Guardians of the Connected World

NETSCOUT

Securing Wireless LAN's.

DO YOU KNOW WHAT YOU DON'T KNOW?

SKIP BAYRO, CISSP, CRISC, CCSE, NSA, CNA
Chief Solutions Architect
NETSCOUT® INC.

Objectives

When we are finished today I hope you have gained some additional insight on:

- How to Know What You Don't Know about your Wireless LAN's
- Some of the risks Wireless LAN threats pose and how to reduce them
- Thoughts on ways to improve your Wireless LAN Cybersecurity doctrine and monitoring process(es)

The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

DO YOU KNOW WHAT YOU DON'T KNOW?

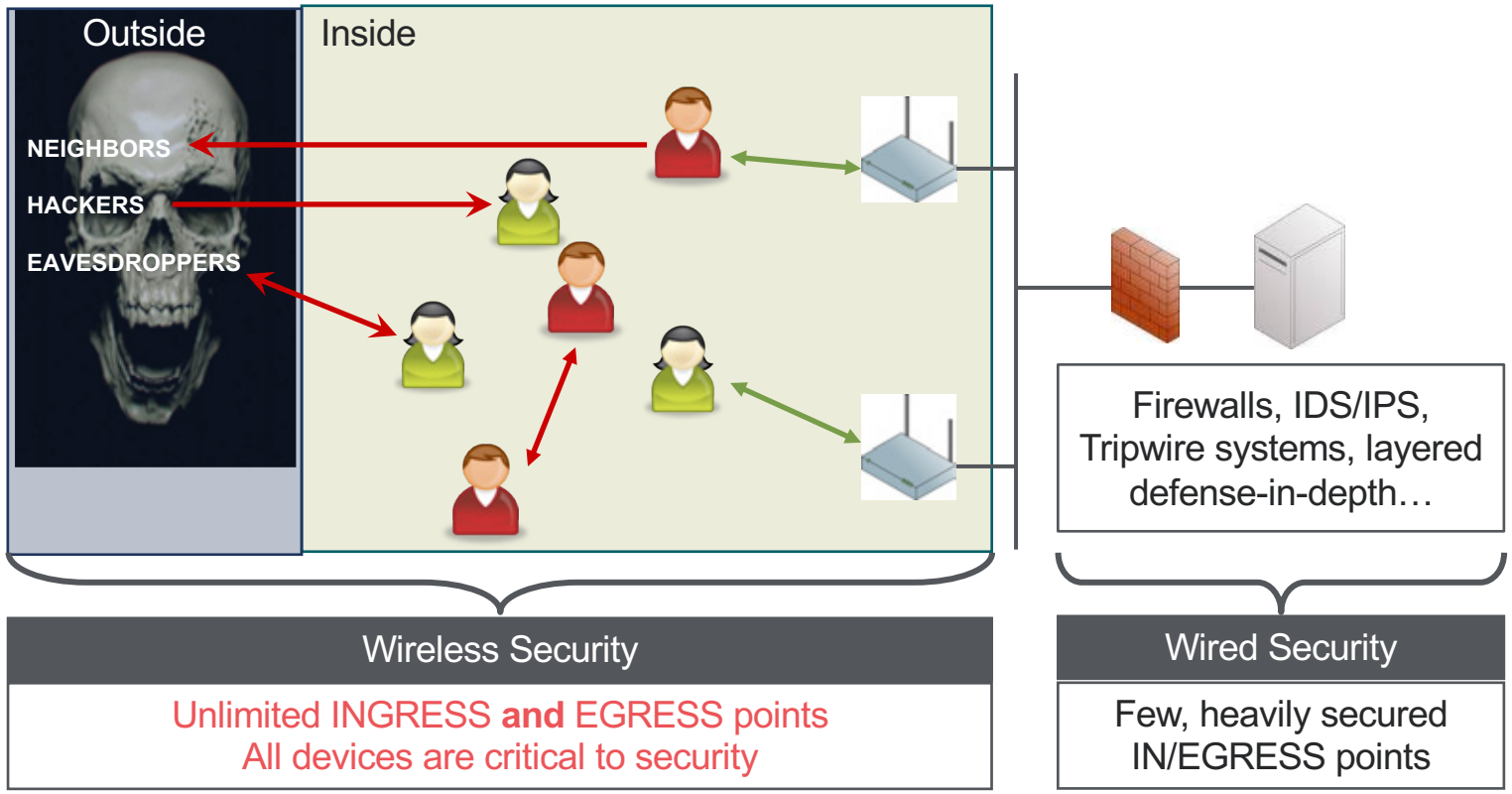
There are risks and costs to a program of action--but they are far less than the long range cost of comfortable inaction.

