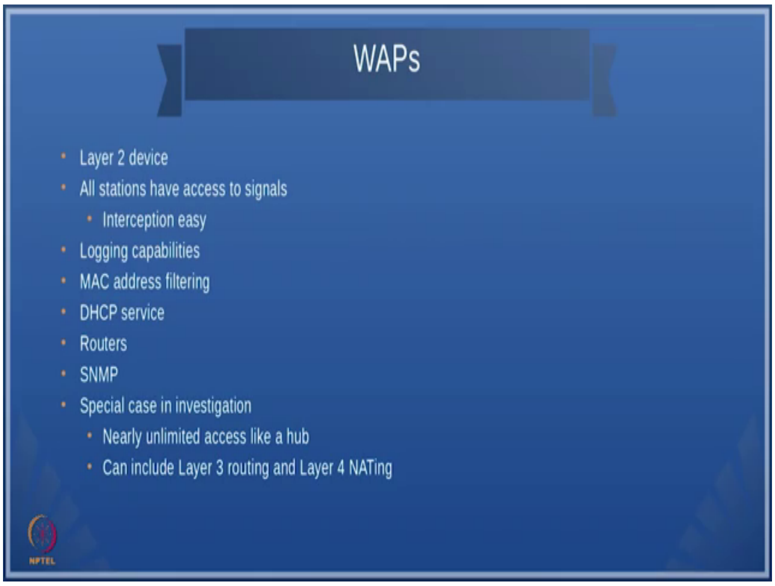
Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 45
Wireless Access Points - Security issues

In the last session, we were discussing a lot about the protocols, the security of protocols and we were talking about the authentication mechanisms that were introduced to improve the security of wireless access networks. In this session, we will talk about wireless access points in general ok.

Most of you would be managing a wireless access point at home because it is wireless, as you know provides lot of convenience in mobility ok. So, you can move inside the house as long as your wireless access point, as excellent signal strength, you do not have to worry about connectivity, not true with Ethernet anyways, ok. So, what are these wireless access points ok?

(Refer Slide Time: 00:58)



WAPs

- Layer 2 device
- All stations have access to signals
  - Interception easy
- Logging capabilities
- MAC address filtering
- DHCP service
- Routers
- SNMP
- Special case in investigation
  - Nearly unlimited access like a hub
  - Can include Layer 3 routing and Layer 4 NATing

These are stations, to which users can connect and if a hacker or a forensic analyst can get access to a wireless access point, then interception of data packets becomes very easy, it is a layer two device similar to the interception that we do for Ethernet, we can also do the interception for wireless LAN also, ok.

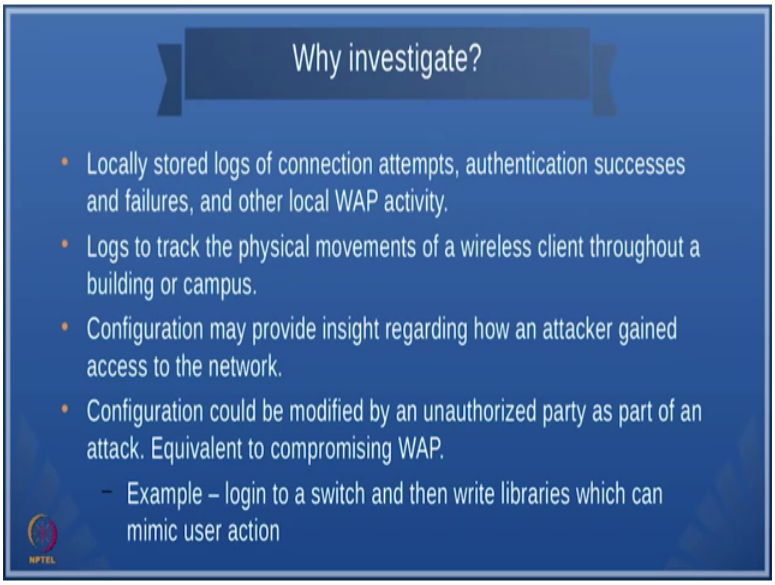
The advantage of wireless access points is that. So, you can categorize them as those wireless access points that you use at home and then you can also categorize wireless access points that are used by enterprises and this wireless access points can be in the form of hierarchy, ok, you can also bridge access points. So, if you if you look at your manual user manual that comes along with your wireless access points, it gives you almost all the features that you can use with access points ok,

From forensic point of view, the wireless access points provide logging features if you take the enterprise, then the logging features are really high, I mean they provide support for SNMP and other things. So, in fact, the enterprise level wireless access points provide much more features and if you buy it from some vendors ok, they also give you software along with these devices to for security monitoring and things like that. So, the other thing that this wireless access points in general ok, even you can do it for the home networks and. In fact, I mean those who are very concerned about security in your home networks what you should do actually. So, that external people do not login is that you should actually take the Ethernet address and put this filter for your device. So, that you can use whatever ip address you wanted will not matter, but only those devices with those Ethernet address will actually be able to access your access point.

So, that is something that if you want a secure network you have to do, and it many of the wireless access point devices like d link or ciscos devices ok, they actually provide you these kind of facility, the other facility that is provided by the access points is DHCP service, I think we had seen all these kinds of service in the introductory session itself, plus they also sometimes some of this wireless access points acts routers they provide support for SNMP which is very good for triggering alerts and things like that and sometimes these access points can also act like naks, ok.

So, it is like even though they are layer two devices they provide services from layer two three and 4 and there is a there is a combination of services that these kind of access points provide that they are more than just switches that used in Ethernet ok. So, so switches sometimes can be dumb whereas, this access points ok, they have much more intelligence embedded in them, therefore, the amount of logs that you get out of the access points are really much higher than what you get out of a switch.

(Refer Slide Time: 04:07)



Why investigate?

