Unit-V

Mangal
Date / /20

Wi-Fi Basics

* Wired Ethernet (802.3) vs Wireless (802.11)
* Comparison of wireless & wired connections
  - Wired Ethernet (faster)
  - More obstacles & interference in Ethernet
  - Drop in performance
  - Not secure as wired.

Wireless clients and NICs

* Computers are connected to wireless LAN with NICs present in computers
* Wireless router regulates traffic
* Two types of mode :- ad hoc & infrastructure
* Adhoc mode — Wireless network adapters. Point-to-point ~~computer~~ communication & peer-to-peer (suitable for small networks)
* Infrastructure mode — Wireless device → ~~communicates with~~ wireless access point (WAP) (Scalable)

To connect wireless equipped device with WAP, all must be configured with same service set ID (SSID)
WAP hears all wireless devices but individual devices cannot hear other devices. [Hidden node problem]
Can be solved using CSMA/CA.
Wireless device listens before sending a packet. If some other device is transmitting, it waits for a random period & tries again.

If first wireless device listens & discovers no other device is transmitting, it sends a short message (Ready-to-send)

Page / /20

WAP modes

- Normal mode:- Central point of connection for client wireless device
- Bridge mode:- One AP communicates with another AP Useful for extending WLAN between buildings
- Client mode:- One AP as client communicates with APs that are not clients
- Repeater mode:- Repeats AP signal to extend the range.

Wireless Communication Standards.

802.11 → 802.11b, 802.11a, 802.11g, 802.11n } Difference in speed & frequencies.

- Wireless devices broadcast by using spread-spectrum technology. Transmits data over wide range of radio frequencies (RFs).
- less noise interference & data rate may speed up/ slow down based on signal quality
- * DSSS (Direct sequence spread spectrum) - Transmission method divided into stream of information transmitted in small bits (mapped to spreading code)
  - resistant to interference, less bandwidth

* FHSS (Frequency Hopping Spread Spectrum)
Broad bandwidth divided into smaller 75 subchannels of 1MHz. Transmitter will transmit in various subchannels.
Supports more wireless devices than DHSS.

* ODM (Orthogonal Division Multiplexing)
Distributes data over carriers that are spaced apart at precise frequencies. Used for digital TV.

Bluetooth basics (802.15-1)

- PAN (Personal Area Network).
- Provides peer-to-peer service
- Uses FHSS technology
- 3 classifications
  - class 1 - Longest range upto 100mts (100mW power)
  - class 2 - Upto 20mts (2.5mW power)
  - class 3 - Upto 10mts (1mW power)

Wi-Fi Security

WEP (Wired Equivalent Privacy) - Data confidentiality
* RC4. Symmetric encryption & uses 64 bit/128 bit keys
* All the bits of the key are not used for encryption [24 bit taken as IV to encrypt each packet with a different key].

* Transmitter & receiver are initialized with secret key that is distributed
* Transmitter uses 24 bit IV ~~& appended to~~ 40 bit secret key & generates PRNG (Pseudo random number generator) (i.e) seed.
* With this seed, it produces key stream of random bytes
* Key stream is XOR'd with PT to obtain CT.
* Transmitter appends ciphertext to IV & sets a bit that indicates it is a WEP encrypted packet.
* Receiver checks to see if that bit is set. If so, it extracts IV & appends to secret key.
* This key stream is XOR'd with ~~PT~~ CT to obtain PT.

Mangal
Date 1/ 20

Wi-Fi Protected Access (WPA)

* Uses TKIP (Temporal Key Integrity Protocol)
* Scrambles keys using hashing algorithm & adds integrity checking feature that verifies if keys have been tampered.
* Strength: Manage integrity check & avoids using encryption with different key for different packets.
* Another WPA authentication protocol - Extensible Authentication Protocol (EAP)

* Facilitates authentication between client & server

Mangal
Date / / 20

* 4 types of EAPOL packets.

EAPOL packets :- Transports EAP packets across LAN.

