INTRO TO ETHICAL HACKING

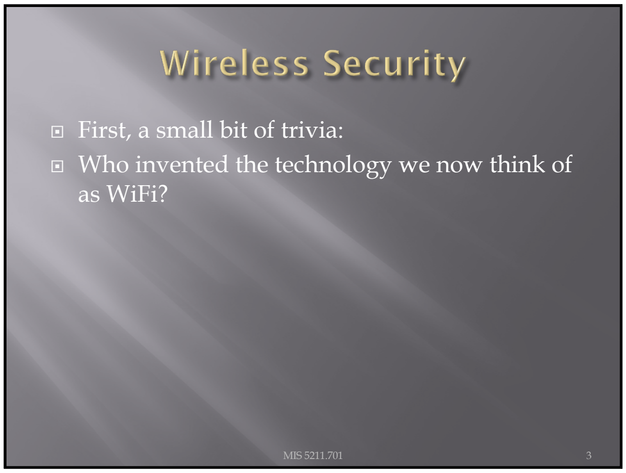
MIS 5211.701
Week 12

1

Tonight's Plan

- Introduction to Wireless Security
- Next Week

2



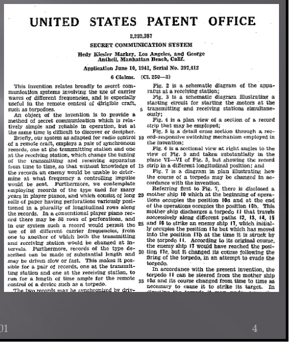
Wireless Security

- First, a small bit of trivia:
- Who invented the technology we now think of as WiFi?

3

The Answer

The Actress Hedy Lamar



UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.

An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

Briefly, our system as adapted for radio control of a remote craft, employs a pair of synchronous records, one at the transmitting station and one at the receiving station, which change the tuning of the transmitting and receiving apparatus from time to time, so that without knowledge of the records an enemy would be unable to determine at what frequency a controlling impulse would be sent. Furthermore, we contemplate employing records of the type used for many years in player pianos, and which consist of long rolls of paper having perforations variously positioned in a plurality of longitudinal rows along the records. In a conventional player piano record there may be 88 rows of perforations, and in our system such a record would permit the use of 88 different carrier frequencies, from one to another of which both the transmitting and receiving station would be changed at intervals. Furthermore, records of the type described can be made of substantial length and may be driven slow or fast. This makes it possible for a pair of records, one at the transmitting station and one at the receiving station, to run for a length of time ample for the remote control of a device such as a torpedo.

The two records may be synchronized by driv-

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the transmitting and receiving stations simultaneously;

Fig. 4 is a plan view of a section of a record strip that may be employed;

Fig. 5 is a detail cross section through a record-responsive switching mechanism employed in the invention;

Fig. 6 is a sectional view at right angles to the view of Fig. 5 and taken substantially in the plane VI—VI of Fig. 5, but showing the record strip in a different longitudinal position; and

Fig. 7 is a diagram in plan illustrating how the course of a torpedo may be changed in accordance with the invention.

Referring first to Fig. 7, there is disclosed a mother ship 10 which at the beginning of operations occupies the position 10a and at the end of the operations occupies the position 10b. This mother ship discharges a torpedo 11 that travels successively along different paths 12, 13, 14, 15 and 16 to strike an enemy ship 17, which initially occupies the position 17a but which has moved into the position 17b at the time it is struck by the torpedo 11. According to its original course, the enemy ship 17 would have reached the position 17c, but it changed its course following the firing of the torpedo, in an attempt to evade the torpedo.

In accordance with the present invention, the torpedo 11 can be steered from the mother ship 10a and its course changed from time to time as necessary to cause it to strike its target. In

- Source: http://www.pixmule.com/hedy-lamarr/ and https://en.wikipedia.org/wiki/Hedy_Lamarr#/media/File:Lamarr_patent.png

4

Security vs Mobility

- Wireless is different
  - Physical security is no longer relevant
    - Access from outside perimeter
    - Users connecting to "other" networks
  - Users and Networks are vulnerable even when not in use

5

More Issues

- Attack tools are cheap
  - Hardware is close to zero
  - Software is zero
- Segregation doesn't work
  - Even with "guest" networks, there still on your wires and can still cause you issues
- Fallacy of "We don't have any wireless"
  - No, you just don't know about the wireless you have

6

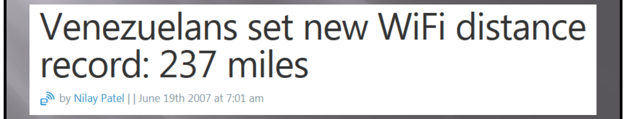
Still More Issues

- Encryption doesn't protect you, at least not completely
- Authentication doesn't protect you, at least not completely
- Firewalls? Really, we're going to go their?
- Why would anybody attack us?

