Week 1

Network Security

- Security is a complex topic
    - **Confidentiality:** Private or confidential information is not made available or disclosed to unauthorized individuals
    - **Integrity:** Information and programs are changed only in a specified and authorized manner
    - **Availability:** Systems must work promptly; Service must not be denied to authorized users
- An adversary is someone who is attacking our system
    - **Eavesdropping:** The interception of information during its transmission over a communication channel
    - **Mitm:** Intercept a stream of data, (sometimes) modify it, and retransmit it
    - **Dos:** Interrupt or degrade a service by overloading it with messages
    - **Masquerading:** The fabrication of information that is purported to be from someone who is not actually the author
- **Symmetric Cryptography**
    - Symmetric ciphers are cryptographic techniques that make it possible to achieve confidentiality (and only confidentiality)
    - The same key is pre-shared between sender and receiver, for the encryption and decryption algorithms
    - Alice and Bob must both share the private key k for the message to remain confidential
    - To achieve both confidentiality and authenticity, it is necessary to use symmetric cipher (confidentiality) + MAC (authenticity). This requires two secret keys (one for the cipher and one for the MAC)
- **Public-Key Cryptography**
    - The receiver shares its public key pk with all senders who want to send it a message and uses its own private key sk to decrypt the messages it receives
    - Protect message m, using key sk to produce signature t, to protect the integrity of messages in the channel

Week 2

Authentication is core in network security

- Determining whether a user should be allowed access to a system
- Single or mutual authentication
- Vulnerable to
    - **replay attacks:** The adversary observed the interaction and used the messages to repeat a communication pattern
    - **relay attacks**
    - **mitm attacks**
- To prevent replay, we leverage a technique called **challenge-response**
    - Nonces (A **n**umber that is only used **once**)

    - Timestamps used for freshness
- Use one key pair for encryption/decryption or signing/verification. Use another for authentication
- A symmetric key for each session
    - Ephemeral
    - Used for confidentiality and/or integrity

Cryptogaphy

- Signatures used to ensure source is trustworthy
- Encryption used to ensure confidentiality

Kerberos

- An alternative system for authentication
- Kerberos is based on symmetric keys, but only requires N keys
- Trusted hardware assumption - KDC
- Ticket Granting Tickets (TGTs)
    - Each TGT contains:
        - Session key
        - User ID
        - Expiration time
    - Allows for stateless resource management
- **Kerberos Login**
    - Alice enters her password
    - Alice retrieves SA and TGT
        - Derives KA from its password
        - Uses KA to request TGT from the KDC
        - KDC generates session key SA and constructs TGT
    - Forward the TGT to access network resources
- **Kerberos Talk to Bob**
    - KDC knows Bob's key KB
    - Alice sends the request, alongside the TGT and an authenticator
    - KDC prepares a communication key for KAB
        - Encrypts it also with KB
        - And tags Alice (to avoid reflection attacks)
    - Alice retrieves KAB and an authenticator it can send to Bob
    - Bob knows its own key KB
    - Alice sends ToBob, and an authenticator encrypted with KAB
    - Bob does not know KAB...
        - But the ToBob token has KAB, encrypted with KB
        - Retrieves KAB and checks the authenticator for freshness
        - Encrypts a reply with the updated timestamp
    - Alice decrypts the reply and checks for freshness
- **Kerberos Security**
    - Key SA is used for authentication
        - Gives confidentiality/integrity for Alice-KDC communication
    - Key KAB used for Alice-Bob communication

        - Trustworthiness from the fact that the KDC encrypt it with KB
        - Only entity with knowledge of KB
        - Bob trusts the KDC!
    - Timestamps are used for authentication and replay protection
    - Timestamps behave like a nonce that is known in advance
    - “time” is a security-critical parameter!