— John F. Kennedy

WLAN VULNERABILITIES CAN COME FROM ANYWHERE
Travel
Bandwidth consuming apps WLAN upgrades
Resources (money/people)
Surveys
Employee skill set
Policy development/implementation
Uptime/outages
Media events
Diagnosis/Misdiagnosing
Truck rolls
BYOD
Auditing
Compliance

What's Unique about WLAN Security

- Non-Wifi environments have limited external attack vectors
- Wi-Fi dramatically increases internal and external attack vectors and risk.



Wireless Threats Can Come From ANYWHERE!

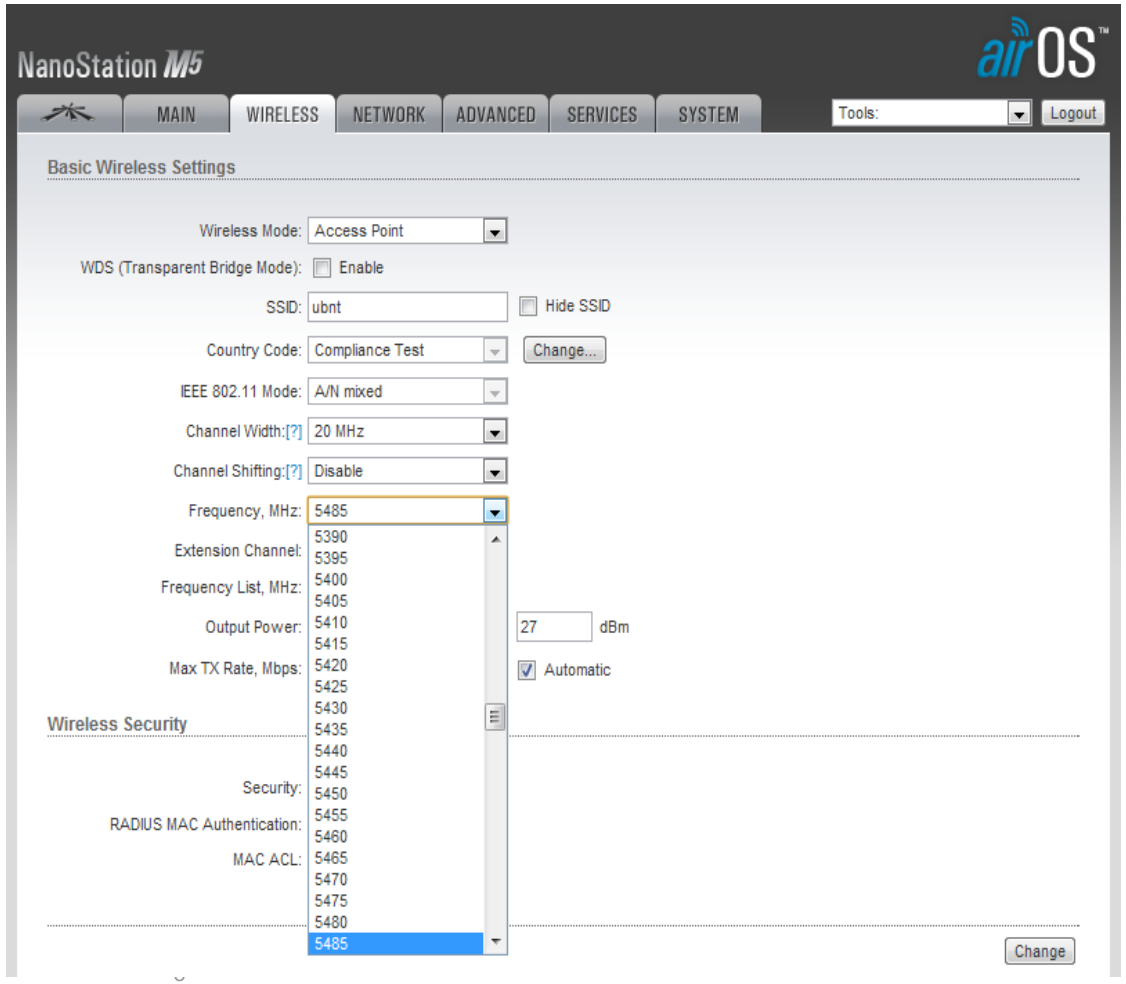
MORE CHANNELS THEN YOU THINK

- The 2.4G ISM and 5G UNII Bands have **210+** WiFi Channels available
- AP's can only channelize to the WiFi channels in their regulatory domain
- The FCC allows AP's to channelize to:
  - 11 WiFi Channels in the 2.4GHz Band
  - 25 WiFi Channels in the 5GHz Band
- This leaves over **175** Channels for an Attacker to "Hide in Plain Sight"

EXTENDED CHANNELS IN THE 5GHz Band

- AP's cannot channelize to extended channels as they must comply with regulatory domain standards
- Using an Access Point for scanning allows for "Hiding in Plain Sight" vulnerabilities as this Rogue AP would go undetected.
- It's not enough to detect rogues WIPS/WIDS must also, capture all characteristics, trace, block, etc. of devices using extended channels.

