IT'S IN THE AIR(WAVES): RF SECURITY YEAR IN REVIEW

Matthew Knight
Senior Security Engineer
Cruise Automation
@embeddedsec
Who’s This Guy

- Matt Knight
- Senior Security Engineer @ cruise
- BE & BA from Dartmouth
- Background in electrical engineering, embedded software, etc.
- TumbleRF fuzzing framework
- Reverse engineered the LoRa PHY in 2016
Shoutout to **Bastille**

- My former employer!
  - Security startup specializing in wireless detection technologies
  - Enterprise product built on Software Defined Radio

- Good people who I learned a ton from
SOFTWARE DEFINED RADIO
AND WHAT IT CAN DO FOR YOU
Software Defined Radio

- Architecture with flexible wideband RF frontend
  - Captures raw radio spectrum
  - Shuttles RF I/Q samples to DSP or host

- Implement arbitrary PHYs in:
  - Software
  - FPGA HDL

Fast iteration! Flexible!
1. Evolving radio technology landscape
2. Technical radio concepts
3. RF reverse engineering workflow
4. Conclusions and key takeaways
EVOLUTION OF NETWORK SECURITY

Historical Background
Packet sniffing in the 1990s
Protocols:

802.3
802.5
$8,000+ (in 1990s dollars)

NETWORK GENERAL PACKET SNIFTER

Installed on a Dolch lunchbox computer
NETWORK GENERAL PACKET SNIFFER

$8,000+ (in 1990s dollars)

Installed on a Dolch lunchbox computer
Packet sniffing in 1998
ETHEREAL // WIRESHARK

+ Monitor mode NICs
ETHEREAL // WIRESHARK

👍

$0

COMMODITY

+ Monitor mode NICs

https://blog.wireshark.org/wp-content/uploads/2013/10/ethereal-0.2.0.png
Packet sniffing since the 2000s
Protocols:
- LoRa
- LTE-M
- GPS
- 802.5
- 802.11
- WiMax
- ENB
- DMR
- 802.3
- HSPA
- LTE
- CDMA
- GSM
- Bluetooth
- Bluetooth LE
- Z-Wave
- SIGFOX
- 802.16
- nRF24
- NB-IoT
- DECT
- 802.15.4
- GPRS
- EDGE
- DECT
- MAX
TONS OF WIRELESS
EARLY SDRS

>>$100K
Early SDRS

>>$100K

PROPRIETARY
Wireless sniffing in 2012
RTL 2832 USB STICK

(not pictured: promiscuous mode driver)
RTL 2832 USB STICK

(not pictured: promiscuous mode driver)
Wireless sniffing in 2018
$8 \rightarrow $1150

ALL THE SDRS
ALL THE SDRS

👍

$8 -> $1150

COMMODITY
Wireless in 2018

- 802.11 is just one piece of the puzzle
- There’s a PHY for every use case
  - Explosion of IoT and Mobile means embedded systems are everywhere
Embedded == Design by Compromise

- Battery powered
- Limited user interaction
- Lack of crypto
- Unsuitable network for firmware updates

- Performance, UX, cost, and delivery are more important than best practices

Literal embedded systems
Industry reliance on SECURITY THROUGH OBSCURITY means...
[PIÑATAS]
Same applies to the **LACK OF VISIBILITY** into PHY layers.
WHAT DOES IT TAKE TO HACK WIRELESS?
Interfacing with an IP network is trivial

- Commodity NICs
- Monitor mode

Known Layer 2 // MAC frame protocols

- 802.3 // Ethernet for wired IP traffic
- 802.11 // Wi-Fi for wireless IP traffic
Wireless* Network Sniffing is Hard

*non-802.11

- Network interface is totally non-trivial
  - Your Wi-Fi NIC can’t sniff wireless traffic from your home security system

- Arbitrary Layer 1 // PHYs
  - There are many ways to make a PHY
  - 802.11 // Wi-Fi is just one example

- How does one speak arbitrary RF?
SOFTWARE DEFINED RADIO
Prototype Integrated Designs

- Develop complex radio algorithms at the speed of software
- Simulate and test in hardware before committing capital to fab an IC
- Right: RTL for an 802.15.4 decoder I wrote
Surveying
Budget Spectrum Analyzer
Design Optimization

- Experimentation platform for physical layer technologies
- Most SDR logic can be run in simulation
- See GNU Radio
Offensive Security Research

- Physical layer attacks, including:
  - Sniffing
  - Jamming / denial of service
  - Selective receiver targeting / IDS evasion

- “Radio Exploitation 101” at DEF CON 25
RF Fuzzing

- TumbleRF
  - Framework for fuzzing RF protocols and fingerprinting chipsets
  - Extensible! Abstracts radio driver specific interface functions into a common API
  - Developed by yours truly and Ryan Speers from River Loop Security

- Released at Troopers 18
  - https://github.com/riverloopsec/tumblerf
Defensive Security Applications

- Real-time monitoring of the entire RF spectrum
  - Single or networked array of Software Defined Radios
  - Real-time analytics and insight
  - Not tied to a single protocol or chipset!

