesses, quarantines, and pandemics
  - Geological:**
    - earthquakes, volcanoes, tsunamis, landslides, and sinkholes
  - Meteorological:**
    - hurricanes, tornados, wind storms, hail, ice storms, snow storms, rainstorms, and lightning
  - Other:**
    - meteors and meteorites, and solar storms
-

# Man-made Disasters

---

- Labor:**
  - **strikes, walkouts, and slow-downs**
- Social-political:**
  - **war, terrorism, sabotage, vandalism, civil unrest, protests, demonstrations, cyber attacks, and blockades**
- Materials:**
  - **fires, hazardous materials spills**
- Utilities:**
  - **power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout from power plant accidents**



# How Disasters Affect Businesses

---

- Direct damage to facilities and equipment
- Indirect
  - Transportation infrastructure damage
    - Delays deliveries, supplies, employees, customers
  - Communications outages
  - Utilities outages

# The Role of Prevention in BCP & DRP

---

- ❑ Not about prevention of the disaster itself,  
but prevention of unpreparedness to handle the disaster
- ❑ More about the reduction in
  - impact of a disaster
  - recovery time

# **BCP and DRP**

---

## **Business Continuity Plan (BCP)**

- Activities required to ensure the continuation of critical business processes in an organization with alternate/backup resources
- Focus is on business processes

## **Disaster Recovery Plan (DRP)**

- Assessment, salvage, repair, and eventual restoration of damaged facilities and systems
- Focus is on infrastructure

## **BCDR: Business Continuity and Disaster Recovery**

# How BCP and DRP Support Security

---

## □ Security pillars: C-I-A

- Availability
- Confidentiality
- Integrity

# **Running a BCP / DRP Project**

---

- Project is:**
  - Development, testing, and maintenance of the BCDR plan
- Pre-project activities**
- Project activities**

# Pre-Project Activities

---

- ❑ Obtain executive support
  - Priority, budget, incentives, completion date, maintenance plan
- ❑ Formally define the scope of the project
  - Should not be outside of executive control
  - Size is a crucial factor
- ❑ Select project team members for planning
  - Middle ground between most experienced and newcomers
- ❑ Develop a project plan
- ❑ Document plan/Develop a project charter



# Developing a Project Charter

---

## Documentation

- Purpose of planning project
- Executive sponsorship
- Scope
- Budget
- Team
- Milestones

## Reviewed and signed

# **Developing BCDR Plan**

---

- Perform business impact assessment
- Develop contingency plans
- Test contingency plans

# **Performing a Business Impact Assessment (BIA)**

---

- Survey all business processes
- Impact assessment of each process
- Perform criticality analysis of all

# Survey Business Processes

---

- Develop interview / intake template
- Interview a representative from each department
  - Identify all important processes
    - Identify dependencies on systems, people, equipment, facilities, etc.
- Organize data into database or spreadsheets
  - Gives a big picture, all-company view

# BIA Process Intake Form

window width and enable scrolling	
<b>Process Name</b>	(name of the process)
<b>Date</b>	(date of the interview)
<b>Interviewer</b>	(name of the person conducting the interview)
<b>Interviewee</b>	(name of the person being interviewed)
<b>Interviewee Contact</b>	(e-mail, phone, location, etc.)
<b>Department</b>	(Interviewee's department)
<b>Process Owner Name</b>	(department manager or other responsible party who is accountable for the performance of the process)
<b>Process Purpose</b>	(why the process is performed)
<b>Process Inputs</b>	(data, people, supplies, or other things that the process uses)
<b>Process Outputs</b>	(data, products, or other outcomes from running the process)
<b>Supplier Dependencies</b>	(names of suppliers that are essential to the ongoing operation of the process)
<b>Personnel Dependencies</b>	(names of staff members who are essential to the ongoing operation of the process)
<b>Asset Dependencies</b>	(list of assets that are essential to the ongoing operation of the process)
<b>Information System Dependencies</b>	(list of IT applications that are essential to the ongoing operation of the process)
<b>Communications Dependencies</b>	(list of communications facilities (phone, FAX, Internet, etc.) that are essential to the ongoing operation of the process)
<b>Facilities Dependencies</b>	(list of facilities that are essential to the ongoing operation of the process)

# **Process Impact Assessment**

---

- After collecting all relevant information**
  - Perform threat/risk analysis
  - Develop impact statements
  - Assess current BCDR capabilities
  - Recommend needed BCDR capabilities

# Threat and Risk Analysis

---

- ❑ Identify threats, vulnerabilities, risks for each key process
  - Rank according to probability, impact, cost
  - Identify mitigating controls

# Develop Statements of Impact

---

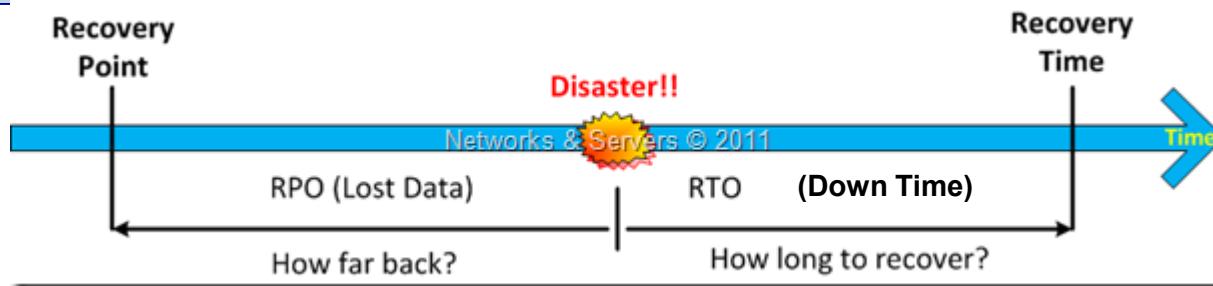
- ❑ For each process, describe the impact on the rest of the organization if the process is incapacitated
- ❑ Examples
  - Inability to process payments
  - Inability to produce invoices
  - Inability to access customer data for business purposes
- ❑ Identify key recovery targets

# Identifying Key Recovery Targets with Metrics

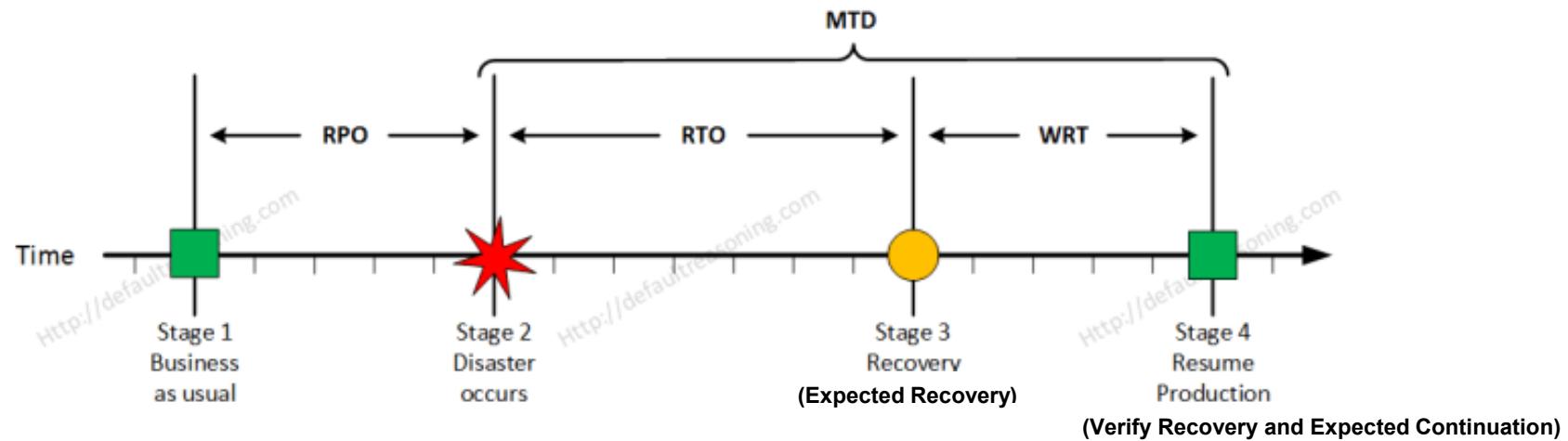
---

- Recovery point objective (RPO)**
  - Maximum acceptable amount of data loss
    - Until the next scheduled backup
- Recovery time objective (RTO)**
  - Maximum period of time processes will be unavailable
    - from disaster onset to resumption of business process
- Work recovery time (WRT)**
  - Time to verify processes/data ready to run
- Maximum Tolerable Downtime (MTD)**
  - Identify the maximum time that each business process can be inoperative before significant damage or long-term viability is threatened
  - $MTD = RTO + WRT$

# RTO, RPO, WRT, MTD



<http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html>



<http://virtualization24x7.blogspot.com/2015/11/what-is-rpo-rto-wrt-mtd.html>

# Data Center Alternatives for Disaster Recovery

TABLE 4-2 Data center alternatives for disaster recovery.

OPTION	DESCRIPTION	COMMENTS
Hot site	Facility with environmental utilities, hardware, software, and data that closely mirrors the original data center	Most expensive option, least switchover time
Warm site	Facility with environmental utilities and basic computer hardware	Less expensive than a hot site, but requires more time to load operating systems, software, data, and configurations
Cold site	Facility with basic environmental utilities but no infrastructure components	Least expensive option, but at the cost of the longest switchover time since all hardware, software, and data must be loaded at the new site
Mobile site	Trailer with necessary environmental utilities that can operate as a warm site or cold site	Very flexible, fairly short switchover time, and widely varying costs based on size and capacity

# Sample RTOs for Alternate Sites

RTO	Technology(ies) required
8-14 days	New equipment, data recovery from backup
4-7 days	Cold systems, data recovery from backup
2-3 days	Warm systems, data recovery from backup
12-24 hours	Warm systems, recovery from high speed backup media
6-12 hours	Hot systems, recovery from high speed backup media
3-6 hours	Hot systems, data replication
1-3 hours	Clustering, data replication
< 1 hour	Clustering, near real time data replication

# Deriving Metrics

---

- Probably an educated guess for many processes
  - Obtain senior management input to validate data
  - Look at past history/records
-

# Record Other Key Metrics

---

## ❑ Examples

- Cost to operate the process
- Cost of downtime
- Profit derived from the process

# Criticality Analysis

---

- Rank processes by metrics criticality
  - Quantitative criteria
    - Low numbers are more critical
      - MTD (maximum tolerable downtime)
        - » RTO (recovery time objective)
        - » RPO (recovery point objective)
      - High numbers are more critical
        - Cost of downtime
        - Revenue rates
    - Qualitative criteria
      - Reputation, market share, goodwill, customer visibility

# Assess Current Continuity and Recovery Capabilities

---

- ❑ For each business process
  - Identify documented
    - continuity capabilities
    - recovery capabilities
  - Identify undocumented capabilities
- ❑ *What if the disaster happened tomorrow*
  - Assess and Recommend Capabilities
    - Adequate?
    - Inadequate?
    - Non-existent?

# Develop BC & DR Plans

---

- ❑ For the most critical processes (based upon ranking in the criticality analysis)
- ❑ Factors to consider
  - Must meet business objectives
  - Budget for plan development
  - Budget for response and recovery effort

# **Steps in BCDR Planning**

---

- Select recovery team members
- Emergency response

# Select Recovery Team Members

---

## Selection criteria

- Location of residence relative to work and other key locations
- Skills and experience
- Ability and willingness to respond
  - Health and family
  - Own transportation

## Identify backups

- Other team members, external

# **Emergency Response**

---

- Personnel safety
- Logistics and supplies
- Salvage and Damage assessment
- Emergency notification

# Personnel Safety

---

- ❑ The number one concern in any disaster response operation
  - Emergency evacuation
    - Accounting for all personnel
  - Administering first-aid

# Public Utilities and Infrastructure

---

- ❑ Often interrupted during a disaster
  - Electricity
  - Water
  - Natural gas
  - Waste

# **Emergency Logistics and Supplies**

---

- Meds
  - Food and drinking water
  - Blankets and sleeping cots
  - Sanitation
  - Tools
  - Spare parts
  - Waste bins
  - Communication means
-

# Salvage and Damage Assessment

---

## Salvage

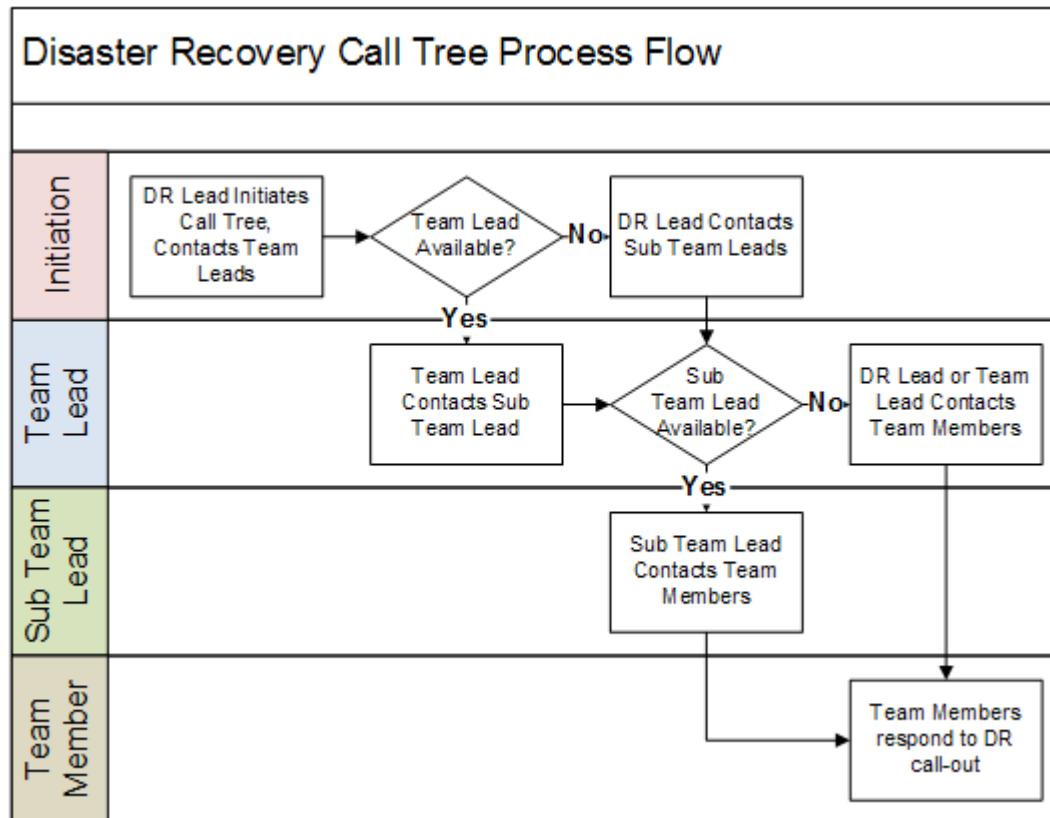
- Identify working and salvageable assets
- Protect remaining assets

## Determine damage to buildings, equipment, utilities

- Requires inside experts
- May require outside experts
  - Civil engineers to inspect buildings
  - Government building inspectors

# Communications

- ❑ Communications essential during emergency operations
- ❑ Call tree



# Communication Considerations

---

- Avoid common infrastructure
- Diversify mobile services
- Consider two-way radios
- Consider satellite phones
- Consider amateur radio

# Notification

---

- ❑ Many parties need to know the condition of the organization
  - Employees, suppliers, customers, regulators, authorities, shareholders, community
- ❑ Methods of communication
  - Telephone, web site, signage, media

# **Business Resumption Planning**

---

## **Alternate**

- **work locations**
- **personnel**
- **communications**
- **assets and equipment**
- **records/data**
- **access to procedures**

# **Restoration and Recovery**

---

- Repairs to facilities, equipment
- Replacement equipment
- Restoration of utilities
- Resumption of business operations in primary business facilities

# **Training Staff**

---

- Everyday operations**
- Emergency procedures**
- Recovery procedures**
- Resumption procedures**

# Testing Business Continuity and Disaster Recovery Plans

---

## ❑ Five levels of testing

- Document review
- Walkthrough
- Simulation
- Parallel test
- Cutover test

# Document Review

---

- ❑ Review of recovery, operations, resumption plans and procedures
  - Performed by individuals
  - Provide feedback to document owners
- ❑ Least impact, lowest risk, least benefit

# Walkthrough

---

- ❑ Group discussion of recovery, operations, resumption plans and procedures
  - Performed by teams
  - Provide feedback to document owners
- ❑ Low impact, lowest risk, moderate benefit

# Simulation

---

- ❑ Walkthrough of recovery, operations, resumption plans and procedures in a scripted “case study” or “scenario”
  - Performed by teams
  - Places participants in a mental disaster setting that helps them discern real issues more easily
- ❑ Low impact, low risk, moderate benefit

# Parallel Test

---

- ❑ Tests actual system readiness and accuracy of procedures
  - Full or partial workload is applied to recovery systems
  - Production systems continue to operate and support actual business processes
- ❑ Moderate impact, low risk, moderate benefit

# Cutover Test

---

- ❑ Tests actual system readiness and accuracy of procedures
  - Recovery systems assume full actual workload
  - Production systems are shut down or disconnected
- ❑ High impact, high risk, high benefit

# **Benefits of BCP and DRP Planning**

---

- Reduced risk
- Improved availability and reliability
- Process improvements
- Improved organizational maturity
- Marketplace advantage

# Maintaining Business Continuity and Disaster Recovery Plans

---

- ❑ Factors that necessitate review and modification of DRP and BCP procedures :
  - Changes in business processes and procedures
  - Changes to IT systems and applications, architectures
  - Changes in service providers
  - Changes in organizational structure

# Industry Standards Supporting BCP and DRP

---

- ISO17799: Code of Practice for Information Security Management. Section 14 addresses business continuity management.
  - BS25999: Code of Practice for Business Continuity Management.
  - ISO17799: Code of Practice for Information Security Management. Section 14 addresses business continuity management.
  - BS25999: Code of Practice for Business Continuity Management.
  - NFPA 1620: The Recommended Practice for Pre-Incident Planning.
  - HIPAA: Requires a documented and tested disaster recovery plan.
-

# Summary

---

- ❑ Natural and man-made disasters affect businesses through direct damage, and damage to transportation and utilities
  - ❑ BCP is concerned with continuation of processes; DRP is concerned with recovery of facilities
  - ❑ Benefits of BCP and DRP include process improvement, reduced risk, and market advantage
  - ❑ The components of a Business Impact Assessment (BIA) are:
    - Inventory processes
    - Perform risk and threat assessment
    - Assign recovery targets
    - Perform criticality assessment
-

# **Summary (cont.)**

---

- Several key metrics are developed in a BIA:**
    - MTD (maximum tolerable downtime)
    - RTO (recovery time objective)
    - RPO (recovery point objective)
    - Possibly others (cost of downtime, recovery)
  - The components of a DRP and BCP plan are:**
    - Emergency response
    - Damage assessment and salvage
    - Communications
    - Personnel evacuation and safety
    - Restoration and recovery
    - Business resumption
-

# Summary (cont.)

---

- ❑ The types of BCP and DRP plan testing are:
  - Document review
  - Walkthrough
  - Simulation
  - Parallel test
  - Cutover test

# **Operations Security**

---

CSC 3570  
IT Security  
Fall 2021

## **Slide Source:**

CISSP Guide to Security Essentials, Gregory, Peter, Chapter 7 and 6  
Fundamentals to Information Systems Security, Kim and Solomon, Chapter 6  
Network Security Fundamental, Mark Ciampa, Chapter 12

---

# High Availability Architectures

---

## □ Goal

- Avoid SPOF
- Maintain/increase uptime
- Reduce downtime

## □ Mechanisms

- Fault tolerance
- Clustering
  - Replication

# Fault Tolerance

---

- Makes devices/network less prone to failure
  - Multiple power supplies
  - Multiple network interfaces
  - Multiple processor units
  - RAID (Redundant Array of Inexpensive /Independent Disks)

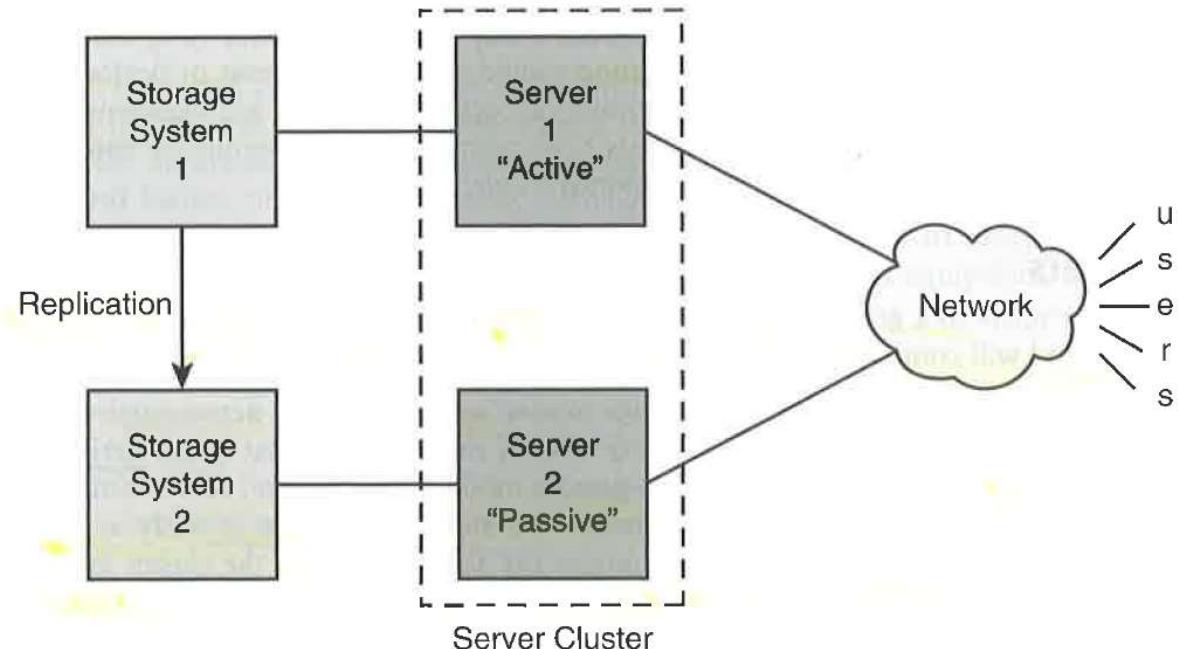
# Clustering

---

- A group of two or more servers that operate functionally as a single logical server
  - Geo-cluster – servers located at great distances from one another
- Modes
  - Active-active
  - Active-passive
    - Failover: when active status is transferred

# Replication

- ❑ An adjunct to clustering, makes current data (and changes) available to all cluster nodes
- ❑ Data changes are transmitted to a counterpart storage system



# Vulnerability Management

---

- Identifying vulnerabilities and taking steps to mitigating the vulnerabilities
- Identification Types
  - Passive
    - Vulnerability reports from external sources
  - Active
    - Penetration testing
    - Application scanning

# Active Vulnerability Management

---

- Application scanning (a.k.a. vulnerability scanning)
  - Scoped for application, typically automated, more focused on knowns than unknowns, the audience is developers
  
- Penetration testing
  - Larger scope, human factor involved, carry out exploits to assess results, more focused on unknowns, broader audience

# Vulnerability Mitigation

---

- Patch management
  - Policy review
  - Code reviews
  - Operations reviews
-

# Patch Management

---

- The process to manage the installation of patches on target systems
- Reduces risks associated with attacks that exploit weaknesses
- Automated tools
  - Saves time and administration
  - Should be focused
    - Unwise to “Spray and pray”

# Change Management

---

- ❑ Management of changes to the environment so that changes affect environment as expected and the environment will operate as authorized
  - Uncontrolled changes can result in conflicts, errors, failures, vulnerabilities
- ❑ Goal
  - Maximize availability, improve stability and minimize risk
- ❑ Types
  - Reactive
    - Business driven, response to external environment
  - Proactive
    - Initiated by management, to achieve a goal

# Change Control Committee/Board

---

- Oversees compliance to procedure
- Ensures changes are
  - Authorized
  - Communicated
  - Scheduled/Implemented
  - Tested
  - Documented
- Board handles
  - Training/Communication/Test plan
  - Back out plan
  - Emergencies

# Change Management Procedure

---

- Request change**
    - Prepare the change
  - Impact assessment**
    - Circulate and review the change
  - Approval**
    - Discuss and agree to the change
  - Build/test/implement**
    - Perform the change
  - Monitor**
    - Recordkeeping
-

# Change Request Form

---

- Change identifier
  - Requester
  - Team leader/manager
  - Agency
  - Change description
  - Change reasons
  - Change date
  - Change components
  - Impact category
  - Risk category
  - Help desk
  - Management checklist
  - Evaluation results
-

# Configuration Management

---

- ❑ Recordkeeping of changes to configuration of hardware, software components
    - Management of baseline settings
  - ❑ Maintained with configuration management database (CMDB)
  - ❑ Enabled with automated tools
  - ❑ Can be used to detect unauthorized changes
-

# Summary

---

- ❑ The concept of *need-to-know* states that individual personnel should have access to only the information that they require in order to perform their stated duties.
  - ❑ The concept of *job rotation* moves individual workers through a range of assignments over time.
  - ❑ The actions of individuals with special privileges should be monitored, to detect potential problems as well as to deter individual wrongdoing.
  - ❑ *Records retention* governs the minimum and maximum periods of time that specific business records must be retained.
  - ❑ *Backups* ensure the survival of business records even if malfunctions, errors, or disasters destroy original records.
  - ❑ *Data destruction* is the process of securely discarding data when it is no longer needed.
-

## Summary (cont.)

---

- ❑ **Resource protection** ensures that the buildings, equipment, and systems used to operate the business are protected from harm, damage, or loss.
  - ❑ A **security incident** is an event in which some aspect of an organization's security policy has been violated.
  - ❑ A **high availability architecture** is a system or application architecture that includes one or more of the following characteristics: fault tolerance, clusters, failover, and replication.
  - ❑ **Fault tolerant devices** typically are equipped with redundant components that can be changed while the device continues operating.
  - ❑ A **cluster** is a group of servers that logically functions as a single server.
  - ❑ A **failover** is an event that occurs in a cluster where the role of an **active server** is transitioned to another server in the cluster.
-

# **Operations Security**

---

CSC 3570  
IT Security  
Fall 2021

## **Slide Source:**

CISSP Guide to Security Essentials, Gregory, Peter, Chapter 7 and 6  
Fundamentals to Information Systems Security, Kim and Solomon, Chapter 6  
Network Security Fundamental, Mark Ciampa, Chapter 12

---

# Topics

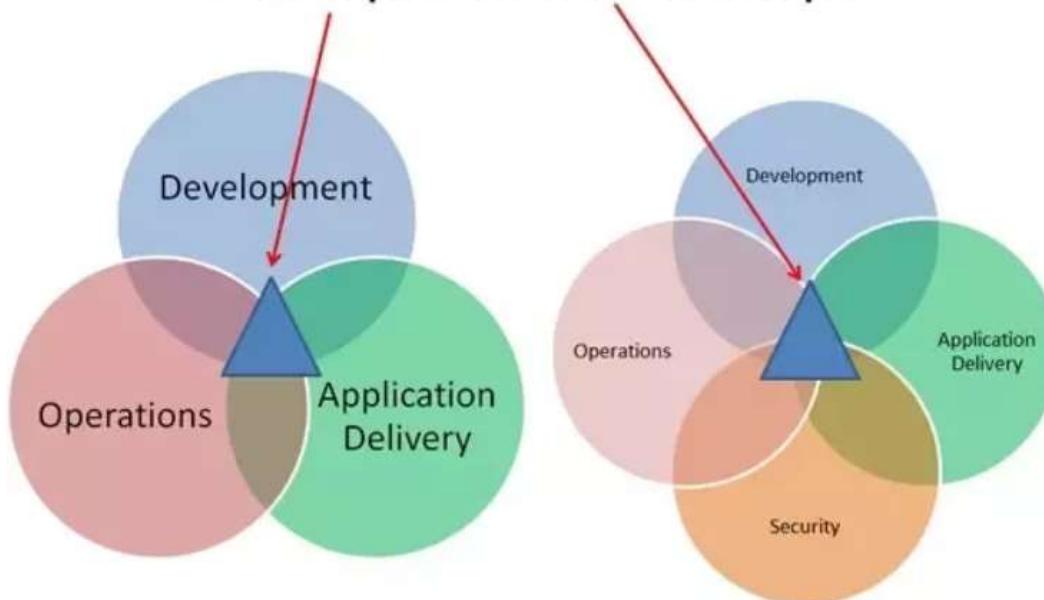
---

- Monitoring
  - Records management
  - Backups
  - Remote access
  - Resource protection
  - Incident management
  - High availability architectures
  - Vulnerability management
  - Change management
  - Configuration management
-

# DevOps, DevSecOps

---

DevOps vs. DevSecOps



# Operations Security (Opsec)

---

- Originated in Military...
- Identifying, controlling, and protecting information/resources which, if it becomes available to a competitor or adversary, could be used to our disadvantage.  
<http://www.wright.edu/rsp/Security/S2unclas/Opsec.htm>
- Is a process by which organizations assess and protect public data about themselves that could, if properly analyzed and grouped with other data by a clever adversary, reveal a bigger picture that ought to stay hidden.  
<https://www.csionline.com/article/3391566/what-is-opsec-a-process-for-protecting-critical-information.html>

# Operations Security (As in CISSP)

---

## ❑ It is about:

- User and environmental controls over machine, media and operations
- Audit and monitoring
- Identification of security events and reporting

## ❑ Important for OPERATIONS SECURITY

- All security principles as it applies to users

– Specially

- Least privilege
- Separation of duty/privilege

» Special cases: creating keys, user accounts, administrative accounts, firewalls etc.



