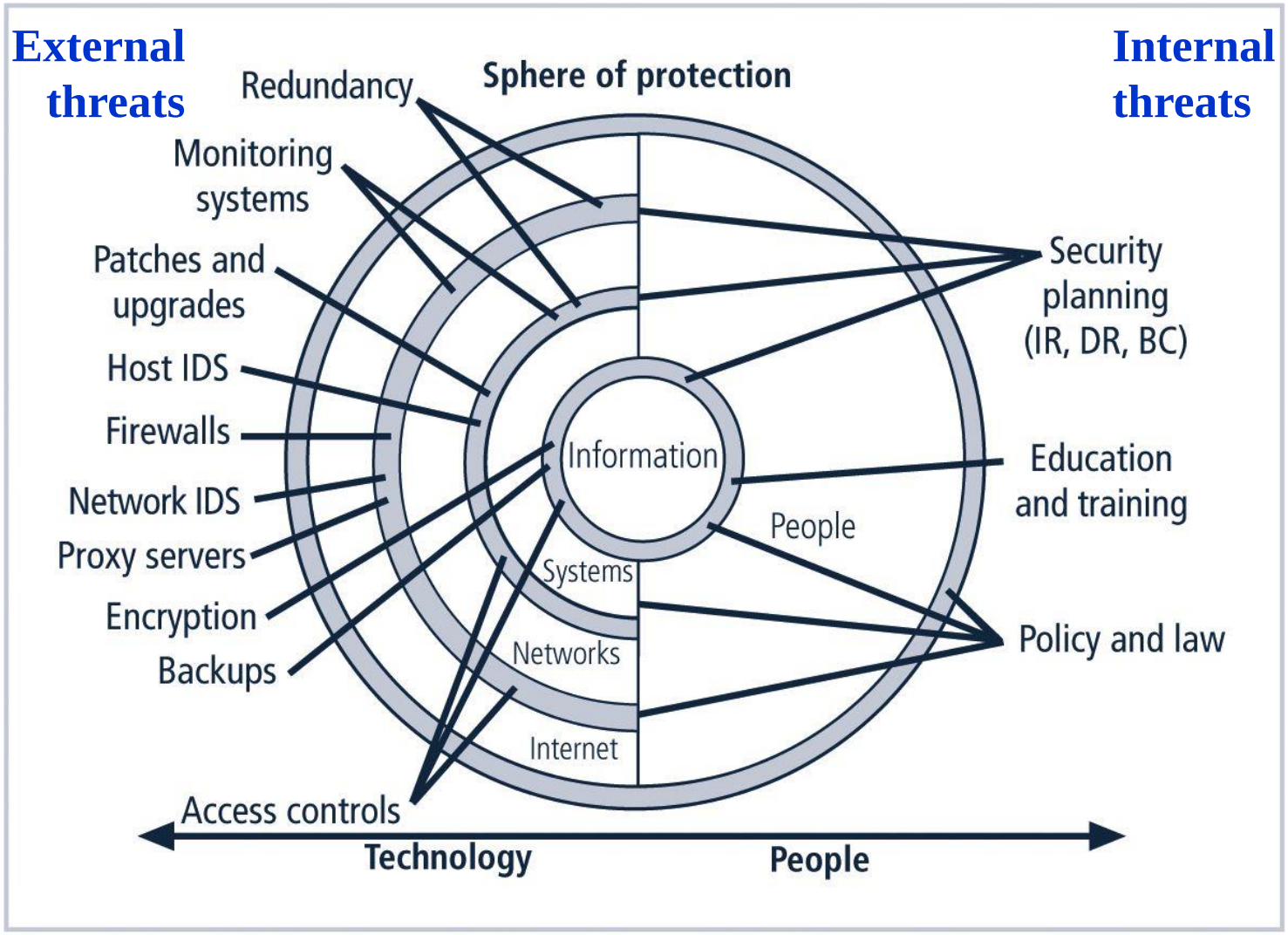
Lecture 10: Protection Mechanisms

EECS711 Security Management & Audit

Objectives

- Access control approaches: authentication, authorization, and biometric access controls
- Firewalls and common firewall implementation approaches
- Discuss the current issues in dial-up access and protection
- Identify types of intrusion detection systems and the strategies on which they are based
- Explain cryptography and the encryption process

Technical Controls



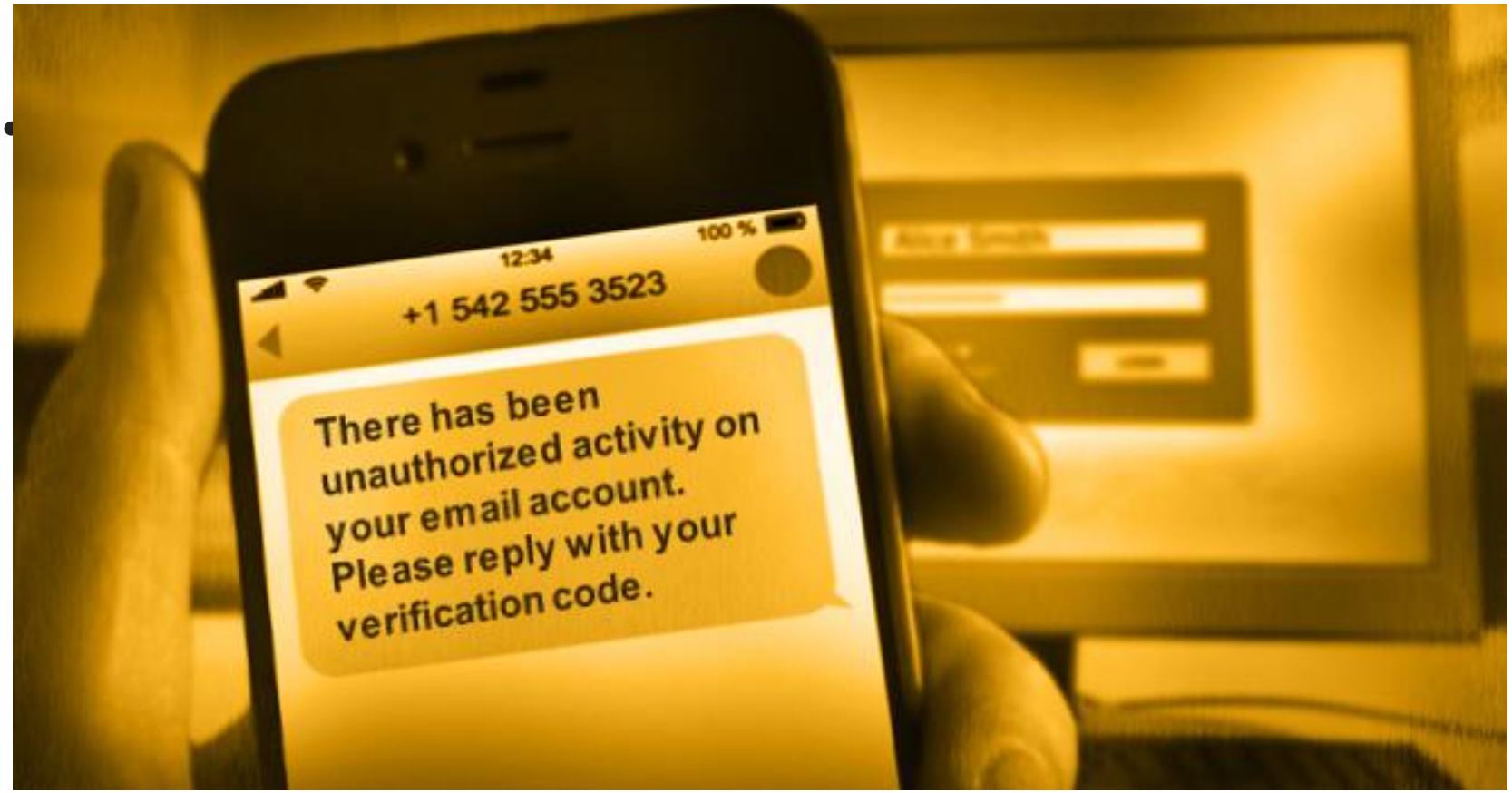
Access Controls

- **Access controls**
  - Regulate the admission of users into trusted areas of the organization
  - Logical access to information systems
  - Physical access to facilities
- Access control involves four processes – **IAAA**
  - Identification
  - Authentication
  - Authorization
  - Accountability

