Certified Wireless Network Professional

Rameshwar Nigam
General Manager
@CWNP

Certified Wireless Network Professional
CWNP
Certitrek GROUP

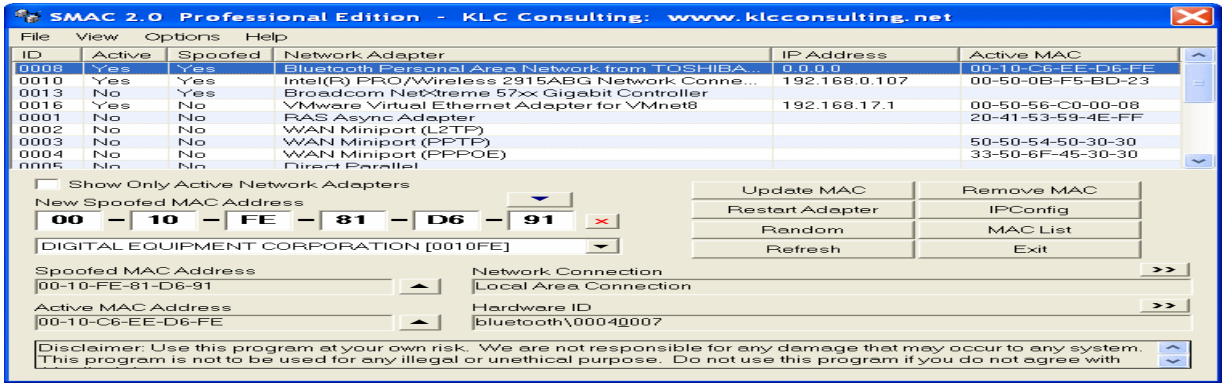
Securing Wireless Networks

Agenda

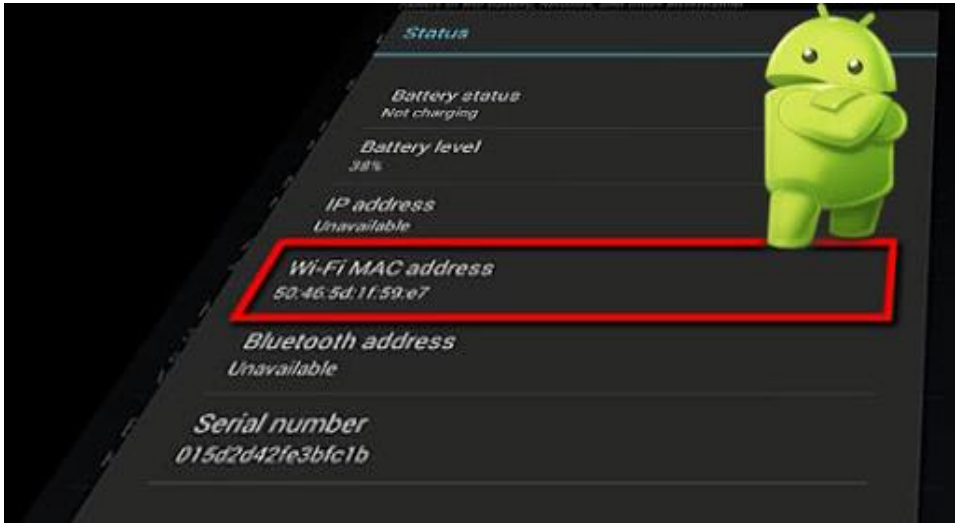
- Types of WLAN attacks
- Security vulnerabilities
- Wi-Fi Ease of use – WPS and it's issues
- How to mitigate the attacks

Certified Wireless Network Professional
CWNP

MAC identity spoof attacks



- MAC spoofing attack is still used with great effect at public-access WLAN hotspot.
- A MAC *piggy-backing* attack is used to circumvent the hotspot captive portal login requirement.
- The intent is not to break into the network, but the exploit the way captive portal works.



