Module Eleven

CSG1105 Applied Communications

May 15, 2020

Network Security

- Information Security has a focus of the protection of the **confidentiality, integrity and availability** of data, often called the **CIA Triad**.
- The added goal of **non-repudiation** is also added
- Networks provide connectivity between computer systems
- The distributed nature of networks provide potential attack points

Where to secure?

- The economic protection of information requires a cost-benefit analysis in order to determine where to invest in protection measures
- **Threat:** - any perceived action that may cause information/economic loss
- **Risk:** - a quantified threat where the probability and consequence are calculated
- **Countermeasure:** - a process, program or hardware intended to alleviate the threat/risk identified
- A countermeasure must be appropriate in implementation that it's cost doesn't outweigh the pontential loss of a threat (ie driving a tank to reduce the consequence of a collision)
- A countermeasure must be appropriately located to have maximum befefit

Countermeasures

- There are numerous countermeasures to identified threats
  - Physical security
  - Policy and training
  - *Authentication*
  - *Encryption*
  - *Firewalls*
  - *Intrusion Detection*
  - Malware/Virus scanning
- The network is often the avenue for attacks, but may not be the appropriate location for a countermeasure
- This module will look at the attacks/countermeasures that require implementation with the network infrastructure

Network Attacks

Figure 1: Interuption

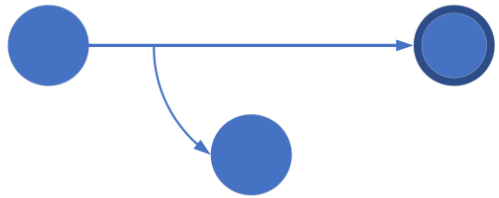


Figure 2: Interception

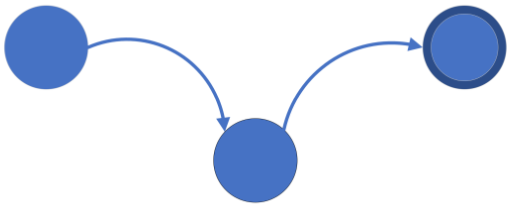


Figure 3: Modification

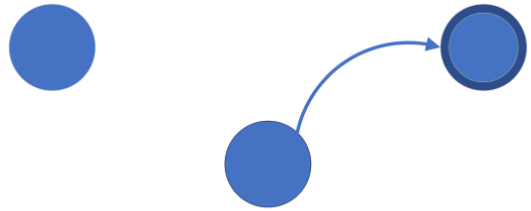
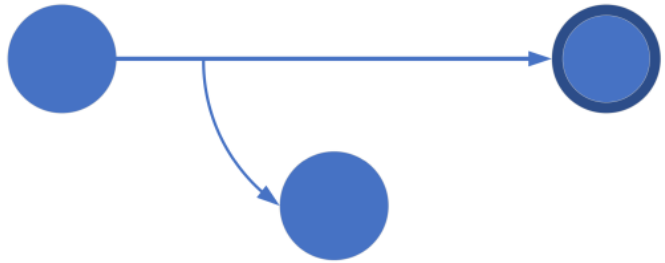


Figure 4: Fabrication

Interruption

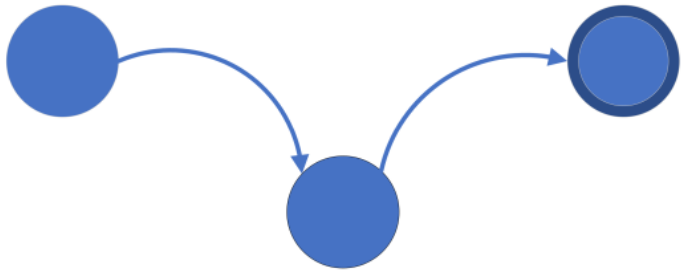
- Generically called **Denial of Service (DoS)**
- May be a physical attack (cable severing, wireless inference) or a logical attack (DDoS from Botnet)
- Intent is to cause financial, reputational damage to target

Interception



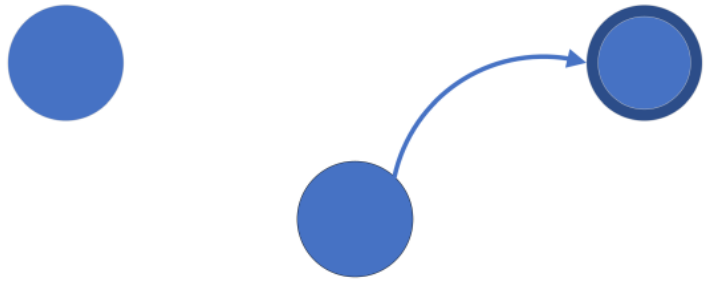
- The accessing of information by unauthorised agents
- May be physical (tapping of a cable, collecting wireless transmissions) or logical (protocol manipulation, man in the middle (MITM))
- Intent is to gather information for multiple purposes including financial, intellegence gathering etc)

Modification



- The interception of an information stream and modification prior to deliver
- May be physical (tapping of a cable, collecting wireless transmissions) or logical (protocol manipulation, man in the middle)
- Intent is to alter transmissions either for financial gain or to influence recipient

Fabrication



- The construction and delivery of a fraudulent message
- May be physical (tapping of a cable, collecting wireless transmissions) or logical (protocol manipulation, man in the middle)
- Intent is create transmissions either for financial gain or to influence recipient