Identification

- **Identification**
  - A mechanism that provides information of an unverified entity that wants to be granted access to a known entity
  - Unverified entity is called a **supplicant**
  - Label applied to the supplicant is **identifier** (ID)
    - ID must be a unique value (can be composite)
    - One-to-one: mapped to one and only one entity within the security domain
    - Account management: close relationship accounts, free accounts, federated accounts
    - Account maintenance
      - How to deal with changes?
      - Notification of changes – helpful but risky

Identification



- Account maintenance
  - How to deal with changes?
  - Notification of changes – helpful but risky

Authentication

- **Authentication**
  - The process of validating a supplicant's purported identity
  - Something you know
  - Something you have
  - Something you are

- Strong authentication
  - **Multifactor**
  - At minimum, two different authentication mechanisms
    - Example: ATM requires a bank card and a PIN

Authentication

- **Something You Know** – verifies identity by means of
  - Password – secret word or combination of characters
  - Passphrase – a plain-language phrase from which a virtual password is derived
    - Ex: May The Force Be With You Always → MTFBWYA
  - Some other unique authentication code (such as a PIN)
- Password selection
  - Length
  - Unpredictability

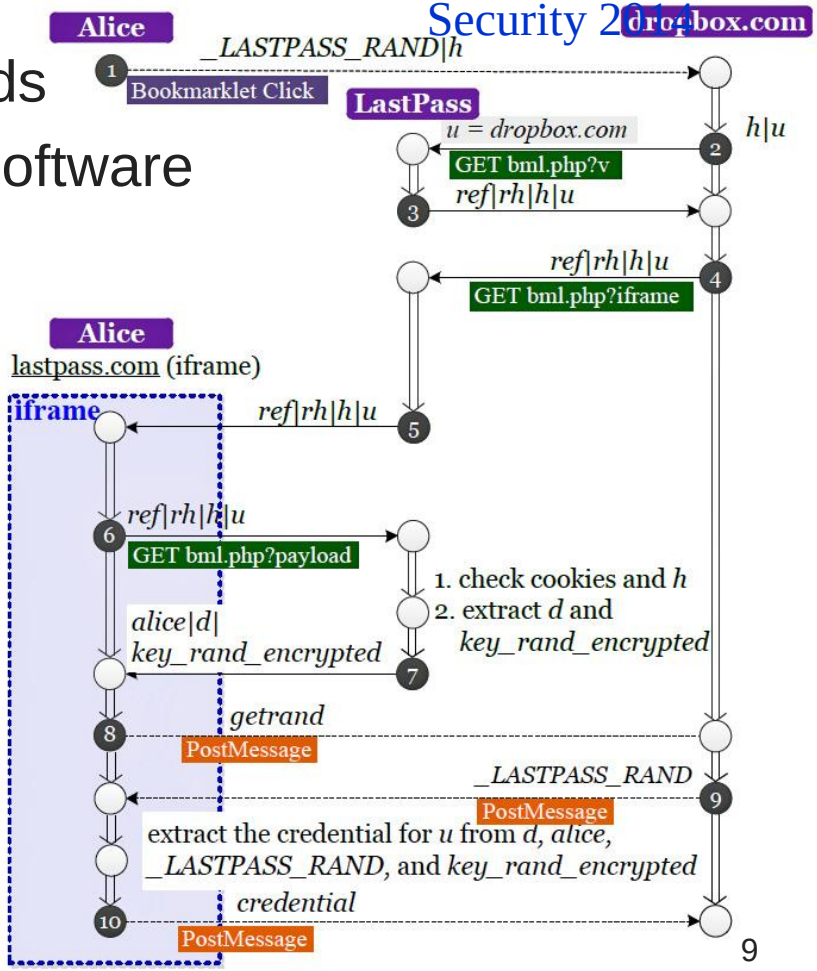
Password Entropy

Character Pool	Available Characters (n)	Entropy Per Character
Digits	10 (0-9)	3.32 bits
Lower-case letters	26 (a-z)	4.7 bits
Case sensitive letters and digits	62 (a-z,A-Z, 0-9)	5.95 bits
All Printable Characters	95	6.57 bits
Dice-ware word list	6^5 (Common Dice-ware word list)	12.9 bits

Authentication

- Password storage
  - For creating strong passwords
  - Password memory support software application
  - Encrypted storage
  - eWallet,
  - KeePass
  - LastPass

2011 LockPass Vulnerability – USENIX Security 2014

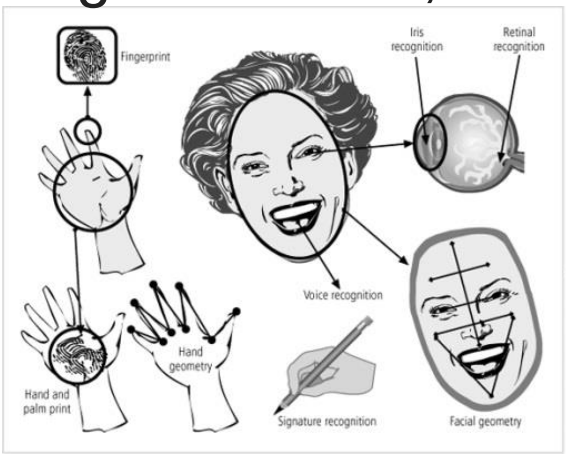


Authentication

- **Something You Have** – makes use of something that the user or system has
  - Dumb card – cards with magnetic strips containing the digital PIN against which user input is compared
  - Smart card – contains a computer chip that can verify and validate information to addition to PINs
  - Synchronous tokens – synchronized with a server, each device uses the time to generate the authentication number that is entered during user login
  - Asynchronous tokens – the server challenges the user with a number and calculates a response
    - Example: Google two-step authentication

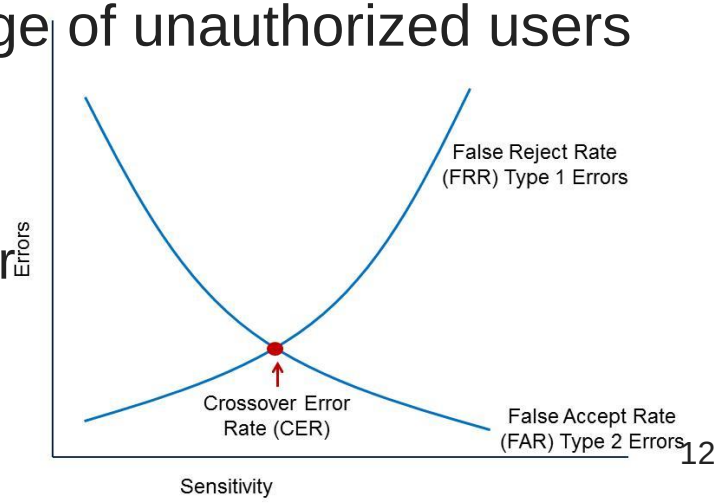
Authentication

- **Something You Are** – takes advantage of something inherent in the user that is evaluated using biometrics, including:
  - Fingerprints (considered truly unique)
  - ID cards with face representations
  - Facial recognition
  - Hand geometry
  - Retina scan (unique)
  - Iris scan (unique)
  - Voice recognition
  - Palm vein authentication
  - Brainprint? – Neurocomputing 2015