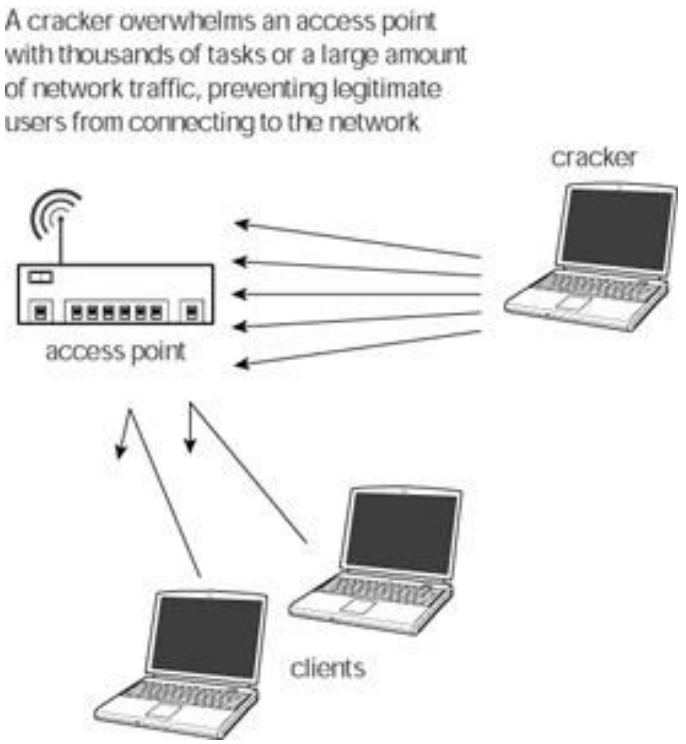
Denial Of Service attacks

Layer 1 DOS Attacks:

- Unintentional Interference
- Intentional Interference
- Queensland attack

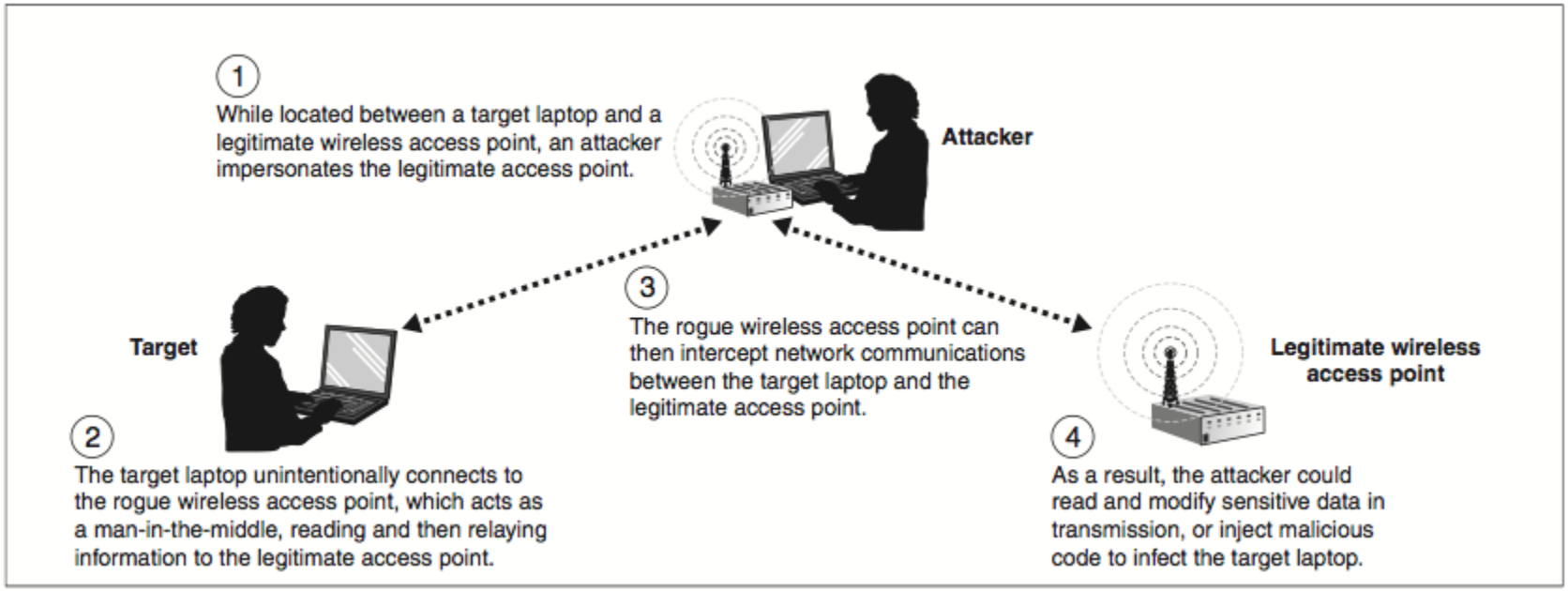
Layer 2 DOS Attacks:

- Illegal Channel beaconing
- Probe response flood
- Association Flood
- Fake AP
- Virtual-carrier attack