# Other Key Concepts

---

## □ Need to know

- Additional condition on top of classification/clearance levels of subjects/objects
- Individuals should only have access to information that they require to perform their assigned duties
  - Reduces risk
  - Increases administrative overhead

## □ Job rotation

- Move individual workers through a range of job assignments
  - Reduces monotony, risk
  - Reduces likelihood that employees will perform inappropriate or illegal actions if they fear being caught when next job rotation occurs

# Monitoring of Users with Special Privileges

---

- Privileged users have more power
  - Mistakes have greater impact
- Record activities of
  - Network administrator
  - System administrator
  - Database administrator
  - Application administrator etc etc
- Benefits
  - Accountability
  - Troubleshooting

# Records Management

---

## □ Types of organizational records

- Personnel
- Operational
- Management
- Financial
- Legal

## □ Activities

- Access management/control
- Records retention
- Backups
- Data destruction

# Records Retention

---

- Policies that specify how long different types of records must be retained
  - Regulation compliance (minimums and maximums)
  - Manage risks
- Consider more time if
  - Risk of loss of important needed information
- Consider less time if
  - Risk of compromise of sensitive information
  - Increase in E-Discovery cost
  - Cost of maintaining info is more than true need

# Backups

---

- Protection against loss due to
    - malicious acts, malfunctions/failures, human errors and disasters
  - Activities
    - Protection of backup media
    - Off-site storage of backup media
    - Data restoration
-

# Protection of Backup Media

---

- Backup media contains sensitive information
- Same level of control (physical and logical) as original information
  - Keep in locked cabinets
  - Least privilege and need to know

# Offsite Storage of Backup Media

---

- Reduce risk of loss of backup media in the event of a disaster that destroys data center
  - Fire, flood, sabotage
- Factors in selecting location
  - Distance from business location
  - Security of transportation
  - Security of storage center
  - Resilience of storage center against disasters
- Cost cannot exceed value of data

# Data Restoration

---

- Periodic testing to ensure that
  - backups are being performed
  - data that is backed up can be restored

# Data Destruction

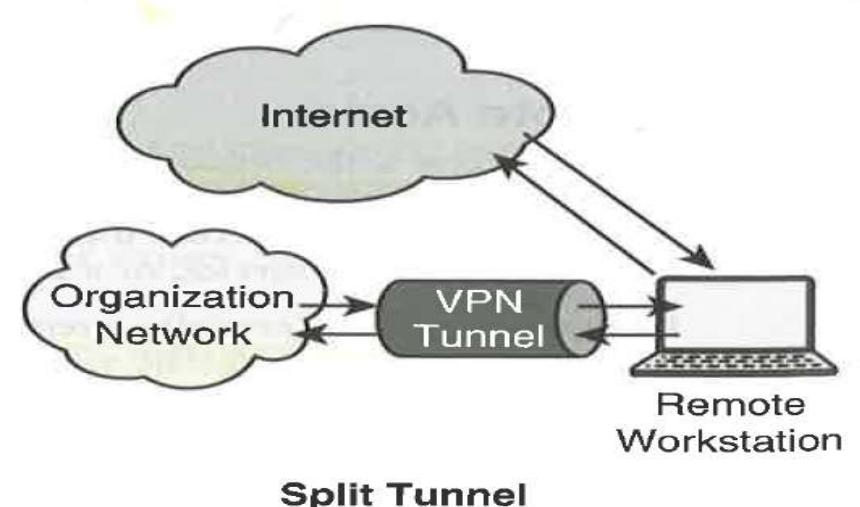
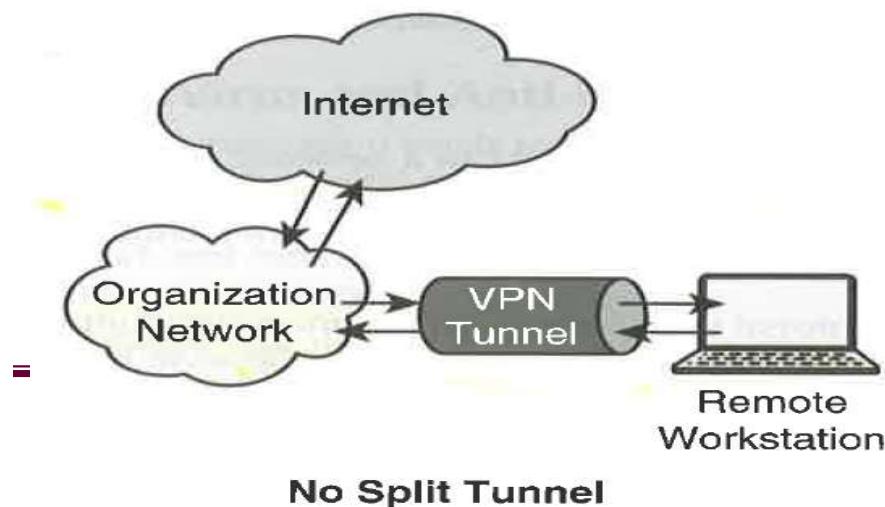
---

- Purpose: ensure that discarded information is truly destroyed and not salvageable by either employees or outsiders
  - Once information has reached the end of its need, its destruction needs to be carried out in a manner that is proportional to its sensitivity
    - Degaussing
    - Shredding
-

# Remote Access

## ❑ Risk mitigation

- Remote client policy
  - Policy regarding company vs non-company owned devices
    - Pros/cons on both
- Remote client security
  - Encryption, strong authentication, anti-malware, firewall, VPN with split tunneling



# Resource Protection

---

- Resources are: facilities, hardware, software, documentation
- Facilities
  - Water and sewage
  - Electricity
  - Fire alarms and suppression
  - Environmental controls
  - Communications
  - Physical security controls

# Resource Protection (cont.)

---

## □ Hardware

- Servers
- Workstations
- Network devices
- Printers, copiers
- Cabling

# Resource Protection (cont.)

---

- Software (proprietary)
  - Usage access control
    - Licensing and distribution
  - Source code access control
    - Confidentiality control
      - Intellectual property
      - Vulnerability exposure
    - Integrity control

# Resource Protection (cont.)

---

## □ Documentation

- **Access control**
  - May contain trade secrets and sensitive information
  - Processes, procedures, and instructions
- **Version control**

# Security Incident Response

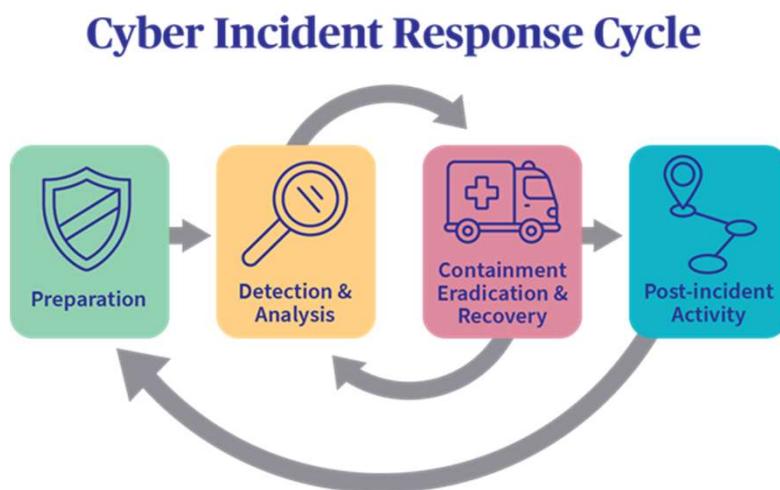
---

- Discipline of creating coordinated response plans in advance of an incident.
  
- Security incident
  - Violation of security policy
  - Causes interruption in normal operations.
    - Can vary in scope, criticality and impact

# Phases

---

- Incident declaration
- Triage
- Investigation
- Analysis
- Containment
- Recovery
- Debriefing



# Incident Declaration

---

- Must be done as soon as someone is aware
- Triggers of incident declarations
  - Observed
    - Apparent malfunctions and outages
    - Obvious malicious activities
  - Reported
    - Threat or vulnerability alerts
    - Customer notification
    - News media notification

# Triage, Investigation, Analysis

---

- Triage
  - Identification clues/information
- Investigation
  - Focused/directed study
  - Assignment of experts
- Analysis
  - Deeper thorough study
    - What really happened
    - How did it happen
    - What is the scope
    - How can it be contained

# **Containment**

---

- Halt the incident
- Prevent further spread or damage
- Prevent its recurrence
- Maybe 1<sup>st</sup> step in incident response depending on criticality
  - May have to collect evidence before commencing containment

# Recovery

---

- Restoration to pre-incident condition
  - Remove unwanted programs and data
  - Repair / replace hardware
  - Reinstall OS or application software
  - Restore damaged / missing data
  - Include measures to prevent recurrence

# Debriefing

---

- Reflect on what happened and on its response
- Propose improvements
  - Technical architecture
  - Technical controls
  - Processes and procedures
  - Security incident response itself
- Preventive measures
  - Strengthen defense in depth strategy to protect assets
  - Strengthen vulnerability and threat awareness capability
    - External alerts, internal issues, IDS/IPS/Honeynets

<https://www.darkreading.com/vulnerabilities---threats/9-sources-for-tracking-new-vulnerabilities/d/d-id/1327186>

---

# Incident Response Training, Testing, and Maintenance

---

- Four types of tests
  - Procedure review
  - Formal training
  - Incident walkthrough
  - Incident simulation

# Incident Reporting Outside of Organization

---

- Reluctance to contact Law Enforcement
  - Embarrassment
  - Disruption of services
  - Difficulty of prosecution
- Required by Law
  - State Security Breach Notification Laws
  - Federal Information Security and Security Breach Notification Laws

# Incident Response Models

---

- **CERT Coordination Center (CERT/CC).**  
<http://www.cert.org/certcc.html> .
  - **Forum of Incident Response and Security Teams (FIRST).**  
[www.first.org](http://www.first.org).
  - **National Institute of Standards and Technology (NIST) special publication 800-61, Computer Security Incident Handling Guide.**  
[www.nist.gov](http://www.nist.gov) .
-

# Example Incident Reporting Plans

---

- <http://www.sans.org/score/incidentforms/>
- <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1506371074.pdf>
- <https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Incident-Response-Plan-template.doc?la=en>

# Incident Reporting Exercises

---

- <https://www.crn.com/slideshows/security/the-10-biggest-data-breaches-of-2021-so-far->
  
  - Fill out Incidence Response Forms for one selected attack
-

# **Risk and Security Management**

---

CSC 3570  
IT Security  
Fall 2021

## **Slide Source:**

**CISSP Guide to Security Essentials, Gregory, Peter, Chapter 1: Security Management Concepts**

**Fundamentals to Information Systems Security, Kim and Solomon, Chapter 1**

---

# Security Management

---

## Strategic level activities

- Governance
- Policy, guidelines, standards, and procedures
- Roles and responsibilities
- Service level agreements
- Secure outsourcing
- Data classification and protection
- Certification and accreditation
- Internal audit

# Governance

---

- Defined: “***Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.***”

– IT Governance Institute

# **Governance Involves**

---

- Provide strategic direction**
  - **Support of risk management**
  - **Support of policies**
  - **Resource allocation and prioritization**
  
- Steering committee/Executive oversight**
  - **Decisions/directions follow up**
  - **Status reporting**

# Policies, Requirements, Guidelines, Standards, and Procedures

---

- Policies: **constraints** of behavior on systems and people. Defines *what, but not how.*
    - Effective policy supports mission, approved, communicated, and assessed
  - Requirements: **required characteristics** of a system or process based on policy
  - Standards: what products, process, technology, and methods will be used as **benchmark** to support implementation of policy
  - Guidelines: **recommendations** on *how* to support a policy with standards
  - Procedures: step by step **detail** instructions on *how to use policies, standards and guidelines*
-

# Examples

---

- Policy:**
  - All remote access must be secured.
- Requirement:**
  - Employees must connect securely.
- Standard:**
  - Use of Virtual Private Network.
- Guideline:**
  - Use Ipsec or tls for vpn
- Procedure:**
  - VPN setup procedure, manual

# Examples

---

- Policy:**
  - Corporate resources only available to employees.
- Requirement:**
  - Employees would need to verify identify before accessing corporate resources.
- Standard:**
  - Use of 2 factor authentication systems.
- Guideline:**
  - Use what you know + what you have .
- Procedure:**
  - Employee password setup procedure, user manual, card setup

# Security Policy Categories

---

## Enforcement wise

- Regulatory
- Advisory
- Informative

## Scope wise

- Organization specific
- System specific
- Issue specific

<https://resources.infosecinstitute.com/certification/cissp-prep-security-policies-standards-procedures-guidelines/>

# Types of IT Security Policies

---

- Acceptable use policy (AUP)**
  - Security awareness policy**
  - Asset classification policy**
  - Asset protection policy**
  - Asset management policy**
  - Vulnerability assessment and management policy**
  - Threat assessment and monitoring policy**
  - Other examples**
    - Email policy
    - BYOD policy
    - Network access policy
    - Remote access policy
    - Audit policy
-

# Tech Security Policies

Type	Title
	<a href="#">801 Information Technology Acceptable Use</a>
	<a href="#">802 Access Control</a>
	<a href="#">803 Email Use</a>
	<a href="#">850 Enterprise Information Security</a>
	<a href="#">851 Information Security Roles and Responsibilities</a>
	<a href="#">852 Password Management</a>
	<a href="#">853 IT Change Management</a>
	<a href="#">854 Data Breach Notifications</a>
	<a href="#">855 Data Classification</a>
	<a href="#">856 Data Security and Handling Policy</a>
	<a href="#">862 Password Policy for Service Accounts</a>

# **Roles and Responsibilities**

---

- Formally defined in security policy and job descriptions**
  - **Ownership of assets**
    - **Access to assets**
  - **Protection of assets**
  - **Use of assets**

# **Service Level Agreements**

---

- SLAs define a formal level of service**
- SLAs for security activities**
  - **Security incident response**
  - **Security alert / advisory delivery**
  - **Security investigation**
  - **Policy and procedure review**

# **Secure (Business) Outsourcing**

---

- Subcontracting to a 3<sup>rd</sup> party**
  - Redirect energy to core mission
  - Efficient use of resources
- Risks associated with Outsourcing**
  - Control of confidential information
  - Loss of control of business functions
  - Accountability – the organization that outsources activities is still accountable for their activities and outcomes

# Data Classification and Protection

---

- Components of a classification and protection program
  - Sensitivity levels
    - “confidential”, “restricted”, “secret”, etc.
  - Marking procedures
    - How to indicate sensitivity on various forms of information (digital and paper)
  - Access procedures
  - Handling procedures
    - Storing, backing up, e-mailing, faxing, mailing, printing, transmitting, destruction

# Certification and Accreditation

---

- ❑ Two-step process for the formal evaluation and approval for use of a system
  - *Certification* is the process of evaluating a system against a set of formal standards, policies, or specifications.
  - *Accreditation* is the formal approval for the use of a certified system, for a defined period of time (and possibly other conditions).

# Internal Audit

---

- ❑ **(Self) Evaluation of security controls and policies to measure their effectiveness**
  - Performed by internal staff/contractor
  - Objectivity is of vital importance
  - Formal methodology
  - Required by some regulations

# Security Strategy Revision

---

- Management is responsible for developing the ongoing strategy for security management
- Past incidents can help shape the future strategies
- Determining factors
  - Incidents
  - SLA performance
  - Certification and accreditation
  - Internal audit

# Summary

---

- ❑ An organization's security program should support its mission, objectives, and goals.
  - ❑ *Security governance* is the set of responsibilities and practices related to the development of strategic direction and risk management.
  - ❑ *Security policies* specify the required characteristics of information systems and the required conduct of employees.
  - ❑ *Security roles and responsibilities* define the ownership, access, and use of assets, and the general responsibilities of managers and employees.
  - ❑ Internal audit is the activity of evaluating security controls and policies to measure their effectiveness.
-

# **Risk and Security Management**

---

CSC 3570  
IT Security  
Fall 2021

## **Slide Source:**

**CISSP Guide to Security Essentials, Gregory, Peter, Chapter 1: Security Management Concepts**  
**Fundamentals to Information Systems Security, Kim and Solomon, Chapter 1**

---

# Concepts

---

- How security supports organizational mission, goals and objectives
  - Risk management
  - Security management
-

# Mission

---

- Statement of its ongoing purpose and reason for existence.



[https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcShBJE37-0VLy\\_v2rScCXfNds1yckxSWJie2Zb\\_etHsp22Q7e10](https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcShBJE37-0VLy_v2rScCXfNds1yckxSWJie2Zb_etHsp22Q7e10)

---

# Example Mission Statements

---

- “*Empower and engage people around the world to collect and develop educational content under a free license or in the public domain, and to disseminate it effectively and globally.*”  
– Wikimedia Foundation
  - “*Creates, advances, and applies knowledge to expand opportunity and economic competitiveness*”  
– TN Tech University
  - “*Raise computer and information security consciousness and proficiency of students in using, designing, developing and operating computing technology.*”  
– TTU Cyber Eagles Club
-

# Goals

---

- Articulate specific accomplishments at the long run that will enable the organization to support its mission.
  
  - Observable, measurable
-

# Example Goals for TNTech

---

- “Ready to hire students”
- “Increased jobs in the regions help by Tech alums”

“Creates, advances, and applies knowledge to  
expand opportunity and economic  
competitiveness”

– TN Tech University

# **Example Goals of TTU Cyber Eagles Club**

---

- Cyber conscious community***
- Peer and mentor network***
- Skilled members***

*“Raise computer and information security consciousness and proficiency of students in using, designing, developing and operating computing technology.”*

– TTU Cyber Eagles Club

# Objectives

---

- Statements of activities that the organization wishes to accomplish.
  - Support the organization's goals and fulfill its mission.
  - Specific milestones.
  - Observable and measurable.
-

# Example Objectives for TNTech

---

- “*Increase retention rate by 20% in two years*”
  - “*Reduce student debt*”
-

# Example Objectives of TTU Cyber Eagles Club

---

- Conduct outreach for community*
  - Help members network with peers and security professionals.*
  - Present opportunities of informational sessions in both cyber offense and defense techniques and tools.*
-

# **Mission, Goals and Objectives**

## **Examples with**

### **WiCyS Organization**

---

- Provide an exclusive job board to hire women in cyber**
  - Diversify cybersecurity workforce**
  - Increase representation for 20% women in cyber to 50% women in cyber**
-

# **Mission, Goals and Objectives**

## **Example Scenario**

---

- You want to create a non-profit organization that enables Tech volunteers to give their times to educate senior citizens about cyber safety.
  
  - Write mission, 2 goals and 2 objectives.
-

# **Security Support of Mission, Goals and Objectives**

---

- Mission, goals, objectives influence the need to protect the organization's assets.**
- Security (or lack of security) influences development and accomplishment of mission, goals, objectives**
  - Risk management
  - Security management

# Risk Management

---

- “*The process of determining the **maximum acceptable level** of overall risk to and from a proposed activity, then using risk assessment techniques to determine the initial level of risk and, if it is excessive, ...”*
  
- “*...developing a strategy to ameliorate appropriate individual risks until the overall level of risk is reduced to an acceptable level.”*

- STEPS:
    - Risk assessment
    - Risk treatment
-

# Risk Assessment

---

## □ Why needed

- To determine
  - current baseline
  - cost effectiveness of security controls

## □ Process

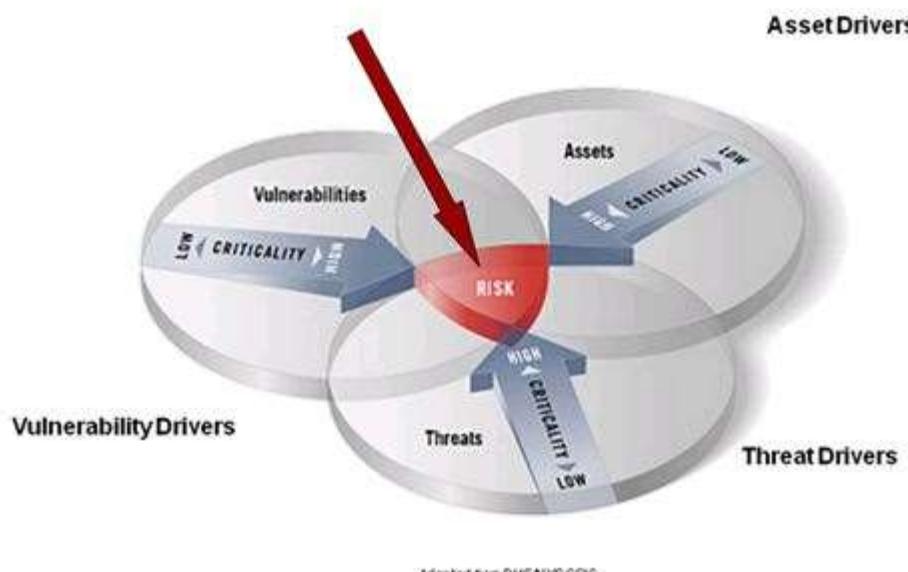
- Identify Risk
  - Evaluate Risk
    - Risks are measured based on asset value, importance, impact, likelihood
    - Risks are prioritized accordingly
-

# Risk Identification

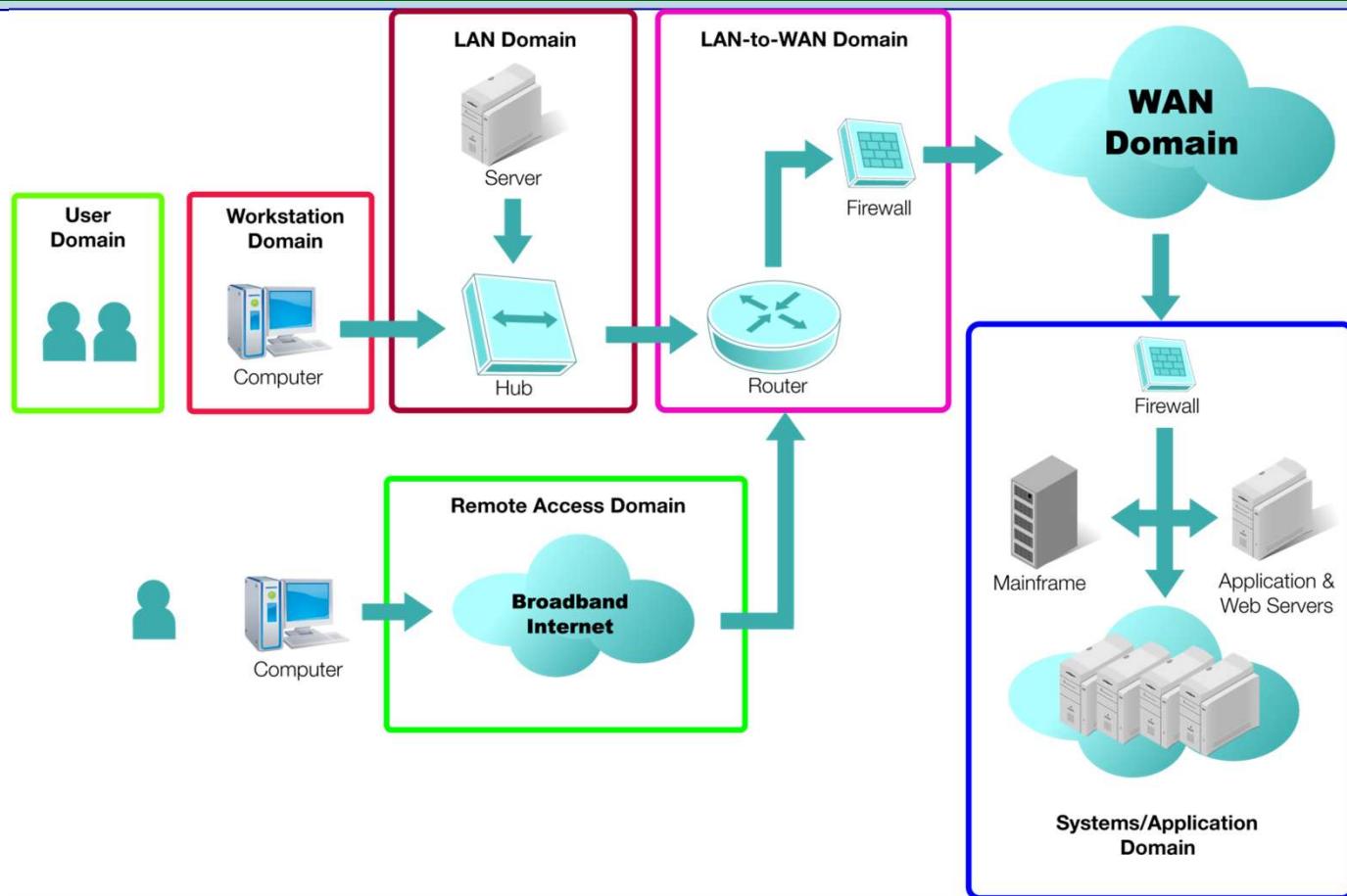
- For a given scope of assets, identify:

- Vulnerabilities
- Threats

Legal Drivers (Bounding the acceptable levels of risk)



# Seven Domains of a Typical IT Infrastructure



# **Risk Evaluation**

---

- Analyze and describe risks in measurable way**
  - Types**
    - Qualitative**
    - Quantitative**
-

# **Qualitative (Subjective) Risk Analysis**

---

## **□ Based on opinion reflecting upon historical data**

Risk level = Subjective measure of probability AND impact

## **□ Probability**

- Likelihood a threat will exploit a vulnerability

## **□ Impact**

- Result if a risk occurs

## **□ Example:**

- If the likelihood that a malware might infect a employee's workstation is high and if the impact is high, then the risk is very high.
-

# Qualitative (Subjective) Risk Analysis

---

Threat	Impact	Probability	Risk	Risk
Flooding	H	L		M
Theft	H	L		M
Earthquake damage	M	M		H
Logical intrusion	H	M		VH