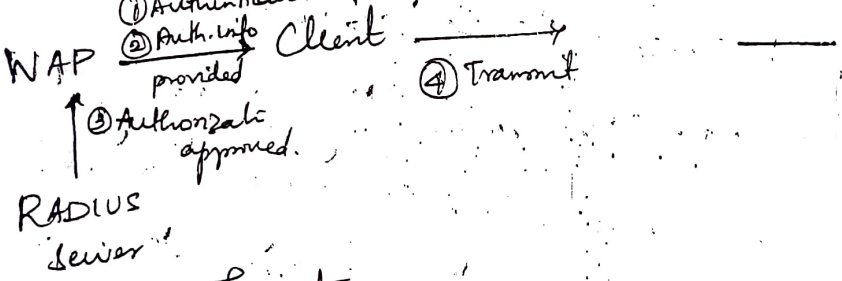
EAPOL start :- Informs authenticator that it wants to authenticate to network.

EAPOL logoff :- Client leaves the network.

EAPOL key :- Used with 802.1x for key distribution

802.1x Authentication

* Port based access control
* Used in conjunction with EAP & used to authenticate devices that attempt to connect to specific LAN port
* EAP in wireless networks works as follows.



Wireless LAN Threats

Wardriving – Discover location using tool like NetStumbler and records location using GPS

Warchalking – Marking buildings and sidewalk to access an exposed company wireless network

Warflying – Same as wardriving but an aeroplane is used.

- Piggybacking
- Wireless hackers who can access sensitive information or crash critical system

Netstumbler

* Windows based GUI tool that sends a stream of broadcast packets & checks organization's wireless LAN coverage
* It can provide details like MAC address, SSID, channel, access point name, vendor, signal strength, GPS coordinates
* Ministumbler for handheld device.
* Netstumbler sends probe request frames that cause APs to respond with information about themselves.
* If WAP has closed network feature, Netstumbler will not get response.
* Even if WAP is in hidden mode, attacker can get SSID by sending a spoofed disassociate message. The spoofed client tries to reassociate with WAP using probe requests by which SSID is revealed.

Kismet

* It is an 802.11 layer 2 wireless network detector running on Linux OS.
* Works with wireless cards.
* Features: Detection of Netstumbler client, hidden SSID decloaking, IP block detection, Ethereal file logging, grouping & custom naming of SSIDs, manufacturer identification, etc.,

Eavesdropping

Mangal
Date from 20 Open

* Attacker can intercept radio signals from WAPs and decode the data that is being transmitted.
* Many wireless equipments are sold with default setting of open WAP's and without encryption turned on. Using this, an attacker can attack and anyone tracing the IP address will be led only to victim & not to attacker.
* Tools – Dsniff, WinSniffer, Cain & Abel.
* Dsniff – Passively monitors network to track usernames, passwords
* WinSniffer – Captures & decodes passwords & usernames of FTP, POP3, HTTP, Telnet etc
  Used by security professionals to audit the network / by attackers to access sensitive information.
* Cain & Abel – Password sniffing & cracking
* LCP – Performs account information import, password recovery, brute force password cracking, hash computing

Rogue & unauthorized access points

* Rogue access point – unauthorized connection to corporate network

* Two threats – employees may install unmanaged AP's & ability to perform WAP spoofing
* Site surveys may be performed by attacker
* AP spoofing – Hacker sets up their own rogue WAP near victims network. If spoofed WAP has stronger signal, attacker will be in middle of all transmissions. When performed in open hot spot, this attack is called evil twin attack

Date

Denial of Service

- Authentication flood attack
- Deauthentication flood attack
- Network jamming attack
- Equipment destruction attack

Exploiting the network

Finding & assessing the network

* First task is to find the network using tools like Kismet / Netstumbler
* You can use directional and omnidirectional antenna to pick up signals from single and all directions respectively.
* Wireshark can help one determine if organization is using Mac filtering.
* To bypass Macfiltering, Change MAC, a MAC spoofing tool is used.

Setting up Aerodump

Mangal
Date / /20

WEP cracking can be done from a single system / from two systems using a suite of tools, Aircrack. It includes

- Airodump : Captures wireless packets
- Aireplay : Performs injection attacks
- Aircrack : Cracks WEP key

* Configure wireless card to capture ARP packet.