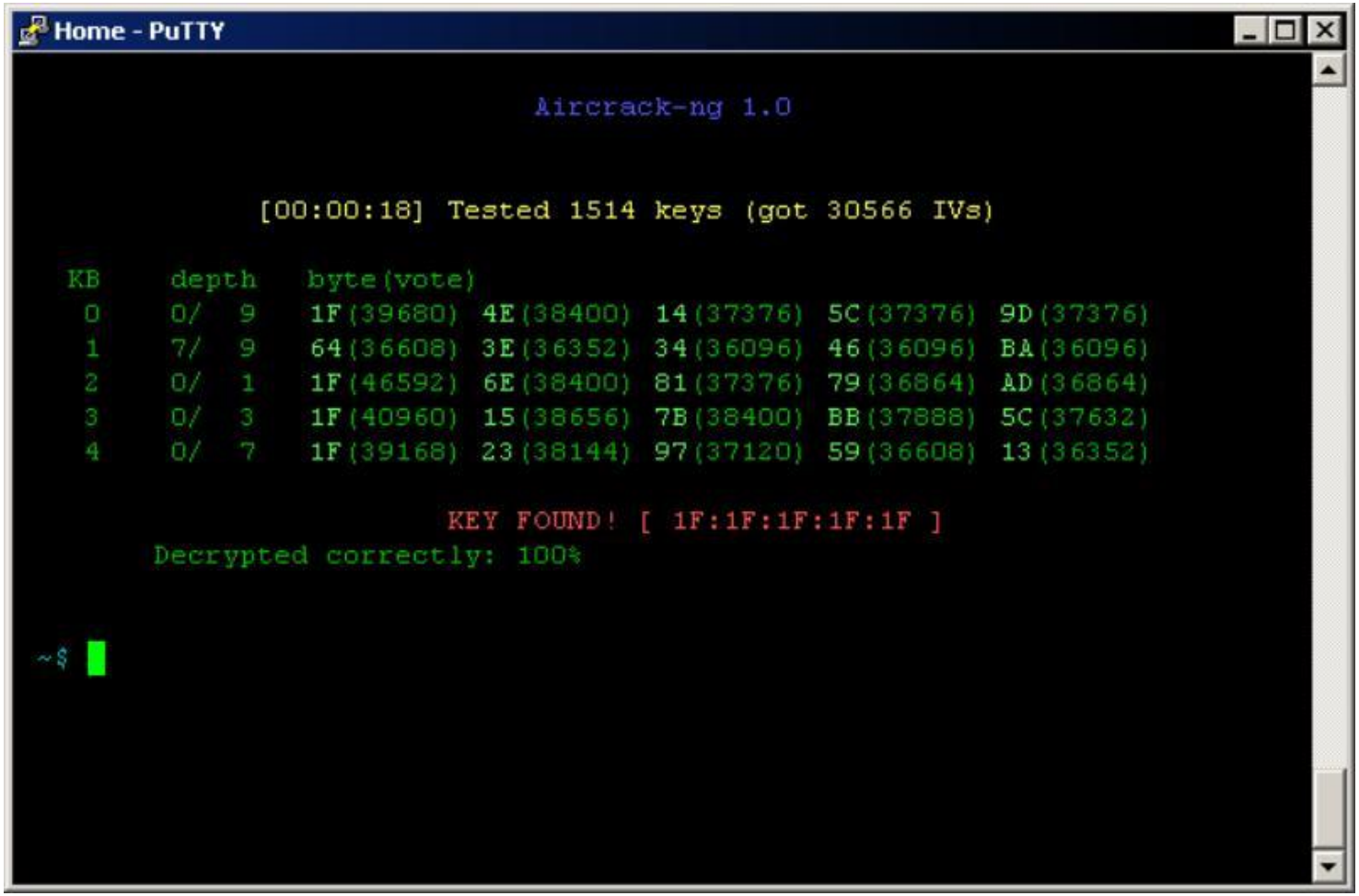


Man in the middle attack

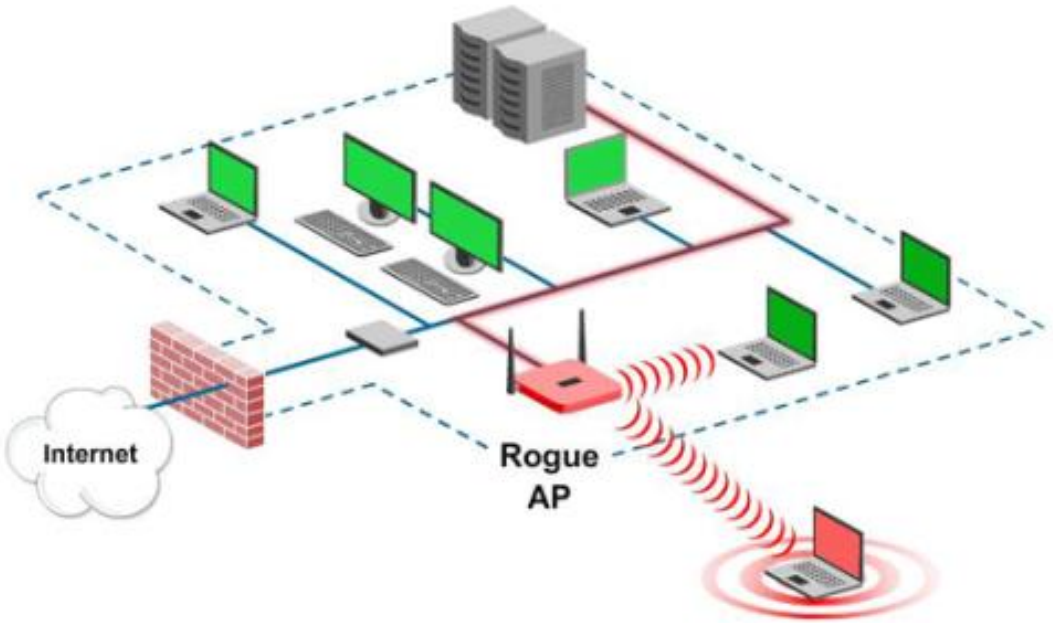
- Evil Twin Attack
- Wi-Fi phishing Attack



Static WEP cracking programs



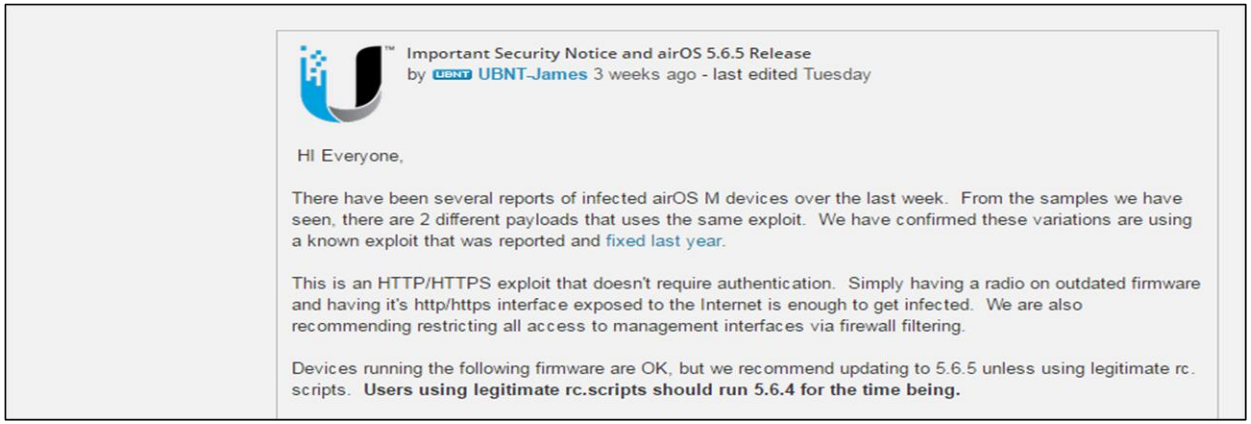
Rogue Access Point attack programs



Potential Risks

- Data Theft
- Data Destruction
- Malicious Data Insertion
- Third-Party Attacks

Wireless Security Vulnerabilities



Important Security Notice and airOS 5.6.5 Release
by UBNT UBNT-James 3 weeks ago - last edited Tuesday

HI Everyone,

There have been several reports of infected airOS M devices over the last week. From the samples we have seen, there are 2 different payloads that uses the same exploit. We have confirmed these variations are using a known exploit that was reported and fixed last year.

This is an HTTP/HTTPS exploit that doesn't require authentication. Simply having a radio on outdated firmware and having it's http/https interface exposed to the Internet is enough to get infected. We are also recommending restricting all access to management interfaces via firewall filtering.