- Locally stored logs of connection attempts, authentication successes and failures, and other local WAP activity.
- Logs to track the physical movements of a wireless client throughout a building or campus.
- Configuration may provide insight regarding how an attacker gained access to the network.
- Configuration could be modified by an unauthorized party as part of an attack. Equivalent to compromising WAP.
  - Example – login to a switch and then write libraries which can mimic user action

Now, why should we investigate a wireless access point ok, one the locally stored logs of the access points will have that the connection attempts that are being made whether the authentication was done was a success or a failure and also other local activity for example, what is the ip address that has being leased because this includes the DHCP server it could also tell you what is the ip address the was leased and for how long it was leased and all those things ok.

So, sometimes I have a pc and I connect to an access point and then I move over to another access point I mean if you look at this called a mobility ok. So, it is not necessary that I should I should be always be connected to one particular access point I can actually move around between two or three access points ok.

What could happen is that if these access points are configured properly, they could also provide the necessary information about the physical movement of the person because if I know a person has being attached to a laptop and that laptop has a specific Ethernet address, then wherever this laptop moves along with the person can be tracked with this kind of access points and so, this in forensic investigations will help you to identify where all this person has moved ok. So, usually people move around to do some kind of hack hacking activity ok.

So, if you could track the physical movement of the person, if I could you this kind of data. Now you might ask me a question. So, sir I mean we know that we could spoof the

Ethernet address as well as we could spoof the ip address. So, how can you do it well I mean these are all possibilities ok? So, if a person is technologically good enough to spoof these addresses and all that ok; yes, it becomes much more difficult to handle this kind of cases ok.

Now, the other advantage of using these logs from access points is that ok. So, you could identify how the attacker had gained the access to the network for example, I had enabled peep or some kind of authentication mechanism. So, I will be able to tell you at what time the attacker, try to login to my machine and to what site he tried to connect, etcetera. So, using this kind of 802 dot 1 x authentication protocols will also help you and many of the companies actually have directory services and they use or radius or diameters and protocols to provide authentication kind of services. So, so, this the logs authentication logs along with these kinds of movements will actually help you establish; what is happened ok.

So, one great problem I mean is see many of a times the network protocols use text messages and the hackers actually use this small what should I say? I mean this text messages are part of legacy as well as you know, I go to a software development person, I would rather have xml files rather than some binary files for exchanging data between 2 modules because it provides more flexibility and independence, etcetera, etcetera, etcetera, but then this causes huge damage with respect to network security because if I start sending text messages and these text messages are not encrypted. Then what could happen imagine a situation if I am an hacker ok I would access one of this access points, because I know access points are the place where lot of data pass through and once I login to the access point, I might put some kind of malware into the access points especially these malware could get triggered if they see. For example, some kind of text data say, let us say a text data is deposit 5000 rupees into my account, ok.

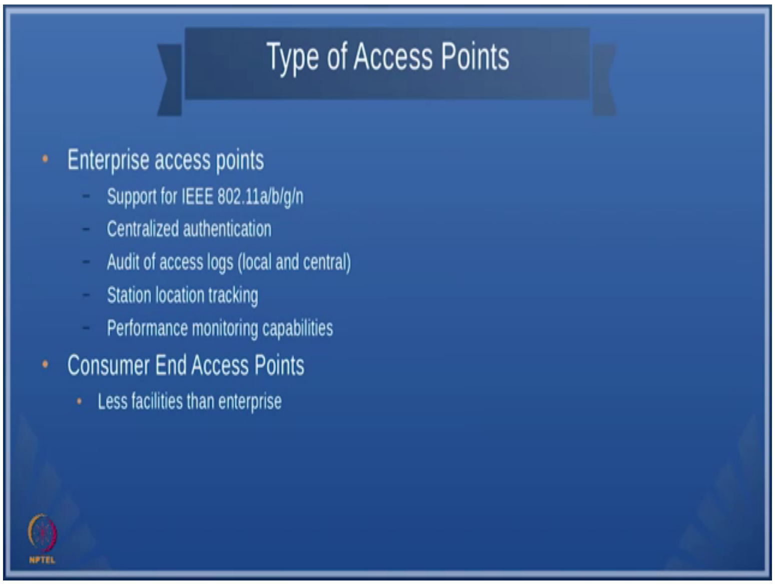
Now, if I sit after an ATM, after the ATM because from the ATM every data goes via some kind of switch or a hardware device. Now if I am able to hack that hardware device. So, even though I might typed 5000 rupees in my keyboard on the ATM, if I have a software sitting behind the ATM, and on the ATM device and it instead of 5000, whenever my account is typed instead of 5000 it sends something as 550,000. So, today you have cash deposit machines. So, I could put 500 rupees, but then if write a malware or some software inside that just adding one more 0 and sending it as a text message because anyhow you are going to send it as a text message ok. So, this kind of text messages lead to lot of problems and believe me, there have being attacks happening based on this kind of loop holes ok.

So, whenever you are on a public medium I mean one of general rule for security is people invent lot of protocols, but many of them do not take into account security has one of the parameters. In fact, in many of the iitef rfcs finally, they had added something known as security considerations and that section is not given much importance. So, you develop a protocol without giving any security consideration that is exactly what is happening in the internet. So, internet was not designed to have security as its feature security was just an add on that was put in to the net these are all some of the reasons why security was we say as put as a add on.

So, they were if you are very happy sending just text messages instead of encrypting them you know that protocols like SNTP, actually send only text messages. So, it is very easy to attack. In fact, not only attack manually I can also write proxy libraries, then place them into the device and these libraries will take care of attacking the network.

So, as I discussed before, there are different types of access points. So, if you take enterprise access points, then these enterprise access points provide much more pieces than features than the consumer and access points ok. So, for example, enterprise access points can provide you performance monitoring capabilities.