7

Leakage

- Signal required to use wireless access means you need to be relatively close
- Signal required to "sniff" traffic means attacker could be miles away with the right conditions



Venezuelans set new WiFi distance record: 237 miles

by Nilay Patel | | June 19th 2007 at 7:01 am

Source:
http://www.engadget.com/2007/06/19/venezuelans-set-new-wifi-distance-record-237-miles/

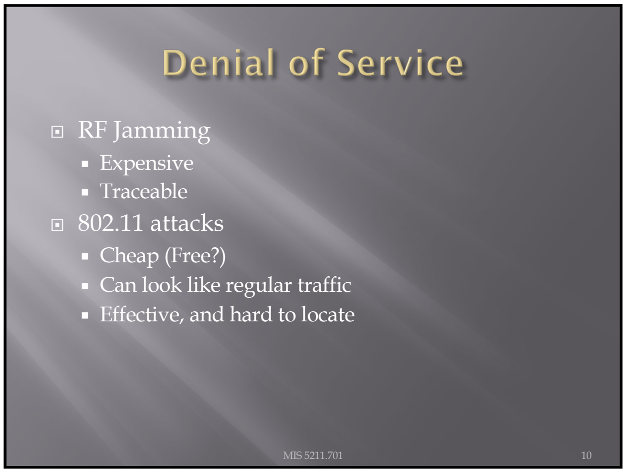
8

Old Ways Are The Worst Ways

- Wireless networking is a shared segment
  - Think "Hub", not "Switch"
- Sniffing is passive
  - No access required
  - No forensic evidence attacker was there
  - Only need some level of physical proximity
- So, you would need to be here, to be safe. Maybe!

Source:
http://www.darkgovernment.com/news/wp-content/uploads/2009/04/area-51-satellite-image.jpg

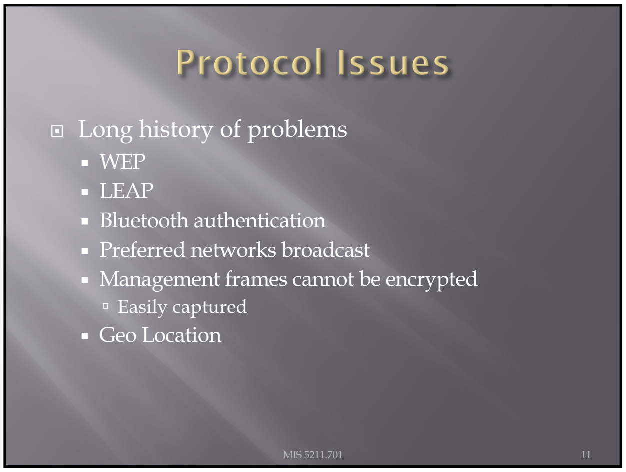
9



Denial of Service

- RF Jamming
  - Expensive
  - Traceable
- 802.11 attacks
  - Cheap (Free?)
  - Can look like regular traffic
  - Effective, and hard to locate

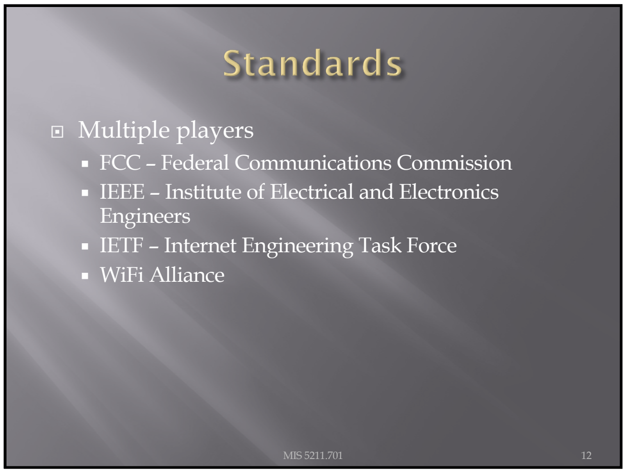
10



Protocol Issues

- Long history of problems
  - WEP
  - LEAP
  - Bluetooth authentication
  - Preferred networks broadcast
  - Management frames cannot be encrypted
    - Easily captured
  - Geo Location

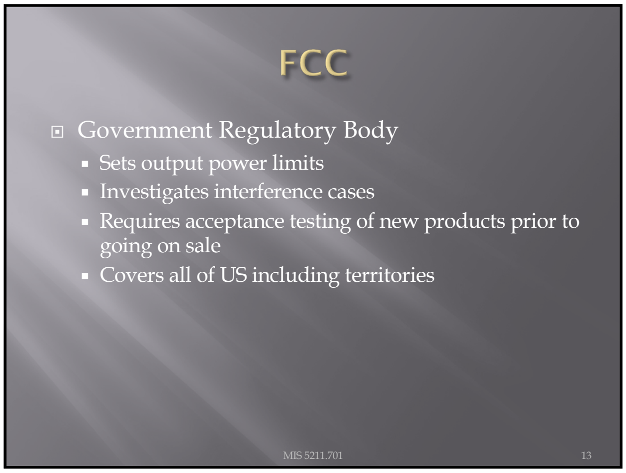
11



Standards

- Multiple players
  - FCC – Federal Communications Commission
  - IEEE – Institute of Electrical and Electronics Engineers
  - IETF – Internet Engineering Task Force
  - WiFi Alliance