Devices running the following firmware are OK, but we recommend updating to 5.6.5 unless using legitimate rc. scripts. **Users using legitimate rc.scripts should run 5.6.4 for the time being.**

CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Homeland Security
Sponsored by the DHS Office of Cybersecurity and Communications

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Vulnerability Note VU#981271

Multiple wireless keyboard/mouse devices use an unsafe proprietary wireless protocol

Original Release date: 24 Feb 2016 | Last revised: 01 Mar 2016

Print | Tweet | Send | Share

Quick Search

Go

Advanced Search »

Wi-Fi ease of use – WPS and its issue

- WPS is a network security standard to create a secure wireless home network
- User can easily configure a network with security protection by using a personal identification number (PIN) or a button located on the access point and the client device.
- WPS was developed by the Wi-Fi Alliance and is a protocol specification that rides over the existing IEEE 802.11-2007 standard.
- Security setup options are *personal information number (PIN), push-button configuration (PBC), Near Field Communication (NFC)* tokens and *Universal Serial Bus (USB)* flash drives.

Authentication (PIN – External Registrar)

IEEE 802.11		
Supplicant --> AP	Authentication Request	802.11 Authentication
Supplicant <-- AP	Authentication Response	
Supplicant --> AP	Association Request	802.11 Association
Supplicant <-- AP	Association Response	

IEEE 802.11/EAP		
Supplicant --> AP	EAPOL-Start	EAP Initiation
Supplicant <-- AP	EAP - Request Identity	
Supplicant --> AP	EAP - Response Identity (Identity: “WFA-SimpleConfig-Registrar-1-0”)	

...the vulnerability

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee --> Registrar	N1 || Description || PK_E	Diffie-Hellman Key Exchange
M2	Enrollee <-- Registrar	N1 || N2 || Description || PK_R || Authenticator	
M3	Enrollee --> Registrar	N2 || E-Hash1 || E-Hash2 ||Authenticator	
M4	Enrollee <-- Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KeyWrapKey}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee --> Registrar	N2 || $E_{KeyWrapKey}$(E-S1) ||Authenticator	proove posession of 1st half of PIN
M6	Enrollee <-- Registrar	N1 || $E_{KeyWrapKey}$(R-S2) ||Authenticator	proove posession of 2nd half of PIN
M7	Enrollee --> Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee <-- Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

Pixie Dust WPS attack/Reaver brute force attack can easily crack WPS PIN

Mitigating the risks

- Wireless Security Auditing
  - OSI Layer 1 Auditing
  - OSI Layer 2 Auditing
  - Penetration Testing
- Wireless Security Policies
  - Functional Policy
  - Government and Industry Regulations
- Wireless Security Monitoring
  - Wireless Intrusion Detection and Prevention System

Wireless Security Audit

Type of Use	Possible Audit/Attack	Tools
Wireless discovery	Eavesdropping, discovery of rogue APs, ad hoc STAs and open/misconfigured Aps	NetStumbler, Kismet, Wellenreiter, WiFiFoFum, WiFi Hopper, Win Sniffer, Wireshark and commercial WLAN protocol analyzer
Encryption/Authentication	WEP, WPA, LEAP cracking, dictionary attacks	Asleap, Aircrack-ng, coWPAtty, AirSnort, WEPCrack, WZCook and THC-LEAP cracker
Masquerade	MAC spoofing, man-in-the-middle attacks, evil twin attacks, Wi-Fi phishing attacks	Airsnarf, Ettercap Karma, Hotspotter, HostAP, SMAC
Insertion	Multicast/broadcast injection, routing cache poisoning, man-in-the middle attacks	Airpwn, WEPWedgie, chopchop, VIPPR, IRPass, CDPsniffer
Denial of Service	Layer 1 and Layer 2 Dos	Airjack, Void11, Bugtraq, IKECrack, FakeAP and RF signal generator

Wireless Security Monitoring

Wireless Intrusion Detection System/Wireless Intrusion Prevention System			
Infrastructure Component	WIPS/WIDS server	Management consoles	Sensors
Architecture Models	Overlay	Integrated	Integration enabled

WIDS/WIPS Inputs		
Multiple Radio Sensors	Sensor Placement	Device Classification
Rogue Mitigation	Device Tracking	Rogue Detection

WIDS/WIPS Analysis		
Signature Analysis	Behavioral Analysis	Protocol Analysis
Spectrum Analysis	Performance Analysis	Reports

References

- CWSP Official Study Guide
- WCN Netspec : http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0ab18336565f5b/WCN-Netspec.doc
- Building a Pentesting Lab for Wireless Network by Vyacheslav Fadyushin, Andrey Popov

Q&A

Dziękuję