(Refer Slide Time: 10:31)

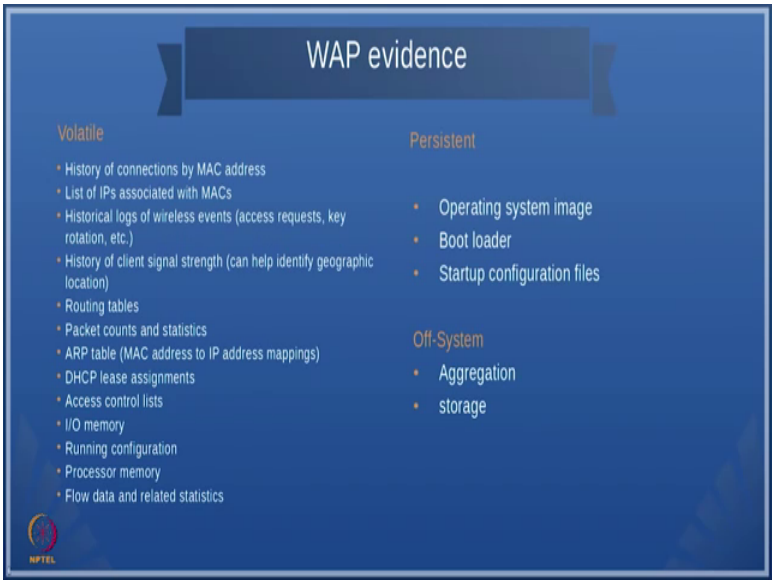


Type of Access Points

- Enterprise access points
  - Support for IEEE 802.11a/b/g/n
  - Centralized authentication
  - Audit of access logs (local and central)
  - Station location tracking
  - Performance monitoring capabilities
- Consumer End Access Points
  - Less facilities than enterprise

It can provide access audit of access logs and then centralized authentication mechanism (Refer Time: 10:36) provided like using radius attacks or something. So, where whenever the authentication happens, it comes to the access point and (Refer Time: 10:44) points goes to the external server authorizes the user and then comes back ok.

(Refer Slide Time: 10:54)



WAP evidence

Volatile

- History of connections by MAC address
- List of IPs associated with MACs
- Historical logs of wireless events (access requests, key rotation, etc.)
- History of client signal strength (can help identify geographic location)
- Routing tables
- Packet counts and statistics
- ARP table (MAC address to IP address mappings)
- DHCP lease assignments
- Access control lists
- I/O memory
- Running configuration
- Processor memory
- Flow data and related statistics

Persistent

- Operating system image
- Boot loader
- Startup configuration files

Off-System

- Aggregation
- storage

So, what of evidence can be collected from WAP ok? So, there are three types of evidences that are collected from a wireless access point, one is the volatile evidences, the other is the persistence evidence and the third is the off system off system issues. So, off system essentially its aggregation of the logs and things like that and where the authenticated etcetera, etcetera, etcetera, etcetera. So, that is that is the easiest part.

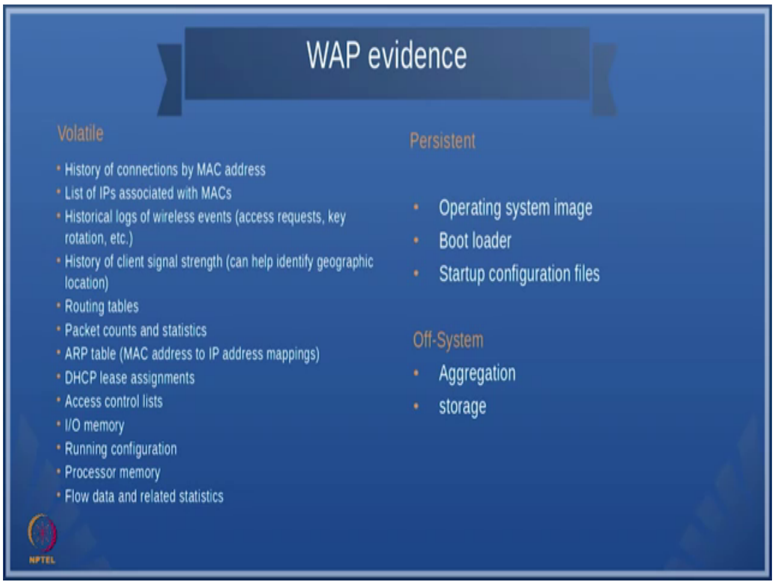
Persistence storage is Cisco for example, Cisco devices, you can do something known as show running config and things like that and then take the configuration of the device. So, when you do forensic analysis you not only how to identify who has hacked, but you might have to tell organization, what are all the corrective actions that the organization can take? Now for example, if there have being configuration break down ok. So, you could tell the organization that this is not the way it should have being configured, it should be configured in such and such a way for all these data you need the operating system image or the boot loader image or the configuration image ok.

For example people who usually forget to upgrade the operating system ok. So, vendors give lot of patches, but people do not bother about putting those patches see because what happens in these kind of places where you need lot of securities that you must be upgrading the system quite frequently to fix any security loop holes ok. So, for that you need this persistence evidence because then if for example, I say that the security patch has being provided for one dot one and my os that is running 1 dot 0 and; obviously, the corrective measure is to bring in place a process by which security lop holes can be plugged immediately.

This kind of forensic activity is not only detecting what went wrong and how it went wrong and all that it is to some extent you should also provide means for correcting the issues ok. So, coming to all volatile kind of evidence there are bunch of stuff has discussed here running configurations volatile see sometimes people want to change some configurations see everything is fine, but then they forget to save the configuration. So, in Cisco routers you can change the running configuration and finally, many people forget to save the configuration then you have to restart the whole process again I mean if you are network administrator, you would know about the problem with this, but then this volatile information includes DHCP lease agreements assignments and then routing tables, etcetera, routing tables tend to change depending on the protocol what the routing protocol gets data.