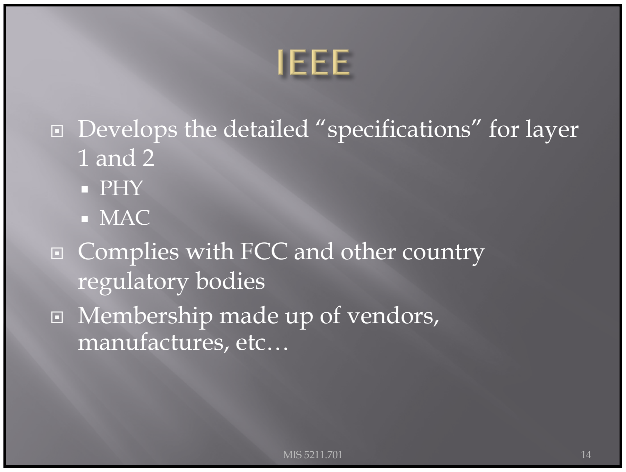
12



FCC

- Government Regulatory Body
  - Sets output power limits
  - Investigates interference cases
  - Requires acceptance testing of new products prior to going on sale
  - Covers all of US including territories

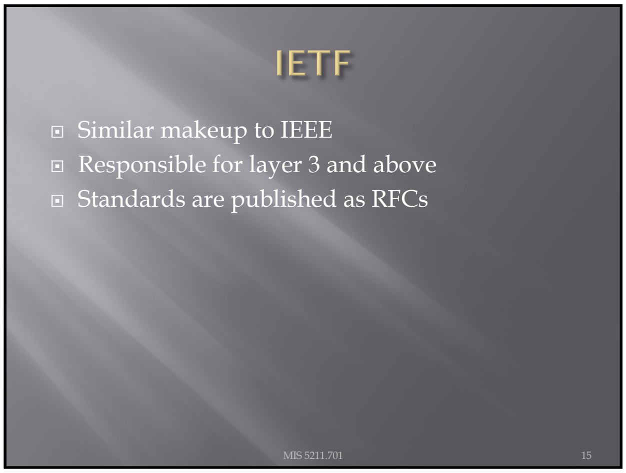
13



IEEE

- Develops the detailed “specifications” for layer 1 and 2
  - PHY
  - MAC
- Complies with FCC and other country regulatory bodies
- Membership made up of vendors, manufactures, etc…

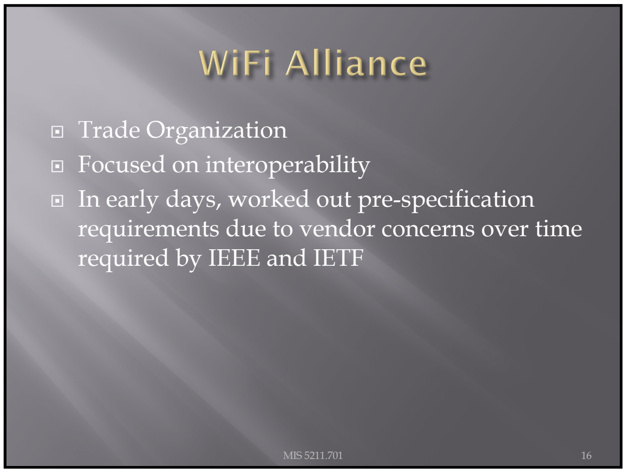
14



IETF

- Similar makeup to IEEE
- Responsible for layer 3 and above
- Standards are published as RFCs

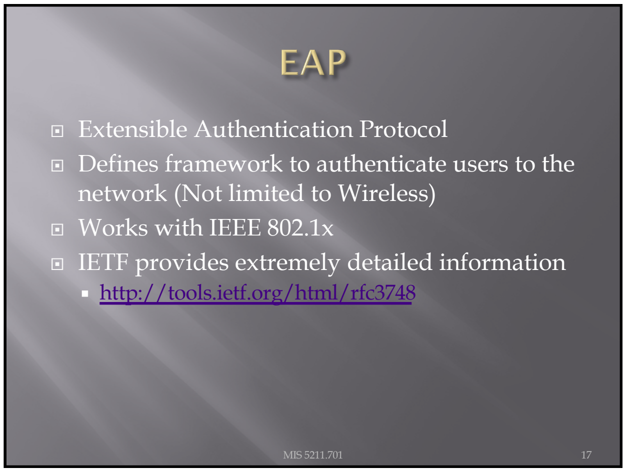
15



WiFi Alliance

- Trade Organization
- Focused on interoperability
- In early days, worked out pre-specification requirements due to vendor concerns over time required by IEEE and IETF

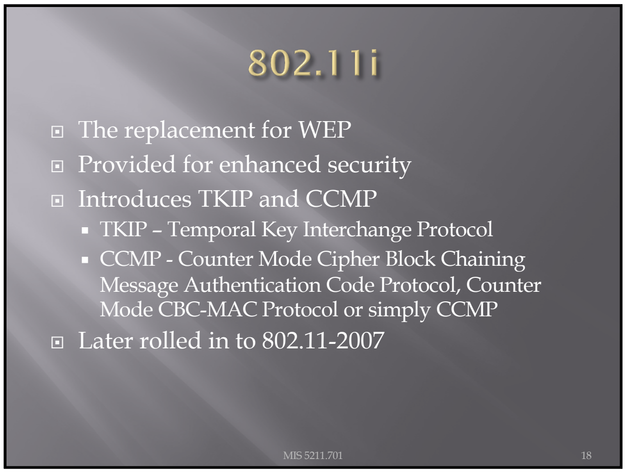
16



EAP

- Extensible Authentication Protocol
- Defines framework to authenticate users to the network (Not limited to Wireless)
- Works with IEEE 802.1x
- IETF provides extremely detailed information
  - http://tools.ietf.org/html/rfc3748