Configuring Aireplay

* Used to inject packets to increase selection of crackable data.
* First step in two-step proces. - Send broadcast message requesting targets physical address.
If target recognizes its address, it replies with MAC address
* If encryption is being used, response is sent as encrypted traffic

Deauthentication & ARP Injection

* When client device becomes deauthinticated, it will try to reauthenticate itself with WAP. During this proces several ARP requests will take place.
* Aireplay tries to capture ARP request so that it can rebroadcast the packet & generate additional traffic

Capturing IVs and cracking WEP key

* When attack is launched, steady stream of packets will be received.
* Approximately 3L and 1L packets to break 64 bit WEP & 128 bit WEP respectively
* Aircrack is used to crack the key.

Other Wireless Attack Tools

- Mognet
- WaveStumbler
- AiroPeek
- Airsnort
- THC wardrive
- AirTraf
- Airmarf
-

Exploiting Bluetooth

* Bluejacking allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices.
* Bluesnarfing - Theft of data, calendar information, or phone book entries.

Tools include

- RedFang
- Bluebug
- Bluesniff
- Bts canner

Securing Wireless Networks

Mangal
Date / /20

Defense in depth. Builds many layers of protection

- Encryption to hide data from unauthorized individuals
- Limiting access based on least privilege
- Providing physical protection to hardware
- Using authentication to verify identity of network users.
- Employing layers of security controls

* One can change the default value of SSID
* Limit access to wireless network to specific network adapters
* MAC filtering uses MAC address assigned to each network adapter to enable / block access to the network
* Site survey - Gather enough information to determine if client has right number & placement of APs to provide adequate coverage throughout the facility. It is also important to see how far the signal radiates outside of the facility. Also useful in detecting interference from other sources that could degrade the performance of wireless networks.

Misuse Detection

* Wireless IDs work like wired ID as it can monitor traffic & alerts administrator of unusual traffic patterns
* Can be centralized / decentralized & should have a

Combination of sensors that collect & forward 802.11 data

Date / /20

* Some wireless IDS can provide general estimate of cracker's physical location.
* Commercial IDS products — AirDefense Rogue Wave, PBN RealSecure Server Sensor
* ~~Open source~~ solutions — AirSnare, WIDZ Intrusion Detection, Snort-Wireless.

Intrusion Detection

Types & Components

Two types :- Network based intrusion detection systems (NIDSs) and host-based intrusion detection systems (HIDSs)

NIDSs

* Examines packet on network & look at data in an attempt to recognize an attack
* NIC is placed in promiscuous mode to identify all packets; not just ones addressed to it
* NIDS can be plugged into hub if system is operating on it.
* If switch is used, port must be spanned/mirrored.
* Advantage :- Can support many sensors to monitor demilitarized zone (DMZ), internal network or specific nodes on network.

* Disadvantage :- It will not detect malicious host made by an intruder logged in at host's terminal

Date / / 20

* Examples :- Snort, Cisco Intrusion Detection System, Symantec Network Sweeper

HIDS

* Monitors traffic on one specific system
* Does not place NIC in promiscuous mode
* Looks for unusual events / patterns that may indicate problems
* Efficiently detects unauthorized accesses & activity
* Examples :- Tripwire, Swatch, Real Secure.

Parts

* Network sensors :- Detect & send data to system
* Central monitoring system :- Processes & analyses data sent from sensors.
* Report analysis :- Counteracts a specific event
* Database & storage components :- Performs trend analysis & stores IP address, information about attacker
* Response box :- Inputs information from the above components & forms a response

