PHY Layer Attacks and Tools in the Cyber-EW Domain

Sean Wallace
swallace@spectrumdefender.com

Ellen Byington
ellen.byington@acquiredata.com

March 2016

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Overview

- Cyber - EW Culture Gap Creates Weakness
- Vectors For Exploits
- Emergent Tools For Exploit & Defense

Same Stuff, Different Tools

Cyber Warfare

Frames, Packets & Bytes

Methods:

- Barrages with Packets
- Send Malformed Bytes
- Deceptive Packets
- Packet Snooping

Electronic Warfare

EM Waves, Volts & Electrons

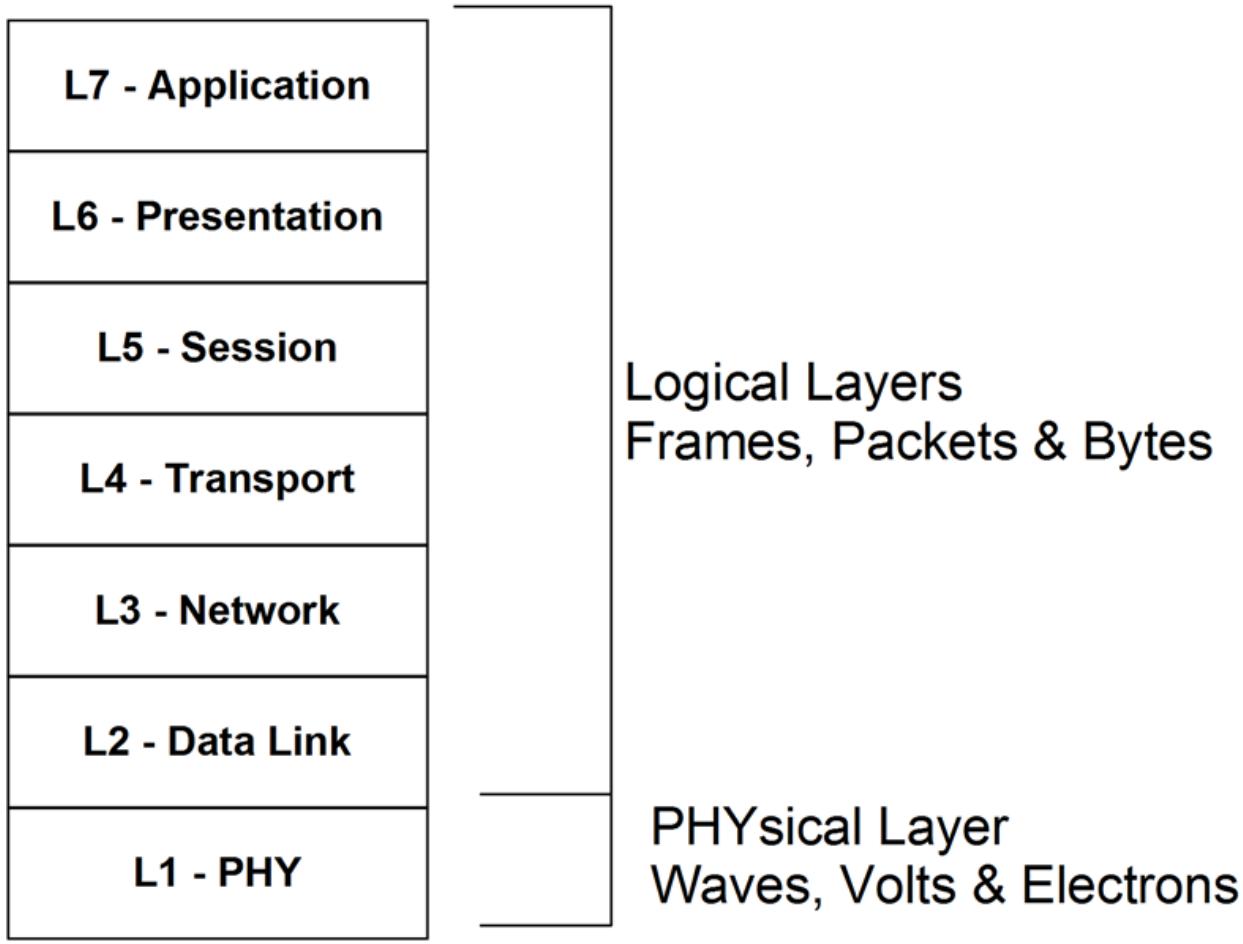
Methods:

- Barrage with RF Power
- Transmit Malformed Signals
- Deceptive Radar Reflections
- EM Emission Sensing

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

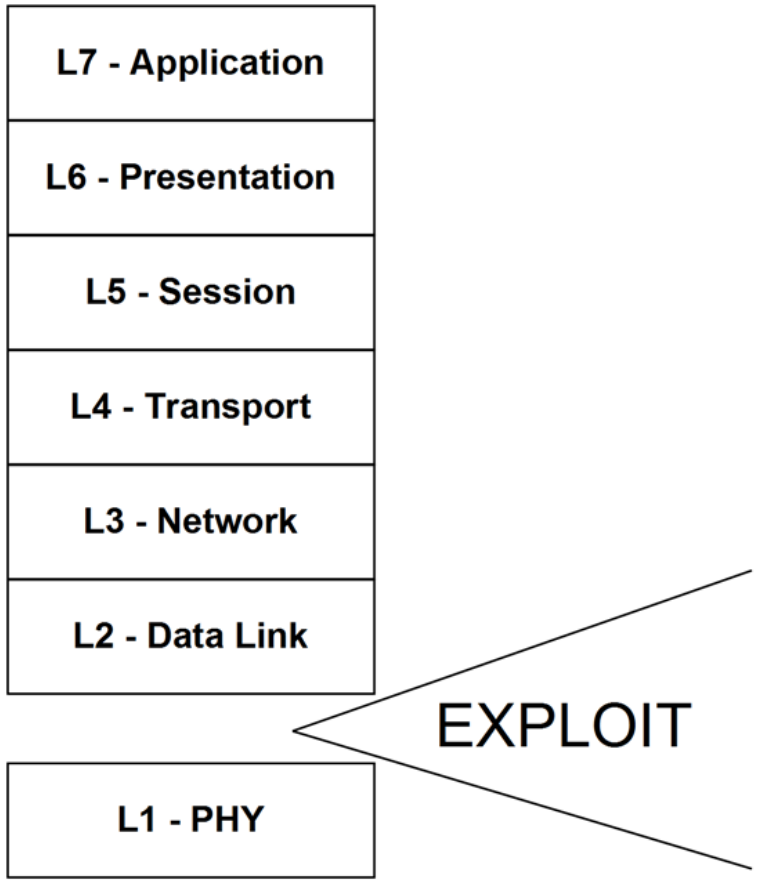
Ooops! Whole Stack Rests on EW…



ACQUIRED DATA SOLUTIONS

Spectrum Defender™

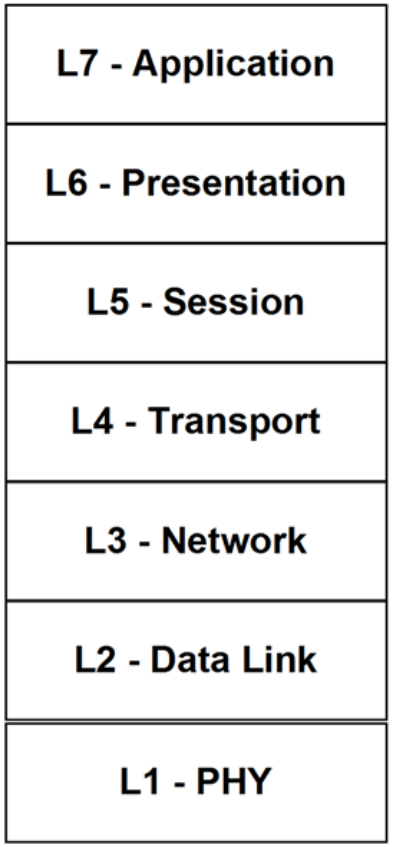
Weakness/Opportunity:
Wedge Exploit into this Knowledge Gap

