IEEE 802.11 - Security Concerns

James Chandra

Abstract: WLANs have become the network of choice over the years due to its many benefits however due to this very reason many threats have become associated to it and is the focus of this paper. The paper also highlights mitigation techniques to tackle the listed threats along with some best practices.

Index Terms: IEEE 802.11, Wi-Fi, WLAN Security

1 Introduction

Networks of any nature emanates its benefits as well as it's share of concerns with the major concern been its security aspect. With the vast range and various types of networks been developed in this modern era the most opted network of choice remains WLAN also identified as IEE 802.11 standard however most just know this as Wi-Fi. The popularity of WLAN has seemed to continually upscale over the years due to many a reasons such as the ease of installation and setup, mobility, flexibility and scalability to name a few. The inception of WLAN or IEE 802.11 was in 1997 and was based on radio technology. Since then there has been many updates to this standard mostly to enhance it's existing potential as well to narrow up on its suspected vulnerabilities

TABLE 1
IEEE 802.11 RELEASES

IEE 802.11	Release Date	Frequency (GHz)	Max Data Rate (Mbps)	Range (m)	
				Indoor	Outdoor
-1997	1997	2.4	2	20	100
a	1999	5/3.7	54	35/-	120/5k
b	1999	2.4	11	35	140
g	2003	2.4	54	38	140
n	2009	2.4/5	600	70	250
ac	2013	2.4/5	450/7000	35	
ad	2012	60	7000	10	
af	2016	0.470-0.710	568		6000
ah		0.9	40		
aj		45/60	7000	10	

2 Components

The two major WLAN components include an access point (AP) which aids in exchanging messages with other WLAN enabled devices via the means of an antenna. It's role is also to authenticate and associate wireless clients to the wireless network. The other component is a Network Interface Card (NIC)/Client Adapter which basically monitors for available frequency spectrum for association and connectivity to AP. They operate in one of two modes which are ad hoc peer-to-peer or infrastructure mode with an AP

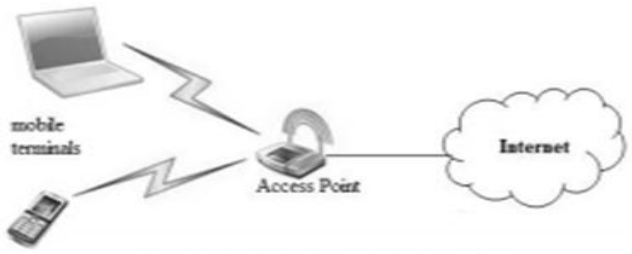


Fig.1. Components of WLAN

3 Applications

The applications of WLAN is vast from home users where ISP's now provide wireless router to which the many "smart" devices connect to. Businesses such as restaurants utilize to take food orders. Automobile industry where cars are now installed with Wi-Fi devices that can share information with regards to maintenance issues. Medical Faculties which now use implantable devices that directly communicates with the doctor. Manufacturing industry are now creating wearable's such as Fit bits for monitoring exercise and sleep to heart monitors.

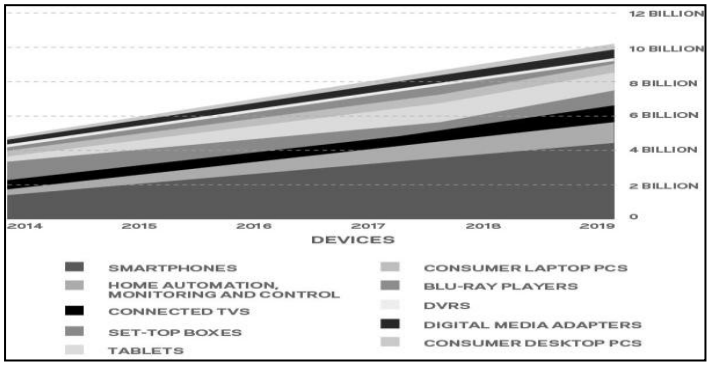
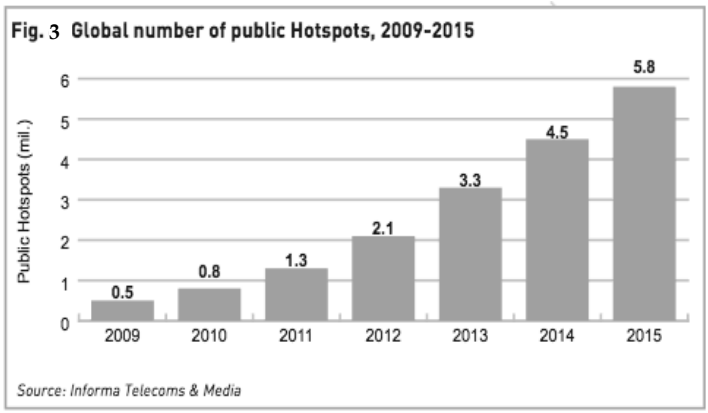


