# Chapter 4

Monday, August 7, 2023 12:16 PM

## Exploring Advanced Security Devices

### Understanding IDSs and IPSs

IDS monitor network and send alerts on SOS events

IPS react to attacks in progress

Same capabilities as packet sniffers - capture traffic and analyze

### HIDS

host-based IDS - IDS installed on device protect individual host

traffic passes through NIC

have expanded to be able to monitor app activity on system

can help detect malware that traditional antivirus might miss

typically install HIDS on every workstation w/ antivirus

sometimes only install on high-risk

sometimes only install on hosts like servers

## NIDS

network based IDS - monitors activity on a network

admin install NIDS sensors or collectors on network devices: switches, routers, firewalls...

like SNMP agents

gather info and send to central monitor network appliance hosting NIDS console

can't detect anomalies on hosts unless they make significant traffic

Unable to decrypt encrypted traffic

Sensors put before/after firewall, on switch, or router

port mirror or port tap - port spanning

allows admin to configure switch to copy traffic the switch

allows admin to send all traffic the switch receives to a single port

can use this to send to a collector that forwards to console

can do the same with routers

## Sensor and collector placement

ex: firewall

firewall will block traffic so sensor on internet side (before) will see all traffic, sensor on intranet side (after) will only see filtered traffic

## Detection methods

two primary detection methods are signature-based and heuristic or behavioral-based (anomaly based)

## Signature-based detection

definition-based

use database of known vulnerabilities patterns

uses database of known
or known attack patterns

ex: recognizing SYN flood attack
patterns

very similar to antivirus security
definitions

need to update IDS signatures
and antivirus definitions

Heuristic / Behavioral Definitions

anomaly-based

start by identifying networks regular
behavior

create performance baseline under
normal operating conditions

continuously compares current behavior
to baseline

can be effective at discovering 0-day

## SYN Flood

common DoS attack

send multiple SYN packets but never completes third part of TCP handshake with ACK packet

systems reserve certain # of resources for connections and once those are used they block all others

## Data sources and trends

IDS collect from raw data sources

firewall logs, system logs, app logs

IDS uses aggregator to store log events from dissimilar systems

like a SIEM

real-time log monitor or periodically poll relevant logs

## Reporting Based on Rules

IDS report on events based on rules

IDS report on

not all events are incidents

alarms ≠ alerts

need higher precedence

## False positives versus False Negatives

false + = alert on non-threat

false − = no alert on threat

adjust configure rules in IDS and set threshold to 1-1000

too low = too many false +

too high = too many false −

based on network activity level and personal preference

## IPS versus IDS - inline versus passive

extension of IDS

HIDS ; NIDS

HIPS ; NIPS

action

IPS takes action

IPS is inline w/ traffic
all traffic passes through IPS

IPS is out-of-band, traffic
doesn't go through it

Some IPS have capabilities like
modify ACL, close processes, or
redirect attack to safe env

both IPS and IDS have packet
sniffing, but IPS can inspect
packets

NIDS can detect and try to
block attack but only after
it starts

IPS is inline so it can prevent
before start

good to put another IPS inside

good to put

intranet

APTs can bypass internet facing IPS

## Honeypots

**Honeypots** - intentionally left open or poorly locked-down system to bait attackers

ex: web server w/ fake data

deceive attackers and divert them from live network

allow observation of attacker

learn new methodologies and 0-days

## Honeynets

**Honeynet** - group of honeypots in separate network or zone, but accessible from primary network

multiple virtual

from primary

often created from multiple virtual servers contained within single physical server

physical server hosting multiple virtual servers will look like separate systems on a subnet