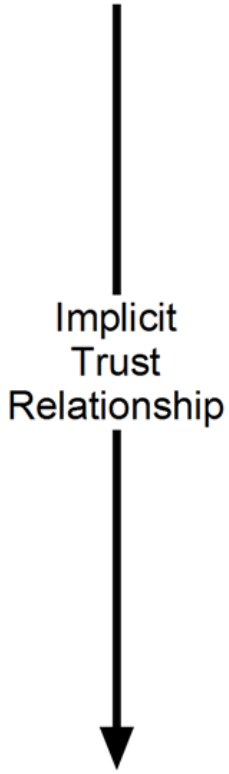


ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Weakness/Opportunity: Implicit Trust





Exception That Proves The Rul

x.509 Identity Certificates &
Public Key Crypto

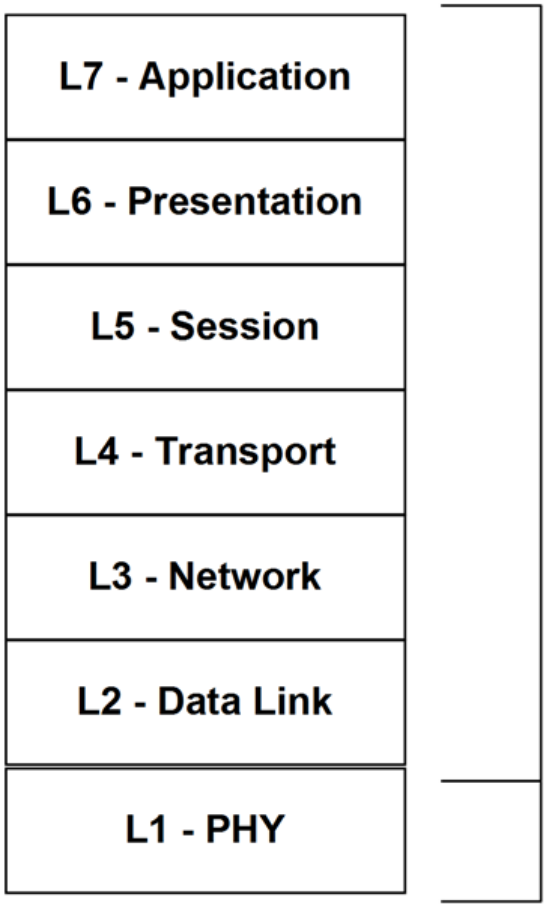
Key Takeway:

PHY is at the Root of
the Trust Hierarchy

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Weakness/Opportunity: Cyber Warrior Toolchain Gaps



Frame & Packet Capture Tools:

Wireshark
tcpdump
libpcap
Pcap libraries,etc....

Nothing, typically....

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Target Identified

TO RECAP…

- Cultural & Knowledge Gap in Community
- Root of All Trust in OSI Model
- Poorly Supported in Cyber Warrior Toolchain

Overview

- Cyber - EW Culture Gap Creates Weakness
- Vectors For Exploits
- Emergent Tools For Exploit & Defense

Which PHY Should We Exploit?

- Copper ETHernet
- Optical ETHernet
- Network Interface Card (NIC's)
- Carrier Circuits
- Wireless Interfaces (various)
  - Stealth & subtlety possible
  - Easier proximity requirements

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Malicious Behavior Examples

- **A**vailability Attacks (Denial of Service)
  - RF Jamming – Broadband denial
  - RF Jamming – Selective SSID denial
  - RF Jamming – Selective frequency band denial
  - Forced disconnect – de-auth msgs
  - Exploit WiFi chipset vulnerabilities at PHY layer (e.g. malformed RF)

Malicious Behavior Examples

- **C**onfidentiality
  - Identify attack targets via RF emission signature (similar to radar signatures)
- **I**ntegrity- Man-In-The-Middle attacks
    - Selectively attack only specified clients at PHY layer
    - Prevent client from communicating with anyone except attacker (jam for everyone but self)

Is (my) Network Vulnerable?