— — — — —

# Quantitative (Objective) Risk Analysis

- Based on asset value (loss and income)
- Annual loss expectancy (ALE)
  - Expected loss for a year

$$\text{SLE} \times \text{ARO} = \text{ALE}$$

- Single loss expectancy (SLE)
  - Total loss expected from a single incident
  - Asset value times Exposure Factor (EF)
    - Exposure : portion of asset damaged
  - $\text{SLE} = \text{Asset (\$)} \times \text{EF (\%)}$
- Annualized rate of occurrence (ARO)
  - Number of times an incident is expected to occur in a year

# Example of Quantitative Risk Assessment

---

## Dropping a laptop computer

- Asset value: \$4,000
- Exposure factor: 50%
- $SLE = \$4,000 \times 50\% = \$2,000$
- ARO = 10% chance of dropping in a year
- $ALE = 10\% \times \$2,000 = \$200$

## Theft of a laptop computer

- Asset value: \$4,000
- Exposure factor: 100%
- $SLE = \$4,000 \times 100\% = \$4,000$
- ARO = 3% chance of theft in a year
- $ALE = 3\% \times \$4,000 = \$120$

## Total Risk Value:

- $\$200 + \$120 = 320$

# Risk Assurance

---

## Assessment of control strategies/countermeasures

- Selection of control strategies/countermeasures depends on
  - Cost &
  - Effectiveness
    - Changes in EF
    - Changes in ARO
- Cost effectiveness evaluation

**Value of safeguard/security control to the company ==**  
**(ALE before implementing safeguard/security control) – (**  
**(ALE after implementing safeguard/security control) +**  
**(annual cost of safeguard/security control)**

<http://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849?show=quantitative-risk-analysis-step-by-step-849&cat=auditing>

---

# **Risk Assessment Methodologies/Standards**

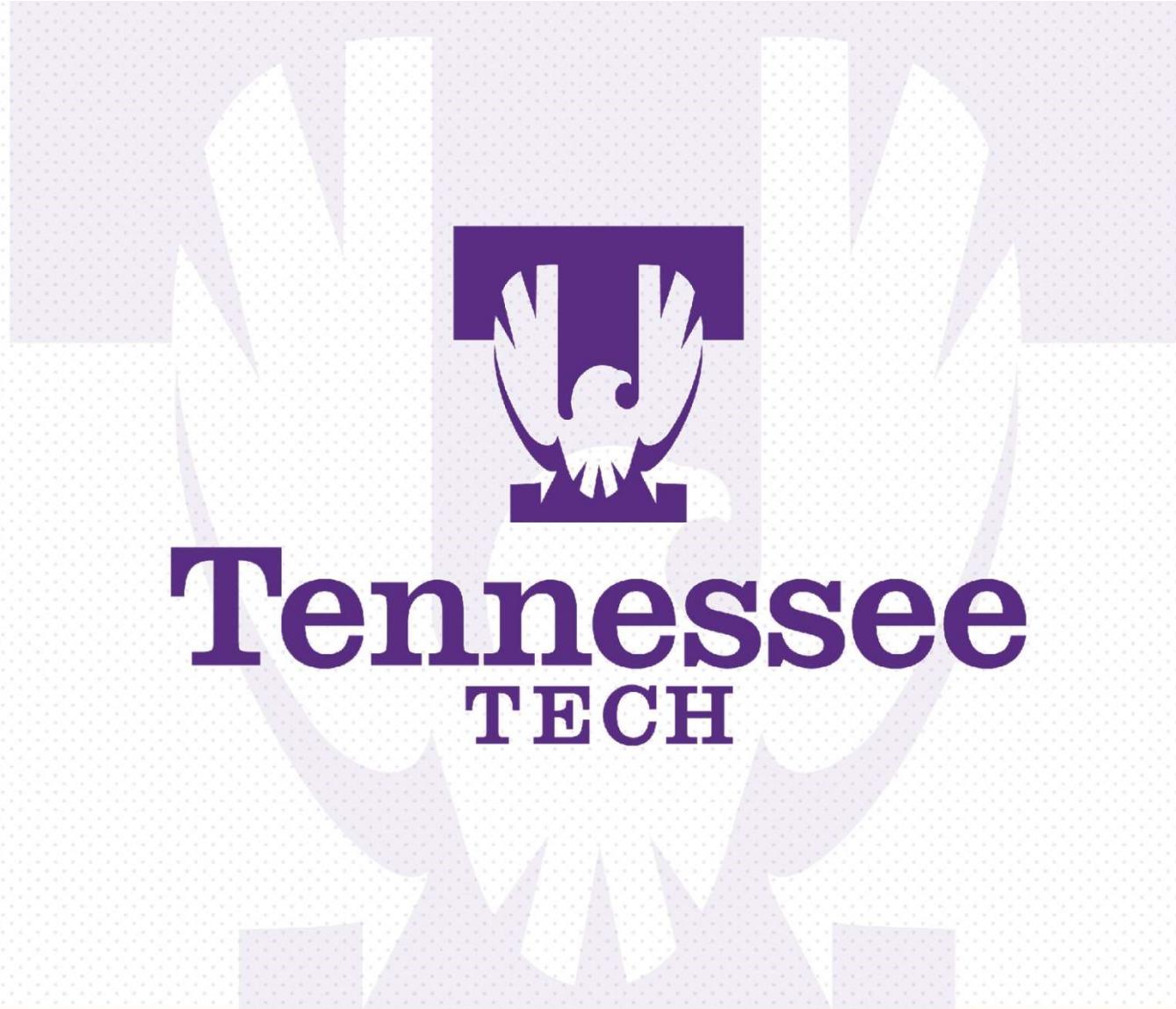
---

- NIST 800-30, Risk Management Guide for Information Technology Systems**
    - NIST Cybersecurity Framework
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
  - FRAP (Facilitated Risk Analysis Process) – qualitative pre-screening**
  - CRAMM (CCTA Risk Analysis and Management method)**
  - Spanning Tree Analysis – Visual**
-

# Risk Treatment/Mitigation

---

- Risk acceptance
    - Taking conscious decision to accept the consequences IF undesirable events occur
  - Risk avoidance
    - Not taking the risk at all
  - Risk reduction
    - Using security controls for potential prevention
  - Risk transference
    - Delegating controls to another entity
-



Department of Computer Science



# Wireless Networking and Security

Department of Computer Science



# Wireless Standards



# Wireless Technology Background

- If you look at the big picture, wireless technology is a wireless hub featuring two-way communication over the same frequency using radio frequencies instead of copper wire.
- These configuration are environmentally vulnerable given that physical surroundings, other EM interference, and even humidity can affect its ability to work correctly.
- Higher radio frequencies, higher data rates, shorter distance
- Lower radio frequencies, lower data rates, longer distance
- Three unlicensed bands for public use: 900MHz and 2.4GHz (Industrial, Scientific, and Medical (ISM) bands), 5GHz (Unlicensed National Information Infrastructure (UNII) band)



4

# 802.11 Standards

- IEEE 802.11 was the original standard operating at 1Mbps and 2Mbps in the 2.4GHz ISM band. The following are amendments to this standard.
- This is not an all-inclusive list. For a more complete list, refer to Wikipedia's 802.11 page at [https://en.wikipedia.org/wiki/IEEE\\_802.11](https://en.wikipedia.org/wiki/IEEE_802.11).
- Note: 802.11f and 802.11t are standalone documents.
- Fun Fact: About 70% of the published bandwidth for a standard is used for management of the wireless network itself. The remaining 30% is called goodput as it is the portion which actually does the work for the end user.



# Some Standards to Remember

- 802.11b
  - Operates in the 2.4GHz ISM band at a max data rate of 11Mbps
  - Was the first commercially popular wireless standard
  - Ability to data-rate-shift {11Mbps, 5.5 Mbps, 2 Mpbs, 1Mpbs}
  - Uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
  - Can also use Request to Send / Clear to Send (RTS/CTS), similar to a TCP handshake except there are four steps {RTS, CTS, Data, ACK}



6

# Some Standards to Remember (cont.)

- 802.11g
  - Operates in the 2.4GHz ISM band at a max data rate of 54Mbps
  - Was the commercial successor to 802.11b (and backward compatible to 802.11b)
  - Ability to data-rate-shift from 54Mbps down to 1Mbps in steps
  - Uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) at 11Mbps and below
  - If only one 802.11b device connects to an 802.11g AP, the entire AP must downgrade to 802.11b to accommodate all clients
    - Orthogonal Frequency Division Multiplexing (OFDM)
    - Direct Sequence Spread Spectrum (DSSS)



7

# Some Standards to Remember (cont.)

- 802.11a
  - Operates in the 5GHz UNII band at a max data rate of 54Mbps
  - Was not commercially available until 2001 and costly preventing it from being widely adopted
  - Ability to data-rate-shift from 54Mbps down to 6Mbps in steps
  - Immune to interference from all of the devices working at 2.4GHz including things like microwave ovens, old cordless phones and Bluetooth devices
  - Not compatible with b/g equipment



8

# Some Standards to Remember (cont.)

- 802.11h
  - Operates in the 5GHz UNII band at a max data rate of 54Mbps
  - A revision of 802.11a
  - Includes the following new features:
    - **Dynamic Frequency Selection (DFS)** – monitors for radar signals and devices operating in the 5GHz frequency, will abandon an occupied channel or mark it as unavailable
    - **Transmit Power Control (TPC)** – allows client and access point to negotiate transmit power thereby reducing the amount of power required to maintain the link while also consolidating active airspace to avoid interference with other devices



9

# Some Standards to Remember (cont.)

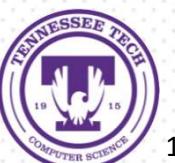
- 802.11n
  - Operates in the 2.4 GHz ISM band and 5GHz UNII band at a max data rate of 108 Mbps
  - Utilizes Multiple-Input, Multiple-Output (MIMO) over up to eight “smart” antennas allowing for simultaneous transmission and reception by dividing the load over the antennas.
  - MIMO allows for frames to be sent by several antennae over several paths which are then recombined by another set of antennae optimize throughput and multipath resistance. This is called spatial multiplexing. (Lammle definition). Up to four spatial streams are used
  - Utilizes block acknowledgement rather than requiring an acknowledgement for every frame.



10

# Some Standards to Remember (cont.)

- 802.11ac
  - Operates in the 5GHz UNII band at a max data rate of 1 Gbps
  - Utilizes Multiple-Input, Multiple-Output (MIMO) over up to eight “smart” antennas allowing for simultaneous transmission and reception by dividing the load over the antennas.
  - Used wider channels (up to 160MHz wide) using a sliding scale {80, 40, 20 MHz) depending on interference.
  - Utilizes block acknowledgement rather than requiring an acknowledgement for every frame.



11

# Wireless Technology

Department of Computer Science



12

# A Little More About the Hardware

- Wireless Access Points (WAP or AP) consist of
  - One or more antennae
  - Wired Ethernet adapter
  - Power input (if not PoE)
- Current APs have additional bridging and routing functions built into the units as compared to their early generation ancestors.
- Antennas can be categorized as omni-directional (point-to-multipoint) or directional/Yagi (point-to-point)



13

# Wireless Networks

- Ad Hoc Mode – Independent Basic Service Set
  - Individual devices communicate in a peer-to-peer fashion (think AirPrint from a mobile device to a printer)
  - Definitely not scalable
- Infrastructure Mode – Basic Service Set
  - Area covered by the AP is called the basic service area (BSA)
  - Devices communicate with the AP only
  - Connection between the AP and wired network is called the distribution system (DS)
  - AP is identified by a service set identifier (SSID)
  - Overlapping of BSAs which allow client roaming creates an extended service set (ESS)



14

# Wireless Controllers

- Typical, stand-alone APs have a full operating systems loaded on the device.
- In enterprise environments, controller-based systems may be used to provide for better management of all the APs included in the wireless solution.
- In a controller-based system, APs use a **split MAC** system. The AP runs a lightweight OS (sometime referred to as thin AP) while the controller runs a full OS complete with management software which interacts with the individual APs. Some APs can work in a hive model allowing for some autonomous systems to be regionally created.
- Controllers and APs communicate via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. This has largely replaced the older, proprietary Lightweight Access Point Protocol (LWAPP).



15

# Mobile Hot Spots

- Mobile Hot Spots allow alternate data networks to be used to support Wi-Fi networks.
- Hot spots may be facilitated by a specialize device or by a common device such as a smartphone.
- The reverse of this idea has also been used to support improved cellular signal in areas where commercial cell signal is week by plugging a micro-tower into a wired, Ethernet network and passing voice packets to a gateway on the Internet.



16

# Other Wireless Networks

- There are many types of networks which are categorized based upon the size and geographic location served. You can see a very interesting map of network sizes in the Wikipedia article on Computer Networks at [https://en.wikipedia.org/wiki/Computer\\_network](https://en.wikipedia.org/wiki/Computer_network).
- Personal Area Networks include:
  - Bluetooth
  - Infrared (IR)
  - Near-Field Communication (NFC)



17

# Bluetooth Design and Security Concerns

- Operates at 2.4 GHz
- Bluetooth networks are called piconets. When piconets are connected via common devices, it is called a scatternet.
- Depending on radio class, Bluetooth devices can have a range between 65 ft and 300 ft.
- Attacks
  - **Bluesnarf** – exploit of OBEX to grab info from a device
  - **Bluejacking** – exploit of OBEX to inject information into a device
  - **Blue Bug** – use of a vulnerability to issue commands into smartphones
  - **Evil Twin** – attacker uses a device to simulate a Bluetooth access point



18

# Site Survey

- Site surveys are an essential part of any large, wireless network deployment.
- Until you fully understand the environment in which a wireless network will operate, you cannot intelligently design the network.
- Considerations such as walls, building materials, wire plant, adjacent businesses, size of population, etc. must be evaluated.
- Once logistical information is gathered, an actual site survey measuring signal strength can be performed using a variety of tools.
- Once the installation is complete, a post-deployment site survey must be completed to determine the success of the initial plan and to make modifications to address any remaining issues. Heat maps can be created to have a visual of actual coverage and determine where additional APs should be added or removed in the case of signal interference.



19

# Wireless Security

Department of Computer Science



20

# Wireless Security Protocols

- Wireless networking relies on the transmission of radio signals through open air where anyone with appropriate receiving equipment can listen.
- In order for this medium to be practical in modern networking, cryptographic and signal management solutions must be developed to allow for widely acceptable use in production network environments.
- Like other security solutions, a layered approach of multiple protocols may be used (some with backward compatibility)



21

# Wireless Security Protocols

- **Wired Equivalent Privacy**
  - An IEEE 802.11 security protocol designed to ensure that only authorized clients can view transmitted wireless information
  - Accomplishes confidentiality by encrypting transmissions
  - Relies on a shared secret key known by the client and AP
  - The shared secret key consists of
    - A 24-bit initialization vector (IV)
    - A 40-bit or 104-bit default key
  - The combined shared secret key (IV + default key) can be either 64-bit or 128-bit. The key is used to create a random number of the encryption process.



22

# WEP by the steps

- Host A, the AP, and Host B all have the shared key before a transaction can begin.
- Host A combines the IV and shared key bits to create a random number for encryption of the plain text.
- Host A sends the IV and encrypted ciphertext to Host B via the AP.
- Host B separates the IV from the encrypted ciphertext.
- Host B combines the IV with its copy of the shared key to decrypt the ciphertext.



# Problems with WEP

- WEP can only use a 64-bit or 128-bit number (of which 24-bits are used for the IV). The short IV limits the strength of the encryption.
- WEP contains a detectable encryption pattern. Since the IV is only 24-bits, there are only 16,777,216 possible values.
- An AP transmitting at 11 Mbps can send and receive 700 packets each second. Using a different IV each time, the AP would create duplicate IV within 7 hours.
- An attacker’s “listening” to traffic for this duration of time could see the duplication and crack the code.



24

# **WPS – Wi-Fi Protected Setup (a dumber WEP)**

- Created for ease of configuration for consumer Wi-Fi products, WPS worked in one of two ways
  - A PIN was printed on a sticker on the side of the router for entry into the connect device
  - The user could push a button (yes, a real button)
- Problems
  - No lockout limit on enter a PIN
  - The last PIN character is a checksum
  - The wireless router reports the validity of the first (four characters) and second (three characters) of the PIN meaning that an attacker only had to guess a four and three character PIN. There were only 11,000 unique PINs.



25

# WPA – Wi-Fi Protected Access

- Two versions
  - WPA Personal (home/SOHO)
  - WPA Enterprise
- Addresses both encryption and authentication
- Implementation fit into the existing WEP engine as to not require hardware upgrades (only software/firmware upgrades)
- Used Temporal Key Integrity Protocol (TKIP) for encryption (wrapping WEP's basic functionality)
- IV was increased from 24 bits to 48 bits, shared key from 64 bits to 128 bits
- Created keys “per packet”
- Includes a Message Integrity Check (MIC)



26

# WPA – Wi-Fi Protected Access

- Preshared Key (PSK) Authentication – a secret value entered on participating devices and APs
- Served as only an interim solution to the problems of WEP
- Constrained by original design of WEP
- Secret key distribution and maintenance was still a struggle
- PSK passphrases could be 8 to 63 characters in length (anything less than 20 characters were subject to brute force cracking)



27

# WPA2 – Wi-Fi Protected Access 2

- Was a complete implementation of IEEE 802.11i (mostly, 802.11i did not allow the use of TKIP)
- Like its predecessor, it had WPA2-Personal and WPA2-Enterprise
- Addressed further issues with encryption and authentication
- Encryption was based upon the Advanced Encryption Standard (AES) block cipher.
- The full name for WPA2 encryption is Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) sometimes designated AES-CCMP.



28

# **WPA2 – Wi-Fi Protected Access 2**

- Authentication for WPA2 Enterprise is implemented as IEEE 802.1x.
- Extensive Authentication Protocol (EAP) (NIST 800-97) is a framework for transporting authentication protocols. Served as a better replacement for Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).
- EAP framework define four types of packets: request, response, success, and failure.
- EAP-TLS uses the Transport Layer Security protocol using digital certificates for authentication



29

# Threats to Wireless Networks

- **Rogue APs (two categories of threats)**
  - **Rogue AP** – an unauthorized wireless access point connected to a wired LAN allowing unmonitored access to the network
  - **Evil Twin** – a man-in-the-middle attack where an access point pretends to be a part of the legitimate WAN for the purpose of siphoning network information
  - Threat can be mitigated via CAPWAP and Radio Resource Management (RRM), assists in location of the rogue and can send a termination signal
- **Ad Hoc Networks**
  - Peer-to-peer networks dynamically created for information sharing where wired LAN information could be leaked by a network member with both a wired and wireless connection
  - mitigated through vendor-provided tagging



30

# Threats to Wireless Networks

- **Key Cracking**

- The process of using tools to sniff a large number of wireless network packets to crack and derive the encryption key (Aircrack, AirSnort, WEP Crack)
- Mitigated by the use of strong passkeys and WPA2

- **Denial of Service (DoS)**

- The process of overwhelming an access point with 802.1x handshake attempts, 802.1x authentication attempts, a flood of legitimate traffic, and radio signal jamming measures
- Mitigated via Management Frame Protection (MFP)

- **Wardriving**

- The practice of driving around looking for and mapping insecure WLANs (e.g. creepy people hanging out in your parking lot with a laptop).



31

# Threats to Wireless Networks

- **ARP Poisoning**
  - WLANs cannot typically verify that an ARP reply sent by a host was in response to a valid ARP request from another host allowing an attacker to establish a man-in-the-middle attack. Requires that the attacker poison the ARP cache of at least two wireless clients.
  - Mitigated by wireless traffic encryption
- **Misassociation (2 forms)**
  - Accidental Association – computer attaches to an adjacent network
  - Malicious Association – using a “Soft AP” to deceive a client
- **Passive Attacks (general deception attacks)**
  - mitigated through WIDS or WIPS



32

# Additional Security Mechanisms

- Captive Portal AP – forces a potential client to authenticate through a single portal agreeing to an acceptable use policy
- Rouge AP Discovery and Mitigation Tools
- Site Surveys
- Virtual Private Networks (for end-to-end encryption)



33

# Wireless Security Myths

- MAC filtering – Listing only the MAC address of the devices allowed on the network fails for anything bigger than SOHO; an attacker can acquire a valid MAC and enter the network with enough sniffing data.
- SSID hiding – While the SSID may not show up in a public list, all devices cache the names of SSID to which they are attached; multiple tools are available to find these SSIDs.
- Disable DHCP – Using static IP address on all devices is not manageable and will not keep a seasoned hacker out of your network.
- Signal suppression – The altering of power to AP antennae and positioning APs away from exterior walls will only keep novices out of the network. Experienced attackers can purchase specialized antennas to improve the gain of weak signals.



34

# Good Things to Read

- IEEE 802.11 series [https://en.wikipedia.org/wiki/IEEE\\_802.11](https://en.wikipedia.org/wiki/IEEE_802.11).
- Wikipedia's Wireless Security [https://en.wikipedia.org/wiki/Wireless\\_security](https://en.wikipedia.org/wiki/Wireless_security)
- DHS – A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family) [https://us-cert.cisa.gov/sites/default/files/publications/A\\_Guide\\_to\\_Securing\\_Networks\\_for\\_Wi-Fi.pdf](https://us-cert.cisa.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf)
- NIST SP 800-121 Guide to Bluetooth Security [https://us-cert.cisa.gov/sites/default/files/publications/A\\_Guide\\_to\\_Securing\\_Networks\\_for\\_Wi-Fi.pdf](https://us-cert.cisa.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf)
- NIST SP 800-97 Establishing Wireless Robust Security Networks <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-97.pdf>
- CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition, Ciampa, Chapter 9, Wireless Network Security
- Guide to Network Security, Whitman, Mattford, Mackey, Green, Chapter 7, Wireless Network Security



35

# **IDS and IPS**

---

**CSC 3570  
IT Security  
Fall 2021**

## **Slide Source:**

**Computer Security, Principles and Practice, William Stallings and Lawrie Brown, 2008, Chapters 6 and 9**  
**Introduction to Computer Security, Matt Bishop, Addison Wesley, 2019, Chapter 22**  
**Security Warrior, Cyrus Peikari and Anton Chuvakin, 2004, Chapter 19**

---

# Concepts

---

## ❑ Intrusion

- A security incident or a combination of multiple such by which an unauthorized user gains access or attempts to gain access to a system or resource

## ❑ Intrusion detection

- A security service that monitors and analyzes system events for the purposes of finding and providing indications of probable intrusions
  - Can detect inappropriate or anomalous activity

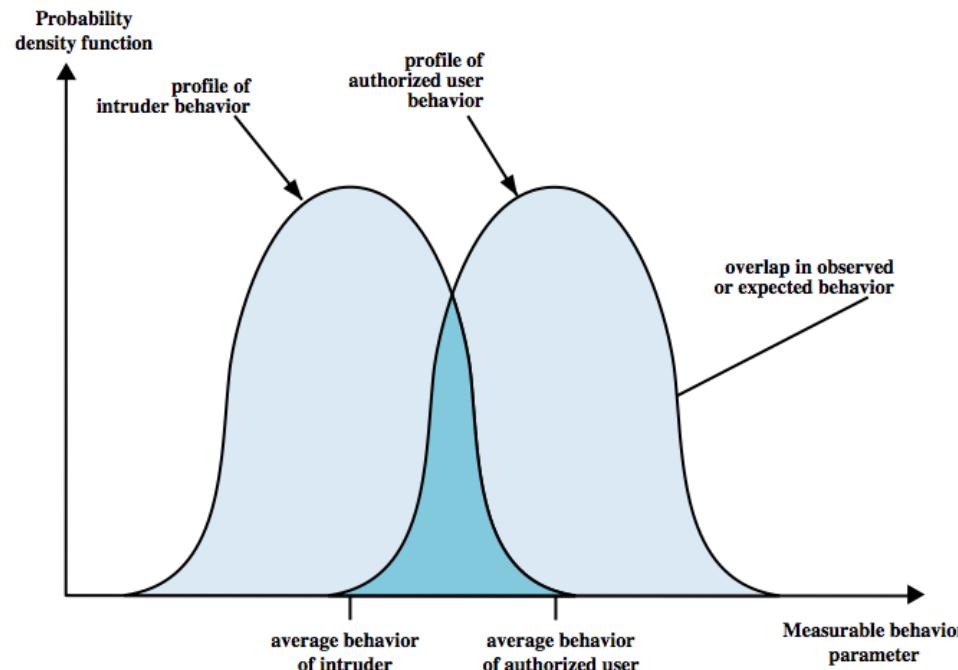
# Basis of Intrusion Detection Systems (IDS)

---

- ❑ Systems under attack/intrusion DO NOT MEET at least one of these normal system conditions
    - Process actions correspond to a set of specifications describing what the processes are allowed to do
    - User, process actions conform to predictable normal pattern
    - User, process actions do not include sequences of malicious actions that subvert the security policy
-

# IDS Principles

- ❑ Intruder behavior differs from legitimate users
  - Can have overlaps as shown



# Sensitivity vs Specificity

---

- Must compromise between these

Defining loosely (sensitivity)

$$\text{Sensitivity} = \text{TP rate} = \text{TP} / (\text{TP} + \text{FN})$$

$$\text{Specificity} = \text{TN rate} = \text{TN} / (\text{TN} + \text{FP})$$

$$\text{FN rate} = 1 - \text{Sensitivity}$$

$$\text{FP rate} = 1 - \text{Specificity}$$

		<i>Intrusion</i>	
		+	-
<i>IDS response</i>	+	TP	FP
	-	FN	TN

TP = true positive (intrusion correctly detected)

FP = false positive (false alarm)

FN = false negative (intrusion missed)

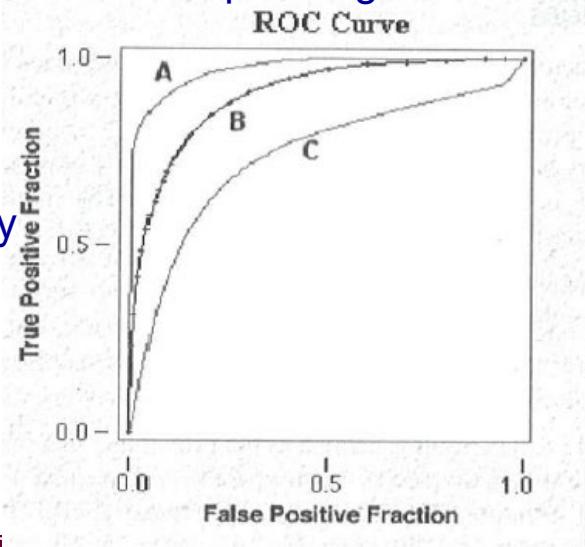
TN = true negative (integrity correctly detected)

---

# IDS Accuracy

- ❑ Depends on sensitivity and specificity
- ❑ Accuracy is proportion of all IDS results (both positive and negative) classified/identified as correct.
- ❑ Accuracy rate=

Receiver Operating Characteristics



1 - Specificity

- ❑ Base rate fallacy problem:  
When actual number of users in a system is very high compared to the low number of actual attacks, then false alarms over shadows true intrusions.