So, these are bunch of volatile evidences. So, when you are working with network forensics of access points, you have to consider group the evidences into three parts and collect it accordingly.

(Refer Slide Time: 13:35)



WAP evidence

Volatile

- History of connections by MAC address
- List of IPs associated with MACs
- Historical logs of wireless events (access requests, key rotation, etc.)
- History of client signal strength (can help identify geographic location)
- Routing tables
- Packet counts and statistics
- ARP table (MAC address to IP address mappings)
- DHCP lease assignments
- Access control lists
- I/O memory
- Running configuration
- Processor memory
- Flow data and related statistics

Persistent

- Operating system image
- Boot loader
- Startup configuration files

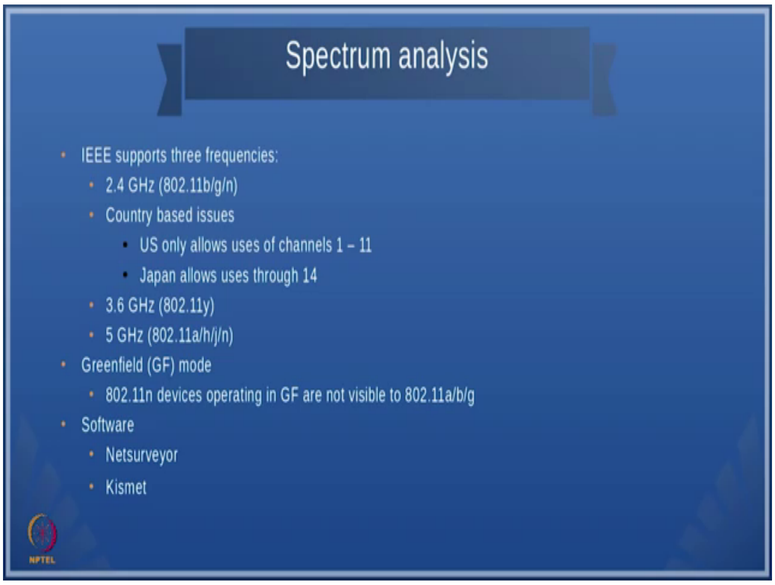
Off-System

- Aggregation
- storage

The most important forensic activity that someone might do network forensic expert might do is spectrum analysis. Now there are some issues in spectral analysis see country based issues are there us only allows channels one to 11 in its routers where as Japan uses 14 channels ok. So, if I can see, what I can do is I can have a device which works on all 14 channels, but what I will do is I will take data from channel 1 to 11 and then send it via 12, 13 and 14 and if you see its very difficult to discover that there is data leaks that are happening.

So, you need to pay aware of as a forensic expert you need to be aware and in this case there is no way you are going to identify because if yours is only a one to 11 channel router which you brought in the us and not a Japanese router, you really have a problem on doing the forensic activity itself ok. So, these types of issues are not a problem in wired networks. So, wireless networks there are there are slightly more issues. So, on our example of issues in wireless network is something known as a green field mode ok.

(Refer Slide Time: 14:42)



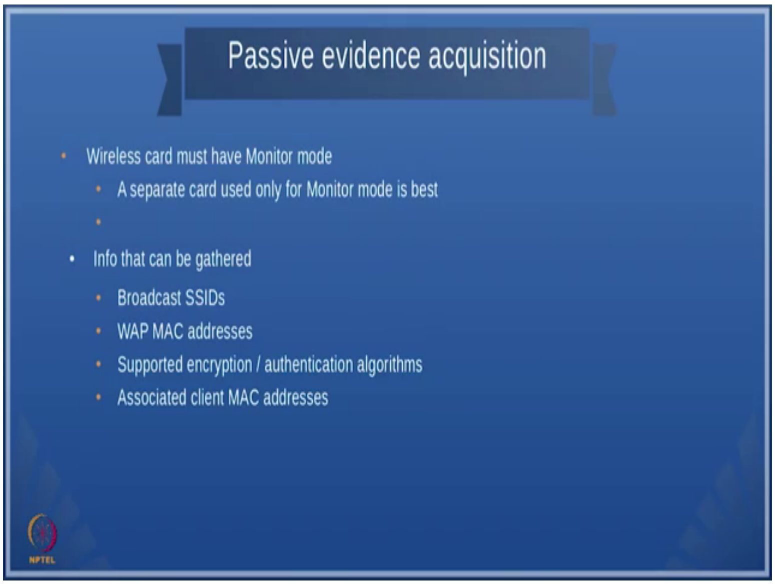
Spectrum analysis

- IEEE supports three frequencies:
  - 2.4 GHz (802.11b/g/n)
  - Country based issues
    - US only allows uses of channels 1 – 11
    - Japan allows uses through 14
  - 3.6 GHz (802.11y)
  - 5 GHz (802.11a/h/j/n)
- Greenfield (GF) mode
  - 802.11n devices operating in GF are not visible to 802.11a/b/g
- Software
  - Netsurveyor
  - Kismet

802 dot 1 1 device operating at green field mode or not visible to 802 dot 11 a 11 b or 11 g networks.

So; that means, someone can be still in your network, but you may not be able to see him at all ok. So, you might have to look at hardware based analysis ok. So, there could be hardware devices can do all these spectrum analysis and along with a software solution something like net surveyor kismet, etcetera. So, this as a network forensic expert, you need to be ware that there are certain channels which may not be visible to you. So, when you do forensics you have to look at all the channels, and get that logs out of the channels because collecting evidence itself is a big problem in wired networks.