Authentication

- *Something You Produce* – makes use of something the user performs or produces
  - Ex: signature, voice pattern, keystroke pattern
- Biometric technologies are evaluated by three criteria:
  - **False reject rate –** percentage of authorized users who are denied access
  - **False accept rate –** percentage of unauthorized users who are allowed access
  - Crossover error rate
    - The point at which the number of false rejections equals the number of false acceptances



Authentication

- Biometric technologies evaluation
  - Effectiveness & Acceptance
    - Increasing acceptance of Iris scanning due to cost

Effectiveness of Biometric Authentication Systems Ranking from Most Secure to Least Secure	Acceptance of Biometric Authentication Systems Ranking from Most Accepted to Least Accepted
• Retina pattern recognition	• Keystroke pattern recognition
• Fingerprint recognition	• Signature recognition
• Handprint recognition	• Voice pattern recognition
• Voice pattern recognition	• Handprint recognition
• Keystroke pattern recognition	• Fingerprint recognition
• Signature recognition	• Retina pattern recognition

Authorization

- Authorization can be handled in one of three ways:
  - Authorization for each authenticated user
    - System performs authentication process to verify each entity
    - Grants access to resources for only that entity
  - Authorization for members of a group
    - System matches authenticated entities to a list of group memberships
    - Grants access to resources based on group's access rights
  - Authorization across multiple systems – **single sign-on**
    - A central authentication and authorization system verifies entity identity
    - Grants a set of credentials to the verified entity

Accountability

- Accountability – ensures that all actions on a system can be attributed to an authenticated identity
- **Logs and Audit**
  - System logs: records maintained by a particular system that has been configured to record specific information
    - system events, performance, network performance, process performance, files/directories, users
  - Applications logs: applications and data in business processes
    - tracking client requests, accounts, resource usage
  - Security software logs
    - antimalware, intrusion detection and prevention, authentication, remote access, vulnerability management

Security Log Management

- **NIST SP 800-92**: Guide to Computer Security Log Management
  - Organizations should develop standard processes for performing log management
    - Develop policies to define mandatory requirements and suggested recommendations
    - Ensure policies and procedures incorporate and support the log management requirements and recommendations
- Log management activities
  - Log **generation**, transmission, **storage**, **analysis**, & disposal

Log Generation

- Configuration of systems to create logs
  - Where to collect
  - Where to store

  - Challenges:
    - Multiple log sources
    - Inconsistent log content, timestamps, and log format
  - Functions:
    - Log parsing
    - Event filtering
    - Event aggregation

Log Analysis and Storage

- Log analysis and storage
  - Transference of log data to an analysis system
  - Security information & event management (SIEM)
- Management functions within log storage
  - Log rotation
  - Log archival
  - Log compression
  - Log reduction
  - Log conversion
  - Log normalization
  - Log file integrity

Log Analysis and Storage

- Management functions within log analysis
  - Event correlation
    - Rule-based correlation
  - Log viewing
  - Log reporting
- Management functions within log disposal
  - Log clearing – removing all entries from the log
    - the specification of when logs may be deleted or overwritten within a system
    - Low impact: 1-2 weeks
    - Moderate impact: 1-3 months
    - High impact: 3-12 months

Log Analysis and Storage

- General suggestions for managing logs:
  - Make sure data stores can handle the amount of data generated by the configured logging activities
  - Rotate logs when unlimited data storage is not possible
  - Archive logs – copy to remote storage locations
  - Secure logs – should be encrypted in case log data store is compromised
  - Destroy logs – once log data has outlived its usefulness, it should be securely destroyed
- Periodical review – auditing

Managing Access Controls

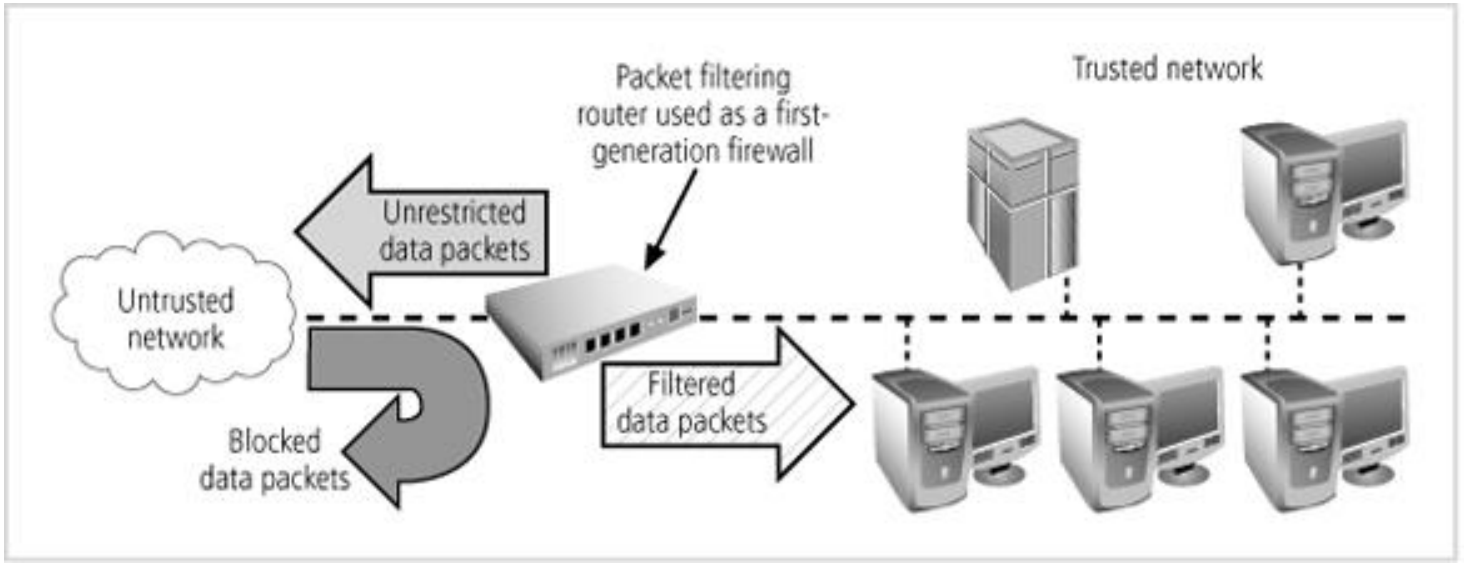
- Access control policy – specifies how access rights are granted to entities and groups
- Must include provisions for:
  - Periodically reviewing all access rights
  - Granting access rights to new employees
  - Changing access rights when job roles change
  - Revoking access rights as appropriate
- Implement access controls in a way that is consistent with the organization's overall philosophy

Firewalls

- **Firewalls**
  - Prevent information from moving between the outside world (untrusted network) and the inside world (trusted network)
- A firewall may be a
  - Separate computer system
  - Service running on an existing router or server
  - Separate network containing a number of supporting devices

The Development of Firewalls

- Packet filtering firewalls – simple networking devices that filter packets by examining every incoming and outgoing packet header
  - Can filter based on IP address, type of packet, port request, and/or other elements present in the packet