- Better understanding of PHY layer vulnerabilities
WHY IS SECURING RF DIFFICULT?

vs. Wired Interfaces
RF vs. Wired: Defining Attributes

RF Interface
- Promiscuity
- RF spectrum is a giant bus!

Wired Interface
- Dedicated interfaces
- Direct electrical access required
Promiscuity Makes Recon Easy

- Promiscuity makes discovering vulnerable devices easy
  - Sniffing
  - Active wardriving
  - Can be done stood off at a distance
Promiscuity and Attribution

- Promiscuity means attribution is difficult
- Is the attacker:
  - On your network
  - On a box on your network
  - In the parking lot?
  - A USPS box delivered to the CEO’s office?
TOP WIRELESS* ATTACKS OF 2017

*proprietary RF protocols and PHY layers
Dallas Tornado Siren Attack

- April 2017, Tuesday @ 1:30AM
- All 156 Tornado emergency sirens in Dallas metro area turned on
- 90 minutes to turn them off

Dallas Tornado Siren Attack

- Vector
  - RF replay attack
  - Retransmitted previously captured PHY frame
  - Sirens were tested quarterly, providing source material

- Theoretical Mitigation
  - Cryptographic authentication w/ freshness (sequence number)

Dallas Tornado Siren Attack Demo

- **Fortress Security System Panic Button**
  - Tornado Siren surrogate 😏

- 433 MHz on-off keying
  - No freshness or authentication
  - Raw IQ replay or decode/resynthesize

- Raw IQ replay demo
[DEMO]
St. Jude Pacemaker Attack

- Pacemaker vulnerabilities
  - 0-days dropped by MedSec + short seller
- RF attacks:
  - Depleting battery in implanted pacemaker
  - Authentication vulnerabilities
Wireless IoT Worms

- Traffic Light Controller Worm
  - Theorized by Cesar Cerrudo
  - Traffic flow sensors and traffic light controllers
    - No encryption
    - No authentication
    - No code signing
Wireless IoT Worms

- Phillips Hue Firmware Worm
  - Eyal Ronen, Colin O’Flynn, Adi Shamir, Achi-Or Weingargen
  - Recovered Phillips Hue firmware signing key via side-channel attack
  - Exploited ZigBee Light Link firmware OTA process to self-propagate

- Excellent paper and video
  - http://iotworm.eyalro.net/
Physical Layer State Machine Attacks

- Thesis
  - Chipset manufacturers implement complicated standards differently

- Attack
  - Send standards-noncompliant transmissions to exploit corner cases in specific PHY layer state machines

- Result
  - Targeted receiver evasion (IDS evasion)
  - Device fingerprinting
Physical Layer State Machine Attack Demo

- 802.15.4 Receiver Evasion
  - Original research by Travis Goodspeed, David Dowd, Ryan Speers, River Loop Security, and others from Dartmouth

- Transmitter:
  - TI CC2420 w/ configurable PHY state machine

- Receiver:
  - TI CC2420 w/ stock PHY configuration
  - Atmel AT86RF230
Physical Layer State Machine Attack Demo

- Standard 802.15.4 preamble and SFD:
  - 0x00000000A7: 4 0x00s + 1 0xA7

- What if we screw with this?
  - 0x00000000FFA7: extra symbols in preamble
  - 0x000000A7: short preamble
[DEMO]
CONCLUSIONS
Conclusions

- We have entered the Golden Age of RF Hacking
- SDR has been commodity for >5 years
- Every RF PHY is in scope!
Conclusions

- Next week you should:
  - Review whether your organization has IoT/BYOD device policies in place
- In the first three months following this presentation you should:
  - Consider adding non-802.11 RF vectors to your threat model

**Awareness + Visibility = Empowerment**

- Within six months you should:
  - Evaluate your organization’s posture relative to RF threats
THANKS

knight@getCRUISE.com
@embeddedsec
QUESTIONS?