Week 3

SSL and TLS

- Kerberos is at the application level - over UDP
- SSL/TLS is a middleware between application and TCP
- Architecture over classical network layers
- SSL/TLS Protocol Stack:
    - **Record Protocol**
        - Message Integrity and Confidentiality
        - Uses key agreed on handshake
    - **Handshake**
        - Most complex protocol
        - Crucial to establish a cryptographic key
    - **Change Cipher Spec**
        - Single message of a single byte
        - Establishes agreed cipher specifications
    - **Alert protocol**
        - TLS alerts
        - Can provoke warning, or terminate connections
    - **Heartbeat protocol**
        - Pings regularly
        - Prevents connection from shutting down
- TLS sessions are ephemeral, connections allow for multiple sessions
- Protocols rely on TLS for secure communication
- HTTPS uses TLS over HTTP
- Attacks at the TLS layer:
    - **Heartbleed:**
        - Small payload disguised as big one
        - Extract; prep (bad) payload; send reply
        - Response contains much more than expected
        - Gets TLS keys, cookies, passwords!

SSH

- SSH Connection Protocol runs on top of the Transport Layer Protocol
- Provides an authenticated, encrypted path to the OS command line over the network
- Relies on an handshake similar to TLS...
- ...but authentication is not certificate-based

- Allows for different channels with different purposes (Session, X11, Forwarded-tcpip, Direct-tcpip)
- Relatively simple

Week 4

IPSec

- IPSec lives at the network layer (OS space)
- Very complex! IPSec not widely deployed (complexity is a major factor)
- IPSec often used in VPNs
- Goals of IPSec: authentication, confidentiality, key management
- **Benefits of IPSec**
    - When implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter. IPSec and firewalls don't always mix well. Some firewalls change authenticated addresses, subverting the datagram structure
    - Transparent to applications and end users
        - Applications can be designed assuming secure channels
        - But that restricts flexibility...
        - What if the application wants to store encrypted messages?
        - Redundant security mechanisms
    - Secures routing architecture
        - Authentication and integrity for all routing messages
        - Protects against attacks such as IP spoofing!
- **Architecture**
    - **Key Exchange Management**
        - Internet Key Exchange (IKE) protocol
        - Done over UDP. This makes it unreliable, and thus is blocked by some firewalls
        - IKE has 2 stages:
            - **Phase 1 -** IKE security association (SA)
                - Comparable to SSL/TLS session (handshake; select cryptographic parameters; choose a master secret)
                - Output of Phase 1: Mutual authentication; Shared symmetric key; IKE Security Association (SA)
            - **Phase 2 -** IPSec security association (SA)
                - Comparable to SSL/TLS connection (ephemeral, uses Phase 1 to select encryption/MAC keys)
                - Outputs: Phase 1 gives us an IKE SA; Phase 2 gives us an IPSec SA; We now have a symmetric session key
            - Unlike SSL, necessity of two phases is not as obvious. If multiple Phase 2s do not occur, then it is more costly to have two phases!
    - Two main functions/Two security header extensions

Encapsulating Security Payload (ESP)	Authentication Header (AH)

Encapsulating Security Payload (ESP)	Authentication Header (AH)
Encapsulated Security Payload	Authentication Header
A combined function for authentication/encryption (integrity and confidentiality)	An authentication-only function (integrity only)
Key exchange function	AH included in IPSecv3 for backward compatibility
Protects everything beyond IP header	Protect everything beyond IP header and some header fields

    - Two modes of operation
        - **Transport mode:** add information/security to the original packet
        - **Tunnel mode:** protect the original packet by encapsulating it into a new IP packet
- IPSec Key Management
    - Handles key generation and distribution
    - Often requires two pairs of keys (one for each direction)
    - Two types of key management: manual and automated
- A Security Association Database (SAD) is used to store long-term parameters associated with each SA
- IP data includes TCP header, HTTP header, ...
- Managing IPSec policy is quite complex
    - Mistakes lead to loss of connectivity
    - Mistakes lead to loss of security
    - Many options to keep track of
- IPSec assures that:
    - A router advertisement comes from an authorized router
    - A router seeking to establish/maintain neighbour relationship with a router in another domain is authorized
    - A redirect message comes back to its authentic original source
    - A routing update is not forged

Week 5

Denial of Service

- Denial of Service attacks aim to disrupt system resources
- Resource categories that can be attacked:
    - Network bandwidth
    - System resources
    - Application resources
- The common tactic is to overwhelm the network
    - **Flooding ping:** The goal of the attack is to overwhelm the capacity of the network connection to the victim organization
    - **Reflexion Attack:** The goal of the attack is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary (Echo-Chargen)