The Development of Firewalls

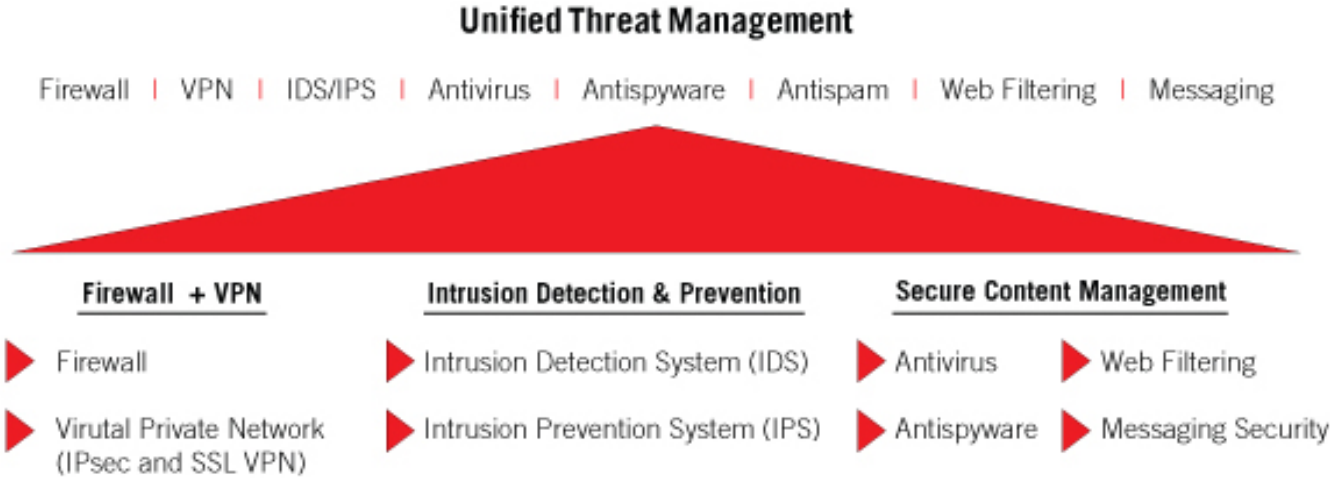
- Application-level firewalls
  - Proxy servers: dedicated computers kept separate from the first filtering router (edge router)
- Demilitarized zone (DMZ) – an intermediate area between a trusted network and an untrusted network
  - Cache server – a proxy server or application-level firewall that stores recently accessed Web content in its internal cache

The Development of Firewalls

- Stateful inspection firewalls – keep track of each network connection established between internal and external systems using a state table
  - Dynamic packet filtering firewalls
  - Understand protocols from information in packet header
  - State tables track the state and context of each exchanged packet by recording which station sent which packet and when
  - Can track connectionless traffic

The Development of Firewalls

- Unified Threat Management (UTM)
  - Networking devices categorized by their ability to perform the work of:
    - Stateful inspection firewall
    - Network intrusion detection and prevention system
    - Content filter and spam filter
    - Malware scanner and filter

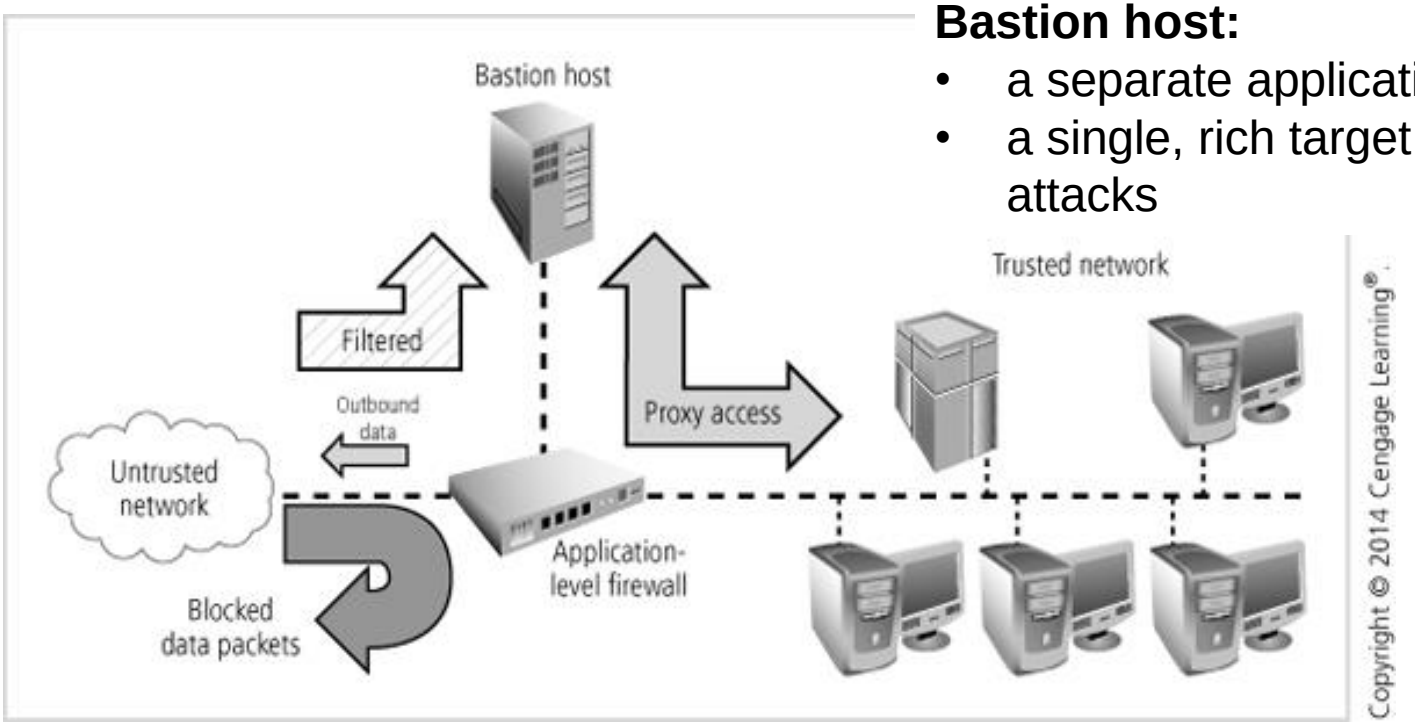


Firewall Architectures

- Four common architectures:
  - Packet filtering routers
  - Screened-host firewalls
  - Dual-homed host firewalls
  - Screened-subnet firewalls
- Packet Filtering Routers – simple but effective means of lowering the risk of an external attack
  - Lacks auditing and strong authentication
  - Large ACLs can degrade network performance

Firewall Architectures

- Screened-Host – combine the packet filtering router with a separate, dedicated firewall such as application proxy server