# **IDS Types**

---

- Passive**
  - Reports with no overhead but cannot take immediate actions
- Active**
  - Reports with delay but can take immediate actions

# IDS Requirements

---

- ❑ Configured according to system security policies
  - ❑ Detect wide variety of intrusions
  - ❑ Detect intrusions in timely fashion
  - ❑ Present analysis in simple, easy-to-understand format
  - ❑ Be accurate
  - ❑ Run continually
    - Fault tolerant
    - Provide graceful degradation of service
    - Resist subversion
  - ❑ Impose a minimal overhead on system
  - ❑ Adapt to changes in systems and users
    - Allow dynamic reconfiguration
  - ❑ Scale to monitor large numbers of systems
  - ❑ Interoperable with other IDSs
-

# **Models of Intrusion Detection**

---

- Anomaly modeling/detection
  - Misuse modeling/detection
  - Specification modeling
-

# Anomaly Modeling/Detection

---

- Analyzes a set of characteristics of system, and compares their values with expected values; report when computation do not match expectation
    - What is usual, is known
      - What is unusual, may be bad
  - Requires training
  - Can detect variations in attacks or new attacks
-

# Anomaly Detection Techniques

---

- Threshold detection
  - Profile based
-

# Threshold Detection

---

- Checks excessive event occurrences beyond a threshold
  - If number falls outside this range, anomalous
- Example
  - Windows: lock user out after  $k$  failed sequential login attempts. Range is  $(0, k-1)$ .
    - $k$  or more failed logins deemed anomalous
- Problems
  - Deciding on threshold
  - Thresholds vary
  - Thresholds can be manipulated

# Profile Based

---

- ❑ Build profile by characterizing past behavior of users
- ❑ Based on analysis of audit records
  - Gather metrics
    - counter, gauge, time, resource utilization
  - Analyze
    - statistical, AI, heuristics, machine learning
- ❑ Problem: need to train system to establish valid profile
  - Use known, training data that is not anomalous
    - The more training data, the better the model
    - Training data should cover *all* possible normal uses of system

# Misuse Modeling/Detection

---

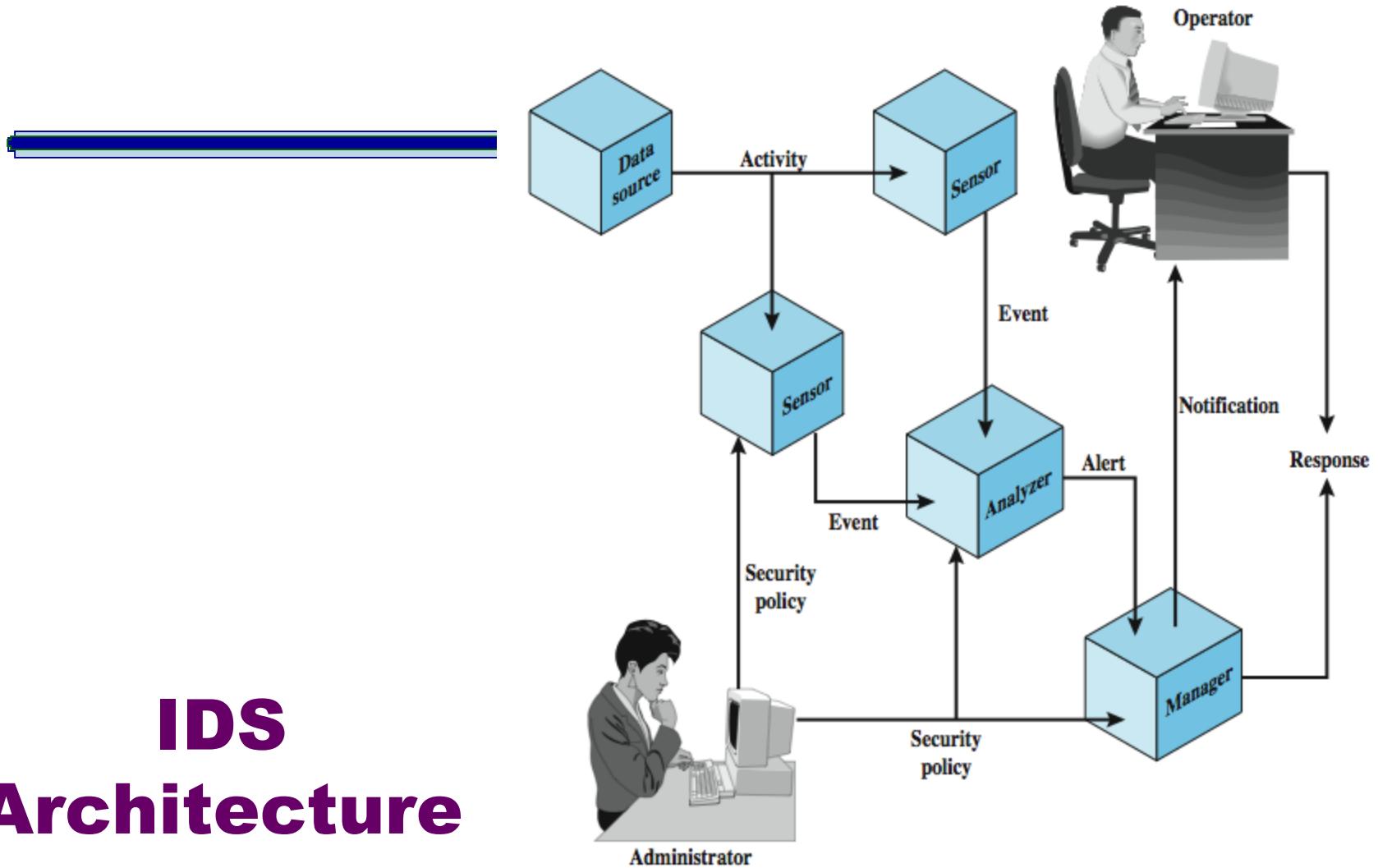
- Descriptions of known or potential exploits grouped into *knowledge*
- IDS matches data against knowledge; on success, potential attack found
  - What is bad, is known
  - What is same, is bad
- Does not require normal profile generation or training
- Cannot detect variations in attacks or new attacks

# Specification Modeling

---

- Descriptions of known states/functions are modelled
- IDS matches data against knowledge; on failure, potential attack found
  - What is specified, is known
  - What is not the same, is bad
- Require knowledge of protection/normal states/functions
- Cannot detect attacks that does not violate what is specified

# IDS Architecture



# **IDS Architecture**

---

- Basically, a sophisticated audit system
    - Sensor/Agent
    - Director/Analyzer
    - Notifier/Manager
-

# Sensors/Agents

---

- Obtains information and sends to director
  - May put information into another form
    - Preprocessing of records to extract relevant parts
  - Collects data
    - On its own
    - On director's request
  - Types
    - Network-based
    - Host-based
-

# Audit Records

---

- A fundamental tool for intrusion detection
- Two variants:
  - Native audit records - provided by all OS
    - Inherent but may not be optimum
  - Detection-specific audit records - IDS specific
    - Additional overhead but specific to IDS task

# **Director/Analyzer**

---

- Filters information from agents**
  - Eliminates unnecessary, redundant records
- Analyzes remaining information to determine if attack under way**
  - Analysis engine can use a number of techniques
    - Statistical
    - AI
      - Pattern matching
      - Neural nets
      - Markov model
      - Fuzzy logic
      - Data mining

# Adaptive Directors

---

- **Modify profiles, rule sets to adapt their analysis to changes in system**
- **Example: use neural nets to analyze logs**
  - **Adapts to users' behavior over time**
  - **Uses learning techniques to improve characterization of events as anomalous**
    - Reduced number of false alarms

# **Notifier**

---

- Accepts information from director**
  - Takes appropriate action**
    - **Notify system security officer**
    - **Respond to attack**
  - Often GUIs**
    - **Use visualization to convey information**
-

# Host-Based IDS

---

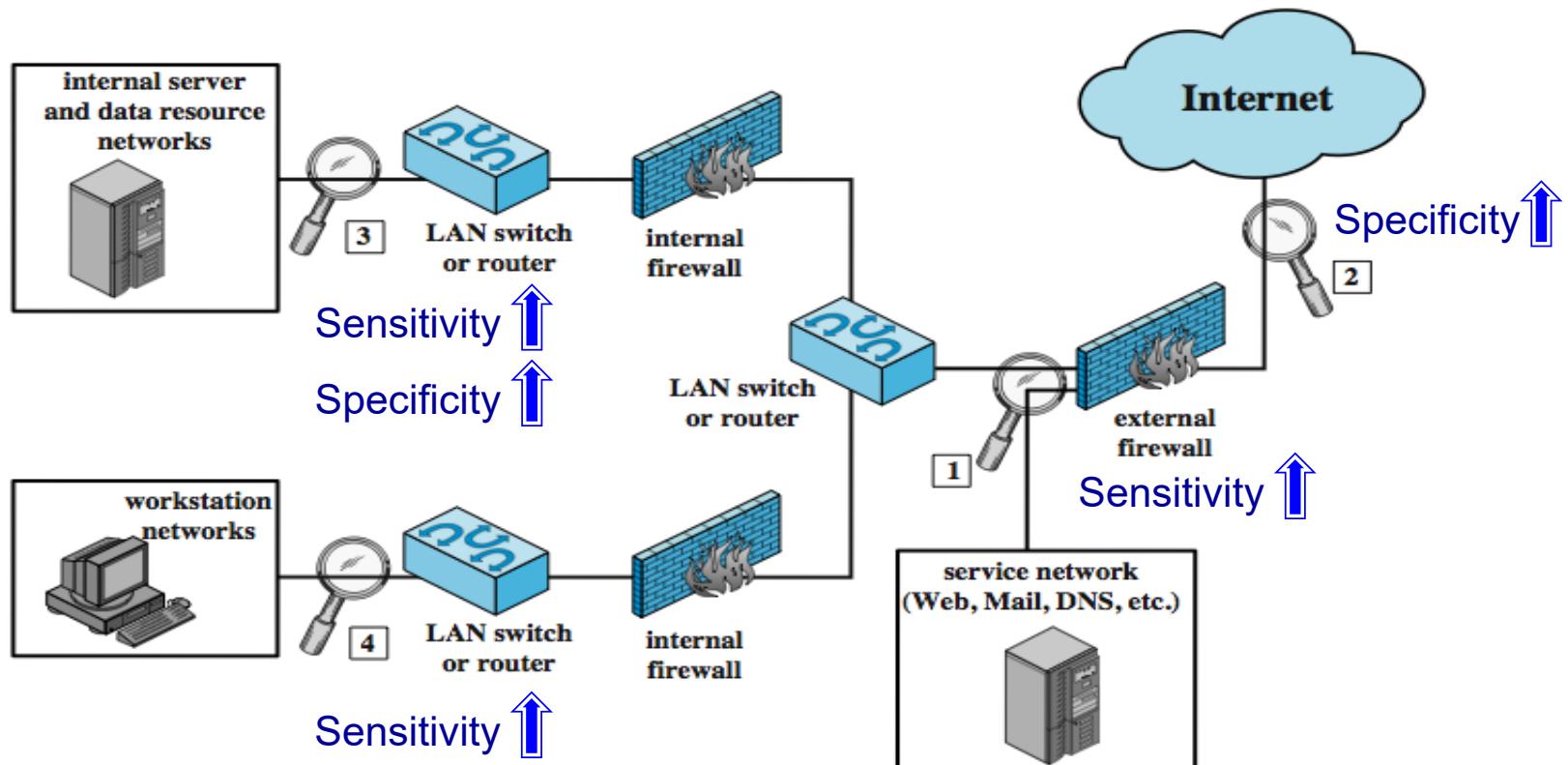
- Monitors single system activity to detect suspicious behavior
  - Obtain information from logs at host machine
  - Typically
    - Can work with encrypted data since it will be decrypted at the host
    - May shed light on success of attack
    - More visibility to internal intrusions
    - Vulnerable to host attacks
    - Consumes resources at host
  - Example:
    - Tripwire
    - Samhain
-

# Network-Based IDS

---

- Obtain information from monitoring traffic (both inbound and outbound) for a large number of hosts
  - May examine network, transport and/or application level protocol activity directed toward systems
  - Types
    - Inline (possibly as part of other net device)
    - Passive (monitors copy of traffic)
  - Typically
    - Provides view of whole network
    - One point of failure
    - Can't work with encrypted data
    - Can't tell if attack was successful
    - Less visibility to internal attacks
  - Example:
    - Snort
    - RealSecure
-

# NIDS Sensor Deployment

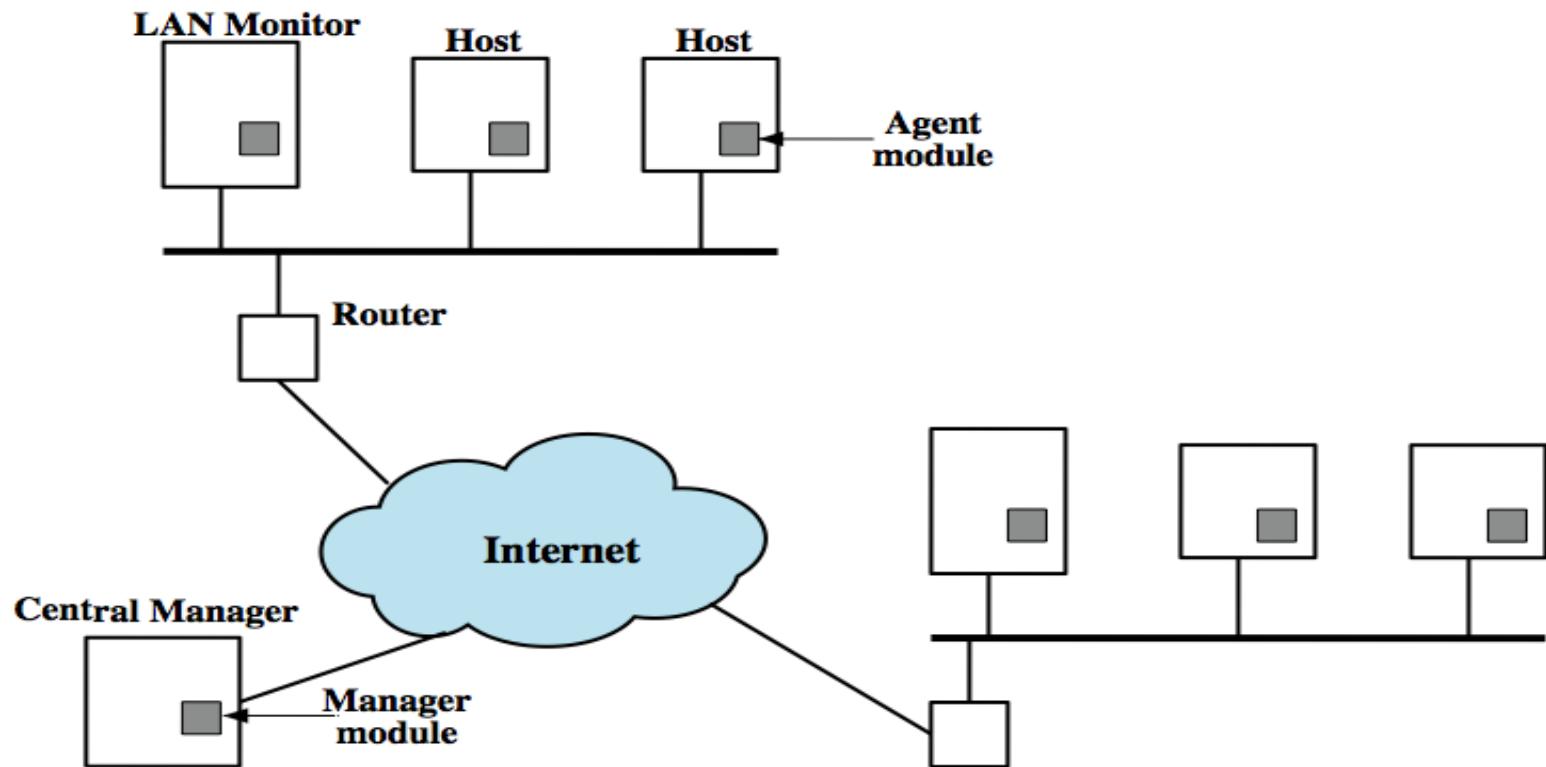


# **IDS Control/Management**

---

- Centralized**
    - Controls are implemented and managed from central location
  - Hierarchical**
    - Data is analyzed as it is passed up through the layers
  - Partially distributed**
    - Centralized reporting of localized analysis
  - Fully distributed**
    - Controls are implemented and managed at each individual location
-

# Distributed (Hybrid Network and Host-Based IDS)



# **IDS is not effective when ...**

---

- it cannot see all traffic
  - IDS is not tuned to its environment
  - limitations of IDS technology are not recognized/addressed
  - no one pays attention to its alerts
  - there is no IDS response policy
-

# Intrusion Prevention Systems (IPS)

---

- **Addition to network devices**
    - adds IDS capabilities to firewall
    - inline to block
    - IPS as itself does not support network functions
  - **May be network or host based**
  - **Underlying detection can be signature or anomaly based**
-

# **Host-Based IPS**

---

- **Can be tailored to the specific platform**
  - e.g. general purpose, web/database server specific
  
- **Can sandbox applets to monitor behavior**
  - May provide file, registry, I/O protection

# Network-Based IPS

---

- **Inline NIDS that can discard packets or terminate TCP connections**
  - **Can provide data flow protection**
    - application payload in a sequence is reassembled before detection
  - **Can identify malicious packets using**
    - pattern matching, stateful matching, AI
-

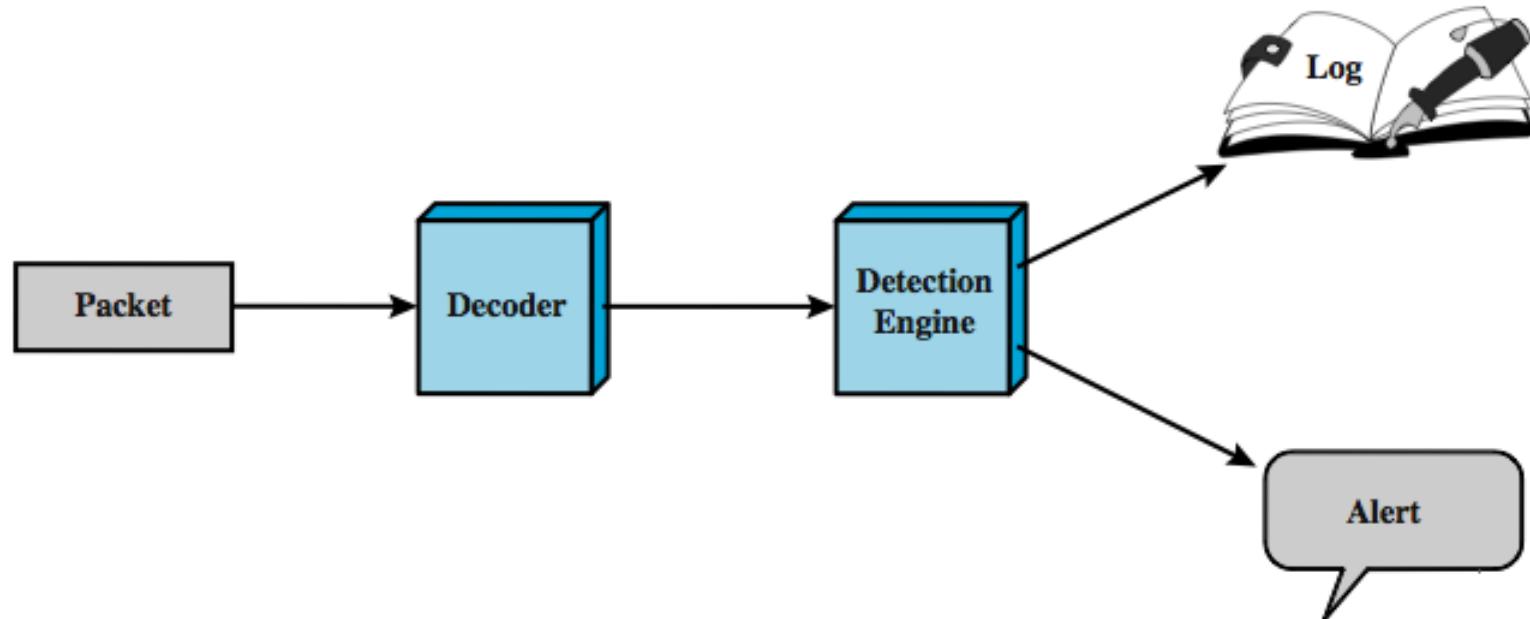
# **SNORT**

---

**Open source signature based IDS (and IPS) – 1998 by Martin Roesch**

- **Lightweight**
    - Highly efficient with small footprint
  - **Real-time packet capture and rule analysis**
  - **Passive (IDS) or inline (IPS)**
  - **Can work on host, server, network device**
  - **Highly configurable**
-

# SNORT Architecture



# SNORT Rule

- Use a simple, flexible rule definition language
- Rule header (Must check)
  - To scan packet headers
  - action, protocol, source IP, source port, direction, dest IP, dest port
- Many options (optional)
  - To scan packet payload in addition to headers
  - What to do after

Action	Protocol	Source IP address	Source port	Direction	Dest IP address	Dest port
--------	----------	-------------------	-------------	-----------	-----------------	-----------

(a) Rule header

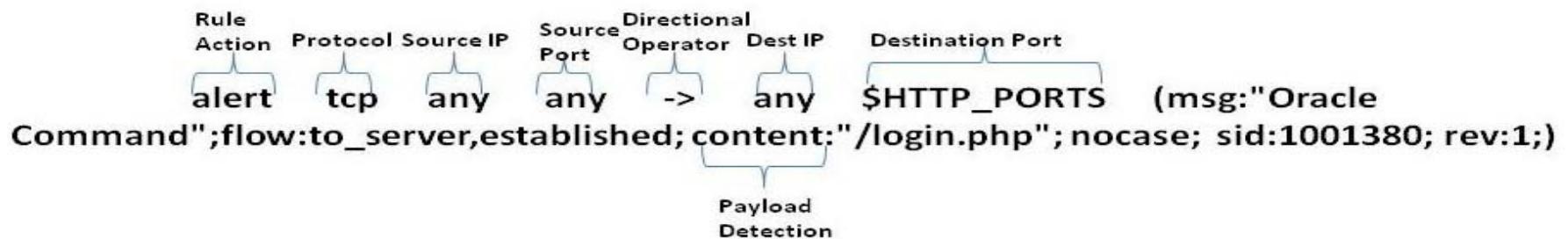
Option keyword	Option arguments	• • •
----------------	------------------	-------

(b) Options

# SNORT Rule Example

## □ Example rule to detect TCP SYN-FIN attack:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```



# SNORT Rule Options Categories

---

- alert tcp 10.1.1.1 any -> 10.1.1.2 80  
**(msg:"foo"; content:"bar";)**
- meat of the detection capabilities
- key value pairs (key:value;)
- types of keywords
- meta-data
- Payload
- non-payload
- post-detection

# **SNORT Rule Option – meta-data**

---

- Msg
  - msg:"my evil attack";
- Reference
  - reference:url,www.snort.org;
- sid
  - sid:100000;
- Rev
  - rev:100000;
- Classtype (see classification.config)
  - classtype:attempted-recon;
- Priority
  - priority:3;

# SNORT Alert Class Types

High Priority Medium Priority Low Priority

Attempted-admin	Attempted-dos	Icmp-event
Attempted-user	<b>Attempted-recon</b>	Misc-activity
Inappropriate-content	Bad-unknown	Network-scan
Policy-violation	Default-login-attempt	Not-suspicious
Shellcode-detect	Denial-of-service	Protocol-command-decode
Successful-admin	Misc-attcak	String-detect
Successful-user	Non-standard protocol	unknown
Trojan-activity	Rpc-portmap-decode	
Unsuccessful user	Successful-dos	
Web-application-attack	Successful-recon-largescale	
	Successful-recon-limited	
	Suspicious-filename-detect	
	Suspicious-login	
	System-call-detect	
	Unusual-client-port-connection	
	Web-application-activity	

# **SNORT Rule Option – payload**

---

- Content
  - content:"foo";
- Nocase
  - content:"foo"; nocase;
- Rawbytes
  - content:"foo"; rawbytes;
- Depth
  - content:"foo"; depth:10;
- Offset
  - content:"foo"; offset:10;
- Uricontent
  - uricontent:"foo";

# **SNORT Rule Option – non-payload**

---

- ack (TCP Acknowledge Number)
  - ack:0;
- dsize (Packet Size)
  - dsize:>10;
- id (IP ID)
  - id:10;
- fragoffset (fragment offset)
  - fragoffset:0;
- fragbits (IP fragment bits)
  - fragbits:MD;

# Writing SNORT Rule Resources

---

- [www.snort.org](http://www.snort.org)
  - [http://www.ussrback.com/docs/papers/IDS/snort\\_rules.htm](http://www.ussrback.com/docs/papers/IDS/snort_rules.htm)
  - <http://resources.infosecinstitute.com/snort-rule-writing-for-the-it-professional/>
  - <http://resources.infosecinstitute.com/snort-rule-writing-for-the-it-professional-part-2-2/>
  - [http://commons.oreilly.com/wiki/index.php/Snort\\_Cookbook/Rules\\_and\\_Signatures](http://commons.oreilly.com/wiki/index.php/Snort_Cookbook/Rules_and_Signatures)
  - [http://snort.datanerds.net/writing\\_snort\\_rules.htm](http://snort.datanerds.net/writing_snort_rules.htm)
-

# SNORT Actions

---

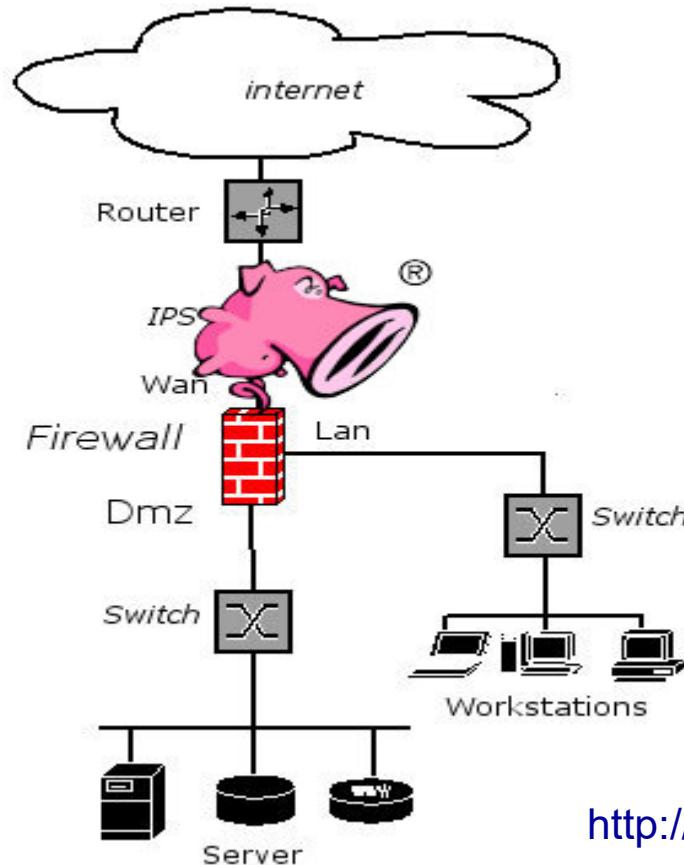
## As IDS

- alert
  - activate
    - dynamic
- log
- pass

## As IPS

- reject
- drop
- sdrop

# SNORT as IPS



<http://www.snortattack.org/node/23>



# **SNORT Support Tools**

---

- Snorby**
  - Snortsnarf**
  - DumbPig**
  - PulledPork** .....
- 
- <https://www.snort.org/>
  - <http://www.snort.org/snort-downloads/additional-downloads>
  - <http://sourceforge.net/>
-