(Refer Slide Time: 15:32)



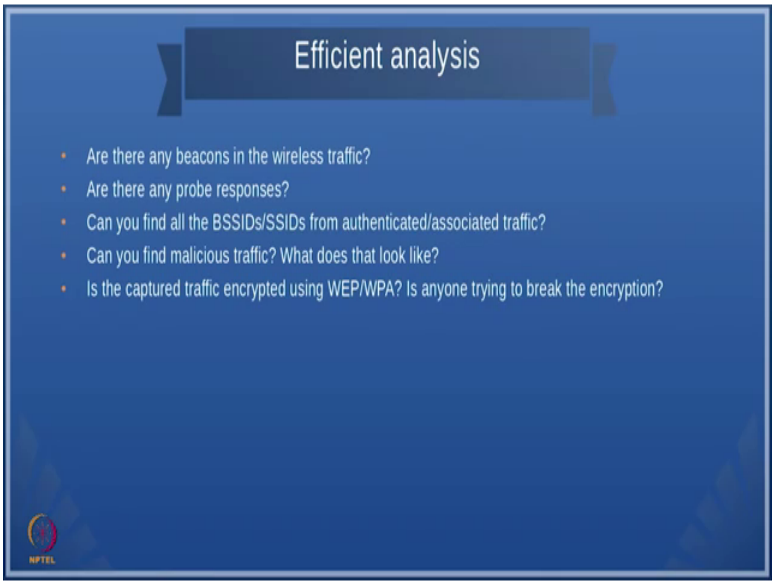
Passive evidence acquisition

- Wireless card must have Monitor mode
  - A separate card used only for Monitor mode is best
  -
- Info that can be gathered
  - Broadcast SSIDs
  - WAP MAC addresses
  - Supported encryption / authentication algorithms
  - Associated client MAC addresses

The other part is that you can actually do passive evidence acquisition ok. So, wireless cards must also have something known as a monitor mode and it is better you purchase some wireless cards in order to solve the previous problem that we discussed ok, you can collect lot of information like you can collect the broadcast SSID, then you can collect the WAP map addresses and encryption algorithms, etcetera, what are the encryption algorithms that are supported or used etcetera.

And then you can also collect the client MAC addresses and coming to the analysis, you should be able to analyze ok.

(Refer Slide Time: 16:13)

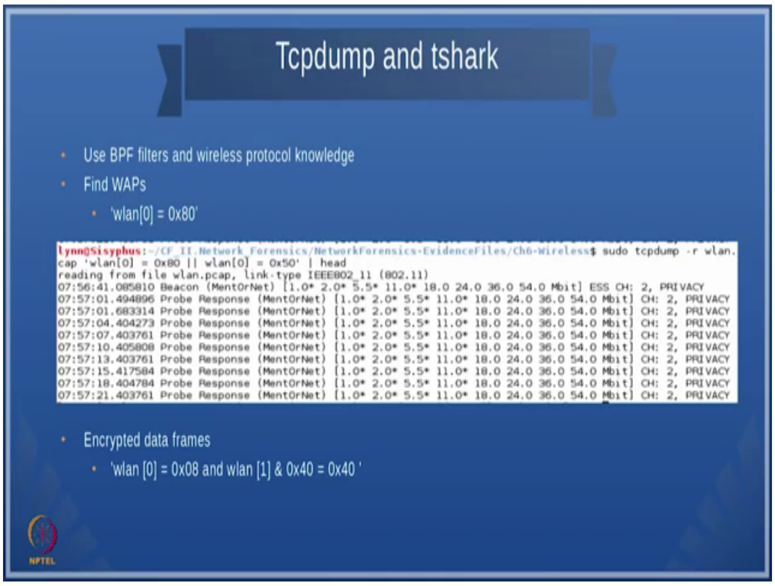


Efficient analysis

- Are there any beacons in the wireless traffic?
- Are there any probe responses?
- Can you find all the BSSIDs/SSIDs from authenticated/associated traffic?
- Can you find malicious traffic? What does that look like?
- Is the captured traffic encrypted using WEP/WPA? Is anyone trying to break the encryption?

What are all the associations? What are probe responses, then what are all beacons that are there ok, can you find unauthenticated traffic authenticated traffic, then authenticated and those traffic that is associated with particular authentication can you find out malicious traffic, etcetera, etcetera are same the analysis more less similar to what we do at wired networks except that you are going to talk about beacon association and things like that and the tools that we previously use like tshark, etcetera, wire shark, etcetera can be used to find out all these options ok.

(Refer Slide Time: 16:48)



Tcpdump and tshark

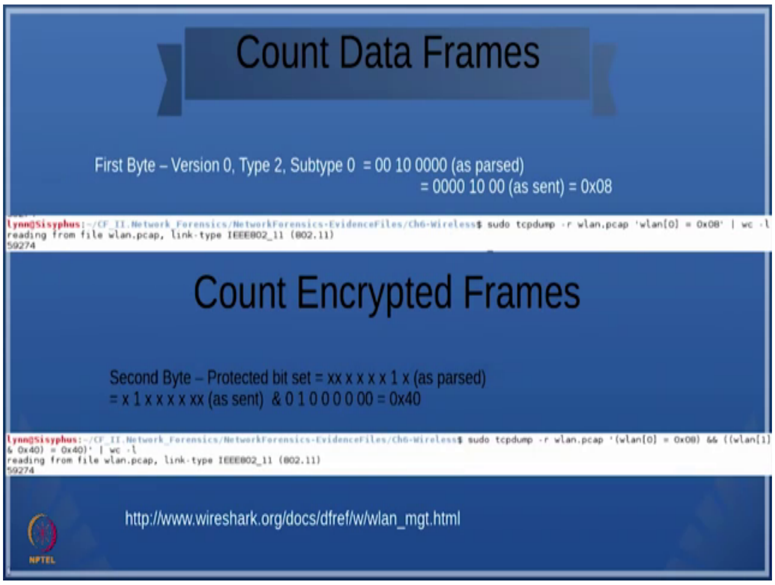
- Use BPF filters and wireless protocol knowledge
- Find WAPs
  - 'wlan[0] = 0x80'

```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.
cap 'wlan[0] = 0x80 || wlan[0] = 0x50' | head
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
07:56:41.085810 Beacon (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 2, PRIVACY
07:57:01.494896 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:01.683314 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:04.404273 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:07.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:10.405808 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:13.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:15.417584 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:18.404784 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:21.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
```

- Encrypted data frames
  - 'wlan [0] = 0x08 and wlan [1] & 0x40 = 0x40 '

So, here is an example if you want to find out WAP, then I just have to look search for wlans 0s parameter 0 x x 0 8 0 and then if you want to search for encrypted frames, you just say 0 the parameters, it would be 0 8 and wlans, one should be 0 x 4 0, then you can find out what type of encryption, etcetera.