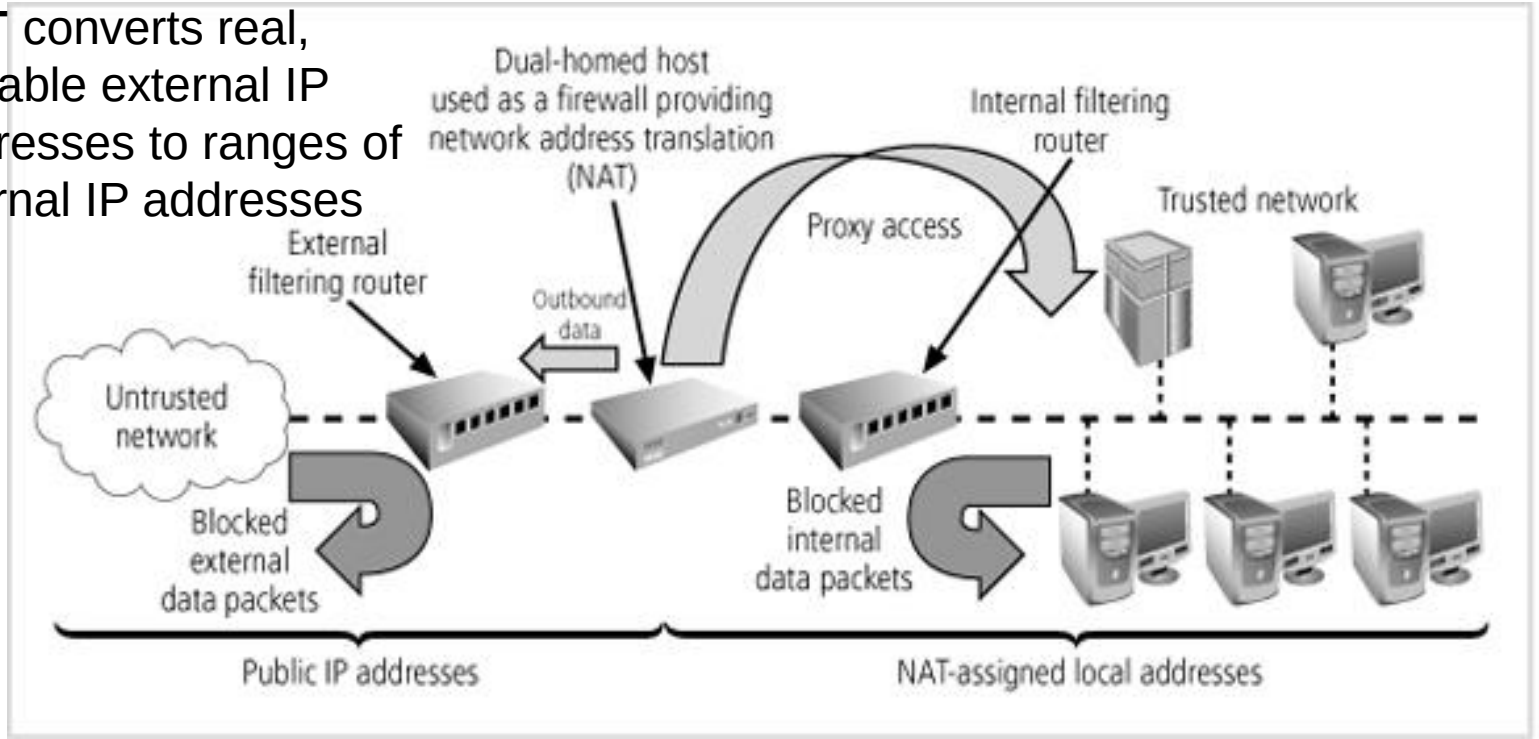
Bastion host:

- a separate application proxy
- a single, rich target for external attacks

Firewall Architectures

- Dual-Homed Host
  - The bastion host contains two network interfaces: one to the external network and one to the internal network
  - All traffic moving between must go through the firewall

NAT converts real, routable external IP addresses to ranges of internal IP addresses

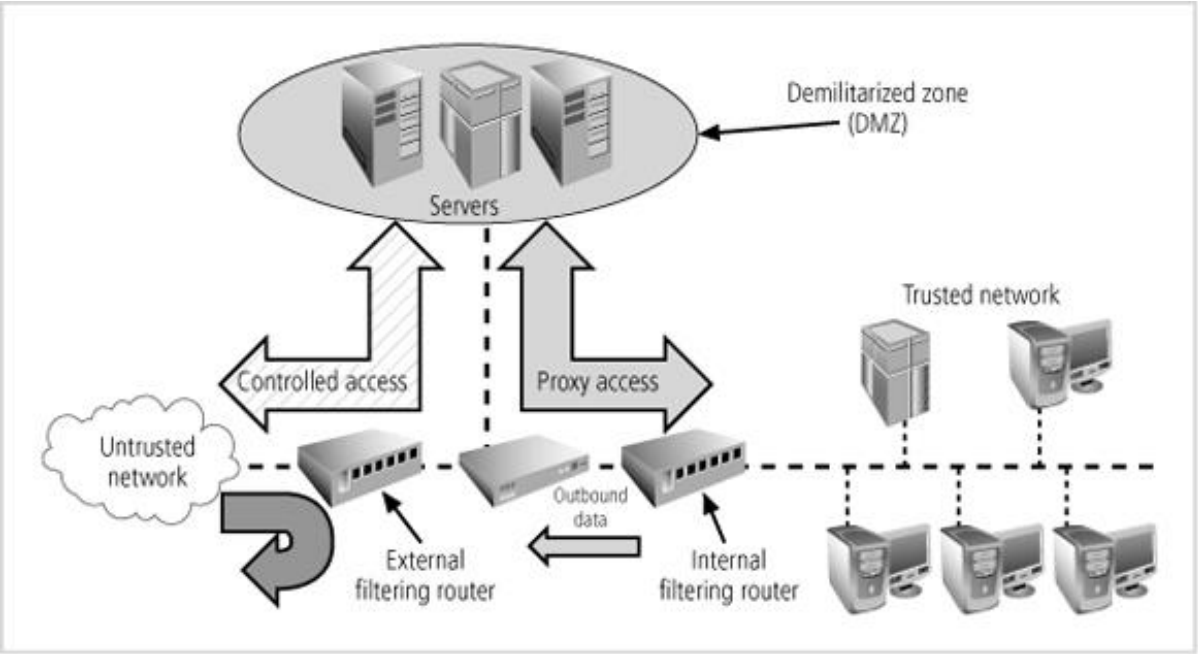


Firewall Architectures

- Dual-homed hosts take advantage of NAT or PAT by preventing external attacks from reaching internal machines with addresses in specified ranges
- Two disadvantages:
  - If the dual-homed host is compromised, it can take out the connections to the external network
  - As traffic volume increases, the dual-homed host can become overloaded
- Big advantage:
  - Provides strong protection with minimal expense

Firewall Architectures

- Screened-Subnet with DMZ
  - One or more internal bastion hosts located behind a packet filtering router, each protecting the trusted network
  - Provides an intermediate area between the trusted network and the untrusted network



Firewalls Limitations

- They are not creative and cannot make sense of human actions outside of their programming
- They deal strictly with defined patterns of measured observation
- They are designed to function within limits of hardware capacity and can only respond to patterns of events that happen expectantly
- They are computers and prone to programming errors, flaws in rule sets, and inherent vulnerabilities
- They are designed, implemented, and configured by people and are subject to human error

Managing Firewalls

- Administrative challenges to firewall operation
  - Training
  - Uniqueness
  - Responsibility
  - Administration
- Selecting firewall
  - What type of firewall technology offers the right balance between protection and cost?
  - What features are included in the base price? What features are available at extra cost?
  - How is easy is set up and configuration? How accessible are the staff technicians who can configure the firewall?
  - Can the candidate firewall adapt to the growing network in the target organization?