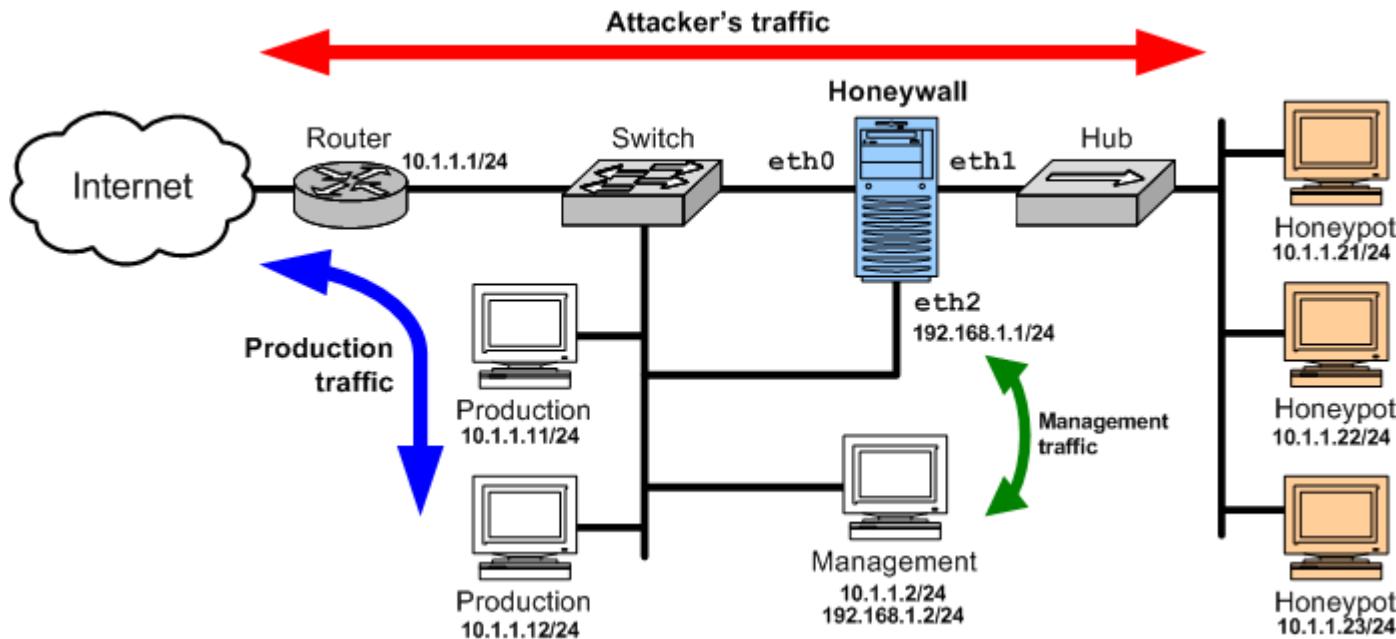
# Honeypots

---

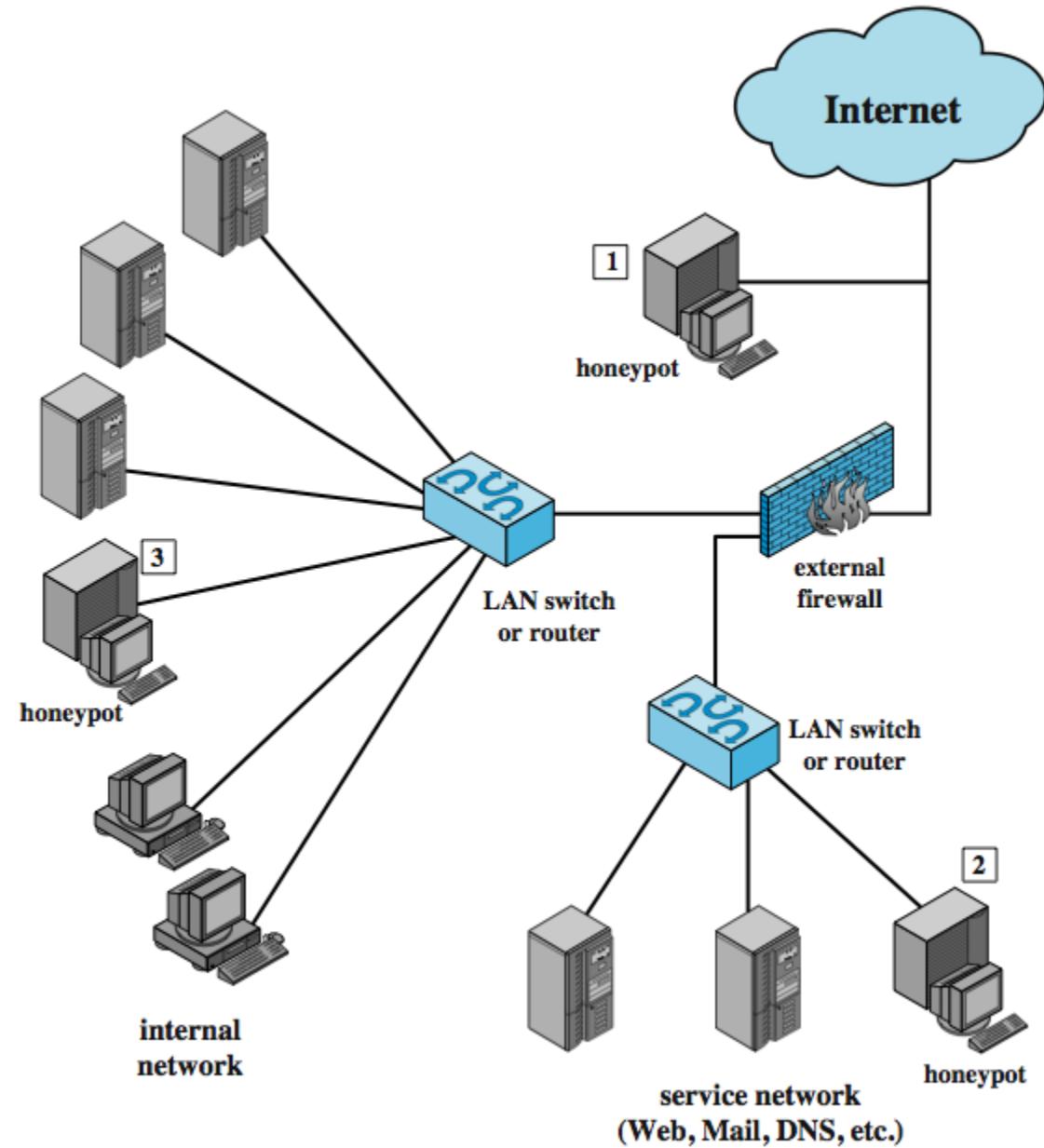
- “A security resource who’s value lies in being probed, attacked or compromised”
    - Honeynet project
  - Are decoy systems
    - divert and hold attacker without exposing production systems
  - Goal
    - Divert malicious traffic
    - Observe intruder activities
    - Contain malicious activities
    - Collect forensic evidence
  - Can be single host
    - Filled with fabricated info
    - instrumented with monitors / event loggers
  - Can emulate an entire networks
    - Honeynets
  - Can be a single file
    - Honeytokens
-

# Honeywall Deployment

Honeywall (honeypot with the abilities of a routing firewall) separates honeynets from inside network



# Honeypot Deployment



# Pros/Cons of Honeypot/nets

---

## □ Pros

- Reduces processing overheads of firewalls/IDSs
- Collects data of high interests
- Reduces false positives
- Detects false negatives

## □ Cons

- Limited view
- More risk
  - Can be fooled/misused/compromised

---

<https://www.acsac.org/2003/papers/spitzner.pdf>

---

# Honey-pot/net Controversy

---

## □ Can be considered illegal

- entrapment, privacy, consent, and liability
  - <http://www.symantec.com/connect/articles/honeypots-are-they-illegal>
  - <https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746>
-

# Defense in Depth Intrusion Response

---

- Prevention
    - IPS
  - Containment
    - Honeypots
  - Detection
    - IDS
  - Recovery
    - Backups
  - Follow-up
    - Use lessons learned
    - Trace-back
    - Back hack
-

# **Firewalls**

---

**CSC 3570**

**IT Security  
Fall 2021**

## **Slide Source:**

**Network Security Essentials, 5/e, by William Stallings, Chapter 12 – “Firewalls”.**

**Introduction to Computer Security, Matt Bishop, Addison Wesley, 2003**

**CISSP Guide to Security Essentials, Gregory, Peter, Chapter 10**

**<https://www.usmd.edu/usm/adminfinance/itcc/firewallpolicynis.pdf>**



# Problem with Free Network Flow

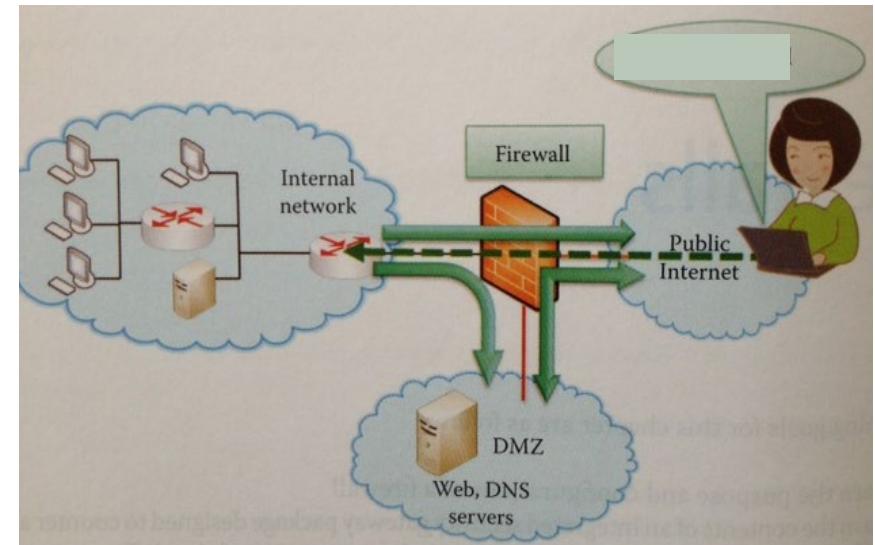
---

What are some CIA issues here?



# Firewalls

- Entity that mediates access to a network
  - Allows/disallows access
  - Based upon policy
- Used for
  - access control
  - audit
  - hiding
  - managing network functions
- Defines a single choke point
  - Could be a SPOF
    - if not implemented correctly



# Firewall Design Goal

---

- Complete mediation
- Only authorized traffic can pass
- Tamperproof





# Firewall Controls

---

## Service control

- Determines the types of network services that can be accessed, inbound or outbound

## Direction control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall

## User control

- Controls access to a service according to which user is attempting to access it

## Behavior control

- Controls how particular services are used
- 



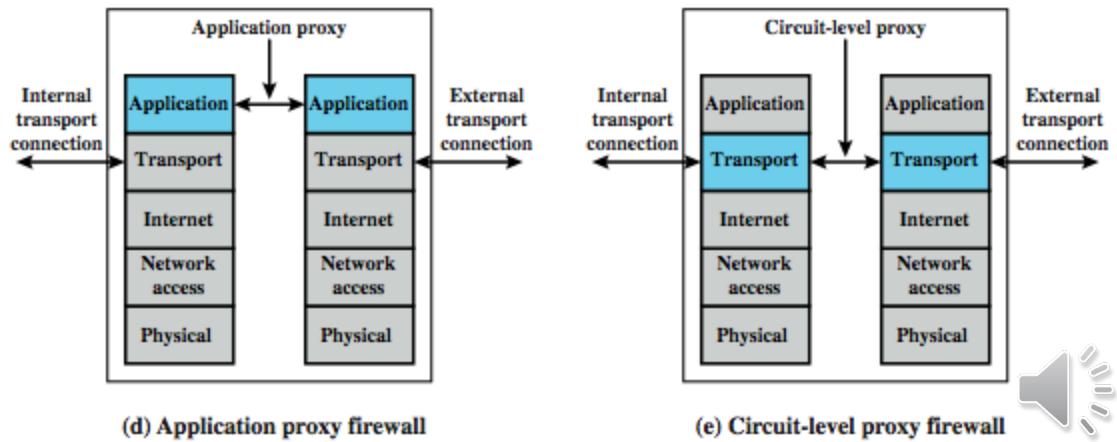
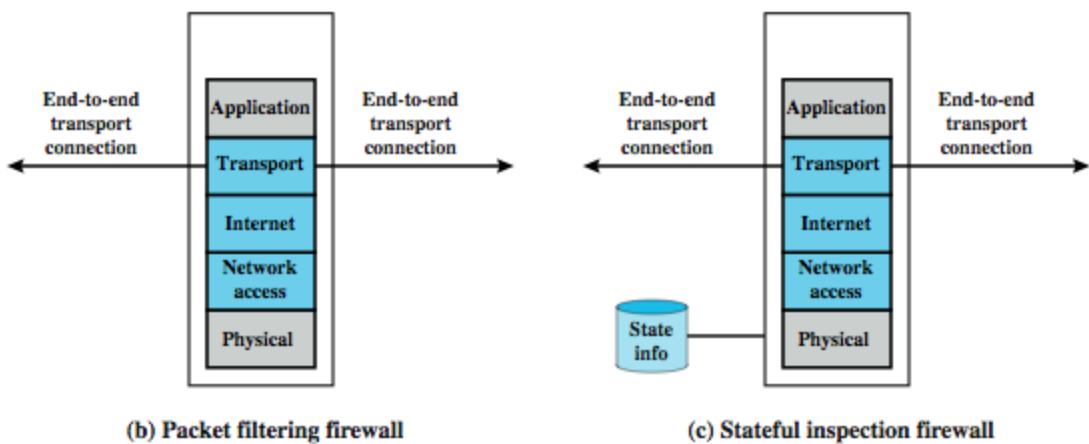
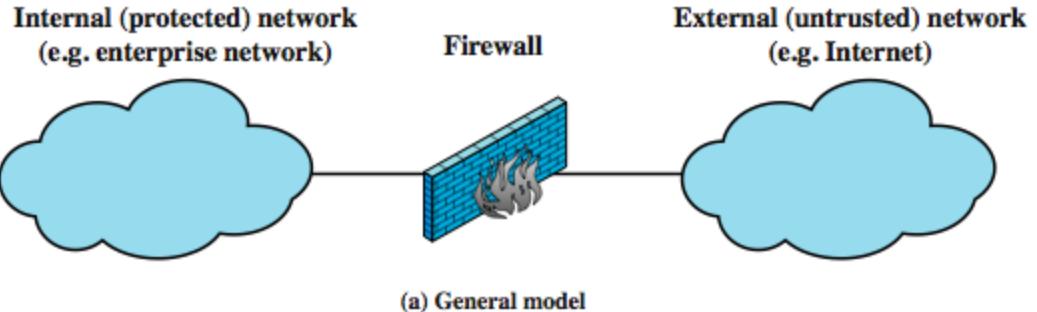
# Firewall Limits

---

- Cannot protect traffic bypassing firewall
    - Dial-in/out
    - Improperly secure wireless LAN
  - Cannot protect against attacks bypassing firewall rules
  - May not protect fully against internal threats
  - Laptop, PDA, portable storage device infected outside and then brought inside
  - Cannot analyze encrypted traffic
- 

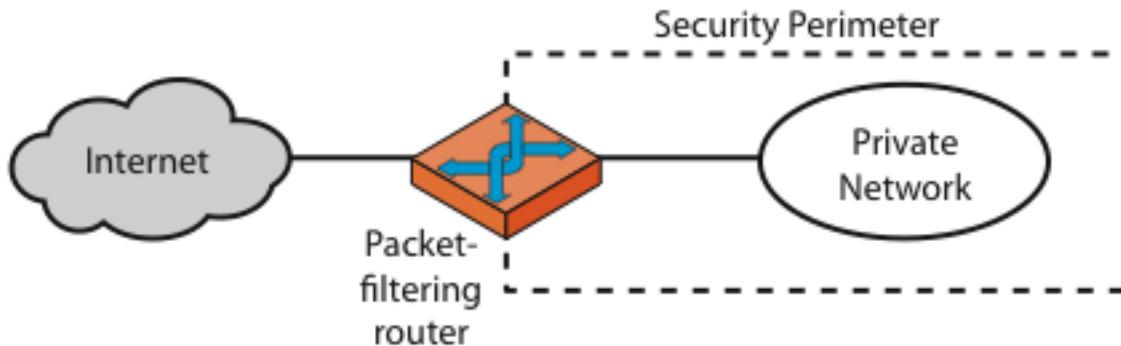


# Types of Firewalls

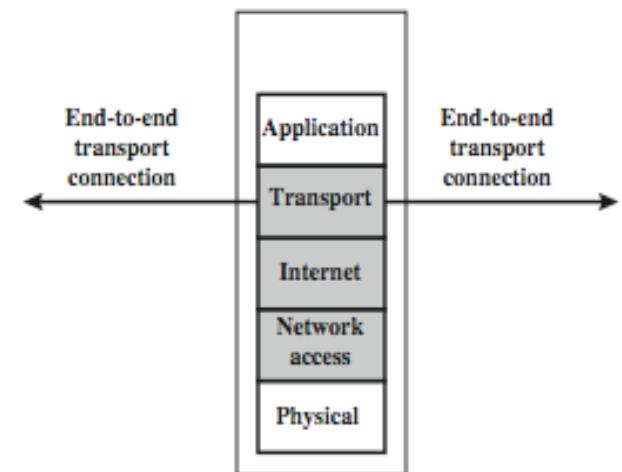


# Packet Filtering Firewall

- 1<sup>st</sup> generation of firewalls
- Also called *network level firewall, shallow filters*
- Somewhat transparent and often router-based
- Access control based on **attributes of packet headers** and a set of access control rules
  - E.g., src/dest IP addr & port, IP protocol, interface
- Does not control access based on packet content



(a) Packet-filtering router



# Packet Filtering Firewall Rules

---

- Typically a list of rules looking for matches on fields
  - if match - rule says if forward or discard packet
    - Can be positive filter (white listing) or negative filter (black listing)
- Two default policies:
  - **discard** - prohibit unless exclusively permitted
    - more conservative, controlled, visible to users
  - **forward** - permit unless exclusively prohibited
    - easier to manage/use but less secure



# Packet-Filtering Example



Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action	Src port	Flag
A	In	External	Internal	TCP	25	Permit	>1023	
B	Out	Internal	External	TCP	>1023	Permit	25	ACK
C	Out	Internal	External	TCP	25	Permit	>1023	
D	In	External	Internal	TCP	>1023	Permit	25	ACK
E	Either	Any	Any	Any	Any	Deny	Any	





# Packet Filter Pros/Cons

---

## □ Strength

- Simplicity
- Transparent to users and are very fast

## □ Weaknesses

- Cannot prevent attack at application level
- Do no support user/application level authentication
- Limited logging functionality
- Improper configuration can lead to breaches
- Vulnerable to attacks on TCP/IP protocol bugs
  - Attacks possible
    - IP address spoofing, source route attacks, tiny fragment attacks



# Attacks and countermeasures

## IP address spoofing

The intruder transmits packets from the outside with a source IP address field containing an address of an internal host

Countermeasure is to discard packets with an inside source address if the packet arrives on an external interface

## Source routing attacks

The source station specifies the route that a packet should take as it crosses the internet, in the hopes that this will bypass security measures that do not analyze the source routing information

Countermeasure is to discard all packets that use this option

## Tiny fragment attacks

The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment

Countermeasure is to enforce a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header





# Stateful Inspection Firewall

---

- ❑ 2<sup>nd</sup> generation of firewalls
  - ❑ Also called **dynamic filters**
  - ❑ Reviews packet header information but also keeps info on TCP connections
    - Single packet may not have enough information
    - Considers “context”
    - Example
      - Stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
      - Only allow traffic for packets matching an entry in this directory
      - May also track TCP SEQ numbers as well
- 



# Example Stateful Firewall Connection State

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established



# Stateful Filter Pros/Cons

---

## □ Strength

- More secure than packet filtering

## □ Weaknesses

- Space and time issues with context storage
  - (cache) overflow
  - Time-outs



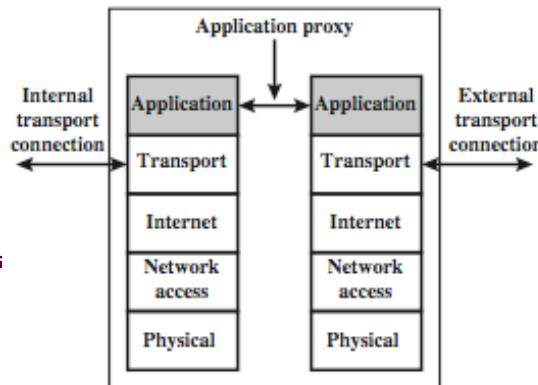
# Proxy Firewall

---

- 3<sup>rd</sup> generation of firewalls
- Access control done with proxies
  - Proxy is an intermediate agent that acts on behalf of an endpoint
- Types
  - Application level
  - Circuit level

# Application-Level Gateway

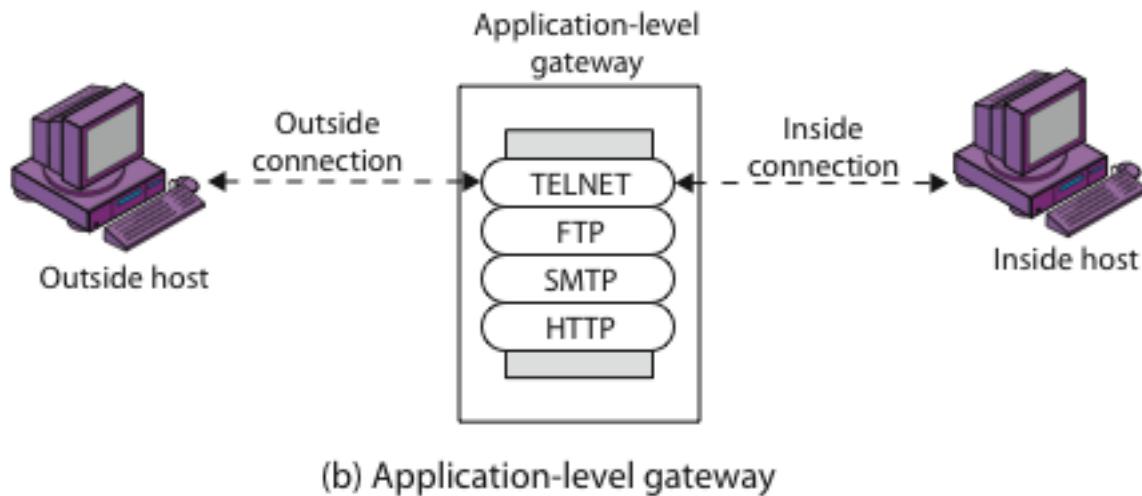
- Also called deep packet inspection filters
- Acts as a relay of application-level traffic
  - Does not permit end to end connection until validated
    - user contacts gateway/proxy with remote host name
    - authenticates themselves
    - gateway contacts application on remote host and relays TCP segments between server and user
- Usually bases access control on content as well as header information
- Must have proxy code for each application to allow traffic



# Application-Level Gateway

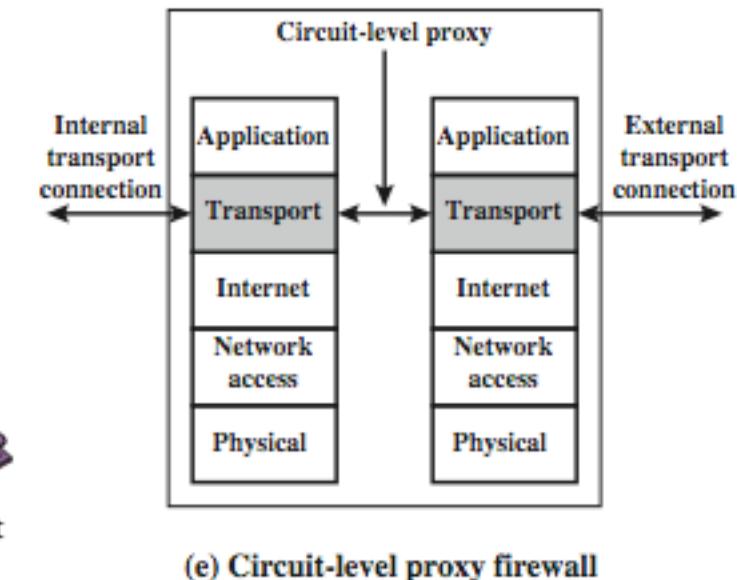
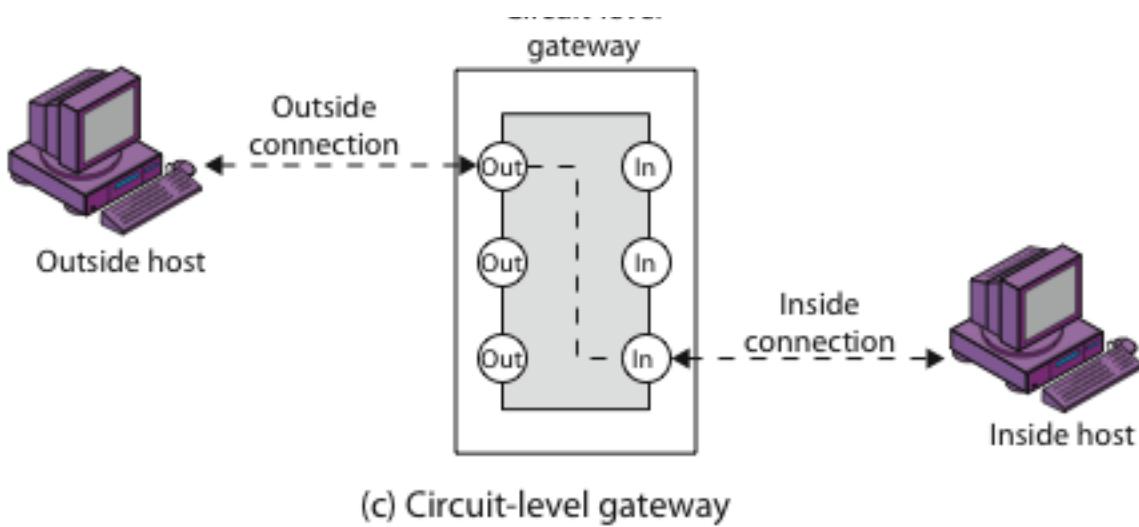
## Pros/Cons

- Provides fine-grained security controls
- More secure than packet filters
- More manageable in policy implementation
- Higher communication and application processing overheads
  - Can degrade network performance



# Circuit-Level Gateway

- Just determines whether relay is permitted and then relays TCP segments from one connection to the other without examining contents
  - independent of application logic



# Circuit-Level Gateway Pros/Cons

---

- Typically used when inside users are trusted
  - Typical use application-level gateway inbound and circuit-level gateway outbound
  - hence **lower overhead**



# **Firewall Basing**

---

- Several options for placing firewall:

- bastion host
- individual host-based firewall
- personal firewall
- network
- In the cloud



# Bastion Hosts

---

- Critical strongpoint in network
- Dedicated machine (a.k.a., hardware FWs)
- Common characteristics:
  - Runs secure OS with only essential services and proxies
  - Each proxy
    - may require additional user authentication to access proxy or host
    - runs as a non-privileged user in isolated domain
    - can restrict features or hosts accessed
    - has limited disk use, hence read-only code
    - audits
    - is small, simple, checked for security
    - is independent of others



# Host-Based Firewalls

---

- Used to secure individual host (server or workstation)
- Available in/add-on for many O/S
- Filter packet flows for the host in question
- Advantages:
  - tailored filter rules for specific host needs
  - protection from both internal/external attacks
  - additional layer of protection to organization firewall



# **Personal Firewall**

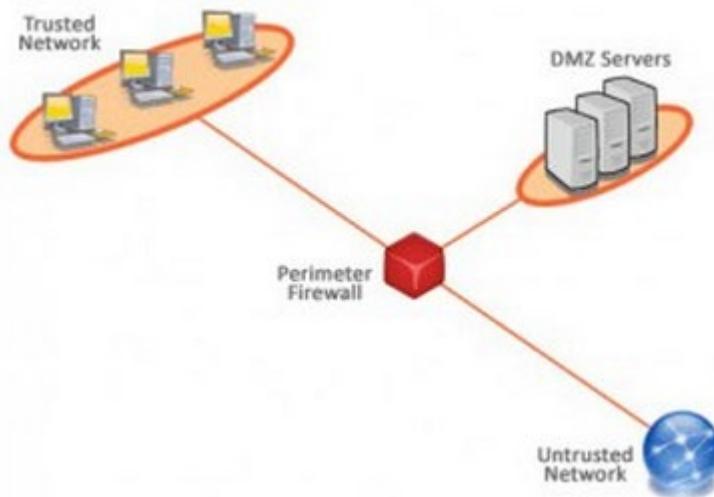
---

- Controls traffic flow to/from PC/workstation**
  - For both home or corporate use**
  - May be software module on PC**
    - or in home cable/DSL router/gateway**
  - Typically much less complex**
  - Primary role to deny unauthorized access**
  - May also monitor outgoing traffic to detect/block worm/malware activity**
- 