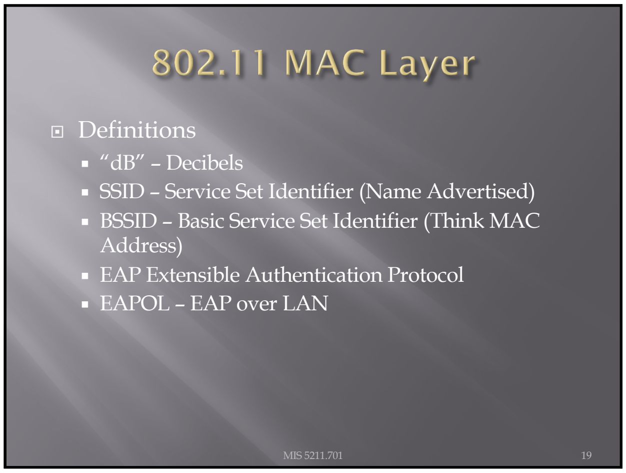
17



802.11i

- The replacement for WEP
- Provided for enhanced security
- Introduces TKIP and CCMP
  - TKIP – Temporal Key Interchange Protocol
  - CCMP - Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP
- Later rolled in to 802.11-2007

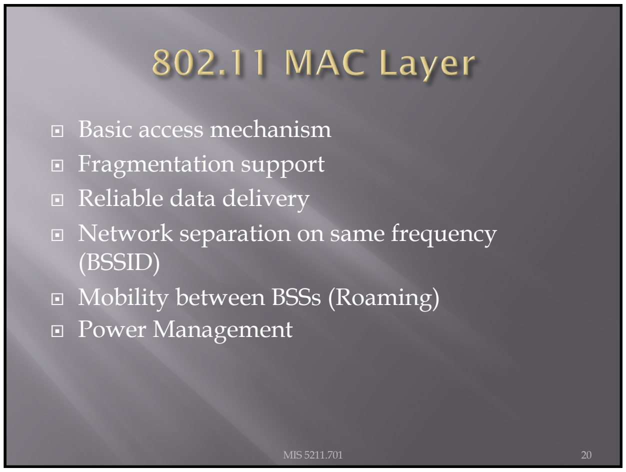
18



802.11 MAC Layer

- Definitions
  - “dB” – Decibels
  - SSID – Service Set Identifier (Name Advertised)
  - BSSID – Basic Service Set Identifier (Think MAC Address)
  - EAP Extensible Authentication Protocol
  - EAPOL – EAP over LAN

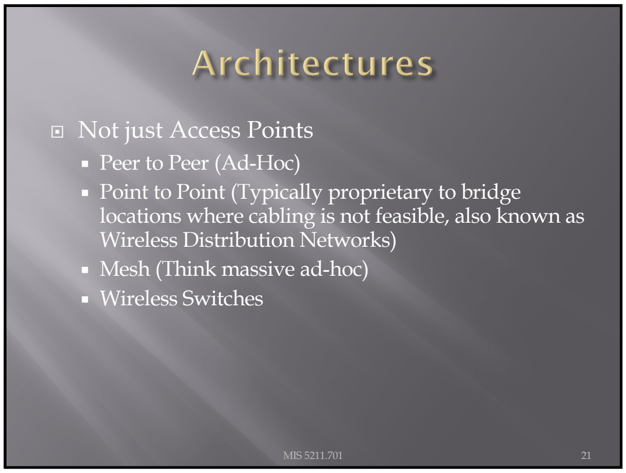
19



802.11 MAC Layer

- Basic access mechanism
- Fragmentation support
- Reliable data delivery
- Network separation on same frequency (BSSID)
- Mobility between BSSs (Roaming)
- Power Management

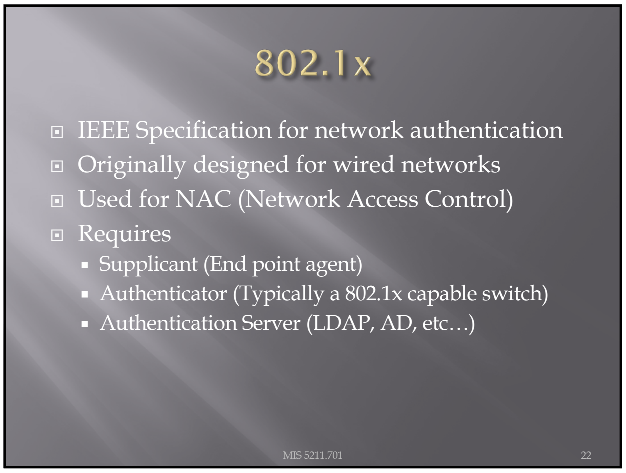
20



Architectures

- Not just Access Points
  - Peer to Peer (Ad-Hoc)
  - Point to Point (Typically proprietary to bridge locations where cabling is not feasible, also known as Wireless Distribution Networks)
  - Mesh (Think massive ad-hoc)
  - Wireless Switches