Ubiquiti airOS and dd-wrt support setting APs on any channel



EXTENDED CHANNELS IN THE 5GHz BAND

- Example of detection of two extended channel APs

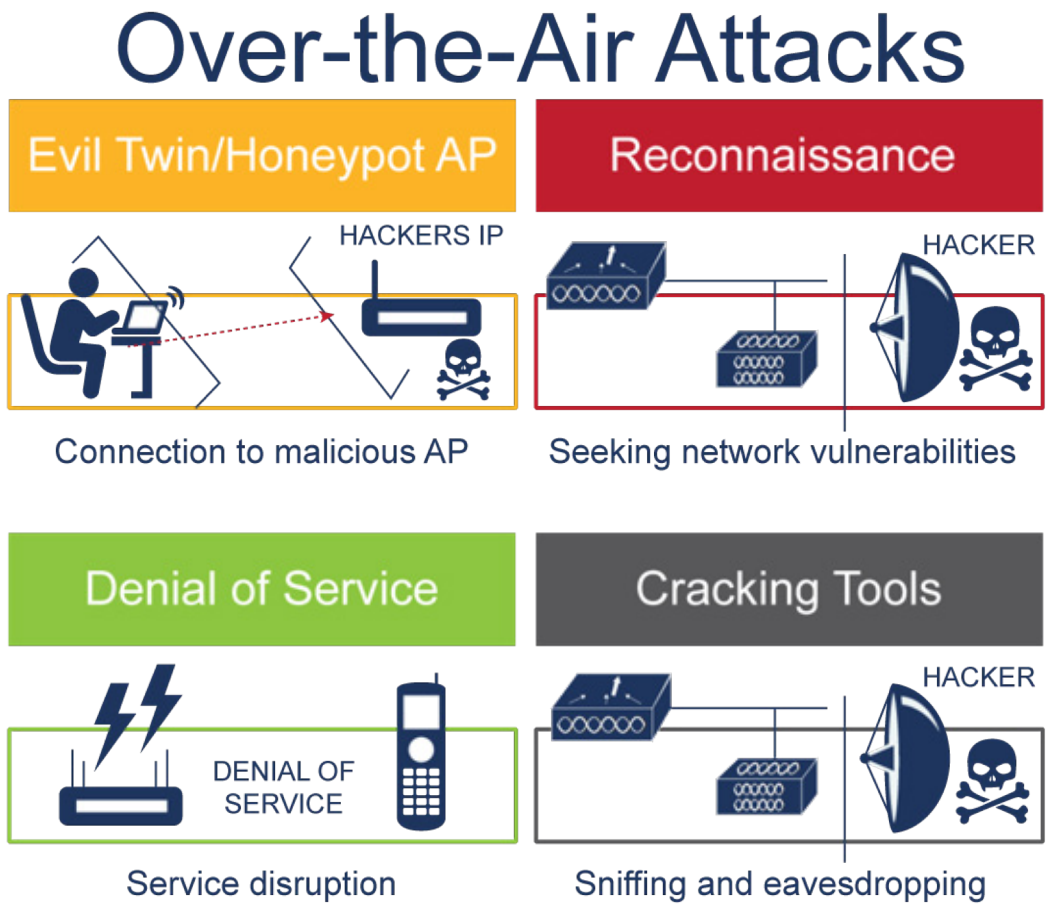
Display Name (170)	ACL	VIP	C	.11	S	SSID	Security	Ow
Intel:5F:F5:52	OK		44	g	-69	DanaherTM	WPA2-E	
Cisco1131-QA	OK		48	a	-58	QACiscoVoice	Open	
lap-baya-1-3	OK		48	n	-92	AuthorizedGuest,...	WPA2-E,Op...	
QA-1200-7	U		48	a	-48	1231-calibration	WPA2-P	
Xirrus:09:EE:E0	U		48	a	-61	xirrus-a	WPA2-P	
KAM-3502i	U		52	n	-75	ahc-ent, ahc-ope...	WEP,WEP,...	
Cisco:E6:36:6F	OK		52	n	-40	air-tek-01, air-te...	WPA2-P,WP...	
Cisco:D2:37:CE	OK		52	n	-71	AuthorizedGuest,...	WPA2-E,Op...	
lap-baya-1-4	OK		52	n	-82	AuthorizedGuest,...	Open,WPA2...	
Cisco-1130	OK		52	a	-39	1130-a	WPA2-P	
Xirrus:09:EE:C0	U		56	a	-54	xirrus-a	WPA2-P	
AIR-CAP3502-2	OK		60	a	-80	air-tek-01, air-te...	WPA2-E,WP...	
Cisco:66:EC:BD	OK		60	n	-57	AuthorizedGuest,...	WPA2-E,WP...	