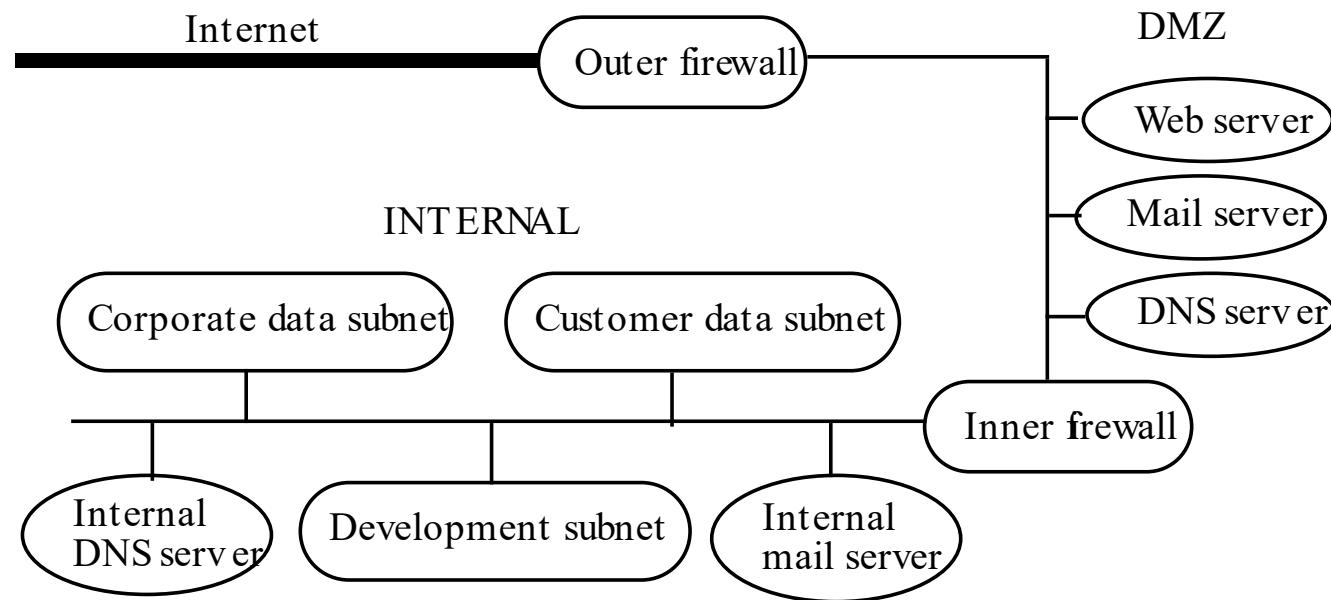


# DMZ

- Bounded by outer and inner firewalls (can be single firewall as well)
- DeMilitarized Zone
  - Network with intermediate trust level
- Portion of network separating internal network from external network
- Can perform different types of checks at boundary of internal & DMZ networks and DMZ & Internet



# Example Usage of Firewalls in a Typical Corporate Environment



# Outer Firewall

---

- Goals: restrict public access to corporate internal network; restrict corporate access to Internet
- Example:
  - Public needs to send, receive email; access web services
    - So, outer firewall allows SMTP, HTTP, HTTPS
    - Outer firewall uses its address for those of mail, web servers
- Typically application proxy firewall
  - SMTP: mail assembled on firewall and checked
  - HTTP, HTTPS: messages checked



# Inner Firewall

---

- Goals: restrict information flow from/to corporate internal network
  - Makes sure there is no communication between the internal servers and the DMZ servers except through the inner firewall
  - Allows control of accesses to some trusted systems
  - Mostly circuit gateway

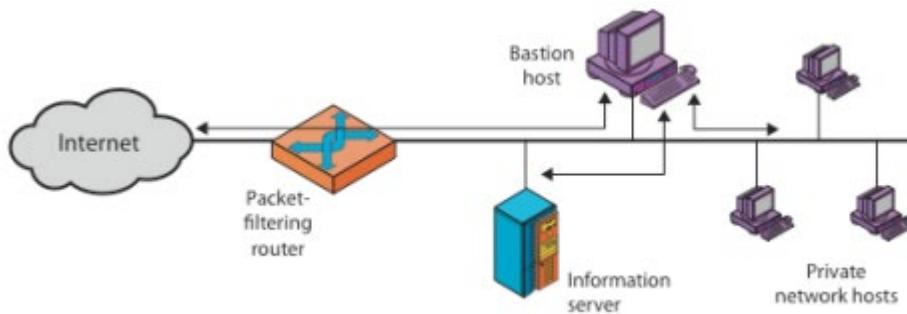


# Firewall Locations and Topologies

---

- Host-resident firewall
  - This category includes personal firewall software and firewall software on servers
  - Can be used alone or as part of an in-depth firewall deployment
- Screening router
  - A single router between internal and external networks with stateless or statefull packet filtering
  - This arrangement is typical for small office/home office (SOHO) applications
- Single bastion inline
  - A single firewall device between an internal and external network
  - This is the typical firewall appliance configuration for small-to-medium sized organizations
- Single bastion T
  - Similar to single bastion inline but has a third network interface on bastion to a DMZ where externally visible servers are placed
- Double bastion inline
  - DMZ is sandwiched between bastion firewalls
- Double bastion T
  - DMZ is on a separate network interface on the bastion firewall
- Distributed firewall configuration
  - Used by some large businesses and government organizations



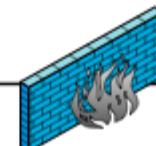


## Screening router

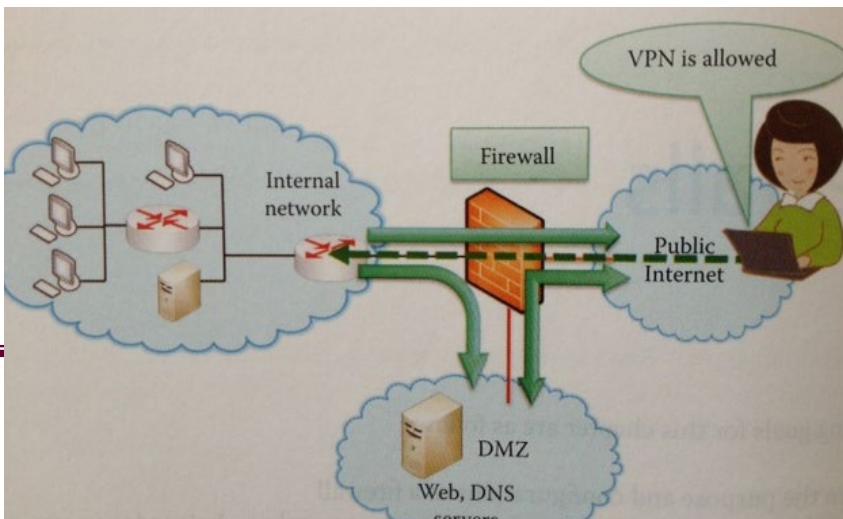
Internal (protected) network  
(e.g. enterprise network)



Firewall



External (untrusted) network  
(e.g. Internet)



## Single bastion inline

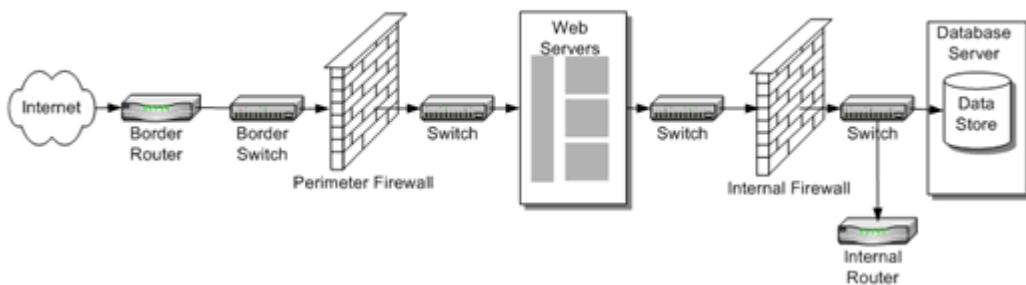
## Single bastion T



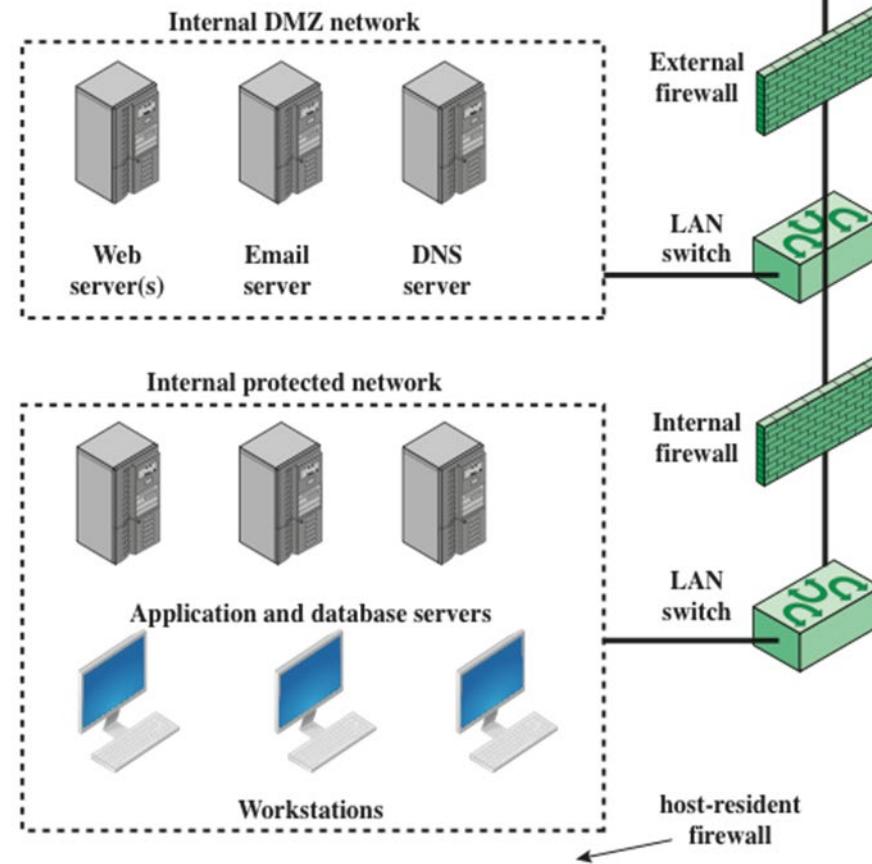
Border Network

Perimeter Network

Internal Network



## Double bastion inline

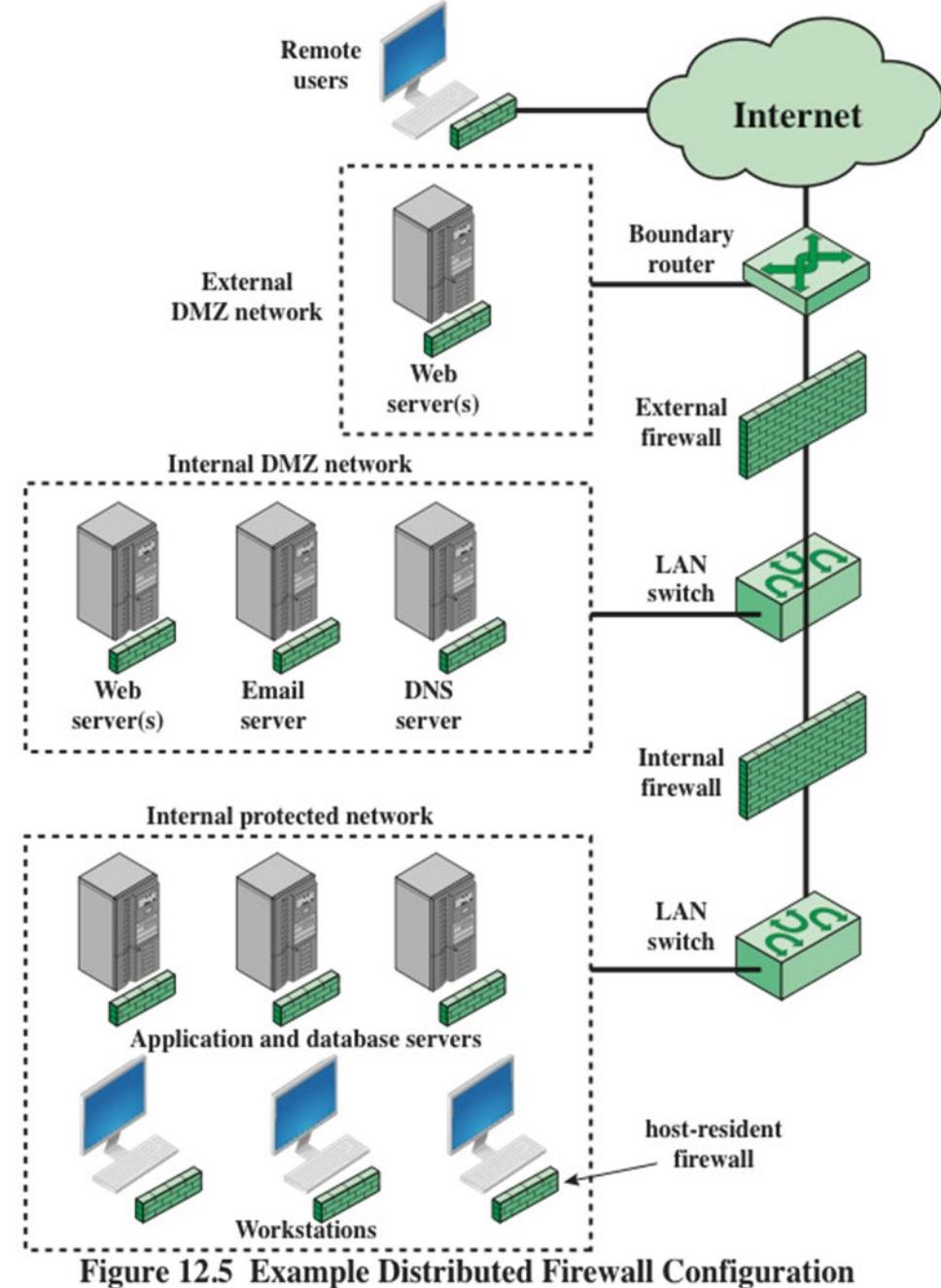


## Double bastion T



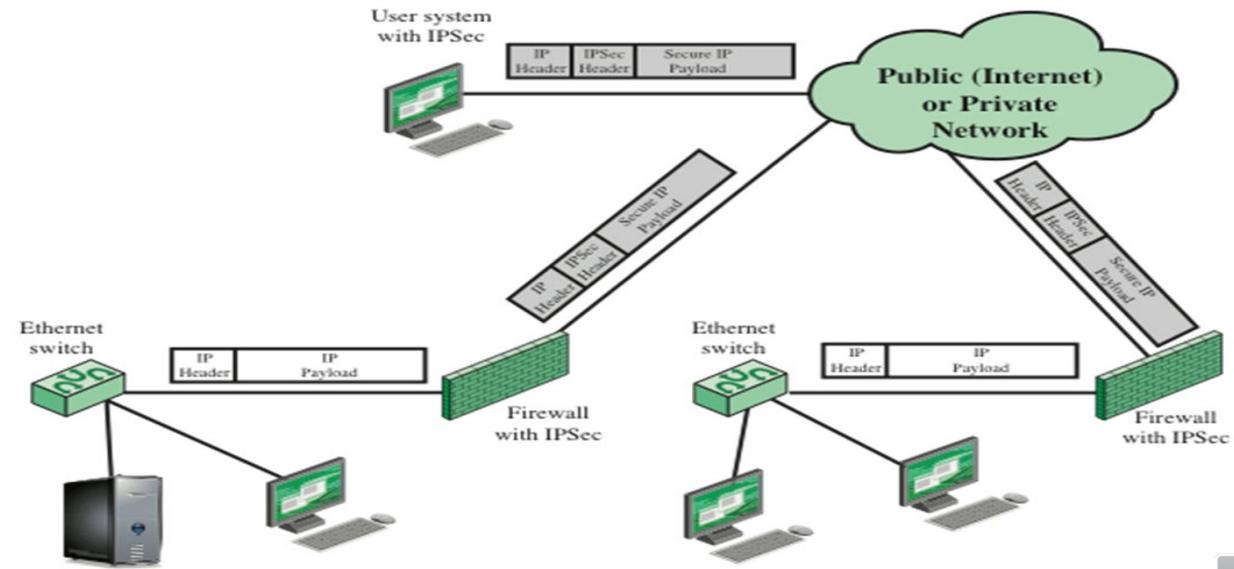


## □ Distributed firewall configuration



# Virtual Private Network (VPN) with Firewall

- ❑ Consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.
- ❑ Firewalls act as Gateway and process encryption (IPsec/TLS) for packets



# Cloud/ Next Generation Firewall

---

- Not on premise!
- Gatekeeper in the Cloud to protect cloud based modern infrastructures
- Features
  - Unified Security Management
  - Integrated Threat Prevention
  - Application and Identity-Based Inspection
  - Hybrid Cloud Support
  - Scalable Performance
- Layered defense combining different types of firewalls with intelligence capabilities



# Deciding the Right Firewall

---

## □ Factors to consider

- What are you protecting
- Who are you protecting from
- What are you protecting against
- Cost
- Efficiency/Performance
- Scalability
- Criticality
- Intelligence





# Points to Recap

- Firewalls (FW) need, limitation,
- Firewall characteristics
- Types of firewalls with pros/cons
  - Packet filtering firewall
  - Stateful inspection firewalls
  - Application level gateway
  - Circuit level gateway
- Firewall basing: what and where
  - Bastion host
  - Host based firewalls
  - Personal firewall
- Importance/need
  - DMZ networks
  - Virtual private networks
  - Distributed firewalls



# Summary

---

- **The need for firewalls**
  - **Firewall characteristics**
  - **Types of firewalls**
    - **Packet filtering firewall**
    - **Stateful inspection firewalls**
    - **Application level gateway**
    - **Circuit level gateway**
  - **Firewall basing**
    - **Bastion host**
    - **Host based firewalls**
    - **Personal firewall**
  - **Firewall locations and configurations**
    - **DMZ networks**
    - **Virtual private networks**
    - **Distributed firewalls**
    - **Firewall location and topologies summary**
- 



# **Access Control**

---

**CSC 3570  
IT Security  
Fall 2021**

## **Slide Source:**

**CISSP Guide to Security Essentials, Gregory, Peter, Chapter 2  
Introduction to Computer Security, Matt Bishop, Addison Wesley, Chapter 4  
Fundamentals to Information Systems Security, Kim and Solomon, Chapter 5  
Information Security Illuminated, Solomon and Chapple, Chapter 2**

---

# Outline

---

- “*what users can do, which data and resources they can access, and what operations they can perform on a system.*”
  - Access Control
    - Parts
    - Models
    - Types
    - Categories
    - Administration
    - Technology
    - Attacks
-

# Access Control

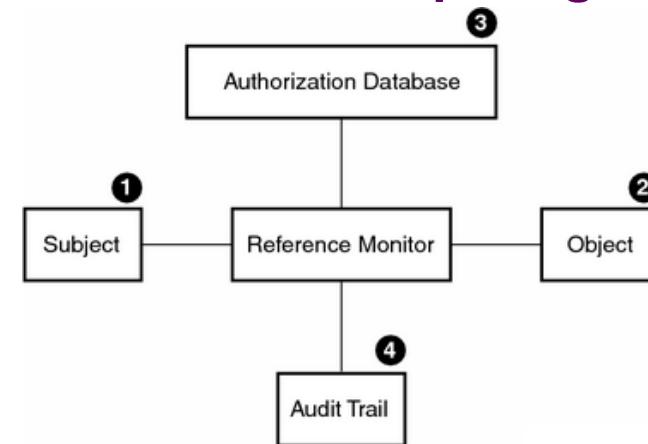
---

- ❑ Collection of methods and components used to protect assets against unauthorized access resulting in security violations
  - Access
    - Read, write, execute, modify
  - Control
    - Mechanisms that allow/disallow/restrict access
- ❑ Defines access relationships between subjects and objects
  - Subjects
    - Active entity who initiates access request
    - Can have clearance labels
  - Objects
    - Passive entity attempted to be accessed
    - Can have classification labels

# Reference Monitor

---

- Responsible for all access control within the computing environment - as per policy
- Properties
  - Simple
  - Complete mediation
  - Tamperproof
- Security Kernel implements Reference Monitor Concept
  - Made up of hardware, software, and firmware components



# File and Data Ownership

---

- Three responsible parties
  - Data Owner
    - Defines policy
    - Sets classification labels
  - Data Custodian
    - Secures/protects data according to policy
  - Data Users
    - Be aware and adhere to policy
    - May have clearance labels

# Classification/Clearance Labels

TABLE 2.2 Military Data Classifications, from Lowest Sensitivity to Highest

Classification	Description
Unclassified	Data that is not sensitive or classified
Sensitive but unclassified (SBU)	Data that could cause harm if disclosed
Confidential	Data for internal use that is exempt from the Freedom of Information Act
Secret	Data that could cause serious damage to national security
Top secret	Data that could cause grave damage to national security

TABLE 2.3 Commercial Data Classifications

Classification	Description
Public	Data not covered elsewhere
Sensitive	Information that could affect business and public confidence if improperly disclosed
Private	Personal information that could negatively affect personnel, if disclosed
Confidential	Corporate information that could negatively affect the organization, if disclosed

Solomon and Chapple, Chapter 2

# Types of Classification Methods

---

**Content-based** classification inspects and interprets files looking for sensitive information. Methods include fingerprinting and regular expression.

**Content-based** answers “What is in the document?”



# Choice of Classification Methods

---



## COMPLIANCE

Compliance data is often structured and/or residing in predictable locations. Leading with a content-based classification will provide the greatest ability to accurately classify PII, PHI, PCI, and GDPR data.



## IP PROTECTION

Intellectual property seldom follows a pattern like a credit card number. To address, this context classification looks to other attributes to assign classification. The application used or the storage location are two ways IP can be classified to support data protection.



## MIXED ENVIRONMENT

Where a mix of regulated data and intellectual property drive enterprise growth, organizations looking to better understand and protect their data look to a blended approach.



## USERS

Data owners should know their data best. A user-based classification approach allows them to apply this knowledge to improve classification accuracy.

# **Example Data Classification Matrix**

---

<https://datamgmt.iu.edu/tools/matrix.php>

---

# Types of Controls

---

- **Technical/Logical**

- Authentication, encryption, firewalls, anti-virus, security models

- **Physical**

- Key card entry, lock, video surveillance

- **Administrative**

- Policy, procedures, standards

# Four Components of Access Control

Access Control Component	Description
Identification	How are they identified?
Authentication	Can their identities be verified?
Authorization	Who is approved for access and what can they use?
Accountability	How are actions traced to an individual to ensure that the person who makes data or system changes can be identified?

# Identification and Authentication

---

- Identification: unproven assertion of identity

- “My name is...”
  - userid

- Authentication: proven assertion of identity

- Userid and password
  - Userid and PIN
  - Biometric

# Authentication Methods

---

- **What the user knows**
    - Userid and password
    - Userid and PIN
  - **What the user has**
    - Smart card
    - Token
  - **What the user is**
    - Biometrics (fingerprint, handwriting, voice, etc.)
  - **Where the user is**
    - Physical location signature
-

# **Authentication Credential Issues**

---

- Weak credential**
  - Forgotten credentials**
  - Compromised credentials**
  - Expired credentials**
-

# Biometric Authentication

---

- Uses a part of user's body as identifying characteristics
- Static and Dynamic
  - Fingerprint
  - Iris scan
  - Signature
  - Keystroke
  - Mouse
  - Voice, etc.