## Honeyfile

honeyfile - file designed to attract attention of an attacker

## Fake Telemetry

telemetry - collecting info like stats and measurements and forwarding to central system for processing

used in infra systems and SCADA

fake telemetry - corrupts data sent to monitoring system

ex: natural gas uses telemetry to drop pressure during high usage

## Securing Wireless Networks

## Securing Wireless Networks

Wireless local area networks WLAN are very popular for home/business

### Reviewing Wireless Basics

Wireless access point AP - connects wireless clients to wired network

also have routing capabilities so commonly called wireless routers

all wireless routers are APs

not all APs are wireless routers not all of them have extra routing capabilities

most APs have physical ports for wired access and wireless transceiver for wireless

wired ports and wireless connections connect through switch component of wireless router

can also include services like

can also include services like NAT, DHCP, routing

wireless networks are broadcast on known frequency bands so anyone can see

## Band selection and channel overlaps

Wireless networks primarily use two radio bands: 2.4 GHz and 5GHz

Wireless devices don't transmit on exactly 2.4 & 5

the two bands have multiple channels that start at 2.4 & 5

signals travel farthest on 2.4

more bandwidth on 5

standard 802.11 b, g, n, & ac

for 2.4

sometimes can change channel to get better performance

## Access point SSID

SSID - wireless

## Access point SSID

**Service set identifier** **SSID** – wireless network name

need to change default

## Enable MAC Filtering

can enable MAC filtering on many wireless routers

**MAC address** - 48-bit hexadecimal that identifies NIC

attackers can easily bypass MAC filter

**wireless sniffer** can identify allowed MAC addresses in network

## MAC cloning

**MAC cloning** – changing MAC address on PC or other device with the same MAC address as the WAN port on an internet facing router

## Site surveys and Footprinting

**Site Survey** – examine wireless env to identify potential issues like

[illegible] wireless network

to identify

noise

do before deploying wireless network

usually do more than once

Wi Fi analyzers - identify activity on channels in wireless spectrum and in 2.4 & 5 frequencies

heat map - color coded rep of wireless signals

can see where in your org has strong/weak signal

Wireless footprinting - detailed diagram of APs and hotspots in org

Wireless Access Point Placement

APs and wireless devices commonly use omnidirectional antenna

devices can connect to AP from any direction

directional antenna is only 1 way

directional antenna is [illegible]
but stronger

## Wireless cryptographic Protocols

wireless networks broadcast over the air, anyone with wireless transceiver can intercept transmissia

early cryptographic protocols like Wired Equivalency Privacy WEP and Wi Fi protected access WPA were vulnerable and are now deprecated

## WPA2 and CCMP

Wi Fi protected Access 2 WPA2 created to replace early crypto protocols

also known as IEEE 802.11i

uses AES and Counter-mode/ CBC-MAC protocol CCMP

[illegible] for extra

CBC

these are good but for extra protection orgs can enable enterprise mode

## Open, PSK, and Enterprise Modes

WPA2 can operate in either open, pre-shared key PSK, or enterprise modes

open = no security; cleartext

PSK = access wireless network anon with PSK or passphrase

this is not authentication only provides a password with no username

authorization w/out authentication

enterprise mode = forces users to authenticate with unique creds before granting access often implemented

before grant

802.1x server, often implemented as RADIUS server which accessed db of accounts

can also provide certificate-based authentication

3 pieces of info for enterprise

- RADIUS server - enter IP of 802.1x server
- RADIUS port - port used by RADIUS server
  default 1812
- shared secret - like a password

When enterprise enabled on AP redirects all attempts to connect to RADIUS server

most homes use PSK, orgs enterprise

WPA3 and Simultaneous Authentication of Equals

WPA3 of Equals

WPA3 is newest crypto proto

uses simultaneous authentication of equals SAE over PSK

provides better sec and better sec when setting up devices with Wi Fi protected setup WPS

Remember

WPA2 uses CCMP (based on AES)

WPA3 uses simultaneous authentication of equals SAE over PSK

Authentication Protocols

Wireless networks support several types of auth

many built on Extensible authentication protocols EAP - auth framework

each method might support or require certificates

method for two systems

EAP - provides method for two systems to create secure encryption key - pairwise master key PMK

protected EAP PEAP - encrypts the comms channel between systems w/ TLS tunnel

requires certificate on server but not client

Microsoft challenge handshake authentication protocol v2

MS-CHAPv2

EAP-FAST - EAP flexible authentication via secure tunneling

replacement for light EAP LEAP

supports certs but optional

EAP-TLS - one of most secure

requires certs on server and clients

client?