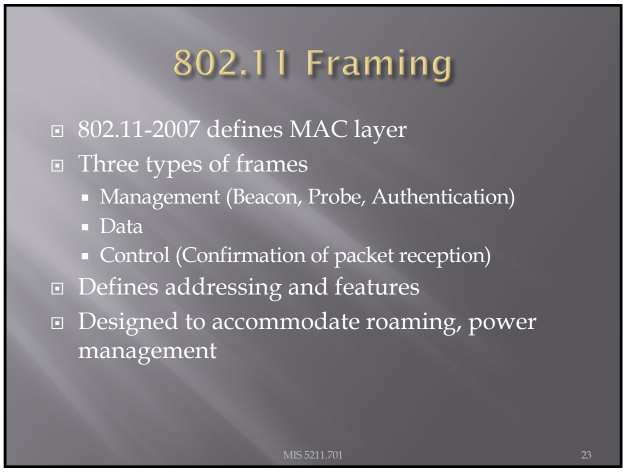
21



802.1x

- IEEE Specification for network authentication
- Originally designed for wired networks
- Used for NAC (Network Access Control)
- Requires
  - Supplicant (End point agent)
  - Authenticator (Typically a 802.1x capable switch)
  - Authentication Server (LDAP, AD, etc…)

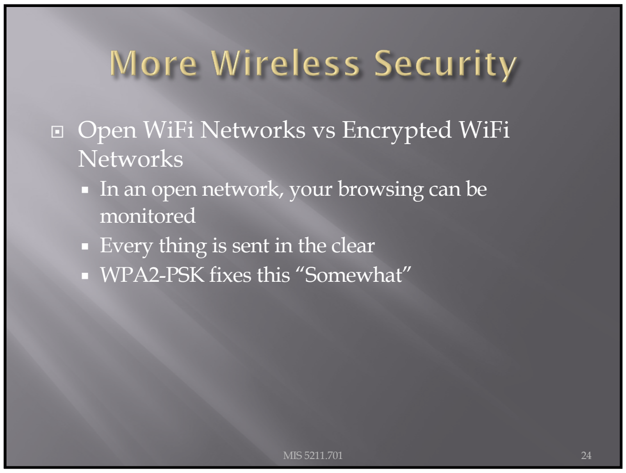
22



802.11 Framing

- 802.11-2007 defines MAC layer
- Three types of frames
  - Management (Beacon, Probe, Authentication)
  - Data
  - Control (Confirmation of packet reception)
- Defines addressing and features
- Designed to accommodate roaming, power management

23



More Wireless Security

- Open WiFi Networks vs Encrypted WiFi Networks
  - In an open network, your browsing can be monitored
  - Every thing is sent in the clear
  - WPA2-PSK fixes this "Somewhat"

24

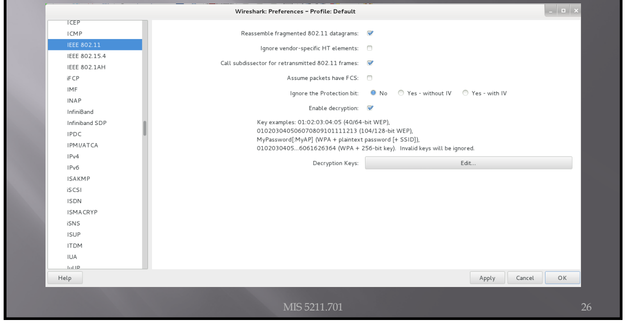
WPA2-PSK

- Uses a pre-shared key (hence the acronym PSK)
  - The pre-shared key is known to all authorized users
  - Anyone with the pre-shared key has what they need to decrypt traffic
  - Wireshark has a built in option to decrypt traffic if you have the key
  - This means WPA2-PSK is not much more secure than no encryption, unless you trust everyone on the network

25

Wireshark WPA2-PSK Decryption

- Edit->Preferences->IEEE 802.11



Wireshark: Preferences – Profile: Default

Reassemble fragmented 802.11 datagrams: ☑

Ignore vendor-specific HT elements: ☐

Call subdissector for retransmitted 802.11 frames: ☑

Assume packets have FCS: ☐

Ignore the Protection bit: ● No ○ Yes - without IV ○ Yes - with IV

Enable decryption: ☑

Key examples: 01:02:03:04:05 (40/64-bit WEP),
010203040506070809101111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405...6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

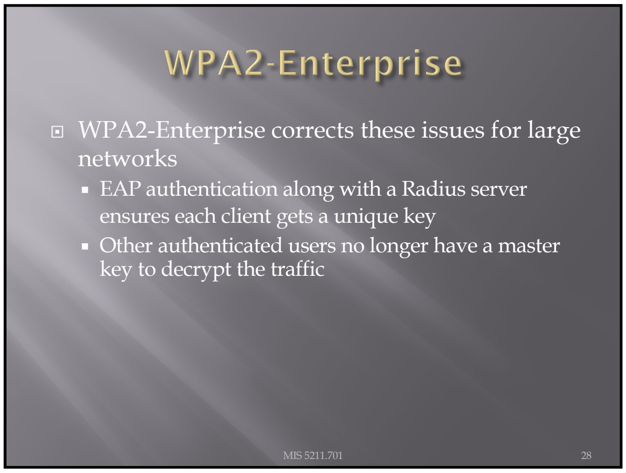
Decryption Keys: Edit...