Cisco1242-engla	U		64	a	-81	QACiscoVoice	Open	
lap-baya-1-5	OK		64	n	-85	AuthorizedGuest,...	WPA2-E,WP...	
Xirrus:09:EE:80	N		64	a	-57	xirrus-a	WPA2-P	
Ubiquiti:F4:F1:E3	U		97	a	-24	ubnt	Open	
Senao:74:AC:73	U		99	a	-28	dd-wrt	Open	
Cisco:9F:74:F0	OK		100	n	-46	eatest	WPA2-P	

Common Wireless Attacks

Spoofed Attacks
WPA Cracking
Flooding
WEP Attack
Asleap
Brute force hidden SSID
Karma
Kismet
Mdk3
Wifitap
SSL Strip
Evil Twin
Virtual Carrier sense
MitM
Reaver
Rogue AP
netstumbler
Honeypot
Fuzzing
AirPWN
Wifi Pineapple
Deauthentication
Scapy
Aircrack-ng
FruityWifi
Hostapd-wpe

Many Types of Attacks & Attack Tools

- Evil Twin/Honeypot
- DOS Attack
- crack.sh
- Virtual Carrier DoS



Many Types of Attacks & Attack Tools

- Rogue AP
- Misconfigured Access Point
- Rogue Client
- Client Mis-assoctiation

Implement a Multi-Dimensional Proactive Scanning / Tracing Policy

Get The Right Tools to Enable Your Team(s) Success!