EAP-TTLS - EAP tunneled TLS
extension of PEAP
allows password authentication
protocol PAP within TLS tunnel
cert on server but not client

RADIUS Federation
federation - two or more entities
share same identity management
system
create federation using 802.1x
and RADIUS servers
orgs must purchase cert from CA
or implement private CA

IEEE 802.1x Security
port security from MAC filtering
or disable ports
can also use IEEE 802.1x - port-based
auth protocol
[illegible] or devices to auth when

auth pro

requires users or devices to auth when they connect to WAP or physical port

wired, wireless and VPN

unames/pwords or certificates

can combine with VLAN

grant access to auth clients

redirect guests to other network

can implement as remote access dial-in user service RADIUS

or diameter server

Remember

Enterprise mode requires 802.1x server

EAP-FAST supports certs

LEAP TTLS require cert

EAP-FAST still

PEAP and EAP-TTLS require cert on server

EAP-TLS requires certs on both

802.1x server provides port-based authentication - only auth Clients can connect to device or network

Controller and access point security important physical security for AP

attacker can connect directly or reset

Captive Portals

captive portal - tech solution forces clients using web browsers to complete process before allowing connect

common examples

common examples

- free wifi
- paid wifi
- alt to IEEE 802.1x - 802.1x can be expensive, can use captive portal for auth

## Understanding Wireless Attacks

most attacks can be avoided by using WPA2 or CCMP

### Disassociation Attacks

disassociation attack - removes wireless client from wireless net

after client auth with WAP, they exchange frames

client is now associated w WAP

a client can send a disassociation frame to disconnect

includes MAC address

in attack, attackers use spoofed disassociation

in attack, attacker
MAC to send disassociation
frame

## WiFi Protected Setup

WiFi protected setup WPS - allows users to configure wireless devices without typing in passphrase

can configure with buttons or PIN

button will auto config device in 30 sec

PIN is entered on AP and enter on new wireless device

open to brute force attacks on PIN

WPS is safe if used w/ WPA3

recommended to disable WPS on all devices

## Rogue Access Point

AP - AP placed in network

## Rogue

rogue AP – AP placed in network without auth

Will not have security measures in place, open to vulns

acts as a sniffer to capture traffic passing through wired network device then broadcasts using AP's wireless

### data exfiltration

can use to connect to network

secure rogue AP will not have SEC

## Evil twin

evil twin – rogue AP with same SSID as legit AP

easy to set up

can use laptop as AP through wireless card

used

wireless card

wireless scanners can also be used to detect rogue AP and evil twin

signal will get stronger as admin get closer

Remember

Rogue AP used to capture and exfiltrate data

Evil twin is Rogue AP of same SSID as legit AP

Jamming attacks

attackers can transmit noise or another radio signal on same frequency used by wireless network

interfere with traffic and degrade performance

called jamming, considered DoS

usually causes all users to lose access

two solutions:

- increase power levels of AP
- use different wireless channels

## IV Attacks

initialization vector IV - number used by encryption systems

wireless IV attack - attempt to guess pre-shared key after discovering IV

some wireless prots combine IV w/ PSK to encrypt data

if IV is reused attacker can easily guess

ex: WEP used only 24-bit IV so many reused

attacker uses packet injection to add packets to data stream

AP responds w/ more packets increasing chances of reuse

[illegible] Attack

increasing

## Near Field Communications Attack

**near field communication NFC**

group of standards used on mobile devices that allow to comm w/ other nearby mobile devices

share pics, files, etc.

used by many point of sale card readers use

**NFC attack** - uses NFC reader to capture data from another NFC device

**eavesdropping attack**

ex: you use your own NFC reader with a boosted signal next to legit card reader to capture

card reader to capture transaction

## RFID Attacks

**radio frequency identification**

RFID systems include RFID reader and RFID tags on objects

Used to track and manage inventory and any type of valuable asset, even animals

dont have a power source, instead have electronics to collect an use power to transmit data stored on device