26

PTK or Pairwise Transient Key

- WPA2-PSK tries to address this issue by use of PTK
- However, the PTK is derived from the PSK
- So… It is easy to capture the PTK if you have the PSK

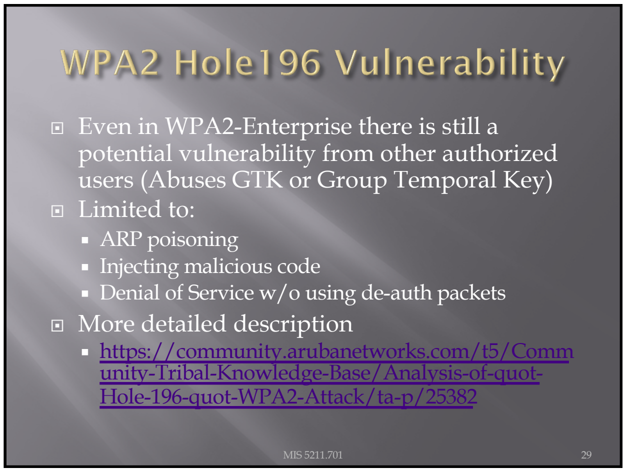
27



WPA2-Enterprise

- WPA2-Enterprise corrects these issues for large networks
  - EAP authentication along with a Radius server ensures each client gets a unique key
  - Other authenticated users no longer have a master key to decrypt the traffic

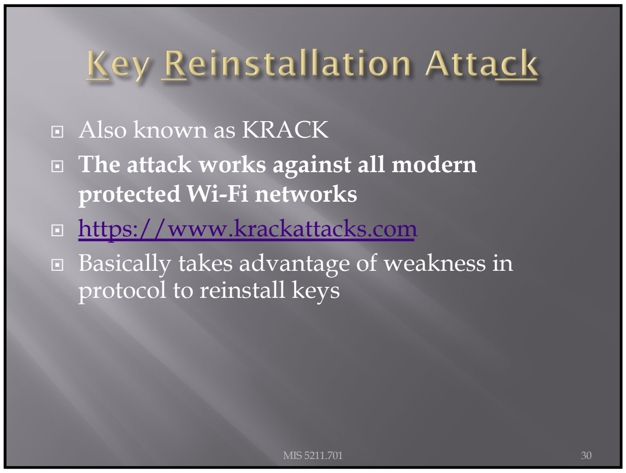
28



WPA2 Hole196 Vulnerability

- Even in WPA2-Enterprise there is still a potential vulnerability from other authorized users (Abuses GTK or Group Temporal Key)
- Limited to:
  - ARP poisoning
  - Injecting malicious code
  - Denial of Service w/o using de-auth packets
- More detailed description
  - https://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/Analysis-of-quot-Hole-196-quot-WPA2-Attack/ta-p/25382

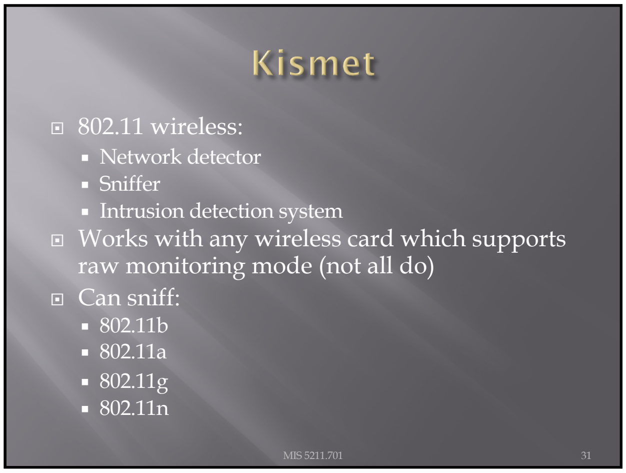
29



Key Reinstallation Attack

- Also known as KRACK
- **The attack works against all modern protected Wi-Fi networks**
- https://www.krackattacks.com
- Basically takes advantage of weakness in protocol to reinstall keys

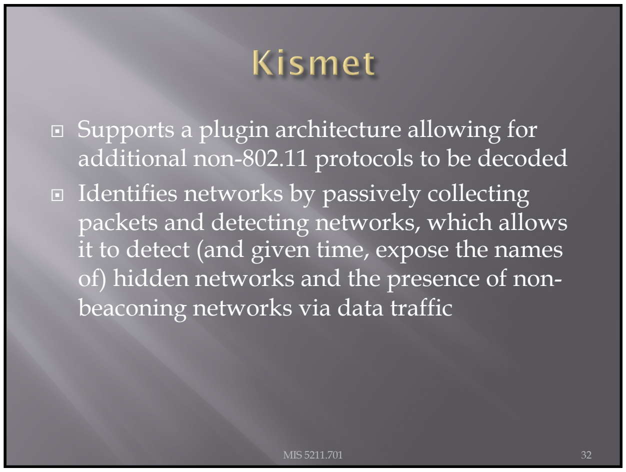
30



Kismet

- 802.11 wireless:
  - Network detector
  - Sniffer
  - Intrusion detection system
- Works with any wireless card which supports raw monitoring mode (not all do)
- Can sniff:
  - 802.11b
  - 802.11a
  - 802.11g
  - 802.11n