Managing Firewalls

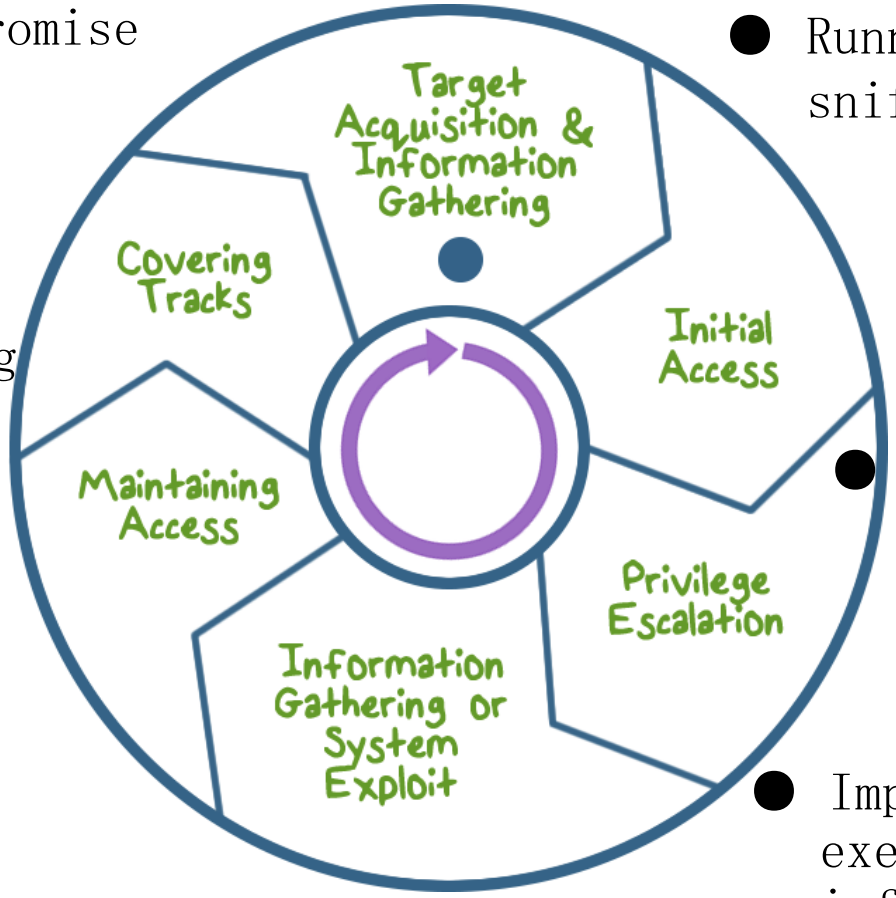
- Configuring firewall rule sets can be complex
  - Logic errors in the preparation can cause unintended behavior
  - Each rule must be placed into the list in the proper sequence
    - Reduces the number of packets that undergo intense scrutiny
    - Proper rule sequence ensures the most resource-intensive actions are performed after the most restrictive ones

Managing Firewalls

- Recommended practices for firewall use
  - All traffic from the trusted network is allowed out
  - The firewall device is never accessible directly from the public network
  - SMTP data is allowed to pass through the firewall and routed to a SMTP gateway to filter and route messaging traffic securely
  - All ICMP data is denied
  - Telnet/terminal emulation access to all internal servers from the public networks is blocked
  - When Web services are offered outside the firewall, HTTP traffic is prevented from reaching your internal networks via the implementation of some form of proxy access or DMZ architecture

Intrusions

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization



- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intrusion Detection and Prevention Systems

- Intrusion detection and prevention system (IDPS)
  - Specialized hardware or software
    - like burglar alarms by detecting a violation, activating an alarm, and reacting to the intrusion
  - Automate surveillance of computers and networks
  - Collect & synchronize records
  - Analyze data for evidence of security violations
    - Can be configured to notify administrators via e-mail and numerical or text paging
    - Require complex configurations to provide the appropriate level of detection and response

Intrusion Detection and Prevention Systems

- Intrusion detection and prevention system (IDPS)
  - Intrusion prevention – specified responses to detected intrusion scenarios
    - Stopping the attack by terminating the network connection or the attacker's user session
    - Changing the security environment by reconfiguring network devices to block access to the targeted system
    - Changing the attack's content to make it benign
    - Triggering events

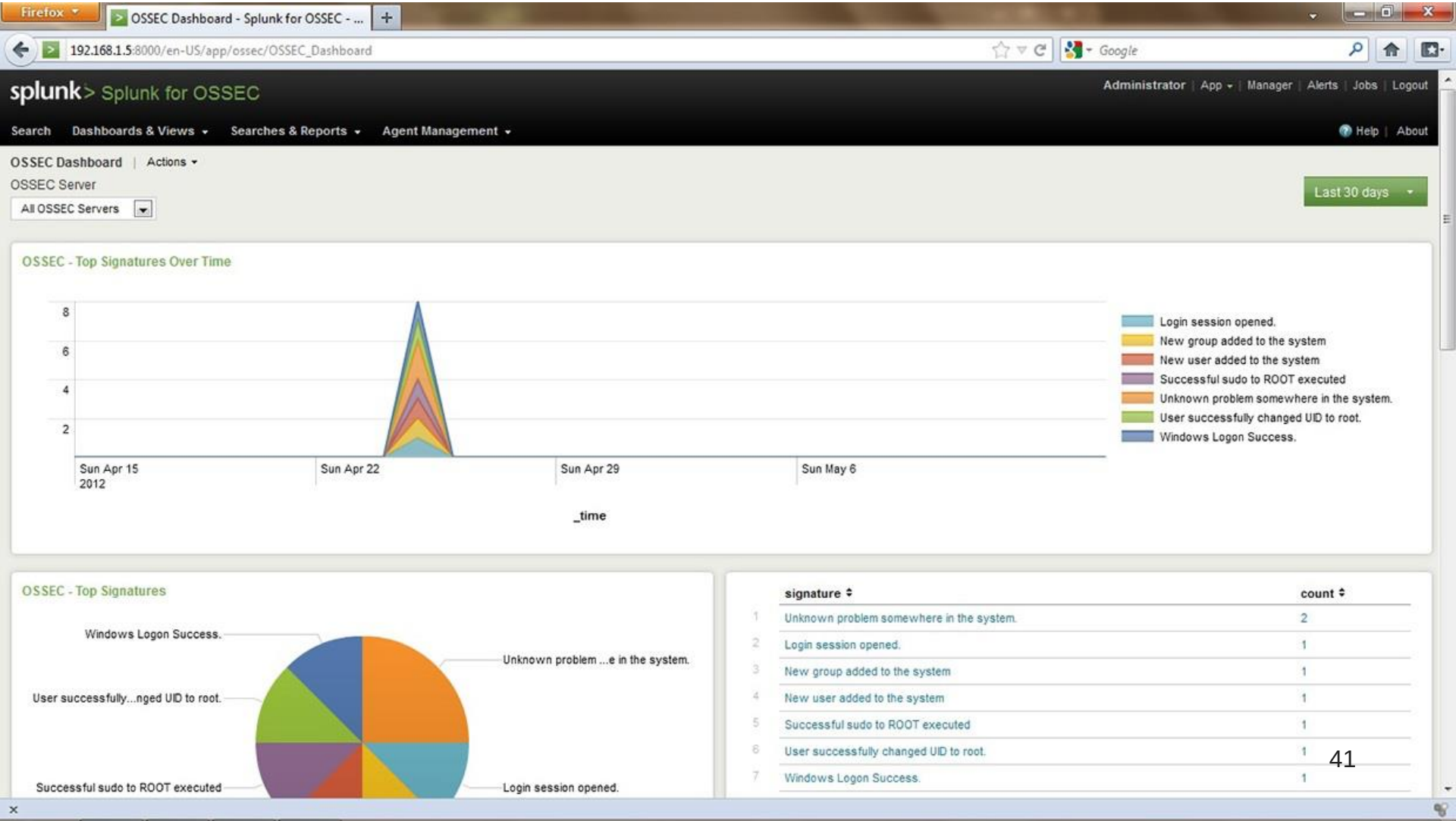
IDPS Process Structure

- Event generator
  - Host
  - Network
  - Application
- Analysis and decision engine
  - Look for attacks and anomalies
- Response and alarm generator
  - Automated disruption
  - Raising security barriers
  - Reports, logs, calls

Host-Based IDPS

- **Host-based IDPS (HIDPS)**
  - Configure and classify various categories of systems and data files
    - E.g., changes to system folders, critical data folders
    - E.g., security software (OSSEC, Tripwire)
  - Can monitor multiple computers simultaneously
    - Store a client file on each monitored host
    - That host must report back to the master console
  - The master console monitors the information from the managed clients
    - Notifies the administrator when predetermined attack conditions occur

Host-Based IDPS



Network-Based IDPS

- **Network-based IDPS (NIDPS)**
  - Resides on computer or appliance connected to segment of an organization's network
  - Monitors at selected points from a number of sensors
    - Passive or inline
  - Looks for patterns of network traffic
    - Large collections of related traffic that can indicate DoS
    - A series of packets that could indicate a port scan
- Hybrid IDPS
  - Installs data collection sensors that are both host-based and network-based
  - Analyzes all data in a central repository