## Common RFID attacks

- **Sniffing** or **eavesdropping** - attacker collects RFID transmissions over air

need to know RFID frequency protocols

need to know RFID

only need to know protocols used by RFID

- replay - config fake tag to mimic legit tag attached to object
  can then steal object without theft being detected
- DoS - if attacker knows frequency, can flood w/ noise

## Bluetooth attacks

bluetooth - short range wireless system used in personal area networks PAN and in networks

range used to be 3m 10ft but often farther

- bluejacking - sending unsolicited bluetooth

**bluejacking** - sending unsolicited messages to nearby bluetooth devices

typically text or images/sound

relatively harmless

**bluesnarfing** - unauth access or theft of info from bluetooth device

access info like email, contacts, calendars, texts

**bluebugging** - gains full access and implements backdoor

can have phone call attacker phone and listen in

when bluetooth devices first configed, configed in **discovery mode**

broadcasts MAC address

attacks are rare because now they require confirmation to pair

attacks

require confirmation

devices

but if no conf, then open to attacks

## Wireless Replay attacks

replays capture packets and modifies them by impersonating one party

WPA2 and 3 are resistant to them but wireless nets without them are still vuln

## War driving and war flying

**war driving** - looking for a wireless network

more common in cars but can do just by walking around

find networks and use directional antennas to find weak signals

admins use in **wireless audit** - active control that examines [illegible] placement,

admins use [illegible]

detective control that can
signal footprint, antenna placement,
and encryption of wireless traffic

war flying - fly around in plane to
intercept transmissions

or drone - only need a little
hardware to scan for nets

## Using VPNs for Remote Access

direct access VPNs allow users to
access private networks via public
network

public most likely internet or
semiprivate leased line from
org

more people working from home connect
to company nets using direct
access VPN

different tunneling proto to encapsulate
[illegible] to protect

different tunneling prot
and encrypt traffic to protect
data

## VPNs and VPN Appliances

possible to create VPN w/ services on
server

ex: Direct Access VPN on
Windows Server

only req is that server has
2 NIC

1 accessible from internet
1 provides access to private net

large orgs use VPN appliance - less
encryption and authentication
typically placed in DMZ

internet firewall forwards
VPN traffic to VPN
traffic

VPN traffic

VPN forwards private traffic to intranet firewall

## Remote Access VPN

Client connects to internet ISP

ISP tunnels to screened subnet w/ direct access VPN server

VPN server requires auth, usually through RADIUS

even though RADIUS can store uname/pword, more common to pass to another server like LDAP

## IPsec as a tunneling protocol

IPsec - way of encrypting data in transit

tunnel mode - encrypts entire packet payload and headers

do intercept traffic

payload

if attackers do intercept traffic they can only see source IP and VPN IP

transport mode - only encrypts payload
common in private networks but not VPN

provides security in two ways:

- authentication - includes authentication header AH to allow each IPsec convo hosts to auth each other before exchanging data

protocol 51

- encryption - includes encapsulating security payload ESP - to encrypt data

protocol 50

uses internet key exchange IKE over port 500 to authenticate clients

...ations SA

clients

Creates security associations SA
for VPN and uses them to
set up secur channel between
client / VPN server

## SSL/TLS as a Tunneling Protocol

Secure socket tunneling protocol SSTP
encrypt VPN using TLS over port 443

Using 443 is good alt when
VPN tunnel must go through NAT
and IPsec is not feasible

OpenVPN and openconnect are
two open source TLS tunnels

## Split Tunnel versus Full Tunnel

'imagine you are connected to VPN
using IPsec from home
how you do an 'internet search
will your pc connect straight to
internet or go through VPN?

internet or go

**split tunnel** - VPN admin determines what traffic goes through encrypted tunnel

ex: encrypt only traffic going to private IP in network

**full tunnel** - all traffic goes through tunnel

might also go through UTM for URL filtering, malware inspection, etc.