WIFI HACKING DEVICES

Smaller, More Capable

- Fully functional portable hacking devices
- Attack landscape has changed
- These devices can be hidden or placed virtually anywhere
- Extremely Stealthy

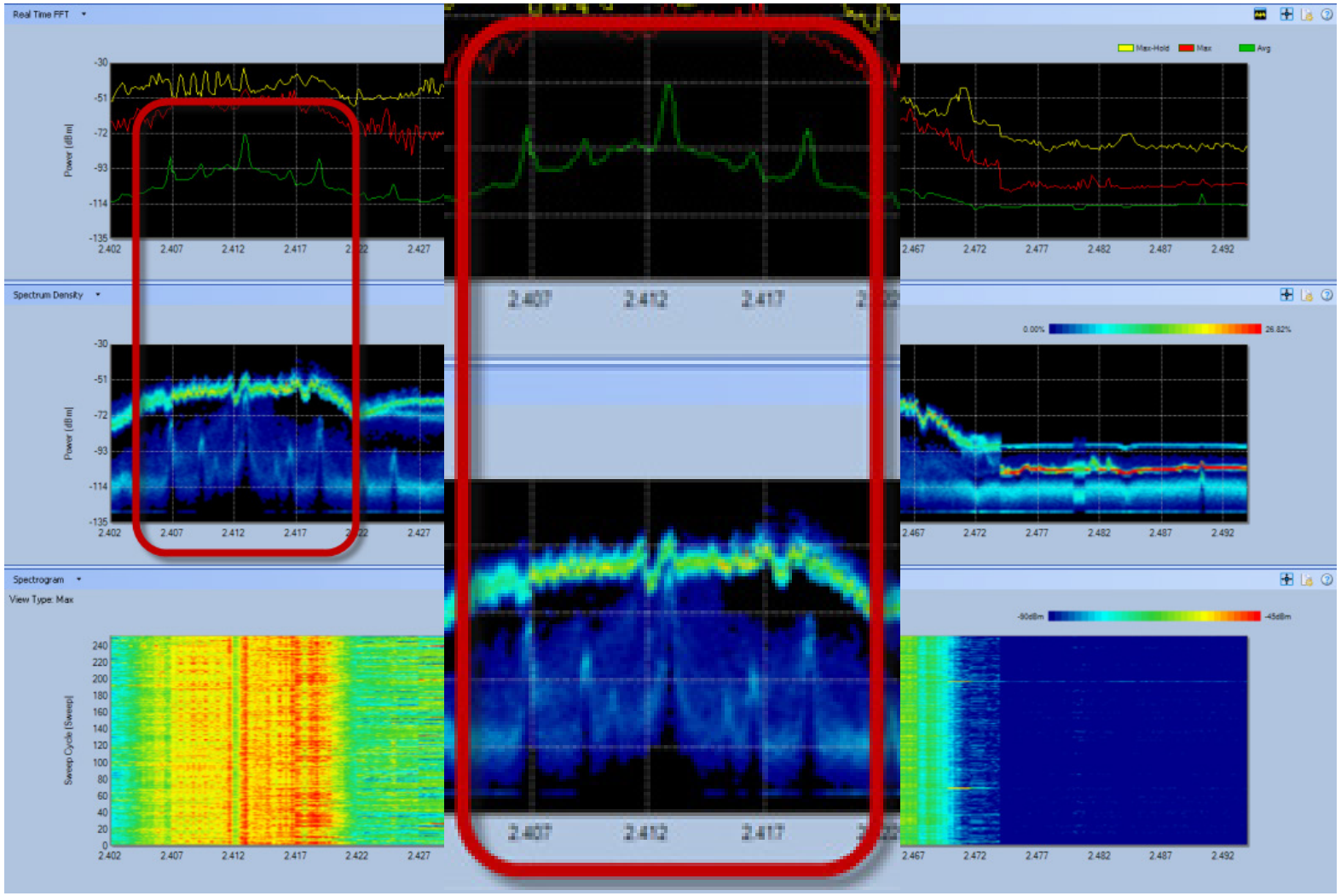
FruityWiFi
Wireless Network Auditing Tool
WWW.FRUITYWIFI.COM

IT’S NOT JUST ABOUT ROGUE AP’S

USING GOOGLE GLASS TO SNATCH PASSWORDS

An application that videos victims tapping passwords into touchscreens and analyzes it to steal the passwords with 90% accuracy from three meters. Applicable with Google Glass, Researchers Xinwen Fu and Qinggang Yue of UMass Lowell and Zhen Ling of Southeast University track the movement of the fingertip and use its position to recognize the input taking shadows, optical flow and other factors into account. Passwords can be stolen even if the person behind the camera can’t read the victim’s screen with the naked eye.