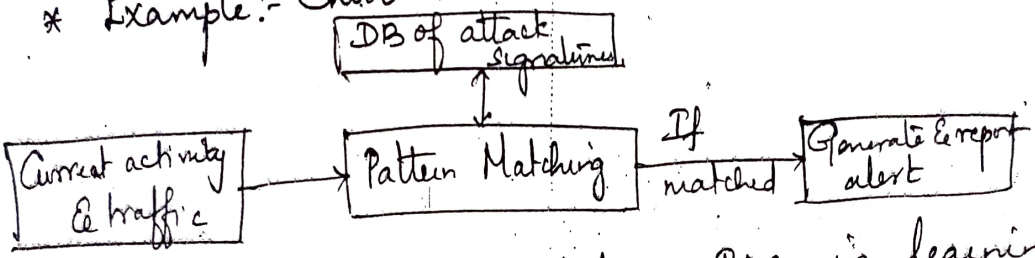
The activity detected by IDS depends upon placement of sensors. These sensors must be tuned so that these may detect intrusions correctly. A good IDS should

report high number of true positives and true negatives.

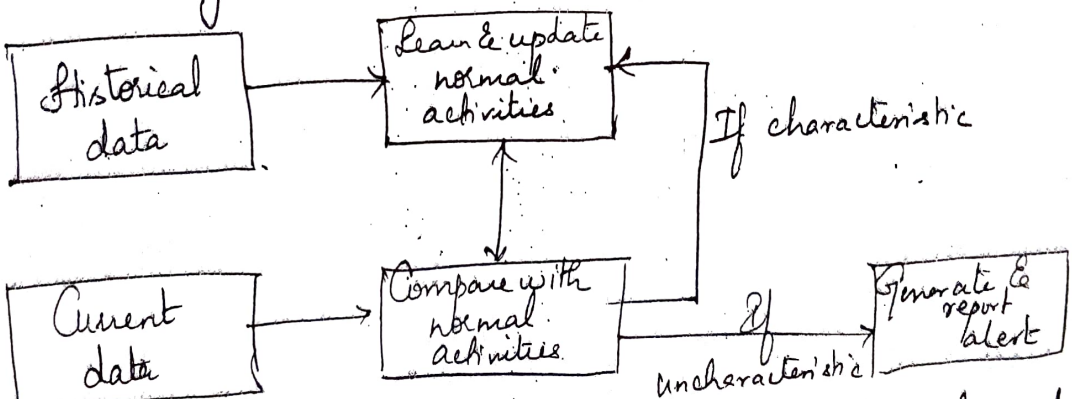
Mangal
Date / /20

IDS Engines

* Signature based (pattern matching) IDS works on identifying an attack based on signatures loaded into database previously.
* Alerts are triggered based on IP packets, SYN packets / malformed ICMP packets
* Example:- Snort



* Anamoly based IDS places IDS in learning mode. so that it can learn what constitutes normal activity



* Performs deep packet inspection (decoding of packets)
* Example:- If DNS responses are detected without DNS request, the activity is termed cache poisoning. IDS uses application layer protocol to detect this activity

Overview of Snort

Mangal
Date / /20

* Freeware IDS
* Operates as network sniffer & logs activity that matches predefined signatures

Platform compatibility

* Snort can be run on Linux, Windows, Solaris, FreeBSD, MacOSX
* If you are running on Linux, one can use precompiled binaries

Features for Linux :- high level of flexibility & does not suffer from overhead as used in Windows
Features for Windows :- Use of familiar interface & existing software and systems.

Assessing hardware requirements

- Network access speed
- Data throughput
- Log & alert retention
- Budget

* Snort can be run on single / multi processor
* Requires lot of disk space.
* At least two NICs - one to monitor traffic & other for remote management of system

Installing Snort on a Windows System

* Can be installed on Windows Vista and Server 2008 (Mangal)
* Database component can be used along with Snort (not MS SQL but MySQL preferable)
* Physical & logical protection
* Physical protection — Limit access to server
* Logical protection — One way data cable. If there are two NICs on Snort server, NIC that is used to monitor traffic only needs the ability to receive traffic & not transmit. (additional layer of protection)

Installing Base Components

* WinPcap and Snort executable
* WinPcap — allow programs to capture low-level packets travelling over network.
* Configure options like Network, rules, output and include settings

Verification of Configuration

* Snort operates in 3 modes.
  - Sniffer mode :- Snort sniffs traffic
  - Packet Logger mode :- Captures and logs traffic
  - Network Intrusion mode :- Stores Snort data in a database for later review.