## Site to Site VPNs

two VPN servers that act as gateways for 2 networks separated geo

ex: HQ and remote office

doesn't take any extra steps from users

contrast to remote access because user makes direct connection and is aware of process

user makes
to VPN and is aware of

## Always on VPN

can be used with site to site or direct access

ex: site to site the two servers always maintain connection

rather than on-demand connection

## L2TP as a Tunneling protocol

Layer 2 tunneling protocol L2TP

used for VPNs but no versions provide encryption

data is encrypted with another protocol like IPsec and passed to L2TP for transport

## HTNLS VPN Portal

HTNCS VPN - allows users to connect through web browser

TLS encryption

can be very resource intensive

infrequent

can be very resource inten...
typically used for quick/infrequent usage for only a few people

## Network Access Control

Network Access control NAC - provide continuous security monitoring by inspecting pcs and preventing them from accessing network

mainly used for non-org devices that connect to network

grant access based on health of system

## Host Health Checks

common health conditions checked

- firewall enabled
- OS up to date
- antivirus up to date

NAC systems use authentication agents or health agents to ... NAC clients

inspect NAC clients

agents are apps or services that check health

if client doesn't pass health check, gets passed to remediation or quarantine network to be provided resources to pass check

NAC can also be used to monitor interval client health

## Agent versus Agentless NAC

permanent agent always on client

dissolvable agent remove themselves

"agentless"

## Authentication and Authorization Methods

VPNs need to ensure only auth entities can access

## PAP

password authentication protocol PAP

PAP

password authentication protocol

used with point to point protocol PPP to auth clients

sends pwords over cleartext

outdated

CHAP

Challenge handshake authentication protocol CHAP also uses PPP, but more secure than PAP

Client and server both know shared secret used in auth process

not sent over cleartext

hashes it w/ nonce

RADIUS

remote authentication dial-in user service RADIUS - centralized authentication service

n and auth requests

authentication

VPN can forward auth requests to RADIUS

or can be used as 802.1x server WPA2 enterprise mode

convenient if org has many VPNs because they all share shared secret

usually passes to domain controller for auth like LDAP

uses UDP

only encrypts pword by default

supports EAP

TACACS+

terminal access controller Access-control System plus TACACS+ - alt to RADIUS

- encrypts entire auth process, not just pword

- licenses and

just pword

- uses multiple challenges and responses between client/server

can interact with kerberos, and Microsoft active directory (MS AD uses kerberos for auth)

can use as auth service for net devices

RADIUS can encrypt entire session with EAP

## AAA Protocols

RADIUS, TACACS+, and Diameter considered AAA protocols

## Assessment Notes

1. Signature-based HIDS reports vulns based on known attacks

2. Want to make heuristic-based [illegible] first?

2. Want to make heuristics, what to make first?

baseline

3. Detect and prevent login failures from other countries

IPS

4. Create password.txt with admin usernames in it

honeyfile

5. Encrypted auth of wireless users using TLS

PEAP

6. Create detailed diagram of wireless AP and hotspots in org

Wireless footprinting

Wireless footprinting

WiFi analyzers show graphs of channel overlaps but not AP

7. Access public wireless hotspot w/out pword

open mode

8. Discovered new AP that can access resources

Rogue AP

9. Got pop up of same org's SSID and later got fraud charge on card

Evil Twin

10. Frequently lose connection w/ network on same days

10. Frequency
wireless network on some days

Wireless jamming attack

11. Attacker can access contacts on phone

Bluesnarfing

12. Implement connection between org offices over internet

Site to site VPN

13. All traffic from VPN client is encrypted

full tunnel

IPsec with tunnel mode
encrypts all traffic within
private net but not

encrypt

VPNs private net but not all traffic from client

14. Ensure all VPN clients are using up to date OS and antivirus

NAC

15. BYOD, want to ensure health check

Agentless