(Refer Slide Time: 17:12)



Count Data Frames

First Byte – Version 0, Type 2, Subtype 0 = 00 10 0000 (as parsed)
= 0000 10 00 (as sent) = 0x08

```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.pcap 'wlan[0] = 0x08' | wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
```

Count Encrypted Frames

Second Byte – Protected bit set = xx x x x x 1 x (as parsed)
= x 1 x x x x xx (as sent) & 0 1 0 0 0 0 00 = 0x40

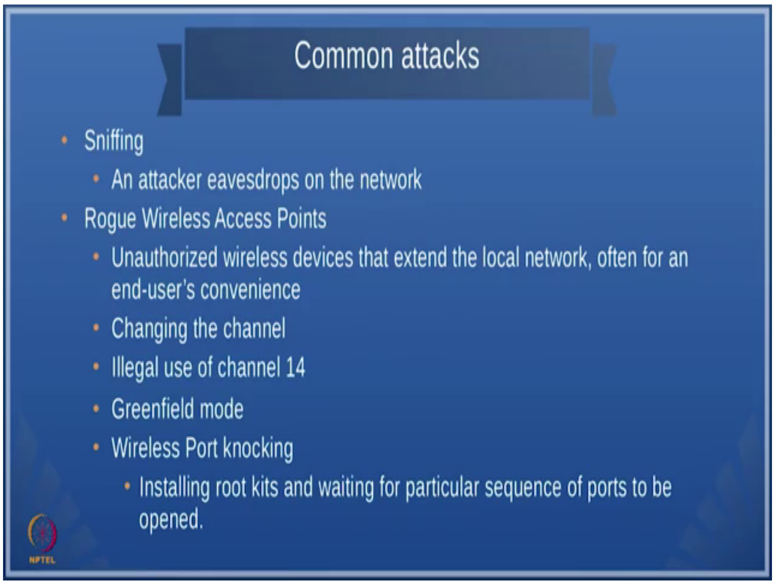
```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.pcap '(wlan[0] = 0x08) && ((wlan[1]
& 0x40) = 0x40)' | wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
```

http://www.wireshark.org/docs/dfref/w/wlan_mgt.html

Similarly, if you want to count the number of data frames you can use tshark and what we would suggest is that ok. So, go to the link that is given there www dot wireshark dot org and it talks about what are the ways in which wireshark and tshark can be used for wlan management this itself is a specific particular huge area ok. So, collecting frames in wired network is different from collecting frames in wireless as we have seen. So, tgis as lot of parameters and things like that ok.

So, one of the things that you should know is; what are the types of attacks that usually happen in wire wireless networks ok.

(Refer Slide Time: 17:54)



Common attacks

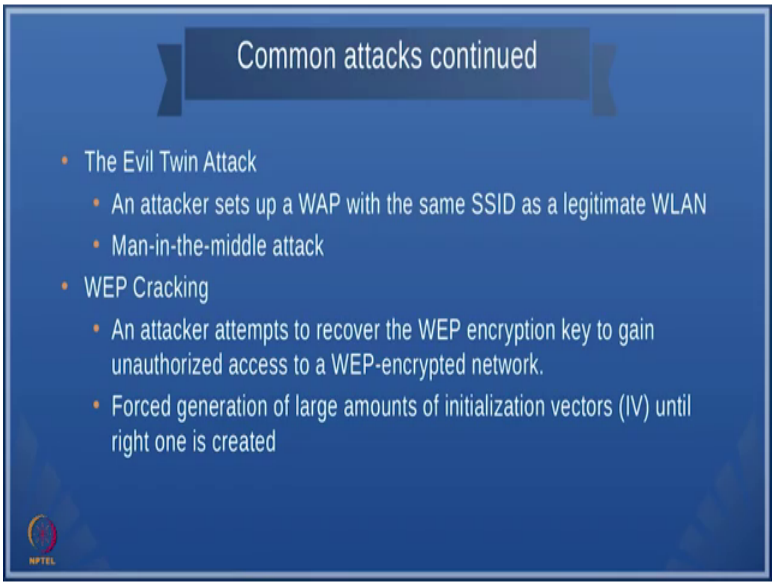
- Sniffing
  - An attacker eavesdrops on the network
- Rogue Wireless Access Points
  - Unauthorized wireless devices that extend the local network, often for an end-user's convenience
  - Changing the channel
  - Illegal use of channel 14
  - Greenfield mode
  - Wireless Port knocking
    - Installing root kits and waiting for particular sequence of ports to be opened.

Sniffing is (Refer Time: 17:54) it can happen both in wired and wireless, the other difference is that one is the rogue wireless access points see in your organization, let us say, you have a access point by name some organization one ok, what I could do is I could bring a router from my home, make the association id as organization one and then give more strength for router and keep it. Now any guy who comes and think that what are router you have brought is companies router you and you hide it somewhere ok. So, they looking at signal strength usually what happens your device connects to the signal strength that is really good. So, yours is a best router that is available. So, everyone will start connecting to you and once people start connecting to you, you can start getting their data, I think we acquisition of evidences very easy ok.