Cool looking clock ISN’T it?



HOW “cool” is it NOW?

802.11 Wireless
Desk Clock
“SPY Cam”

This tiny wireless camera inside the clock above the “12”

2.4 GHz Wireless Receiver

This device (and others like it) were discovered in the executive offices of a financial services company

WRONG! WPA/802.1X EAP-PEAP IS 100% SECURE.

Copyright © and ownership of the Image and likeness of Actor Rowan Atkinson (AKA Mr. Bean) belongs to Mr. Atkinson

ANATOMY OF AN 802.1x HONEYPOT CRACK

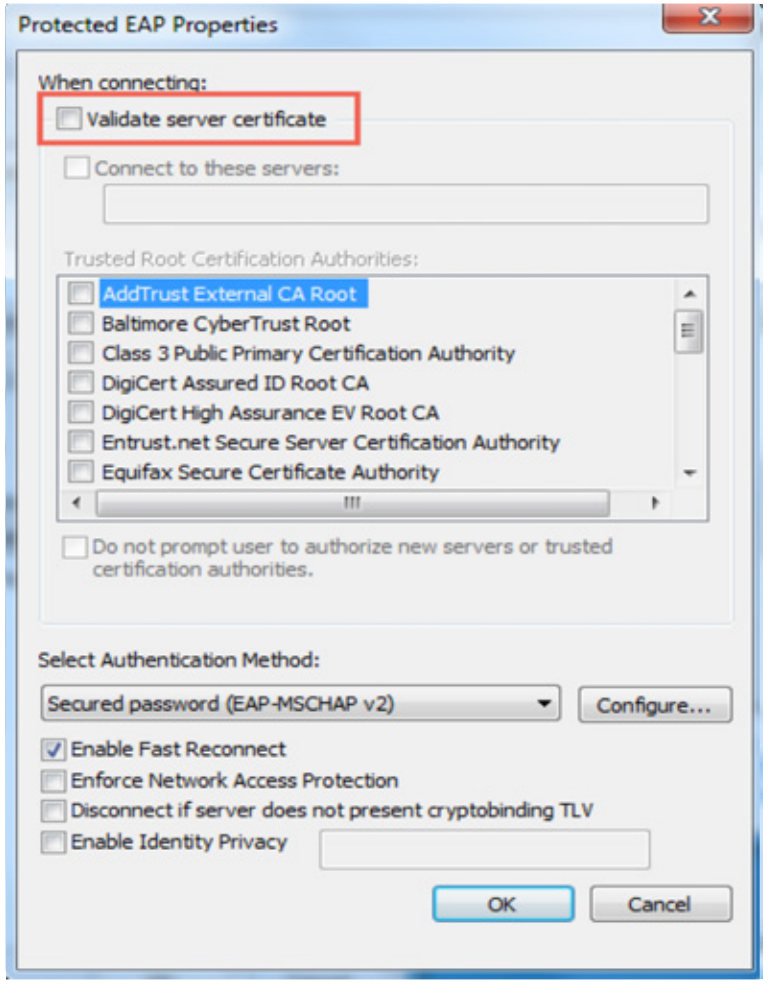
- **crack.sh** (https://crack.sh) formerly **CloudCracker** (created by Moxie Marlinspike)
- Credential Cracking Service guaranteed to crack a MSCHAPv2 challenge and response, DES, PPTP VPN, NTLM, (and more) in 26 hours or less for variable (cheap) fee depending on crack desired.
- Used to take days to exhaust the DES key space, now hours

+

Behind **crack.sh** is a system with 48 Xilinx Virtex-6 LX240T FPGAs. At 16,000,000,000 keys/sec per FPGA this equates to:

768 Trillion Keys/sec

ALL IS NOT LOST!