Fig 2. *Projection, Household Owned WLAN Enabled Devices*

4 Growth



5 CURRENT & EMERGING THREATS

TABLE 2
AUTHENTICATION ATTACKS

Type of Attack	Description	Methods and Tools
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed, vendor default or cracked WEP keys.	WEP Cracking Tools
PSK Cracking	Recovering a WPA/WPA2 PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
802.1X EAP Downgrade	Forcing an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets.	File2air, libradiate
802.1X Password Guessing	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password Dictionary
802.1X LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker

TABLE 3
ACCESS CONTROL ATTACKS

Type of Attack	Description	Methods and Tools
War Driving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software AP
Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

TABLE 4
AVAILABILITY ATTACKS

Type of Attack	Description	Methods and Tools
AP Theft	Physically removing an AP from a public space.	"Five finger discount"
Queensland DoS	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
802.11 Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	FakeAP
802.11 Associate / Authenticate Flood	Sending forged Authenticates or Associates from random MACs to fill a target AP's association table.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject, LORCON
802.11 Deauthenticate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Aireplay, Airforge, MDK, void11, commercial WIPS
802.1X EAP-Start Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.	QACafe, File2air, libradiate
802.1X EAP-Failure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Sending a malformed 802.1X EAP Identity response known to cause some APs to crash.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Sending EAP type-specific messages with bad length fields to try to crash an AP or RADIUS server.	QACafe, File2air, libradiate

TABLE 5
INTEGRITY ATTACKS

Type of Attack	Description	Methods and Tools
802.11 Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + Injection Tools
802.1X EAP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay.	Ethernet Capture + Injection Tools between AP and authentication server

6 MITIGATION TECHNIQUES

6.1 SSID
Changing the default SSID of an AP or simply disabling SSID broadcast. Making use of VPN authentication by placing an AP behind a VPN server however if there are multiple APs then they may be connected to a switch and the switch to the VPN server.,

6.2 DHCP
Most WLANs make use of DHCP however if static IP's are used and DHCP is disabled then it may limit the chances of the attacker obtaining a valid IP address to validate itself to an AP.

6.3 AP Placement
It is best practice to place APs physically in non-disclosed/secured areas and logically to place them behind corporate firewalls. To minimize radio wave propagation in non-user areas it is recommended to orientate AP antennas away from public areas and boundaries.

6.4 Policies
Every organization must have in place as well as enforce certain WLAN policies which enforces monitoring, proper usage, limitations to certain channels and data rates. They must also have in place WLAN focused Intrusion detection systems which must provide 24/7 monitoring and response if policies are in threat of violation

6.5 Tools
There addition to the best practices and measures there are several commercial tools that have been developed to provide protection for WLANs to some extent. A common example is AirDefense that provides WLAN intrusion protection and management. There are also a good range of freeware tools available such as NetStumbler, WaveStumbler to name a few.

7 CONCLUSION
As wireless networks are gaining popularity at a staggering rate its weakness are also been exploited to a somewhat alarming rate to which various mechanisms have been identified to mitigate them however there is no one solution to completely be relied upon however continuous upgrade of security knowledge and best practices should provide any organization a fighting chance.

REFERENCES
[1] Abrams, Marshall D. Jajodia, Susshil G. and Podell Harold J. Information Security: An Integrated Collection of Essays, in IEEE Computer Society Press, Los Alamitos, CA: USA. 1995.

[2] AirDefense, Inc. Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise. 2002: Pp. 9-10

[3] Gast, Mathew. 802.11 Wireless Networks: The Definitive Guide, Second Edition. Sebastapol, CA: O'Reily & Associates, Inc, 2005: pp. 50-60

[4] Molisch, Andreas. Wireless Communications. Wiley-IEEE Press. 2005:Pp2-4

[5] Rappaport, Theodore. Wireless Communications: Principles and Practice. Prentice Hall. 2002. Pp.5-7

[6] Plotter, Bruce and Fleck, Bob. 802.11 Security. Sebastopol, CA: O'Reily & Associates, Inc 2002. Pp.5-9. Ross, John

[7] Treek, Denis. An integral framework for information systems security management

[8] Computers & Security. Vol22. New York: Macmillan, 2003. Pp.337-360

[9] Whitson, G. Computer security: theory, process and management, J. Comput. Small Coll, 18. (2003)57-66