**RSA**Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: TECH-R02

#### CHANGE

Challenge today's security thinking

### Six Things Security Professionals Need to Know About Wireless

#### Dr. Avril Salter, CCNP-W, CCNA-S

Chief Wireless Architect Salter & Associates @avrilsalterUSA



### What we are going to discuss

New wireless mechanisms



Implication to analyzing wireless traffic and network security

Illustrations are Wi-Fi



Concepts apply to Wi-Fi and mobile networks

 Wi-Fi operates in licenseexempt spectrum
 Mobile networks operates in licensed spectrum Regulations and laws on spectrum usage differ

#### **Protocol and spectrum analyzers**

#### **Protocol analyzer**

AirPcap USB wireless capture adapter nr. 00 - Wireshark					×	
Eile Edit View Go Capture Analyze Statistics Telephony Iools Help						
≝ ₩ & # ₩   = ,, x 2 =   0, + + + 7 ±   = =   0, 0, 0, 1   ₩ 1 5, %   12						
Filter:      Expression Clear Apply						
802.11 Channel: 5180 [A 36]  Channel Offset: 0 FCS Filter: All Frames Wireshark Wireless Settings Decryption Keys						
Info	New Column	New Column	New Column	New Column		
Beacon frame, SN=746, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	57 dB	5180 [A 36]		
Beacon frame, SN=747, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	57 dB	5180 [A 36]		
Beacon frame, SN=748, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	58 dB	5180 [A 36]		
Beacon frame, SN=749, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	58 dB	5180 [A 36]		
Beacon frame, SN=750, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	57 dB	5180 [A 36]		
Beacon frame, SN=751, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	57 dB	5180 [A 36]		
Beacon frame, SN=752, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	58 dB	5180 [A 36]		
Beacon frame, SN=753, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	58 dB	5180 [A 36]		
Beacon frame, SN=754, FN=0, Flags=C, BI=100, SSID="Ocean5"	Ocean5	6.0	58 dB	5180 [A 36]		
Data, SN=755, FN=0, Flags=.pF.C		6.0	58 dB	5180 [A 36]		
A DE LA COMPANY A DE LA CARD CARD "ALLAS"	· · · · · · · · · · · · · · · · · · ·	~ ~	no de	F100 F+ 363		
B Frame 132: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) B Radiotap Header VO, Length 26 B EEE 802.1 Data, Flags: .pF.C B Data (48 bytes)						
000         00         01         10         6f         18         00         01         195         03         78         00         0	X B S7} K@ J1. R# Z.				_	
File: "C:\Users\Avril\AppData\Local\Temp\ Packets: 76100 Displayed: 76100 Marked: 0 Dropped: 0			Profile: Default			

#### **Spectrum Analyzer**



**RSA**Conference2015

#RSAC

#### Why you need both

#### **Packet Analyzer**

- Need to know what is on the network
  - To see what exactly is going on with the network at a protocol level
  - Inappropriate use of bandwidth
  - Find potential intruders

#### **Spectrum Analyzer**

- Need to know what is using the physical medium
  - To see what is exactly going on with the network at the physical layer
  - Find interference
  - Find potential rogue devices

# **Tools for analyzing traffic over-the-air**



# **Transition to MIMO**

Mechanism	Performance advantage
Spatial Multiplexing	Higher data rates
Space Time Coding	Improves SNR
	- Coverage
Beamforming	Extends the range where
	higher data rates can be attained
Multi User-MIMO	Increases throughput



# **Defining MIMO**



= n x m MIMO

#### **Spatial Multiplexing**

#### 2x2 MIMO





# Implications to security professionals



# How many receiving antennas do you have?

**#RSAC** 

# **Defining beamforming**



Source: http://people.rit.edu/andpph/photofile-c/splash-water-waves-4565.jpg

**RSA**Conference2015

#### **Creating radiation patterns**

![](_page_10_Figure_1.jpeg)

**RSA**Conference2015

### **Antenna reciprocity**

# It is common practice to describe antenna characteristics from the perspective of the transmitter

![](_page_11_Picture_2.jpeg)

#### **Multi-User MIMO**

If subscribers are spatially separated

- Create two beams using the same channel
- Increases capacity

# Users can hear their signal, can you!

![](_page_12_Figure_5.jpeg)

# Implications to security professionals

- Over-the-air captures are significantly more complex
  - Arguably wireless is more secure
    - Hackers would need techniques that minimize use of MU-MIMO
      - E.g. Disruptive interference
- Spectrum and packet captures shift to the network
  - Access Point (AP) / Base Station (BS)

#### **Transition to cloud computing**

#### **Cloud managed WLANs**

- Eliminates specialized equipment
- Configure and manage thru a browser interface

![](_page_14_Figure_4.jpeg)

#### **Cloud radio access networks**

- Virtualization of the base station
  - Enables new deployment scenarios
  - Benefits of the data center realized at the network edge
    - Shared resources
    - Leverage general purpose processors
  - Moves content and applications closer to the end user

### **Cloud Radio Access Network (C-RAN)**

![](_page_15_Figure_1.jpeg)

Server platform General Purpose Processors

![](_page_15_Figure_3.jpeg)

# Six things you need to know

- You need both a packet and a spectrum analyzer
- You need to know how many receiving antennas you have
- Beamforming is happening, and will impact your ability to eavesdrop
- MU-MIMO enables multiple transmissions in the same frequency channel
  - Making eavesdropping over-the-air extremely difficult
- Wireless networks are transitioning to a cloud / virtualization based architecture
- Wireless spectrum and packet traffic analysis on the wireless AP/BS is of increasing importance

#### #RSAC

#### What you should do now

- Get and become familiar with using spectrum and packet analyzers
- Understand the limitations of the antenna technologies you are using for analyzing over-the-air traffic
- Check to see if your organization is implementing wireless cloud based solutions

# Thank you for listening ©

![](_page_18_Picture_1.jpeg)

#### www.linkedin.com/in/avrilsalter @avrilsalterUSA

![](_page_18_Picture_3.jpeg)