⑥

You are only vulnerable if your clients are not validating certificates

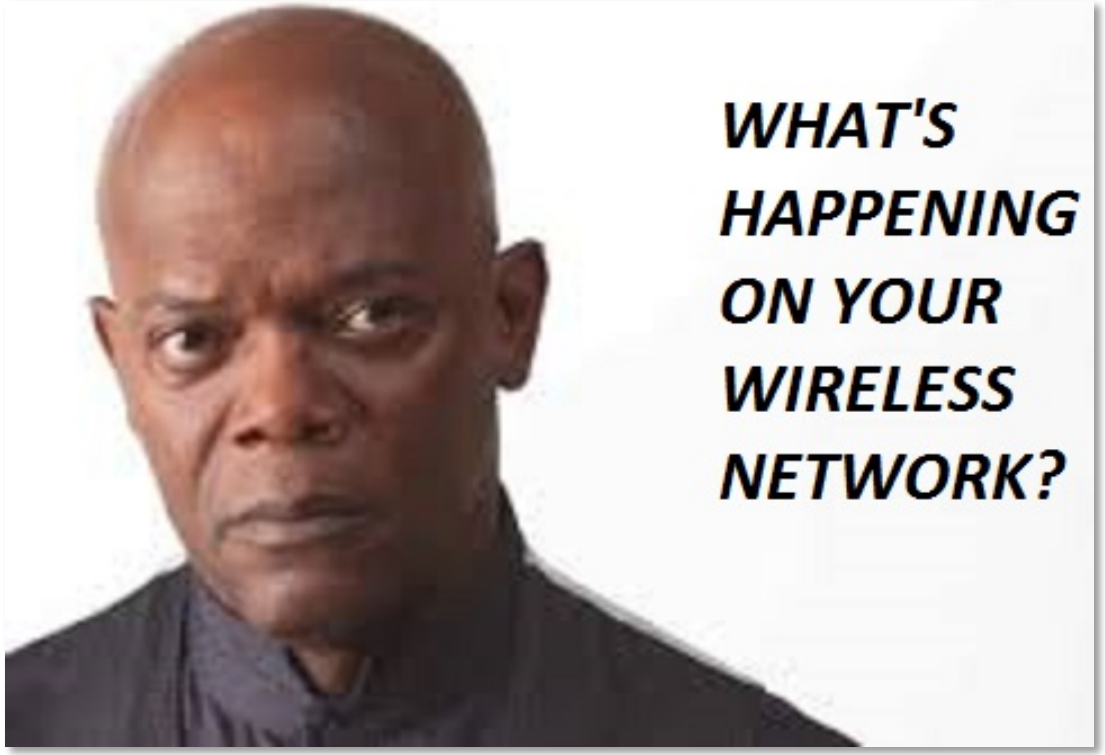
PROACTIVE WIRELESS LAN SECURITY

“You need to be lucky all the time. We only need to be lucky once!”

— Message from The IRA to Prime Minister Margaret Thatcher after a failed assassination attempt.