Network-Based vs. Host-Based

Network-based IDS	Host-based IDS
• Broad in scope • Examines packet headers and entire packet • Near real-time response • Host independent • Bandwidth dependent • No overload • Slow down the networks that have IDs clients installed • Detects network attacks, as payload is analyzed • Not suitable for encrypted and switches network • Does not perform normally detection of complex attacks • High false positives rate • Lower cost of ownership • Better for detecting attacks from outside and detect attacks that host-based IDS would miss	• Narrow in scope, monitor specific activates • Does not see packet headers • Responds after a suspicious entry • Host dependent • Bandwidth independent • Overload • Slow down the hosts that have IDS clients installed • Detects local attacks before they hit the network • Well-suited for encrypted and switches environment • Powerful tool for analyzing a possible attack because of relevant information in database • Low false positive rate • Require no additional hardware • Better for detecting attacks from inside and detect attacks that network-based IDS would miss

Signature-Based IDPS

- **Signature-based IDPS**
  - AKA. knowledge-based detection, misuse detection
  - Uses known malicious data patterns or attack rules
    - Signature approach: anti-virus, network traffic scanning
    - Rule-based approach: NIDPS (Snort)
- Weakness:
  - Signatures must be continually updated as new attack strategies emerge
  - The time frame over which attacks occur

Anomaly-Based IDPS

- **Anomaly-based IDPS**
  - AKA. behavior-based detection
  - Statistical approach
    - Collects normal traffic data to establish a baseline
    - Periodically samples network activity
    - Uses multivariate, time-series models
  - Knowledge-based approach
    - Developed during training to characterize data into distinct classes
  - Machine learning approach
    - Develops a model to classify data as normal or anomalous
    - Bayesian networks, Markov model and HMM, clustering, outlier detection, neural networks

Anomaly-Based IDPS

- **Anomaly-based IDPS**
  - Can detect new types of attacks
  - Difficulty in selecting suitable metrics, developing knowledge, or assuming/labeling accepted behavior
  - High false positives
  - Require much more overhead and processing capacity than signature-based versions

Managing Intrusion Detection and Prevention Systems

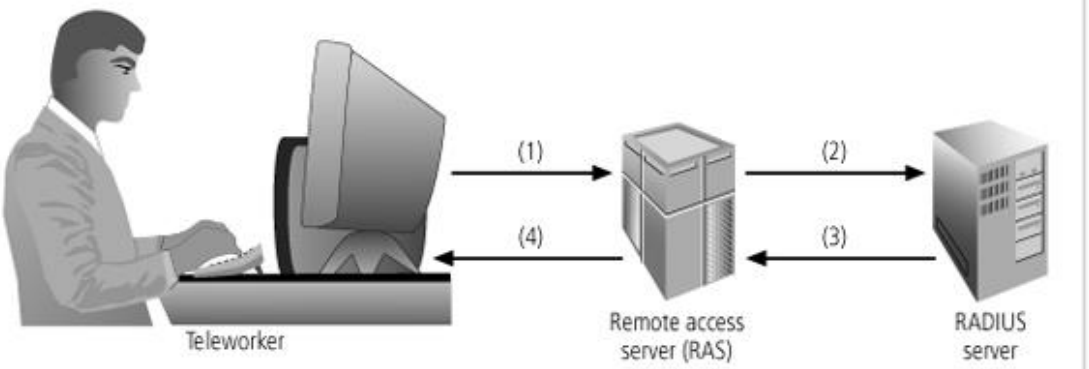
- Properly configure IDPS
  - differentiate between routine circumstances and low, moderate, or severe threats to the security of information assets
  - use technical knowledge and adequate business and security knowledge
- Properly configure IDPS agents (sensors)
  - a piece of software that resides on a system and reports back to a management server

Remote Access Protection

- Secure dial-up connections
  - Unsecured dial-up access represents a substantial exposure to attack
    - Get into the target network through unsecured modems
  - War-dialing
    - Attackers can use a device called a war-dialer
      - THCScan
    - Automated phone-dialing program dials number after number in a configured range, looking for modem carrier tone

Remote Access Protection

- Secure dial-up connections
  - Technologies have improved means of authentication for dial-up connections: **RADIUS**, **TACACS+**
  - Remote Authentication Dial-In User Service (RADIUS)
    - Client requests connection to a remote access server (RAS)
    - The central RADIUS server authenticates client's credential



Remote Access Protection

- Organizations with dial-up remote access must:
  - Determine how many dial-up connections it has
  - Control access to authorized modem numbers
  - Use call-back whenever possible
  - Use token authentication if at all possible

Wireless Networking Protection

- Secure wireless networks
  - Scope:
    - **WAP** (wireless access points)
    - **Footprint: t**he geographic area within which there is sufficient signal strength to make a network connection
  - Wifi attacks
    - **Wardriving:** moving through a geographic area or building, actively scanning for open or unsecured WAPs
      - WEP is completely broken!

Wireless Networking Protection

- Secure wireless networks
  - A number of encryption protocols are used
  - **Wired Equivalent Privacy (WEP)**
    - In the IEEE 802.11 wireless standard
    - Several flaws: reusing RC4 key, short key length
  - **Wi-Fi Protected Access (WPA)**
    - A set of protocols: WPA, WPA2
    - Based on AES
    - Can use an IEEE 802.1X authentication server

Wireless Networking Protection

- Secure wireless networks
  - **WiMAX** (Worldwide Interoperability for Microwave Access)
    - 802.16e wireless network
    - Higher bandwidth, larger coverage, and greater user #
    - Has a security layer to address authentication, authorization, encryption, and exchange MAC PDUs with the physical layer
  - **Bluetooth**
    - A standard for short-range wireless communications
      - Offers approximately a 30-foot range
    - Securing Bluetooth enabled devices
      - turn off Bluetooth when not needed
      - Do not accept incoming communications unless you know the requestor

Scanning and Analysis Tools

- Scanning Tools
  - **Port scanners**
    - Software to identify active computers on a network, active ports and services on those computers
      - nmap, unicornscan, …
    - Secure open ports, remove unnecessary ports
    - Detect scanning: short period of time, non-listening port
  - **Vulnerability scanners –** variants of port scanners
    - Automated tools that scan hosts and networks for known vulnerabilities and weaknesses
      - Identify exposed user names and groups, open network shares, configuration problems and other vulnerabilities
      - Nessus, OpenVAS, BoomScan, …

Scanning and Analysis Tools

- **Packet sniffer**
  - Software to collect and analyze copies of packets
    - Wireshark, Snort, Sniffer, Aircrack-ng
  - Provides a network administrator with information to help diagnose and resolve networking issues
- **Content Filters**
  - A software or a hardware/software appliance that allows administrators to restrict content that comes on a network
    - restriction of access to Web sites, spam e-mail
- **Trap and Trace**
  - Honey pots: providing simulated rich content areas to attract potential attacker
    - Distracting, tracing back

Scanning and Analysis Tools

- Some drawbacks:
  - Tools cannot simulate creative behavior of human attackers
  - Most functions by pattern recognition – previously known issues
  - Prone to errors, flaws, and vulnerabilities of their own
  - Subject to human errors
  - Using hackware – You get what you pay for
  - Tool usage and configuration must comply with an explicitly articulated policy
    - The policy must provide for valid exceptions
    - Content filters: some governments, agencies, institutions, and universities have established policies or laws to protect user's right to access content