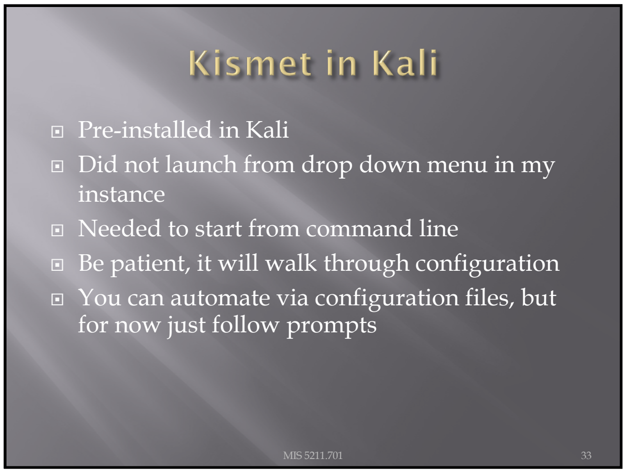
31



Kismet

- Supports a plugin architecture allowing for additional non-802.11 protocols to be decoded
- Identifies networks by passively collecting packets and detecting networks, which allows it to detect (and given time, expose the names of) hidden networks and the presence of non-beaconing networks via data traffic

32



Kismet in Kali

- Pre-installed in Kali
- Did not launch from drop down menu in my instance
- Needed to start from command line
- Be patient, it will walk through configuration
- You can automate via configuration files, but for now just follow prompts

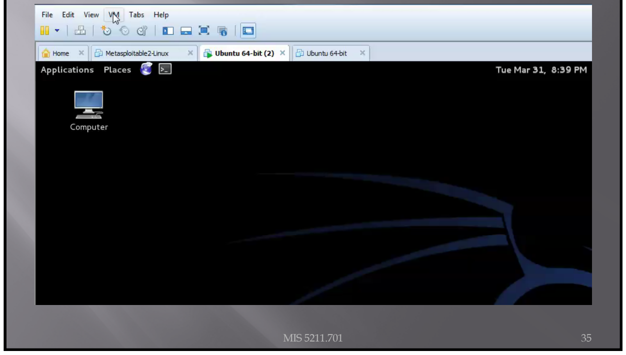
33

Getting Started

- We will
  - Get USB Wireless Adapter working with Kali
  - Launch and configure Kismet
  - Explore a little bit

34

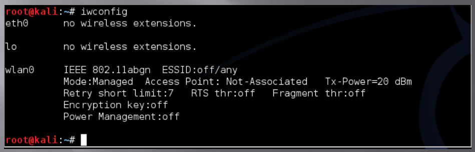
Connecting Wireless Card



35

Checking Card

- Use the command: iwconfig
- This should give something like the following:



```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11abgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~# 
```

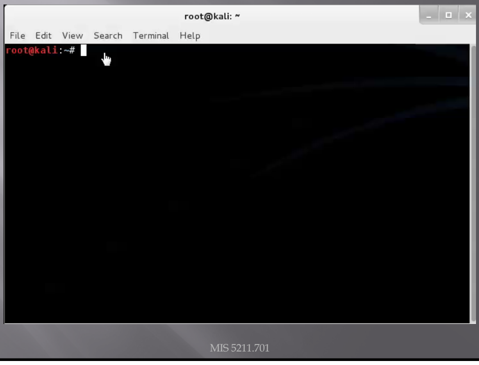
36

Kismet

- Kismet is a wireless network detector, sniffer, and intrusion detection system. Kismet works predominately with Wi-Fi (IEEE 802.11) networks, but can be expanded via plug-ins to handle other network types.
- Features
  - 802.11 sniffing
  - Standard PCAP logging (compatible with Wireshark, TCPDump, etc)
  - Client/Server modular architecture
  - Plug-in architecture to expand core features
  - Multiple capture source support
  - Live export of packets to other tools via tun/tap virtual interfaces
  - Distributed remote sniffing via light-weight remote capture
  - XML output for integration with other tools
- http://kismetwireless.net/

37

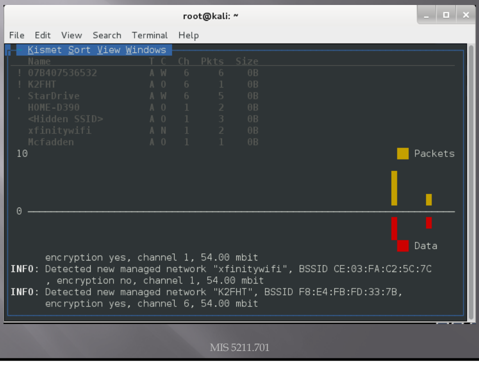
Starting Kismet



```
root@kali:~# 
```

38

Kismet Example



```
  Name                     T C  Ch  Pkts  Size
! 07B407536532             A W   6     6    0B
! K2FHT                    A O   6     1    0B
. StarDrive                A W   6     5    0B
  HOME-D390                A O   1     2    0B
  <Hidden SSID>            A O   1     3    0B
  xfinitywifi              A N   1     2    0B
  Mcfadden                 A O   1     1    0B
10

0
      encryption yes, channel 1, 54.00 mbit
INFO: Detected new managed network "xfinitywifi", BSSID CE:03:FA:C2:5C:7C
      , encryption no, channel 1, 54.00 mbit
INFO: Detected new managed network "K2FHT", BSSID F8:E4:FB:FD:33:7B,
      encryption yes, channel 6, 54.00 mbit
```