So, this rogue wireless access points can have these are unauthorized wireless devices that extend the local network and often for end users convenience and essentially I mean, what you could do is you could just play with it if you get access to all the people data ok. So, there are other things that you can do as I told you playing with the channels using channel 14 for sending your data and then one of the most important stuff is known as wireless port knocking.

So, what it does is that say I see a particular pattern of data that comes in to me and immediately what I do is I just if particular once a particular sequence of ports are opened, then I open up my software because I scan for what are the kinds of port that I would like to see once I see those kind of ports I open that I mean I what I do is I actually start running my software its start of root kit ok. This is exactly, what I told you in the previous two slides back where someone can go and hack some kind of a switch and do this. So, if the switch looks at I am trying to scan set number of ports, then my software will get activated and then start attacking.

(Refer Slide Time: 19:59)

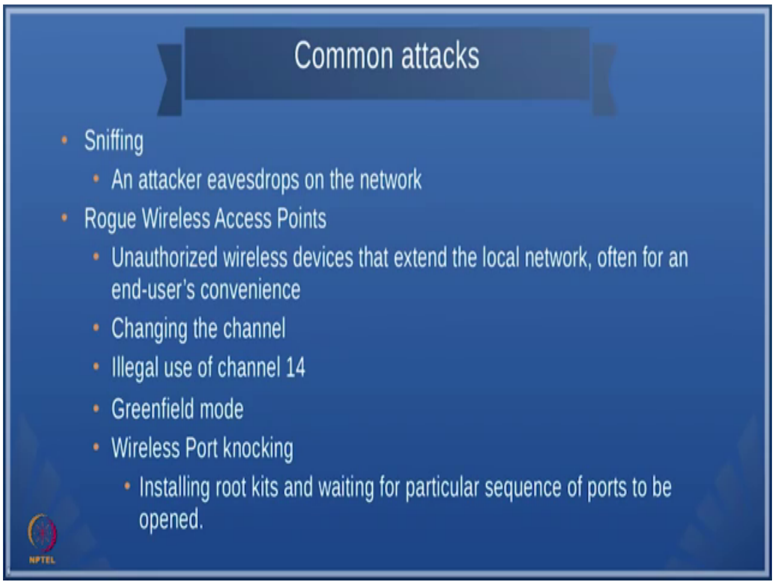


Common attacks continued

- The Evil Twin Attack
  - An attacker sets up a WAP with the same SSID as a legitimate WLAN
  - Man-in-the-middle attack
- WEP Cracking
  - An attacker attempts to recover the WEP encryption key to gain unauthorized access to a WEP-encrypted network.
  - Forced generation of large amounts of initialization vectors (IV) until right one is created

There also something known as evil twin attack, I mean which is similar to the rogue.

(Refer Slide Time: 20:01)



Common attacks

- Sniffing
  - An attacker eavesdrops on the network
- Rogue Wireless Access Points
  - Unauthorized wireless devices that extend the local network, often for an end-user's convenience
  - Changing the channel
  - Illegal use of channel 14
  - Greenfield mode
  - Wireless Port knocking
    - Installing root kits and waiting for particular sequence of ports to be opened.

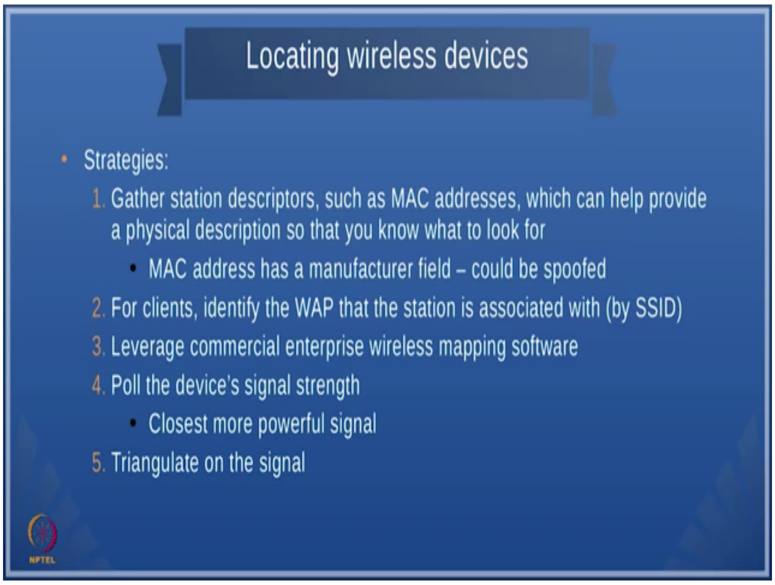
Access points rogue, wireless access point is actually a is what should I say your organization has a legal router, wireless access point for extending the range of your router whereas, evil twin is I do it with a malicious user as a malicious user, ok.

So, in this way it is a lot of man in middle attack ok. So, what I do is I connect, I bridge my wireless access point to some other network, but then get the data from you and then send it this network that can be done and final one what we can do is web cracking ok. So, the difference between the evil twin attack and the rogue access point is the rogue access point could be installed by the company itself and this evil twin is you actually install maliciously to get malicious data you install the same web ok.

Web cracking is something as I told you, it can be used for web cracking the other things that we can use is locating the wireless networks see what you can do is you can actually once I know the signal strength and other things I will able to ga gather the station descriptor such as MAC address etcetera and what you can do is you can start plotting where your devices are ok. There are lot of software that allow you to do the plotting ok. This basically why people use the software is to provide wireless devices at the right places, ok.

So, they do something known as a wireless kind of scanning and then study the spectrum what is the signal strength how many users are there and so on. So, that I can minimize the number of routers and provide maximum coverage.