Good Guys Think: "I am not vulnerable. I have a ***policy*** that does not allow wireless access points anywhere on the secure network"

Bad Guys Think: "I will be able to exploit this network forever without detection since the operator is in denial"

Wired to Wireless Bridges in your Network

- Laptops
- Scanners
- Printers
- Phones
- Wireless Mouse & Keyboard
- GPS NTP servers
- Satellite Receivers
- Passport Readers
- Thermostat
- Other IOT

ACQUIRED DATA SOLUTIONS

Spectrum Defender™

Laptops as a Bridge

- Abundance of Radios in Laptops
  - Many can not be disabled with a hardware switch
  - Sometimes it's hard to even enumerate all of the radios in a given laptop
  - Examples of typical radios:
    - Wi-Fi 2.4GHz
    - Wi-Fi 5GHz
    - Bluetooth
    - CDMA
    - LTE
    - RFID/NFC
    - Proprietary Wireless Mouse

Printers as a Bridge

- Many printers have Wi-Fi standard now
- Unprotected firmware flash procedures
- Embedded operating systems with ip routing possibilities (e.g. iptables)
- USB ports on front panel – printer in a common access hallway!
- Does your “No Wi-Fi” printer actually have the chip removed from the circuit board? Or is it just disabled in firmware? (see above)

Creative Malicious Behaviors

- PHY Attack via GPS-based NTP Server
  - Parking lot attack
  - Slow-down / Speed-up clocks
  - Alter clocks and interfere with scheduled tasks such as overnight backup procedures

Creative Malicious Behaviors

- Data Leakage via PHY Layer Steganography
  - WiFi PHY layer has headers with “reserved bits” that could be used for outbound data leakage
  - Completely undetectable data leakage from logical layer perspective
  - Exists in every standards compliant WiFi implementation

Creative Malicious Behaviors

- Secret Routes
  - Example 1: Printer on secure network compromised to enable WiFi and connect to public WiFi from hotel across street
  - Example 2: Smartphone and laptop pair with each other over Bluetooth. Smartphone has malware with secret bridge/routes between Bluetooth & carrier's LTE network

Overview

- Cyber - EW Culture Gap Creates Weakness
- Vectors For Exploits
- Emergent Tools For Exploit & Defense

How Can We Defend?

- NOT using Logical Layer tools such as Wireshark, tcpdump,etc…
- PHY Layer tools needed to:
  - Monitor (Compare Against Baseline)
  - Capture (Record behavior for analysis)
  - Replay (Repeatability!)
  - Attack (Initiate an attack vector)

Electronic Warfare Solutions

- Standard tools in the EW warrior's toolchain:
  - Spectrum Monitor
  - RF Recorder
  - RF Player
  - Jammer

- Cyber domain needs similar tools

ViaSat

CACI
EVER VIGILANT

NORTHROP GRUMMAN

BOSCH
Invented for life

USA
United Space Alliance

NAB
NATIONAL ASSOCIATION OF BROADCASTERS

ACQUIRED DATA
SOLUTIONS

Spectrum Defender™

Ideas for Cyber Adaptations

- Alarm on Electromagnetic (EM) Environment Change From Baseline

- Archive EM Environment during Exercises for Offline Analysis
  - Library of EM Environments
  - *Wireshark for PHY*

Ideas for Cyber Adaptations

- Launch PHY Layer Attack Vectors
  - Can't really be done with COTS NIC's
- Automated searches for unusual activity in PHY Layer headers and reserved bits
  - Stego detection
- Query EM Environment records for list of all SSID's present during exercise
  - Even for the briefest of moments….

Ideas for Cyber Adaptations

- Examine PHY Layer Activities Which are Otherwise Invisible to Traditional Logical Layer Tools

Next Steps

- Acquired Data Solutions welcomes discussions with interested partners who have ideas re. adaptations needed to move these EW tools into the Cyber domain.
  - Prioritization is key!

PHY Layer Attacks and Tools in the Cyber-EW Domain

Sean Wallace
swallace@spectrumdefender.com

Ellen Byington
ellen.byington@acquiredata.com

March 2016

ACQUIRED DATA SOLUTIONS

Spectrum Defender™