# Biometric Authentication Problems

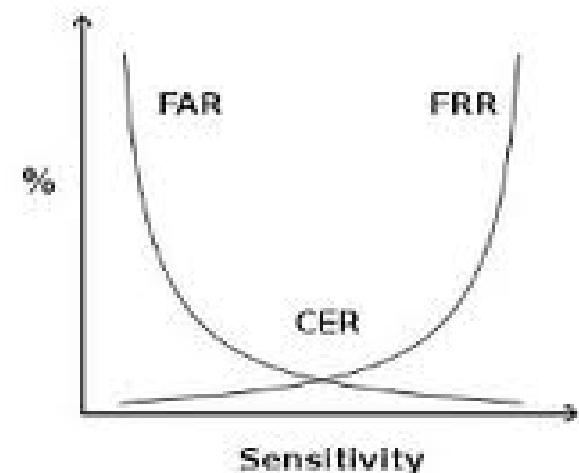
---

- Cost of implementation and maintenance
- Changes in user's characteristics
  - Sudden changes
  - Gradual changes
- False readings
  - False Reject Rate (FRR)
  - False Accept Rate (FAR)

# Biometric Authentication Problems

---

- Cost of implementation and maintenance
- Changes in user's characteristics
  - Sudden changes
  - Gradual changes
- False readings
  - False Reject Rate (FRR)
  - False Accept Rate (FAR)
- Crossover Error Rate
  - Smaller is more accurate



# Two Factor Authentication

- First factor: what user knows
- Second factor: what user *has or is or where*

- Password token
  - USB key
  - Digital certificate
  - Smart card
  - Biometric
  - Location signature



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with  
RSA SecurID software token

- Without the second factor, user cannot log in
  - Defeats password guessing / cracking

# **Two Factor Authentication Problems**

---

- Cost of implementation and maintenance
- Lost/Stolen devices
- Forged devices

# Models of Access Control

---

- Discretionary Access Control (DAC, a.k.a., Identity Based AC)**
    - Owner controls access (based on identity), *may be transferrable*
  - Mandatory Access Control (MAC, a.k.a., Rule Based AC, Lattice based AC)**
    - Higher level authority/entity controls access based on security clearance, *cannot be transferrable*
  - Role Based Access Control (RBAC, a.k.a., task-based, non-discretionary AC)**
    - Based on roles, *cannot be transferrable, can change*
  - Originator Controlled Access Control (ORCON)**
    - Originator (*may not be the owner*) controls access
  - Content Dependent Based Access Control**
    - Content or data values restrict access, *finer level of control*
-

# Rule-Based Access Control

Explicit Rules Grant Access

## Users



Jane



Fred



Albert



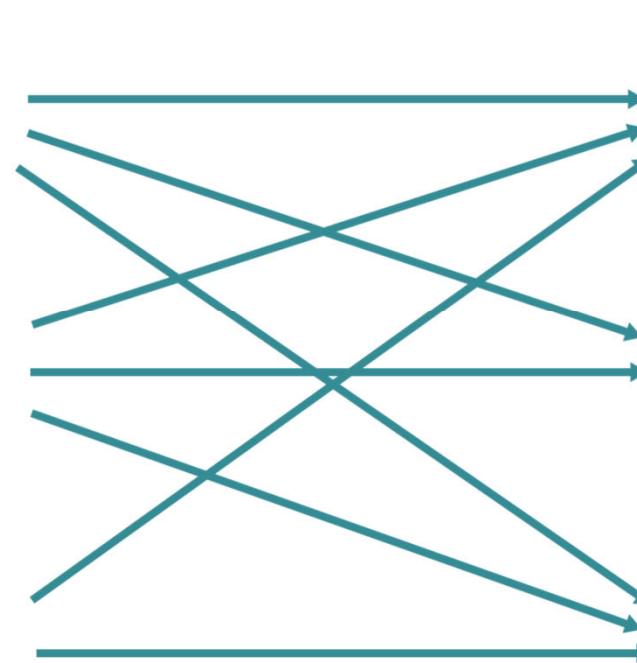
Customer  
Service  
Application



Inventory  
Application

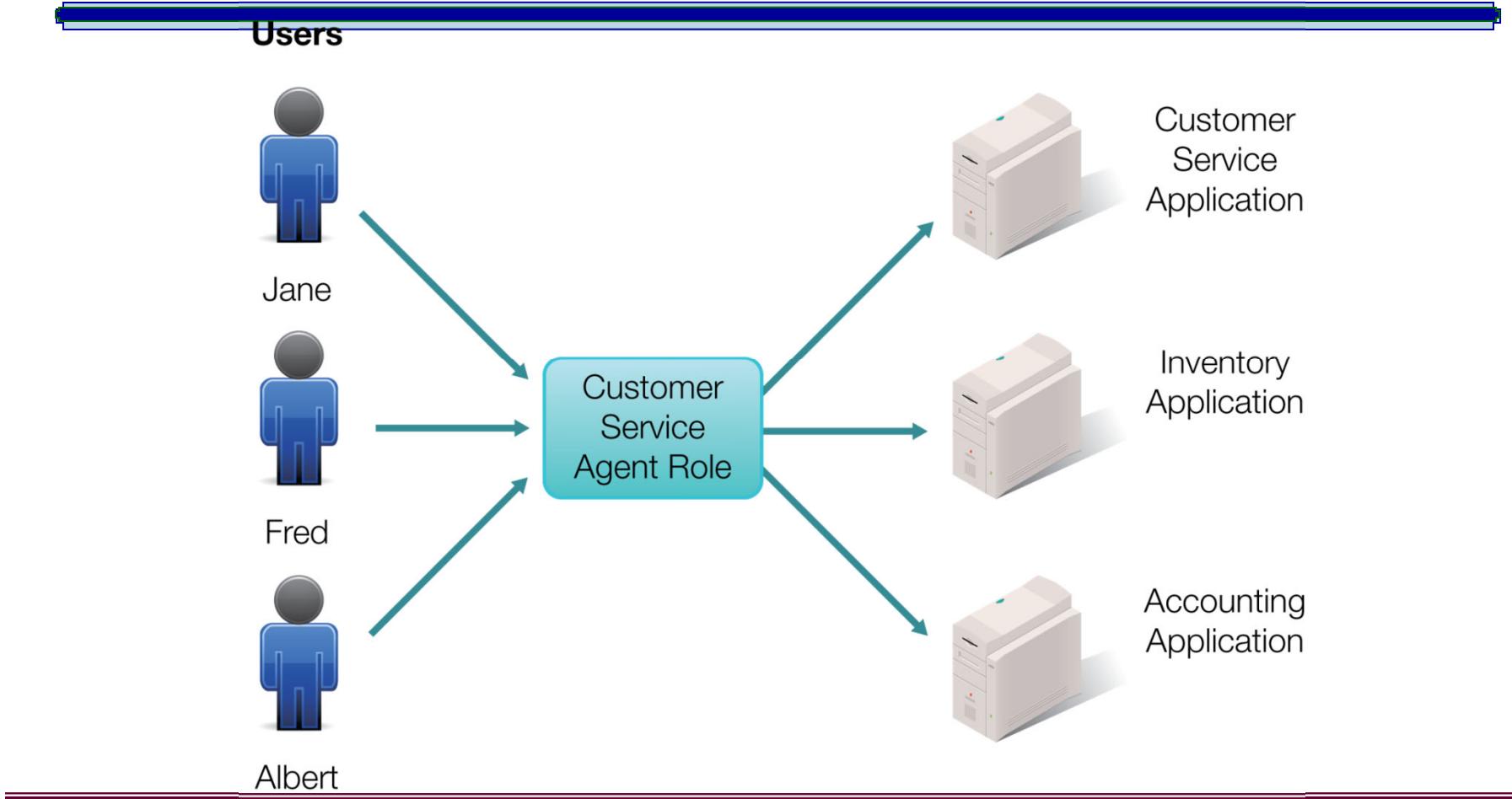


Accounting  
Application



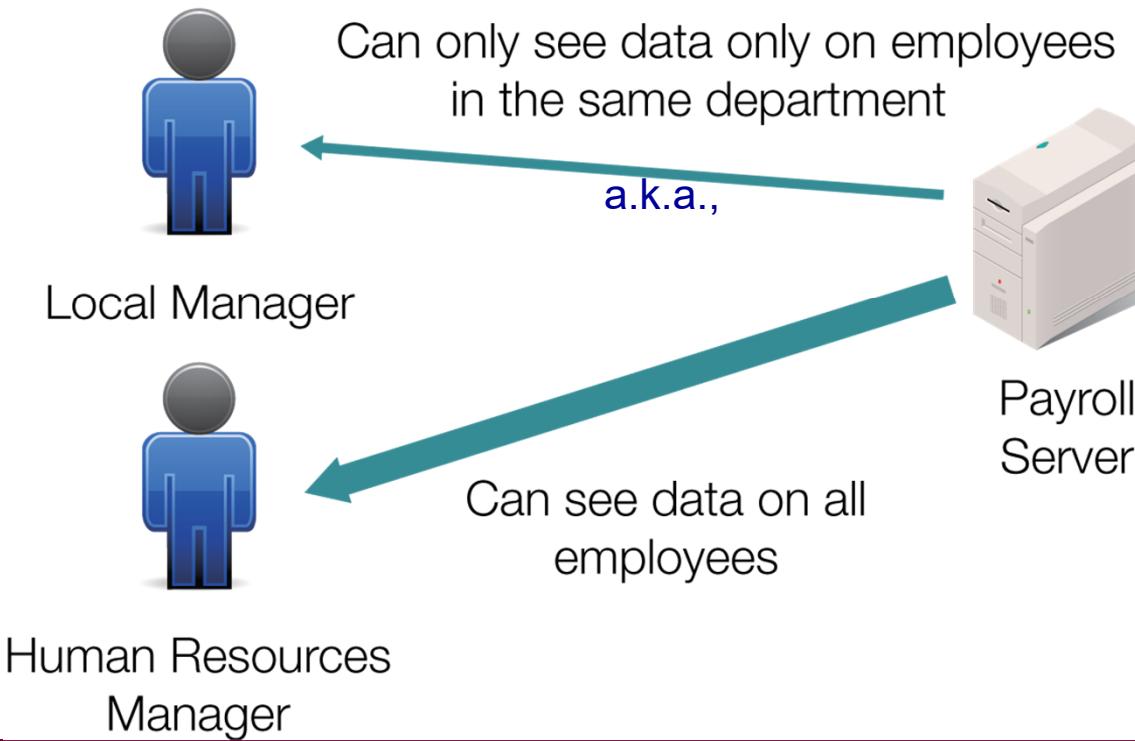
# Role-Based Access Control

Implicit Rules Grant Access



# Content-Dependent Access Control

## Access Based on Values in Data (i.e., Department)



# Access Control and Capabilities List

- Access control list (for each object)
  - Denotes one or more subjects right to a specific object
- Capabilities list (for each subject)
  - Denotes a subject's access to one or more objects

OBJECT ↓

	Word Processor	Uninstaller	Doom Game
Operating System	Read Authority	Write Authority	No Authority
Confidential Docs	R/W Authority	No Authority	No Authority
Saved Games	No Authority	No Authority	R/W Authority

Set Of Capabilities

Individual Access Control List

# **Access Control vs Capabilities List**

---

- Choice is driven by:**
  - Size and nature of subjects and objects
  - Revoking access issues

# **Categories of Controls**

---

- Deterrent controls**
  - Preventive controls**
  - Detective controls**
  - Corrective controls**
  - Compensating controls**
  - Recovery controls**
-

# Deterrent Controls

---

- ❑ Pre-incident controls
- ❑ Designed to prevent specific actions by influencing choices of would-be intruders
- ❑ Cannot actually prevent or even record events
  - Signs
  - Guards, guard dogs
  - Razor wire
  - Authentication system



# Preventive Controls

---

- Pre-incident controls
- Block or control specific events
  - Firewalls
  - Anti-virus software
  - Encryption
  - Key card systems
  - Locks
  - Fencing
  - Authentication system



# Detective Controls

---

- ❑ Control for incident in progress
- ❑ Monitor and record specific types of events
- ❑ Does not stop or directly influence events
  - Video surveillance
  - Audit/Event/Access/Transaction logs
  - Intrusion detection system



# Corrective Controls

---

- Post-incident control to prevent failure
- “Corrective” refers to *making it function better*
  - Can be preventive, detective, deterrent
- Examples
  - Improved spam filter rules
  - Anti-virus new signatures
  - WPA Wi-Fi encryption
  - Security policy addendum
  - 2 factor authentication system

# Compensating Controls

---

- ❑ Post incident
- ❑ Control that is introduced that compensates for the *absence, weakness or failure* of a control
- ❑ Examples
  - Sandbox
  - Monthly review of logs
  - Distributed firewalls

# Recovery Controls

---

- ❑ Post-incident control to recover systems
- ❑ Examples
  - System restoration
  - Database restoration

# Access Control Service

---

- Request userid and password
  - Password stored encrypted or hashed
- Makes a function call to a network based access control service to validate userid and password

# Access Control Administration

---

- Centralized access control
- Decentralized access control

# Centralized Access Control

---

- Single entity/authority manages access control
  - Entity can be administrative or technical
- Good because
  - Reduces
    - administration time to manage/maintain user accounts
    - design errors
    - training time
    - auditing time
    - maintenance time
- Bad because
  - SPOF
  - Performance issues

# Centralized Authentication/Access Control Choices

---

- LDAP**
  - Active Directory
- RADIUS**
  - Diameter
- TACACS**
  - XTACACS
  - TACACS+
- CHAP (Challenge-Handshake Authentication Protocol)**
- Kerberos**

<https://resources.infosecinstitute.com/security-plus-authentication-services-radius-tacacs-ldap-etc-sy0-401/#gref>

# Decentralized Access Control

---

- Access control decisions handled locally
  - Not by centralized entity
- Examples:
  - PAP (Password Authentication Protocol)
- Eliminates SPOF problem
- Allows flexibility
- Faster adoption of changes
- Can result in
  - Gap or overlapping rights
  - Loss of standardization

# Single Sign-On (SSO)

---

## Authenticate once

- Access multiple information systems within a trusted group without having to re-authenticate into each
- Same credential (userid+password)

## Centralized session management

## Weakness:

- Intruder can access all participating systems if password compromised
- Intruder can access all participating systems if session is hijacked

## Best to combine with two-factor/strong authentication

---

# Reduced Sign-On

---

- Like single sign-on (SSO), single credential for many systems
- No inter-system session management
  - User must re-authenticate (sessions can not be hijacked)
- Weakness:
  - Intruder can access all systems if password is compromised
- Best to combine with two-factor strong authentication

# Access Control Attacks

---

## □ Attack objectives

- Abuse access controls
- Attack access controls
- Bypass access controls
- Deceive access controls

## □ Attack mechanisms

# Password Guessing

---

- ❑ Brute force attacks
- ❑ Dictionary attacks
  - Common words
  - Spouse / partner / children / pet name
  - Significant dates / places
- ❑ Countermeasures
  - strong, complex passwords, aggressive password policy

# Password Cracking

---

- Obtain/retrieve hashed passwords from target
- Run password cracking program
  - Runs on attacker's system
- Attacker logs in to target system using cracked passwords
- Countermeasures:
  - frequent password changes
  - controls on hashed password files

# Buffer Overflow

---

- Cause malfunction in a way that permits illicit access
- Send more data than application was designed to handle properly
  - “Excess” data corrupts application memory
  - Execution of arbitrary code
- Countermeasure
  - “safe” coding that limits length of input data
  - filter input data to remove unsafe characters

# Directory Traversal

---

```
<?php  
echo file_get_contents('/var/www/sandbox/uploads/' . $_GET['file']);  
?>
```

- Knowing this URL, you probably would be able to read:

- /var/www/sandbox/uploads/../../../../etc/passwd
- /var/www/sandbox/../../../../etc/passwd
- /var/www/../../etc/passwd
- /var/../../../etc/passwd
- /etc/passwd!

- This could reveal code, database files, personal information, account details, etc.

# Script Injection

---

## □ SQL Injection

```
<?php  
$userName = $_GET[ 'uName' ];  
$results = mysql_query("SELECT age, grade, teacher FROM students WHERE  
studentName = $userName");  
?>
```

- One of the ways it can be exploited as:

SELECT age, grade, teacher FROM students WHERE studentName = 'mayub42'; DROP TABLE students

- The simplest way to detect the presence of such bugs:

- ' OR 1 =' 1 | This returns all rows (Constant true)
  - ' AND 0 =' 1 | This returns no rows (Constant false)
-

# Script Injection

---

- Insertion of scripting language characters into application input fields
  - Execute script on server side
    - SQL injection – obtain data from application database
  - Execute script on client side – trick user or browser
- Countermeasures
  - strip “unsafe” characters from input

# Data Remanence

---

- ❑ Data that remains after it has been “deleted”
- ❑ Examples
  - Deleted hard drive files
  - Data in file system “slack space”
  - Reformatted hard drive
  - Discarded/lost media: USB keys, backup tapes, CDs
- ❑ Countermeasures
  - Improve physical controls
  - Use proper sanitization techniques

# Denial of Service (DoS)

---

- ❑ Actions that cause target system to fail, thereby *denying service* to legitimate users
  - Cause malfunction
  - Overwhelm
- ❑ Distributed Denial of Service (DDoS)
  - Large volume of input from many (hundreds, thousands) of sources
- ❑ Countermeasures
  - input filters, patches, high capacity

# Eavesdropping

---

## ❑ Interception of data transmissions

- Login credentials
- Sensitive information

## ❑ Methods

- Network sniffing
- Wireless network sniffing
- Shoulder surfing
- Conversation in public places

## ❑ Countermeasures

- Encryption
- Security awareness training

# Spoofing/Masquerading

---

- Specially crafted network packets that contain forged address of origin
  - TCP/IP protocol permits forged MAC and IP address
  - SMTP protocol permits forged e-mail “From” address
- Countermeasures
  - router / firewall configuration to drop forged packets
  - judicious use of e-mail

# Malicious Code

---

- ❑ Viruses, worms, Trojan horses, spyware, key logger
- ❑ Harvest data or cause system malfunction
- ❑ Countermeasures
  - anti-virus, anti-spyware, security awareness training

# Emanations

---

- Electromagnetic radiation that emanates from computer equipment
  - Network cabling
  - Wi-Fi networks
- Countermeasures
  - shielding, twisted pair network cable, LCD monitors, lower power or eliminate Wi-Fi

# Social Engineering

---

- ❑ Tricking people into giving out sensitive information by making them think they are *helping* someone
- ❑ Methods
  - In person
  - Via media
- ❑ Countermeasures
  - security awareness training

# Accountability with Audit Log Analysis

---

- Regular examination of audit and event logs
  - Threshold based/clipped logging is common
- Detect unwanted events
  - Attempted break-ins
  - System malfunctions
  - Account abuse
- Audit log protection
  - Write-once media
  - Centralized non-accessible audit logs

# Points to Ponder Recap

---

- Reference monitor
  - Data classification
  - File and data ownership
  - Components (autheication vs authorization)
  - Biometric issues
  - Models (DAC, MAC, Role, Originator, Content)
  - Types (Technical/ physical/ administrative)
  - Categories (deterrent/ preventive/.....)
  - Administration (centralized vs distributed)
  - Single sign on vs reduced sign on
  - Attacks on access control
-

# Summary

---

- ❑ *Identification* is unproven assertion of identity
  - ❑ *Authentication* is proven assertion of identity
  - ❑ *Biometric authentication* includes something the user *is*.  
Examples include fingerprint, hand scan, iris scan
  - ❑ Authentication standards include LDAP, TACACS, RADIUS, and Diameter
  - ❑ Single sign-on (SSO) provides a single identity with session management across applications
  - ❑ Reduced sign-on provides a single identity across applications but no session management
-

# **Summary (cont.)**

---

- Access controls are attacked by several methods, including buffer overflow, script injection, malicious code, denial of service, eavesdropping, spoofing, social engineering, phishing, and password attacks**
- Types of controls: technical, physical, administrative**
- Categories of controls: detective, deterrent, preventive, corrective, recovery, compensating**
- Access controls are tested with penetration testing, application vulnerability testing, and code reviews**

# **Security Baselines**

---

**CSC 3570  
IT Security  
Fall 2021**

**Slide Source:**

**Security+ Guide to Network Security Fundamentals, Mark Ciampa, 2<sup>nd</sup> edition, Chapter 4**

---

# Security Baseline

---

- Minimum security requirements that are acceptable
  - Set of basic security objectives that must be met
  - Can be different for different hosts/systems
- To achieve baseline
  - Harden: process of reducing vulnerabilities
- Items should be hardened:
  - Operating systems
  - Applications
  - Networks
  - Data

# Hardening

---

## ❑ General hardening techniques (**WULAI**)

- Weed
- Update
- Log
- Access control
- Isolate

# Disabling Nonessential Process/Services

---

- ❑ First step in establishing a defense against computer attacks is to turn off all nonessential processes/services
  - Background programs
    - Special tasks
    - Support operating system

# Background Program In Windows

---

- ❑ In Microsoft Windows a background program is called a process
  - Process can provide multiple services to the operating system indicated by the service name, such as AppMgmt, eventlog
  - Users can view the display name of a service, which gives a detailed description, such as Application Management, Event Log
    - Service name and display name may not be the same

# Security Problems with Services

---

- ❑ Services are hidden but active
- ❑ Services may not require user intervention
- ❑ Services can have vulnerabilities
- ❑ Services typically run with local account privileges
- ❑ Services can provide non-apparent entry points into the system
  - TCP and UDP are based on port numbers
  - Socket: combination of an IP address and a port number
    - The IP address is separated from the port number by a colon, as in 198.146.118.20:80
  - Attackers can attach malicious applications to the ports

# Service Modes

---

- A service can be set to one of these (primary) modes (more variations exists):
  - Automatic
  - Manual
  - Disabled
- Determining which service modes to use can be challenging
  - Name not always meaningful
  - Other services can depend on one
  - One process can provide multiple services
  - <http://www.tenforums.com/tutorials/4499-services-start-stop-disable-windows-10-a.html>
  - <http://www.askvg.com/beginners-guide-to-configure-windows-10-services/>

# Applying Updates

---

- ❑ Operating systems are intended to be dynamic
- ❑ Changes happen because
  - Users' needs change
  - New technology (hardware/software) is introduced
  - New vulnerabilities are found
  - New attacks are unleashed
- ❑ Update options
  - Automatically download and install
  - Automatically download and ask permission to install
  - Just get notifications of availability

# Updates Types

Table 4-3 Software updates

Software Update	Description
Security patch	A broadly released fix for a specific product addressing a security vulnerability
Critical update	A broadly released fix for a specific problem addressing a critical, nonsecurity related bug
Update	A broadly released fix for a specific problem addressing a noncritical, nonsecurity related bug
Hotfix	A single package composed of one or more files that addresses one user's problems and is generally not distributed to others
Update rollout	A collection of security patches, critical updates, updates, and hotfixes released as a one package
Service pack	A cumulative set of hotfixes, security patches, critical updates, and updates created since the release of the product, including many resolved problems that have not been made available through any other software updates, and design changes or features requested by users
Integrated service pack	A version of a product released with a service pack in one package
Feature pack	A release of a product that adds functionality but does not address security issues (usually included in the product in the next version of the software)
Version	A major new release of the software incorporating all previous updates along with new features

# Restricting Access

---

- ❑ Another means of hardening an operating system is to restrict user access
- ❑ Generally, users can be assigned permissions to access folders/directories and the files contained within them
- ❑ Permissions
  - List, Read, Write, Read Execute, Modify, Full
- ❑ Permissions should follow security principles
- ❑ Permissions depend on policy

# Group Policy

---

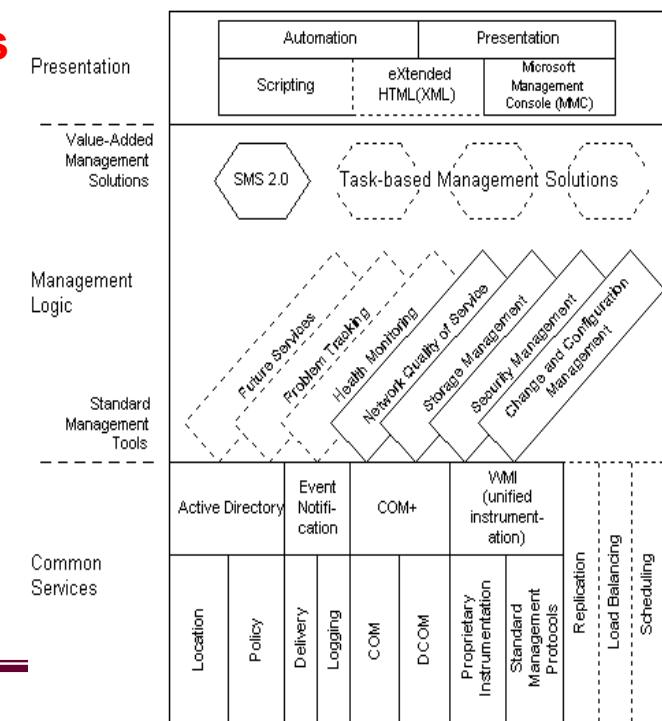
- **Group Policy Object (GPO) settings:**
  - Applies to group of computers/objects
    - Used to manage users' desktop environments
  - Groups can belong to certain site/domain/organization
- **Policy processing order (Precedence order is reverse):**
  - Local GPO
  - Site
  - Domain
  - Organizational

[https://msdn.microsoft.com/en-us/library/aa374155\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa374155(v=vs.85).aspx)

[https://technet.microsoft.com/en-us/library/dn581922\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx)

# Microsoft Management Console

- Microsoft Windows provides a centralized administrative tool called **Microsoft Management Console (MMC)**
- Provides administrators an interface to manage system
  - Accepts administrative tools called **Snap-ins**
    - Group Policy Management
    - Microsoft Exchange Server
    - Active Directory
    - Services
    - Event Viewer
    - Security Template



# Security Template

- MMC Snap-in**
- File/template with security configurations**
  - Collection of security settings for various areas

Area	Configurable Items
Account Policies	Password, lockout, and Kerberos settings.
Local Policies	Audit, user rights, and security options. ("Security Options" consist primarily of security-relevant registry values.)
Event Log	Settings for system, application, security and directory service logs.
Restricted Groups	Policy regarding group membership.
System Services	Startup modes and access control for system services.
Registry	Access control for registry keys.
File System	Access control for folders and files.

- Security templates depending on level of security**
  - **Default** <https://technet.microsoft.com/en-us/library/cc960645.aspx>
  - **Secure** [https://msdn.microsoft.com/en-us/library/ms933182\(v=winembedded.5\).aspx](https://msdn.microsoft.com/en-us/library/ms933182(v=winembedded.5).aspx)
  - **Highly secure** <https://msdn.microsoft.com/en-us/library/bb742512.aspx>
  - **Windows 2000 Server** [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc960645\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc960645(v=technet.10))

# Hardening Operating Systems/Applications

---

- ❑ You can harden the applications that run on the local client or operating system that manages and controls the workstation or the network, such as Windows Server or Novell NetWare
- ❑ Scanning tools
  - Windows (Security Compliance Toolkit SCT)
  - Linux (Lynis)

# Hardening Servers

---

- ❑ Tightening server settings to prevent attacks
- ❑ Customize security templates for every server role in your organization
- ❑ Apply security principles
- ❑ Server roles each have role-specific considerations, including:
  - Access rights that should be permitted
  - Services that should be enabled
  - Audits that should be enabled

<http://www.tecmint.com/linux-server-hardening-security-tips/>

---

# Hardening Web Servers

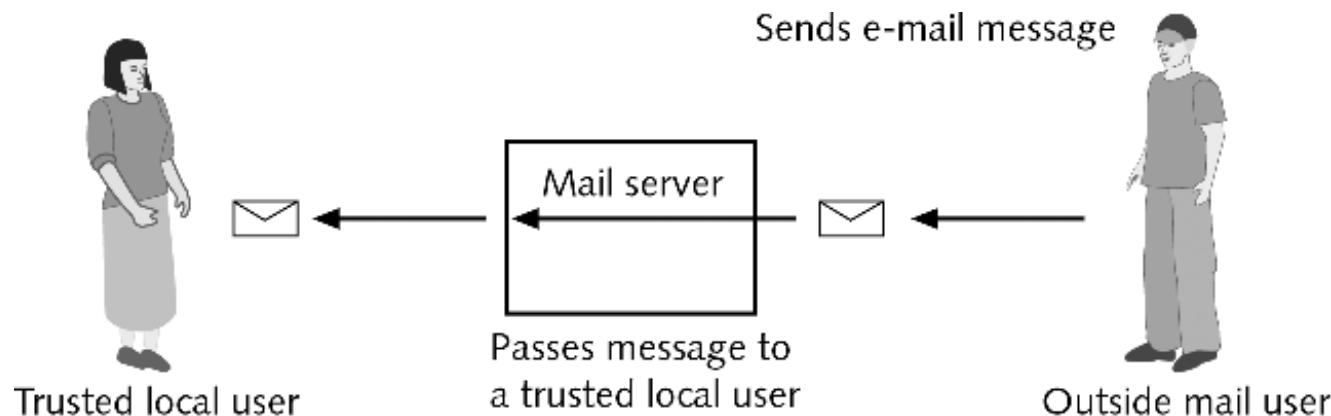
---

## □ General steps

- Update patches, service packs
- Audit/log activities
- Restricted access rights for web surfer's ability to write and execute
  - Web content files read only
- Isolate web server from internal network
- Delete sample files with potential security holes
- Delete unnecessary scripts that are not needed
- Sanitize user input before processing
- Encrypt sensitive info to and from server

# Mail Servers

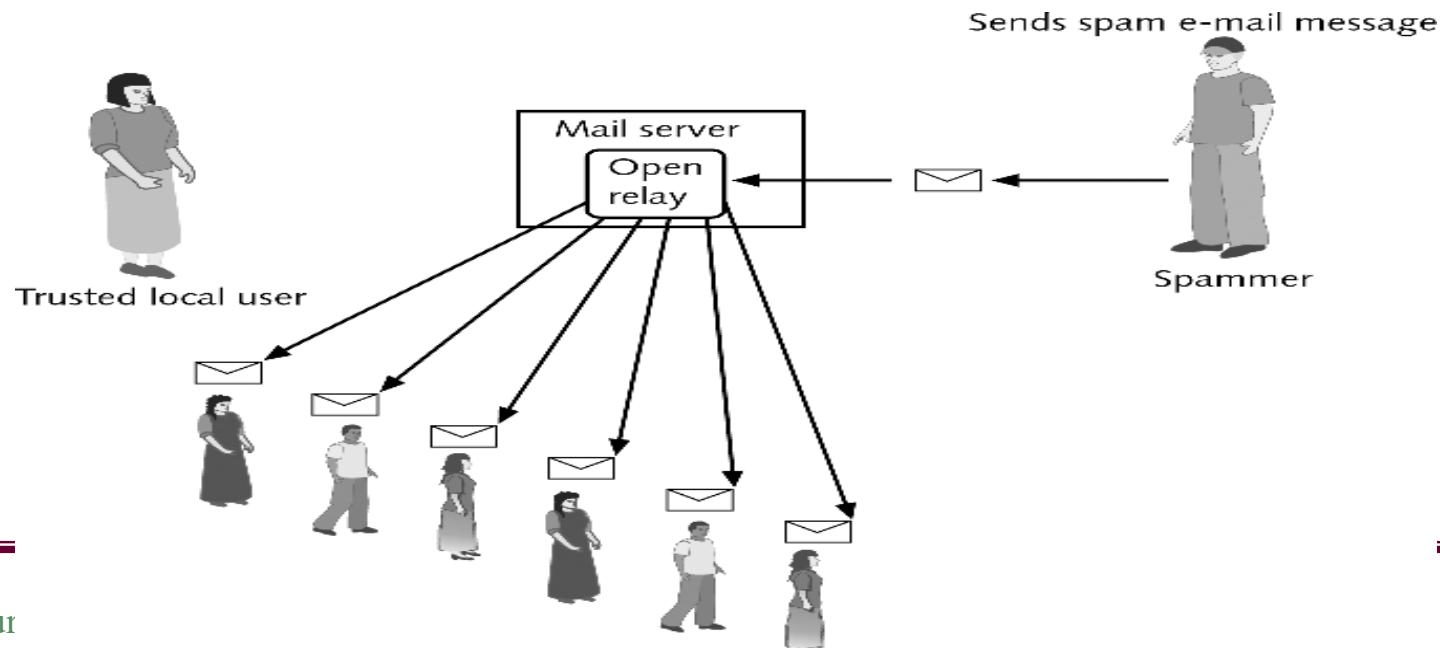
- In a normal setting, a mail server serves an organization or set of users
- All e-mail that is sent through the mail server is assumed to be from a trusted user or received from an outsider and intended for a trusted user