RAPID DETECTION IS THE NEW PREVENTION

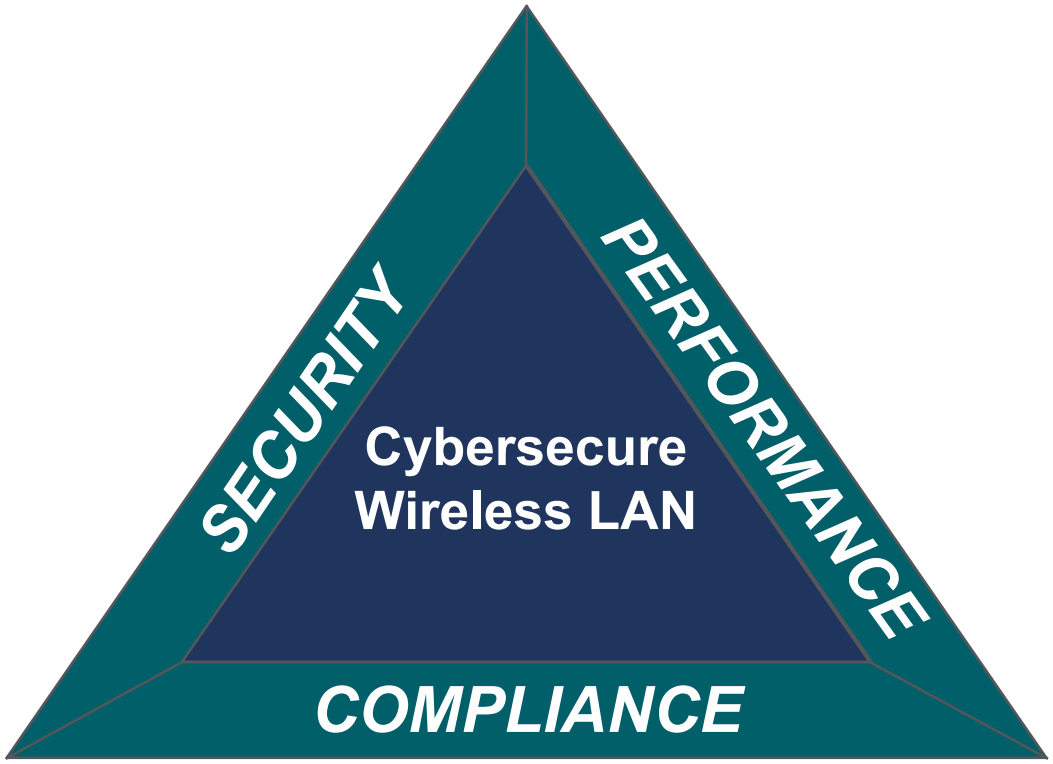
- Wireless (RF) allows **Unlimited** Ingress Points
- WIPS **AND** WIDS is required
- **Complete** Wireless LAN and RF visibility is Critical
- Deep Packet Inspection is key to rapid anomalous protocol attack detection



Copyright © and ownership of the Image and likeness of Actor Samuel L Jackson belongs to Mr. Jackson

Wireless LAN Security Triangle

- Similar to the “Fire Triangle” a “Cybersecure” wireless network must address three distinct areas or it is at risk of compromise or failure
  - Security
  - Performance
  - Compliance



What is Wireless LAN Cybersecurity?

- The unremitting monitoring, protection and defense of the “Airspace” and wireless devices in use within wireless network
- Ensuring and Validating Wireless LAN Performance and Availability
- Providing for Confidentiality, Integrity and Availability of data within and transiting the WLAN “Cloud”
- Ensuring non-repudiation of wireless endpoints within the WLAN “Cloud Perimeter”
- Validation that requisite FIPS, and other National Security Compliance standards are met.

MONITORING PART-TIME VS DEDICATED OVERLAY

SEPERATION OF DUTIES & RESPONSIBILITIES

- AP Integrated Solution can be a single point of failure & DoS Vulnerability

- Dedicated Overlay, provides reliable & low impact Wireless LAN Cybersecurity monitoring

TWO BASIC TYPES OF WLAN CYPERSECURITY DOCTRINE

LOCKING THE DOOR!

CCT/TACP Controllers and PJ's are thorough, relentless and never quit! Think like them!

Know your adversaries and ensure that your Wireless LAN Cybersecurity protection doctrine is up to the task. Ensure they:

- Monitor/Scan the **entire** UNII and ISM airspace 24x7x365
- Provide **complete** visibility of all wireless devices
- Detect and prevent hundreds of possible intrusions through distributed, purpose built WIDS/WIPS sensors (SoD&R)
- Have Dynamic Threat Updates capability for rapid detection of all WLAN threats and exploits
- Automatically capture DPI forensics to isolate and remediate attacks.
- Include remote troubleshooting and forensic analysis tools to:
  - Strategically and Tactically remediate WLAN Security, Performance and Compliance issues
- Employ with a wide range of customizable reports such as ongoing Security Posture, network health checks, and compliance checks to name a few
- Keep up to date on exploits and vulnerabilities
  - US-CERT, CVE, BH/DefCON, etc…

KEEP
CALM
AND
ASK
QUESTIONS
www.keep-calm.net

THANK YOU !

skip@netscout.com