(Refer Slide Time: 21:47)

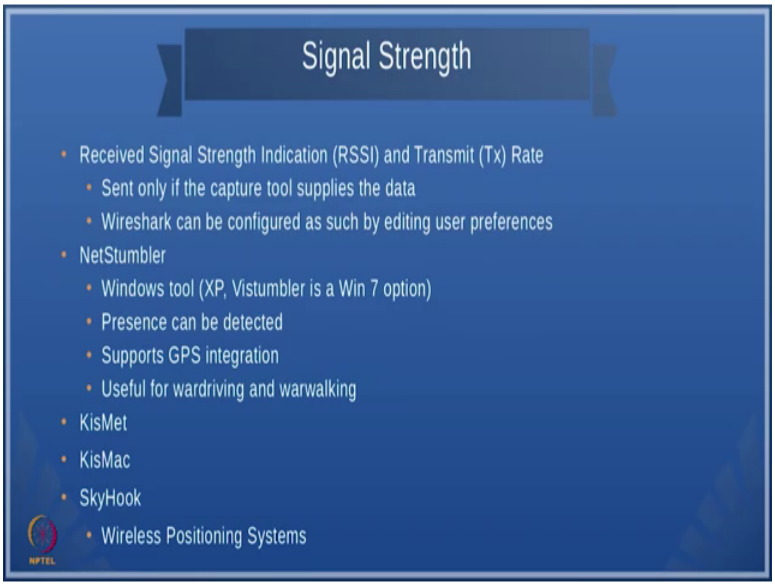


Locating wireless devices

- Strategies:
  1. Gather station descriptors, such as MAC addresses, which can help provide a physical description so that you know what to look for
     - MAC address has a manufacturer field – could be spoofed
  2. For clients, identify the WAP that the station is associated with (by SSID)
  3. Leverage commercial enterprise wireless mapping software
  4. Poll the device's signal strength
     - Closest more powerful signal
  5. Triangulate on the signal

Now, the same strategy can be used in other way to find out which device is close to me to identify a person and all where the person is, etcetera. So, all these things can be done by locating by the idea of placing the wireless devices in a particular place in organization to get maximum benefit out of wireless network can also be used to track the wireless devices or the rogue wireless devices that are connected to the network. So, both can be done.

(Refer Slide Time: 22:17)

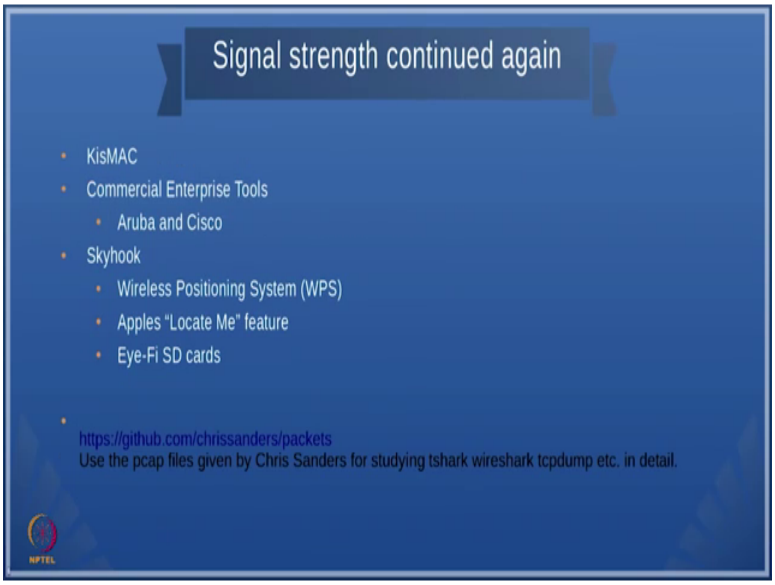


Signal Strength

- Received Signal Strength Indication (RSSI) and Transmit (Tx) Rate
  - Sent only if the capture tool supplies the data
  - Wireshark can be configured as such by editing user preferences
- NetStumbler
  - Windows tool (XP, Vistumbler is a Win 7 option)
  - Presence can be detected
  - Supports GPS integration
  - Useful for wardriving and warwalking
- KisMet
- KisMac
- SkyHook
  - Wireless Positioning Systems

So, there are many software which you can do it ok. So, the software uses RSSI transmit rate, etcetera, netstumbler is one software that is available only on windows ok, it supports GPS integration. So, the other one is KisMet, KisMac, SkyHook which is a wireless positioning system and so on ok.

(Refer Slide Time: 22:35)



Signal strength continued again

- KisMAC
- Commercial Enterprise Tools
  - Aruba and Cisco
- Skyhook
  - Wireless Positioning System (WPS)
  - Apples “Locate Me” feature
  - Eye-Fi SD cards
- https://github.com/chrissanders/packets
  Use the pcap files given by Chris Sanders for studying tshark wireshark tcpdump etc. in detail.

There are also other software which you can use for this kind of activity like KisMac and SkyHook, etcetera. Now, before I end the session, I just wanted to tell you about this website ok.

So, it is called github dot com slash chrissanders and packets. So, if you want to gain more expertise until now we are looking at evidence acquisition and then we are looking at how to analyze the packets. So, this website is has lot of packet dumps ok, which he has provided the person the owner of the website has provided free of cost ok, you can actually download this pcap files and then have your wireshark open this pcap files and then start studying or start doing the forensics he tells you what type of attack he has logged the packets for. So, try to find out how you can find out those attacks using the dumps.

(Refer Slide Time: 23:34)

Works Cited

Davidoff, S., & Ham, J. (2012). *Network Forensics Tracking Hackers Through Cyberspace*. Boston: Prentice Hall.

So, as usual our reference book is this network forensics tracking hackers through cyberspace ok. So, we will in the next session, what will do is will do a case study. Now, in this case study, what we are going to do is we are going to actually use a tool ok. So, until now we had talked about tshark and other things, but will be actually using tool to identify and tell and show that how work can be done easily by network forensic if they go for some kind of tools to do their job.

Thank you very much.