Countermeasures

- Physical/Infrastructure
- Authentication/Authorisation
- Encryption
- Firewalls
- Intrusion Detection

Physical Infrastructure

- Secured wiring closets with monitoring of access (Alarms, CCTV)
- Redundant power supplies and Uninterruptable Power supplies (UPS)
- Deactivation of unused ports
- VLANs: subnets with users at similar classification levels

Authentication

- A network user is remote to servers/services provided
- Authentication method needs to:
  - `Identify user`
  - `Allow access to resources based on identity`
  - `Be secure over network connections`
- No clear-text authentication (old systems like *telnet* and *ftp*), authentications to be hashed or encrypted
- Wi-Fi AP use of RADIUS, KERBEROS, X509 & Digital Certificates

Encryption

- Impossible to physically secure end-to-end network connections, especially WAN
- Encryption is used to protect transmissions between communication end points
- Previously discussed in Wi-Fi and VPN connections
- Details of encryption implementation methods are beyond the scope of this unit, but some general discussion of techniques is required

Symmetric Encryption

- Symmetric encryption requires both ends have the same **encryption key**
- Requires a secure method of key distribution
- High performance, requires lower processing power
- Examples DES (obsolete), AES

Asymmetric Encryption

- Asymmetric encryption uses a **Private Key** and a **Public Key**
- Public key may be published and used by anyone
- Message encrypted by public key can only be decrypted using private key
- Message encrypted by private key can only be decrypted using public key (used for **non-repudiation & digital signatures**)
- Lower performance, requires more processing power - slower
- Examples RSA and Elliptic Curve cryptography

Combination Methods

- Some systems, such as SSL use a combination of Asymmetric and Symmetric encryption
- Session Key exchange is done using Asymmetric
- Bulk encryption performed using Symmetric encryption with key obtained with AE
- Session keys changed periodically to enhance security

Key Sizes

- In general, the longer the key, the better the security
- AES has available key sizes of 128,192 and 256 - 256 bits recommended
- RSA, which is susceptible to factorisation, key of 2048 bits recommended
- EC key of 256 is equivalent to RSA key of 3072 bits
- When keys are derived from passwords (eg Wi-Fi PBKD2), the longer the password the better

Digital Signatures

- A digital signature is a **Message Digest** encrypted with a private or public key
- A message digest is where a message has had a cryptographic (one-way) hash function applied to it. If any bit in the message is changed, a very different hash will result.
- A **Digital Certificate** is a public key that the owner has been verified by a **Certificate Authority** and has been digitally signed by that authority
- The most common format for Digital Certificates is defined by **X.509** and codified in **RFC5280**
- Digital Certificates are required for SSL/TLS and are also used for signing electronic documents such as PDFs to verify the origin (Cross-ref **Non-Repudiation**)
- Digital Certificates are also used to verify that software has come from identified source

Secure Sockets Layer (SSL)

- SSL/TLS is a shim layer between *Application and Transport Layers*
- Originally developed for communications between web client and server
- May also involve authentication using **Digital Certificates**
- Uses TCP port 443 by default (Firewall friendly)
- Most web sites now use HTTPS (HTTP over SSL/TLS) by default
- Susceptible to *MITM* attacks if certificates not checked (some employers put a SSL proxy on the Firewall to permit inspection of traffic)
- Is now used in **ssh** (secure shell) and **SSLVPN** and others

IPSec

- originally developed for IPv6, then backported to IPv4
- Two protocols - Authenticating Header (AH) and Encapsulating Security Payload (ESP)
- Two modes
  - Transport mode - only payload encrypted
  - Tunnel mode - entire packet encrypted
- Can be used host to host or network to network
- See Module Ten for IPSec VPN

Firewalls

- In a building, a Firewall is a **rated** barrier to prevent or slow the spread of a fire
- A network Firewall is a filter to block undesirable traffic and to permit and monitor authorised traffic
- Ideally, it is the **only** access to/from the Internet for a LAN
- Permitted traffic is defined by a **Security Policy**
- General principle is *"That which is not expressly permitted is prohibited"

Firewall Actions

- Packet filtering - Packets are filtered against a set of rules. Packets not selected for access by the rules are discarded
- Connection Proxy - no direct connections to the Internet, all are via the Firewall and may apply additional screening (eg email spam and malware screening)
- Stateful Inspection - The Firewall maintains state information about connections and compared to persistent data store. If an incoming packet is not part of an existing connection or contains inconsistent status information, it will be dropped

Filter Rules

- Each router type will implement filters in a unique way
- Generic example

action	src	port	dest	port
permit	*	*	spam	25
permit	<net >	*	*	*
permit	*	>1024	*	*
refuse	*	*	*	*

- Filters are on a per interface basis and different sets apply to incoming and outgoing connections separately

Intrusion Detection Systems (IDS)

- System alerts administrators whenever an intrusion is detected
- Some IDS respond to intrusions automatically
- Need to place in multiple locations on the network
- Anomaly model systems
  - Based on AI techniques
  - Take measurements of normal activity – the alarm is raised when network activity changes from the norm
- Misuse detection systems
  - Detect known hacker behaviour patterns
  - Virus scanning software usually uses this method

Intrusion Detection Systems

- Cisco NGIPS
  - Sensor appliances
- Many commercial offerings
- Snort
  - Open source
- Linux Intrusion Detection System (LIDS)
  - Kernel patch for Linux systems to detect intruders on that system