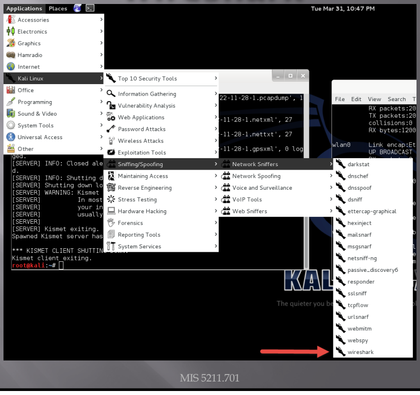
39

Wireshark

- Pre-installed in Kali

40

Wireshark

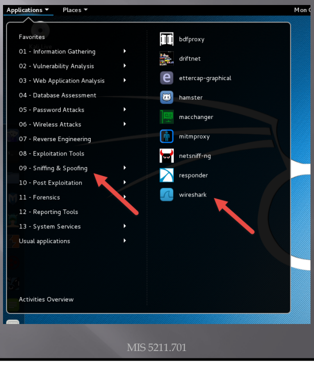


```
22-11-28-1.pcapdump', 1
-11-28-1.netxml', 27
-11-28-1.nettxt', 27
-11-28-1.gpsxml', 0 log
ged.
[SERVER] INFO: Closed ale
d.
[SERVER] INFO: Shutting d
[SERVER] Shutting down lo
[SERVER] WARNING: Kismet
[SERVER]          In most
[SERVER]          your in
[SERVER]          usually
[SERVER]
[SERVER] Kismet exiting.
Spawned Kismet server has

*** KISMET CLIENT SHUTTIN
Kismet client exiting.
root@kali:~#
```

```
         RX packets:20
         TX packets:20
         collisions:0
         RX bytes:1200

wlan0    Link encap:Et
         UP BROADCAST
```

41

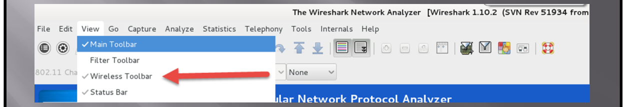
Or



42

Startup of Wireshark

- Will throw an error due to running as root in Kali, just click OK and move on
- Will need to turn wireless menu on by going to View tab and clicking on “Wireless Toolbar”



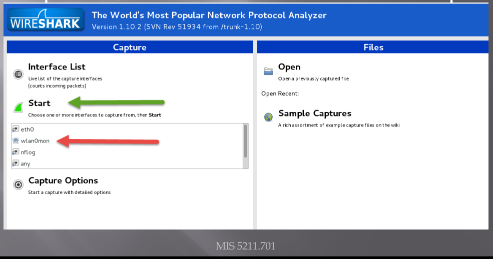
The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
✓ Main Toolbar
Filter Toolbar
✓ Wireless Toolbar
✓ Status Bar
802.11 Cha
None
ular Network Protocol Analyzer

43

Configuring Interface

- Select “wlan0mon”
- Click on “Start”
- Be patient, it will take a minute or so to update

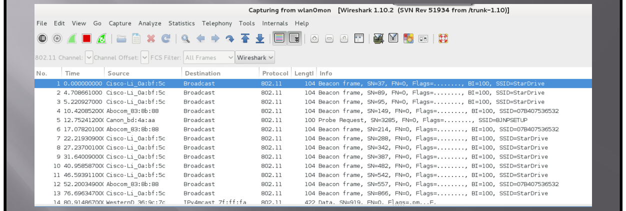


The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)

WIRESHARK
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
wlan0mon
nflog
any
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki

44

More Wireshark



Capturing from wlan0mon [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
802.11 Channel:
Channel Offset:
FCS Filter: All Frames
Wireshark

```
No.  Time         Source             Destination        Protocol Lengtl Info
   1 0.000000000  Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=37, FN=0, Flags=........, BI=100, SSID=StarDrive
   2 4.708661000  Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=89, FN=0, Flags=........, BI=100, SSID=StarDrive
   3 5.220927000  Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=95, FN=0, Flags=........, BI=100, SSID=StarDrive
   4 10.42085200( Abocom_83:8b:88    Broadcast          802.11     104 Beacon frame, SN=149, FN=0, Flags=........, BI=100, SSID=07B407536532
   5 12.75241200( Canon_bd:4a:aa     Broadcast          802.11     100 Probe Request, SN=3285, FN=0, Flags=........, SSID=BJNPSETUP
   6 17.07820100( Abocom_83:8b:88    Broadcast          802.11     104 Beacon frame, SN=214, FN=0, Flags=........, BI=100, SSID=07B407536532
   7 22.21930900( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=288, FN=0, Flags=........, BI=100, SSID=StarDrive
   8 27.23700100( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=342, FN=0, Flags=........, BI=100, SSID=StarDrive
   9 31.64009000( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=387, FN=0, Flags=........, BI=100, SSID=StarDrive
  10 40.95858700( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=482, FN=0, Flags=........, BI=100, SSID=StarDrive
  11 46.59391100( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=542, FN=0, Flags=........, BI=100, SSID=StarDrive
  12 52.20034900( Abocom_83:8b:88    Broadcast          802.11     104 Beacon frame, SN=557, FN=0, Flags=........, BI=100, SSID=07B407536532
  13 76.69634700( Cisco-Li_0a:bf:5c  Broadcast          802.11     104 Beacon frame, SN=866, FN=0, Flags=........, BI=100, SSID=StarDrive
  14 80.91486700( WesternD_36:9c:7c  IPv4mcast_7f:ff:fa 802.11     422 Data, SN=919, FN=0, Flags=.pm...F.
```

45

Questions

?

MIS 5211.701

46

46