**Figure 4-6** Normal mail server function

# Open Mail Relay

- ❑ In an open mail relay, a mail server processes e-mail messages not sent by or intended for a local user and relays to outside user
- ❑ Abused by spammers



# Hardening Mail Servers

---

## □ General steps

- Use authentication
- Isolate mail server from internal network
- Disallow open relay
- Remove all other applications
- Limit connections
- Verify senders
- Use blacklist
- Encrypt sensitive messages
- SPF – Sender Policy Framework
- DKIM – Domainkeys Identified Mail
- DMARC – Domain-based Message Authentication, Reporting and Conformance
- <https://www.mailhardener.com/kb/email-hardening-guide>
- <http://www.vircom.com/security/top-10-tips-to-secure-your-email-server/>

# Hardening FTP Servers

---

- ❑ File Transfer Protocol (FTP) server is used to store and access files through the Internet
- ❑ FTP servers can be set to accept anonymous logons that can be abused
- ❑ Hardening tasks
  - Making sure anonymous is turned off
  - Use whitelist, if needed
  - Read only permissions
  - Limit authentication attempts
  - Use Secure FTP (SFTP) instead (based on SSH)

# Hardening DNS Server

---

- ❑ A Domain Name Service (DNS) server makes the Internet available to ordinary users
  - DNS servers can be queried to transmit all domains and IP addresses of which they are aware (called zone transfer)
  - Can be used by attackers for malicious purpose
    - Disallow zone transfer
    - Permit restricted zone transfer
    - Encrypt zone transfer
  - DNSSEC – DNS Security Extensions

<https://www.sans.org/reading-room/whitepapers/dns/securing-dns-zone-transfer-868>

<https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en>

# Hardening Print Server

---

- ❑ Print/file servers on a local area network (LAN) allow users to share documents on a central server or to share printers
- ❑ Hardening tasks
  - Access to only trusted users
  - Access rights
    - Disallow access to jobs requested by others
    - Read access for public folders
    - Read and write on group folders
    - Physical access control
  - Encryption at Rest for print jobs

# Hardening DHCP Server

---

- ❑ A DHCP server allocates IP addresses using the Dynamic Host Configuration Protocol (DHCP)
- ❑ DHCP servers “lease” IP addresses to clients
- ❑ Hardening tasks
  - Authenticate clients

<http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>

# Hardening Data Repositories

---

## ❑ Data repository

- Container that holds electronic information
- Company databases

## ❑ Attack on/with

- DBMS application
- DB commands
- Data in DB

# Directory Service

---

- ❑ Directory service
  - Database stored on the network that contains all information about users and network devices along with privileges to those resources
- ❑ Active Directory is the directory service for Windows containing access control information
- ❑ Active Directory is stored in the Security Accounts Manager (SAM) database
- ❑ The primary domain controller (PDC) server houses the SAM database
  - Can have backup domain controllers (BDCs)
- ❑ Active Directory needs to be protected

# Hardening Networks

---

- Two-fold basic process for keeping a network secure:
  - Properly configure it
  - Secure the network with necessary updates
    - Update Firmware (along with software and hardware)

# Network Configuration

---

- ❑ You must properly configure network equipment to resist attacks
  - Filter traffic
  - Change default ports, credentials
  - Turn off unnecessary updates and services
  - Encrypt communication

# **Recaps to Ponder**

---

- What/why baseline**
- WULAI**
- Why weeding of services is important**
- Modes of services**
- Updates types and their differences**
- Hardening different servers: things that are common and things that are unique and why**
- MMC and security template**

# Summary

---

- ❑ Establishing a security baseline creates a basis for information security
  - ❑ Hardening the operating system involves applying the necessary updates to the software
  - ❑ Securing the file system is another step in hardening a system
  - ❑ Applications and operating systems must be hardened by installing the latest patches and updates
  - ❑ Servers, such as Web servers, mail servers, FTP servers, DNS servers, print/file servers, and DHCP servers, must be hardened to prevent attackers from corrupting them or using the server to launch other attacks
-

# **Security Principles**

---

CSC 3570  
IT Security

**Slide Source:**

**Introduction to Computer Security, Matt Bishop, Addison Wesley, Chapter 12**

---

# **Security Principles**

---

- 1975 Saltzer and Schroeder's fundamental principles of security**
  
  - Benefit:**
    - used in design, implementation and/or configuration to prevent loopholes
    - used as the basis of a review checklist
  
  - Main goal: restriction with simplicity**
-

# The Principles

---

- Open design
  - Fail-safe defaults
  - Least privilege
  - Economy of mechanism
  - Separation of privileges
  - Complete mediation
  - Least common mechanism
  - Psychological acceptability
-

# Least Privilege

---

- A user/application/service should be given only those **privileges** necessary to complete its task
  - *Privilege means permissions determining direct actions on the entity in question*
  - **Function controls** assignment
  - **Minimal set of rights**
    - Rights added as needed, discarded after use

## Principle of Least Authority

- A user/application/service should be given only those **authorities** as necessary to complete its task

*Authority means what effects it has on the entity in question either directly or indirectly through another user/application/service*
-

# **Fail-Safe Defaults**

---

- Default action is to deny access**
    - **Exclude-fail is better than permit-fail**
    - **Permit as needed**
  - If unable to complete task, undo**
-

# **Economy of Mechanism**

---

- Keep it as simple as possible
  - Simpler means less can go wrong
-

# **Complete Mediation**

---

- Check every access**
    - Every time
  - No bypass**
-

# **Open Design**

---

- ❑ **Strength of security should not depend on secrecy of design or implementation (or configuration)**
    - **Does not apply to information such as passwords or cryptographic keys**
-

# Separation of Privilege

---

- Require multiple conditions to grant privilege/access
  - Separation of duty

# Least Common Mechanism

---

- Mechanisms/Resources should not be shared
  - Information can flow along shared channels

# **Psychological Acceptability**

---

- Security mechanisms should not add to difficulty of accessing resource
  - Hide complexity introduced by security mechanisms
  - Ease of installation, configuration, use
  
- Principle of Least Astonishment
  - Mechanisms should be designed so that users understand the reason the mechanism works the way it does and its simple to understand
    - The result of performing some operation should be obvious, consistent, and predictable....

---

<http://c2.com/cgi/wiki?PrincipleOfLeastAstonishment>

# The Principles

---

- Open design ➤ No secrecy
  - Fail-safe defaults ➤ No default permit
  - Least privilege ➤ No more privilege than needed
  - Economy of mechanism ➤ No complexity
  - Separation of privileges ➤ No single responsibility
  - Complete mediation ➤ No bypass
  - Least common mechanism ➤ No sharing
  - Psychological acceptability ➤ No hardship/surprises
-

# Interesting Reads

---

- <https://buildsecurityin.us-cert.gov/articles/knowledge/principles/design-principles>
  - <http://emergentchaos.com/the-security-principles-of-saltzer-and-schroeder>
-

# **Introduction to Basic Security Concepts**

---

**CSC 3570  
IT Security  
Fall 2021**

**Slide Source:**

**Introduction to Computer Security, Matt Bishop, Addison Wesley, Chapter 1**

---

# Security Concepts

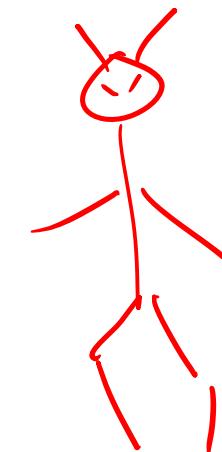
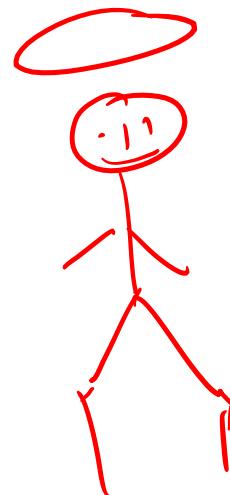
---

- Threat classes
  - CIA Triad
  - Defense in depth
-

# Two Sides in IA

---

- Defensive Side
- Offensive Side



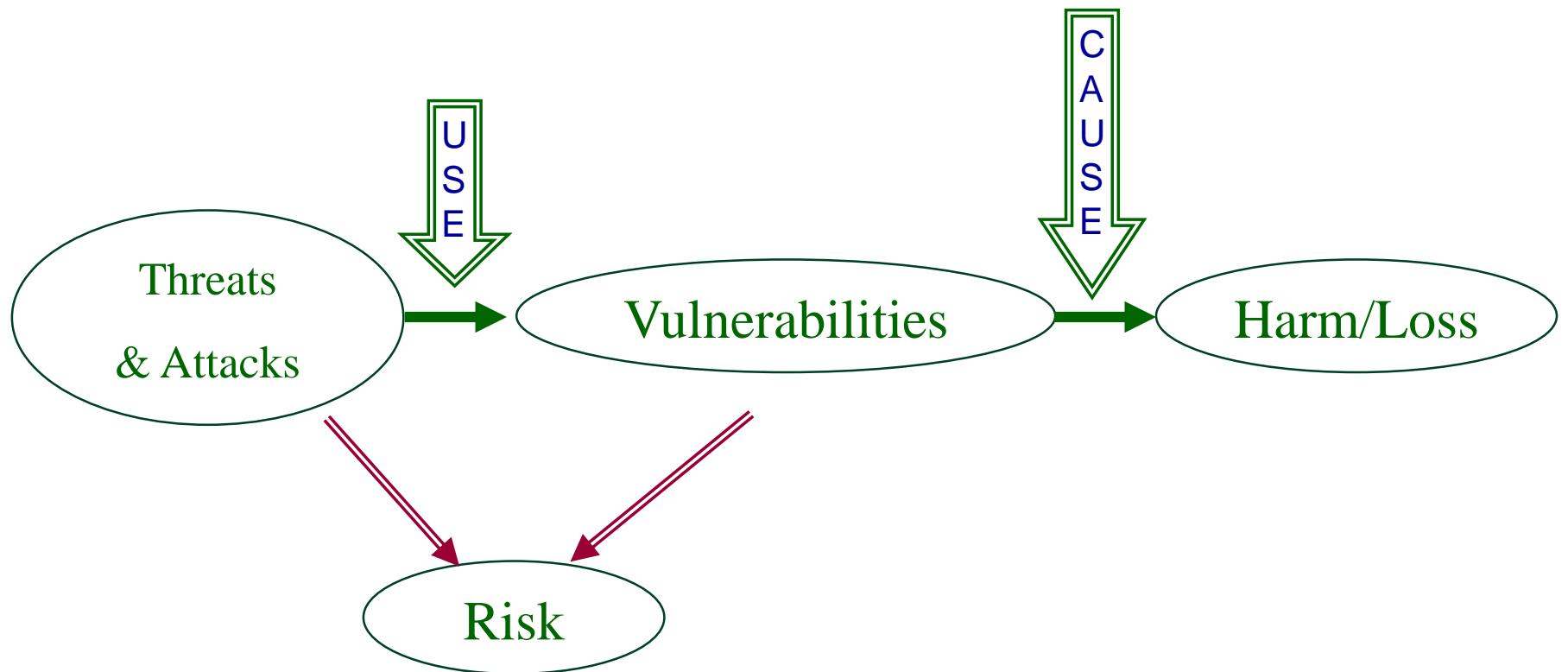
# Offensive and Defensive Operations in IA

---

- **Defensive Operations**
    - Legal (Security Control)
  - **Offensive Operations**
    - Illegal (Security Violation)
      - Unintentional
        - Outsider
        - Insider
      - Intentional
        - Outsider
        - Insider
    - Legal (Security Testing, a.k.a, Penetration Testing)
      - Outsider working for insider
      - Insider
    - Legal & Illegal (Cyber Warfare)
      - Government/Agency against Government/Agency
-

# Offensive Goal

---



# Terms

---

## Threat

- Agent that can inflict harm to an asset or cause security violations

## Attack

- Infliction of harm to an asset or causing security violations

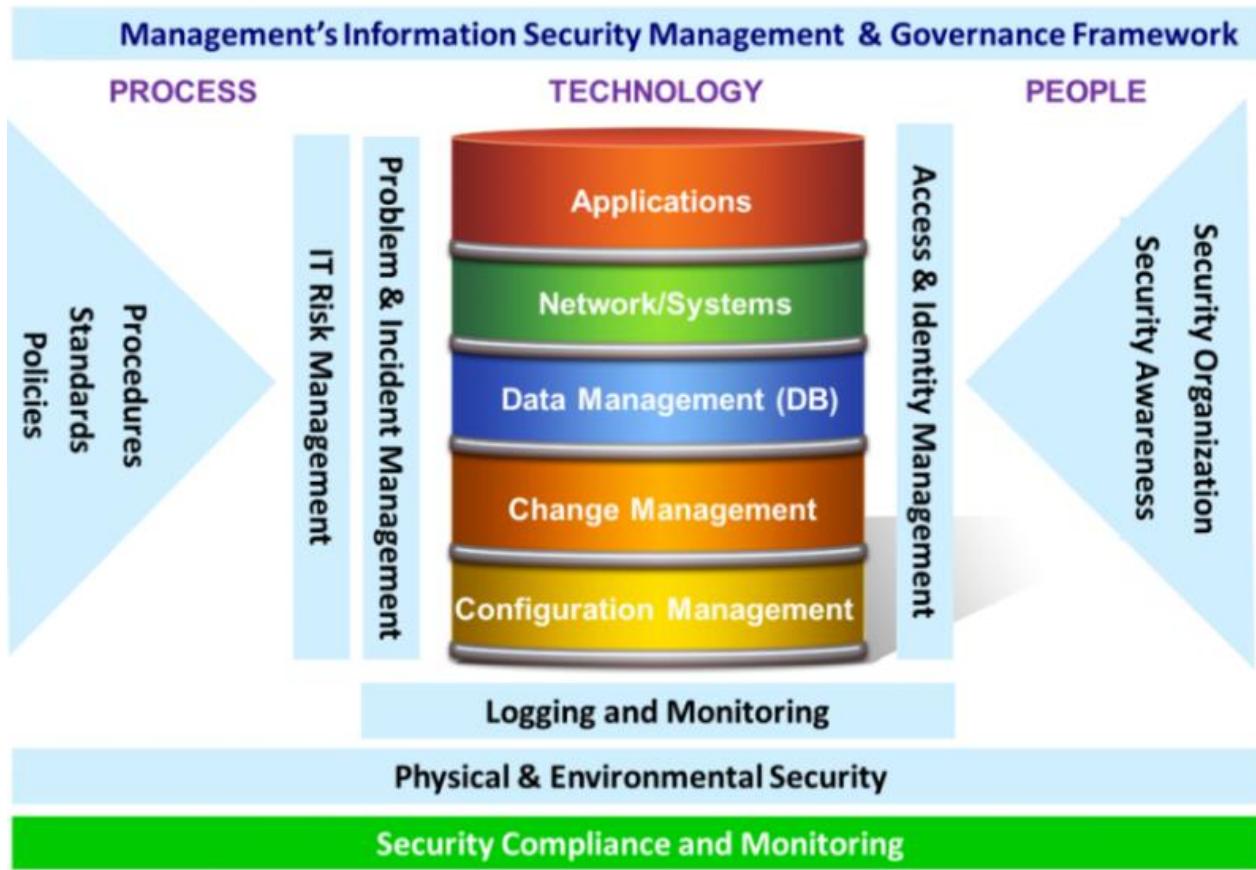
## Vulnerability

- A weakness in security procedures or system design, implementation, or operation that can be used to cause security policy violation

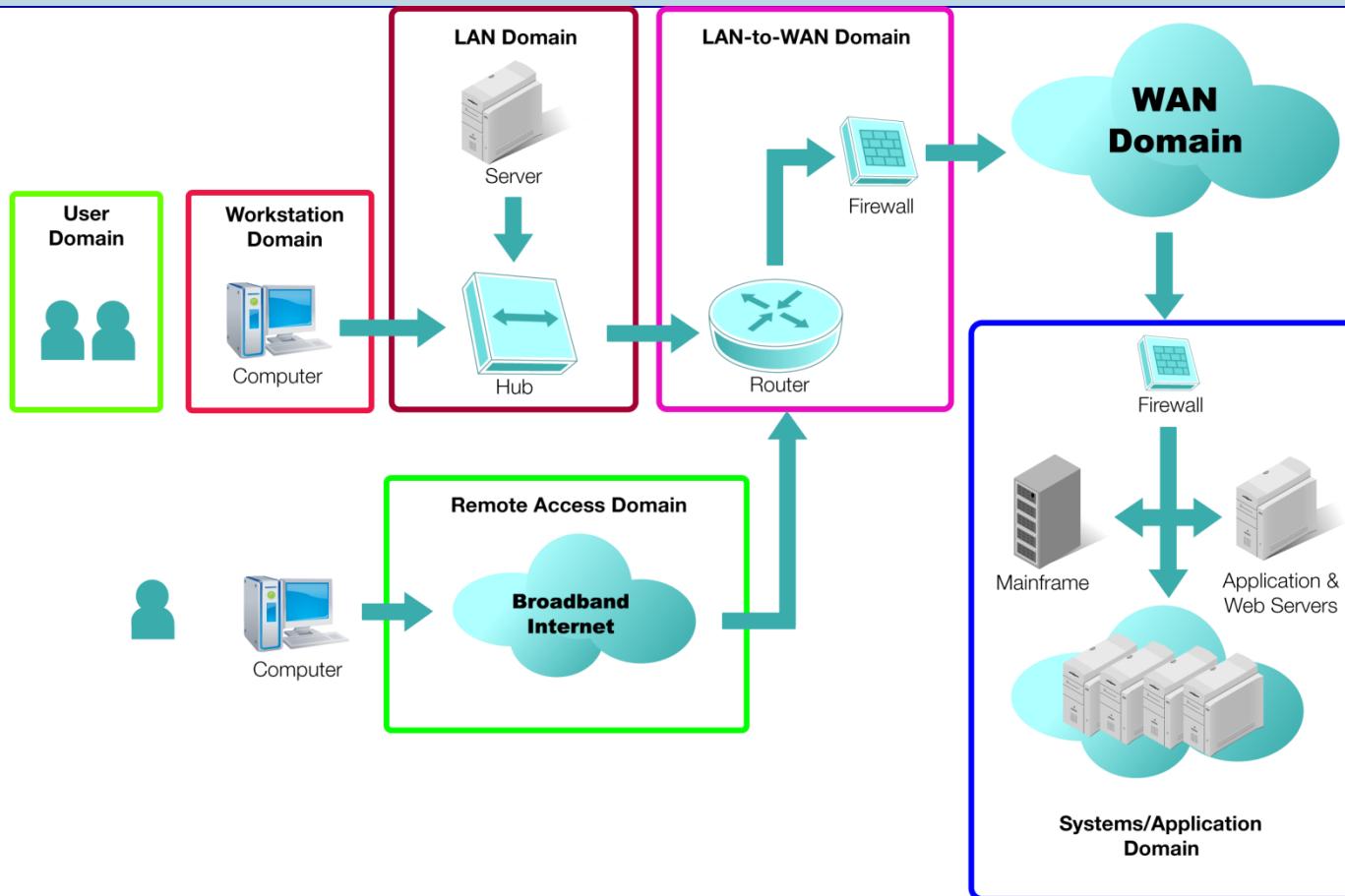
## Risk

- Likelihood that a particular threat can exploit a particular vulnerability or a set of vulnerabilities to violate security policy
-

# IT Infrastructure Management



# Seven Domains of a Typical IT Infrastructure



# General Classes of Threats

---

- Disclosure
  - Deception
  - Disruption
  - Usurpation
-

# **Unauthorized Disclosure**

## **Threat Consequences, and the Types of Threat Actions That Cause Each Consequence**

**(Based on RFC 2828/4949 Internet Security Glossary)**

Threat Consequence	Threat Action (attack)
<b>Unauthorized Disclosure</b>  A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	<b>Exposure:</b> Sensitive data are directly released to an unauthorized entity. <b>Interception:</b> An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. <b>Inference:</b> A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. <b>Intrusion:</b> An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

<http://www.rfc-base.org/txt/rfc-2828.txt>

Slide Courtesy: Mary Ellen Weisskopf, UAB

# **Unauthorized Deception**

## **Threat Consequences, and the Types of Threat Actions That Cause Each Consequence**

**(Based on RFC 2828)**

Threat Consequence	Threat Action (attack)
<b>Deception</b>  A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	<b>Masquerade:</b> An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. <b>Falsification:</b> False data deceive an authorized entity. <b>Repudiation:</b> An entity deceives another by falsely denying responsibility for an act.

<http://www.rfc-base.org/txt/rfc-2828.txt>

Slide Courtesy: Mary Ellen Weisskopf, UAB

# **Unauthorized Disruption**

## **Threat Consequences, and the Types of Threat Actions That Cause Each Consequence**

**(Based on RFC 2828)**

Threat Consequence	Threat Action (attack)
<b>Disruption</b>  A circumstance or event that interrupts or prevents the correct operation of system services and functions.	<b>Incapacitation:</b> Prevents or interrupts system operation by disabling a system component.  <b>Corruption:</b> Undesirably alters system operation by adversely modifying system functions or data.  <b>Obstruction:</b> A threat action that interrupts delivery of system services by hindering system operation.

<http://www.rfc-base.org/txt/rfc-2828.txt>

Slide Courtesy: Mary Ellen Weisskopf, UAB

# **Unauthorized Usurpation**

## **Threat Consequences, and the Types of Threat Actions That Cause Each Consequence**

**(Based on RFC 2828)**

Threat Consequence	Threat Action (attack)
<b>Usurpation</b>  A circumstance or event that results in control of system services or functions by an unauthorized entity.	<b>Misappropriation:</b> An entity assumes unauthorized logical or physical control of a system resource. <b>Misuse:</b> Causes a system component to perform a function or service that is detrimental to system security.

<http://www.rfc-base.org/txt/rfc-2828.txt>

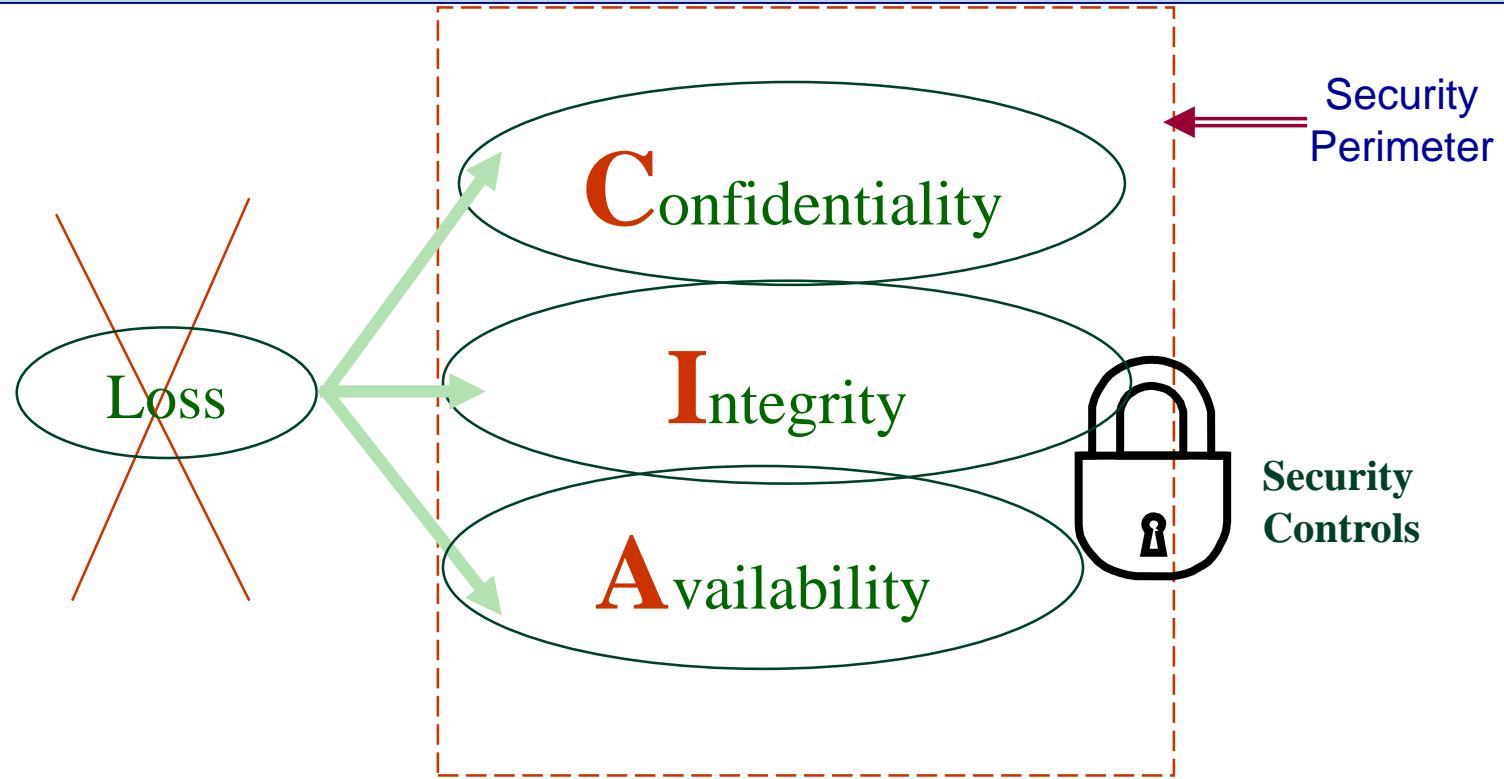
Slide Courtesy of: Mary Ellen Weisskopf, UAB

# **Specific Types of Attacks**

---

- Snooping/Sniffing
  - Spoofing
  - Modification
  - Repudiation of Origin
  - Delay
  - Denial of Receipt
  - Denial of Service
-

# Defensive Goal



# CIA Goal of IA

---

- Confidentiality
  - Keeping data and resources hidden
- Integrity (Data and Origin)
  - Keeping data (and data sources) and resources uncorrupted
- Availability
  - Keeping data and resources usable
- Accountability (a.k.a. Non-Repudiation)
  - Holding one accountable for action

# CIA: Confidentiality, Integrity, Availability

---

- The three pillars of security: the CIA Triad
  - **Confidentiality:** *information and functions can be accessed only by properly authorized parties*
  - **Integrity:** *information and functions can be added, altered, or removed only by authorized persons and means*
  - **Availability:** *systems, functions, and data must be available on-demand according to any agreed-upon parameters regarding levels of service*

# Privacy Goal

---

- Protection and proper handling of sensitive personal information to control the access of others to self
  
- Privacy is a right of individuals
  - Confidentiality can relate to individuals, organizations, assets

# Venues for Security Controls

---

- Hardware
  - Software
  - Data
    - In processing
    - In transit
    - In storage
  - People
-

# Defense in Depth

---

## 1) Prevent

- Securing an environment to avoid penetration

## 2) Deter

- Applying protection mechanisms to hurdle intruder efforts and thus causing delays in achieving a malicious goal

## 3) Detect

- Ensuring visibility of suspicious activities

## 4) Response

- Reacting to security incidents by notification, eradication, interdiction, prosecution
- Continuing to survive to some extent

## 5) Recover

- Assessing and repairing damage
- Improving