- **Smurf Attack:** Exploits IP broadcast addresses and spoofed source addresses to overload a targeted device or network with bogus traffic
- **SYN Spoofing:** Attacks the ability of a server to respond to future connection requests (overflows tables used to manage TCP connections). Legitimate users are denied access to the server

Distributed Denial of Service

- Use multiple systems to generate attacks
- Attacker uses a flaw in operative system or in a common application to gain access and install a program on it (zombie)
- This method can be applied to gain access to large collections of such systems, which are then used to perform attacks (botnet)
- **Botnets and Attacks**
    - Corrupted machines zombified to help with attacks
    - Botnets are hierarchical systems of zombies
    - Used to upscale attacks
    - **HTTP flood:**
        - Attack that bombards Web servers with HTTP requests from many different hosts.
        - Spidering: Start from an HTTP link and follow all links on a Website recursively
        - Slowloris: Send legitimate HTTP requests that never complete
    - **DNS Amplification Attack:**
        - Use DNS requests with spoofed source IP address being the target. Exploit DNS behavior to convert a small request to a much larger response. Attacker sends request to multiple well connected servers, flooding the target
        - Mitigating DNS Amplification
            - Reduce the total number of open DNS resolvers
            - Restricting a DNS resolver to only respond to queries from trusted sources
            - Have ISPs actively detect spoofed IP addresses
            - **DDoS Blackhole Routin:** Traffic is routed into a null route and is lost. An aggressive countermeasure to blocking DDoS attacks. Often too severe a measure
    - NTP Amplification Attacks
        - An innocuous service for clock synchronization...
        - Same method as previous attacks
    - Simple Service Discovery Protocol
        - Used by Universal Plug and Play (UPnP) to advertise and search for services/devices over the network
        - Attack is based on a UDP request over M-SEARCH...
- Denial-of-Service Monitoring
    - 150$ are sufficient to acquire a week-long DDoS attack on the black market
    - More than 2000 daily DDoS attacks can be observed world-wide
    - 1/3 of all downtime incidents can be attributed to DDoS attacks

Countermeasures

- Hard to counteract
- Requires proactive policies and spoofing prevention
- And a good back-up plan for when they happen

Week 7

Firewalls as the first line of defence

- Establish the criteria under which packets come in/go out
- Can be deployed in a variety of ways
    - Packet filter - network
    - Stateful packet filter - transport layer
    - Application proxy - application layer
- No clear-cut "best" practice
- Depends on security requirements

Firewall deployment/configuration

- Firewall efforts can be done in multiple ways
    - **Bastion hosts:**
        - Critical strongpoint in the network
        - Host application/circuit-level gateways
        - Common characteristics:
            - Runs secure O/S, only essential services
            - May require user auth to access proxy or host
            - Each proxy can restrict features, hosts accessed
            - Small, simple proxies, security-checked
            - Limited disk use, read-only code
    - **Host-based firewalls:**
        - Used to secure an individual host
        - Available in/add-on for many O/Ss
        - Filter packet flows
        - Often used on server
        - Advantages: Tailored filter rules for specific host needs; Protection from both internal/external attacks; Additional layer of protection to org firewall
    - **Personal firewalls:**
        - Controls traffic flow to/from PC
        - For both home and corporate usage
        - Can be a software module on a PC
        - Or in a DSL router/gateway
        - Characteristics: Typically much less complex than its counterparts; Primary role to deny unauthorized access; May also monitor outgoing traffic to detect/block malware activity
- Firewalking vulnerability
- IPTables to establish access rules

Week 8

Understanding system intrusion

- A wide range of threats
    - From expert cyber criminals
    - ...to script-kiddies

Intrusion Detection Systems

- Intrusion countermeasure based on (potentially complex) patterns
- Mainly host-/network- based, depending on monitoring capabilities
- Different methodologies for detection
    - Signature Detection
    - Anomaly Detection
- Configuration requires nuanced understanding of system
- Responses to intrusion can also vary widely