Cryptography

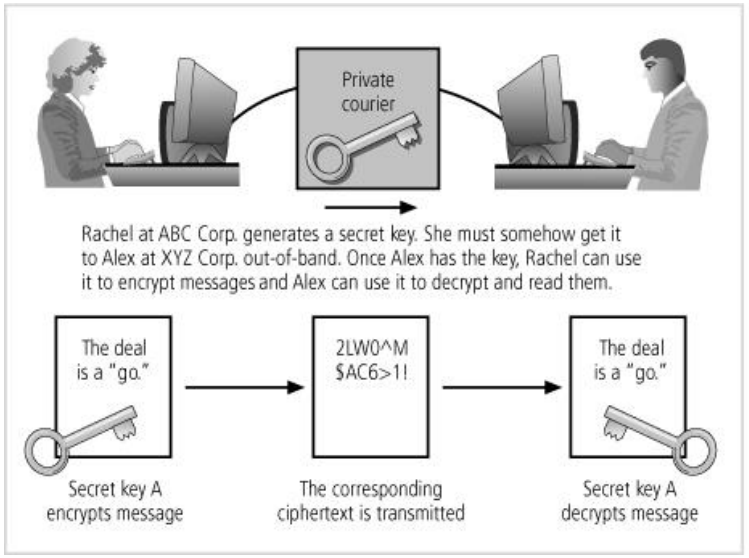
- The science of encryption is known as **cryptology**
  - **Cryptography**
    - the set of processes involved in encoding and decoding messages so that others cannot understand them
  - **Cryptanalysis**
    - the process of deciphering the original message (plaintext) from an encrypted message (ciphertext) without knowing the algorithms and keys used to perform the encryption

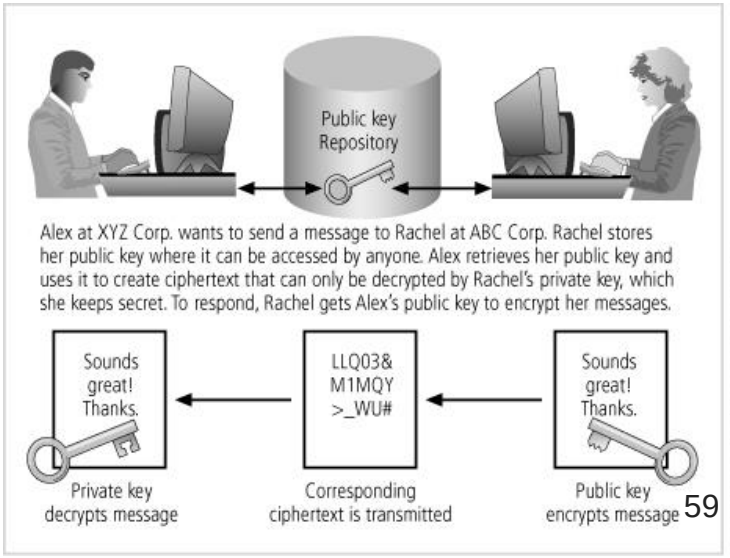
Encryption Operations

- Common Ciphers
  - **Substitution cipher** – substitute one value for another
    - Polyalphabetic substitutions use two or more alphabets
  - **Transposition cipher** – rearranges the values within a block to create the ciphertext
    - AKA. Permutation cipher
  - **XOR cipher** – the bit stream is subjected to a Boolean XOR function against some other data stream
  - **Vernam Cipher** – uses a set of characters for encryption operations only one time and then discards it
    - Developed at AT&T and also known as the “one-time pad”
  - **Book or Running Key Cipher**

Encryption Operations

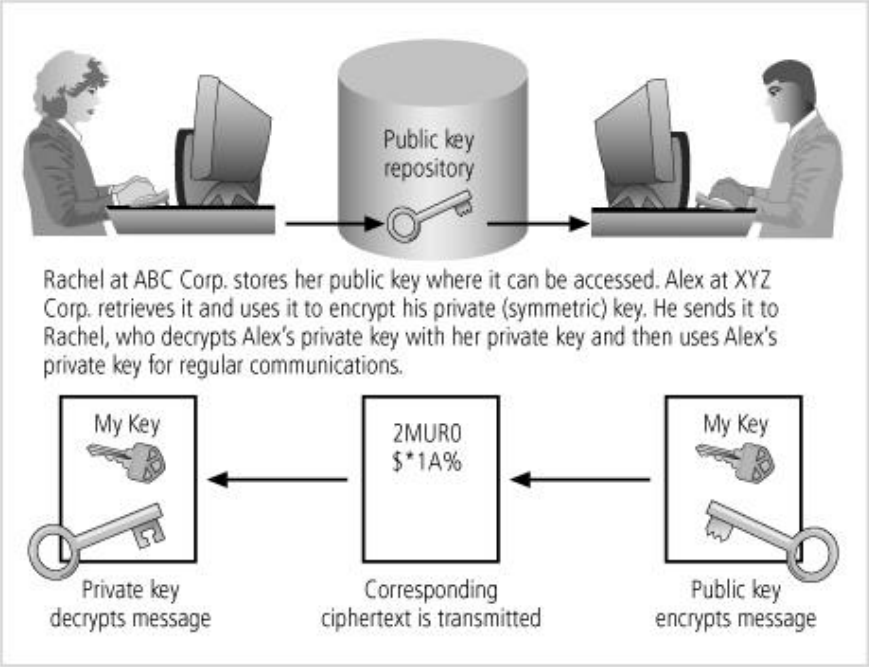
- Symmetric Encryption – use the same secret key
  - Also known as private key encryption
  - DES, AES, 3DES, Twofish, RC4,
- Asymmetric Encryption – use two different keys
  - RSA, ECC





Encryption Operations

- Hybrid Systems
  - Use asymmetric encryption to exchange symmetric keys
  - A widely use is based on Diffie-Hellman key exchange
    - Securely exchange private keys between two parties



Encryption Operations

- Digital Signature
  - Schemes for demonstrating the authenticity of a digital message or content
    - Provide nonrepudiation
  - Can use a reversed asymmetric encryption process
    - Use a private key to encrypt a message
    - Use the corresponding public key to decrypt
  - **Digital certificate**
    - Block of data attached to a file
      - certify that the file is from the organization it claims to be from and has not been modified from the original format
    - **Certificate Authority** (CA)

Encryption Operations

- **Public Key Infrastructure (PKI)**
  - Set of hardware, software, and cryptosystems necessary to implement public key encryption
    - Systems that issue digital certificates to users/servers
    - Systems with computer key values to be included in digital certificates
    - Tools for managing user enrollment, key generation, and certificate issuance
    - Verification and return of certificates
    - Key revocation services
  - Provides Authentication, Integrity, Confidentiality, Authorization, and Nonrepudiation

Using Cryptographic Controls

- Can be used to support several aspects of business:
  - Confidentiality and integrity of **e-mail** and attachments
    - Secure Multipurpose Internet Mail Extensions (S/MIME)
    - Pretty Good Privacy (PGP)
    - Privacy Enhanced Mail (PEM)
  - Authentication, confidentiality, integrity, and nonrepudiation of e-commerce transactions
    - Secure Sockets Layer (SSL): HTTPS, FTPS
  - Authentication and confidentiality of remote access
    - Secure Shell (SSH)
    - IP Security (IPSec): VPN connections
  - A higher standard of authentication
    - Kerberos: Single Sign-On

Managing Cryptographic Controls

- Important managerial issues are:
  - Don’t lose your keys!!
  - Know who you are communicating with
  - Give access only to those users, systems, and servers with a business need - a principle known as “least privilege”
  - Every cryptosystem has weaknesses
  - Trust in the CA?
  - It may be illegal to use a specific encryption technique when communicating to some nations
  - There is no security in obscurity
  - Implement correctly: well-constructed policy, well supported, tools correctly configured and used
- Technical controls are essential but cannot ensure security alone