GNURadio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

MATT KNIGHT // MARC NEWLIN // BASTILLE NETWORKS

RADIO EXPLOITATION 101

CHARACTERIZING//CONTEXTUALIZING//CLASSIFYING RF ATTACKS

APPLICATIONS OF SDR IN SECURITY RESEARCH

OFFENSIVE WIRELESS TECHNIQUES

PHY && MAC LAYERS

WIRELESS THREAT TAXONOMY

Abridged from

DEF CON

WHO ARE THESE GUYS

- Matt Knight
  - Software Engineer and Security Researcher @ Bastille
  - Reverse engineered the LoRa wireless protocol in 2016
  - BE & BA from Dartmouth

matt@Bastille.net
@embeddedsec

- Marc Newlin
  - Security Researcher @ Bastille
  - Discovered Mousejack vulnerability in 2016
  - Finished 3rd in DARPA Spectrum Challenge in 2012
  - Finished 2nd in DARPA Shredder Challenge in 2010

marc@Bastille.net
@marcnewlin

AGENDA

1. Historical retrospective of wired and wireless security tech development
2. Methods of Wireless Exploitation
   - Techniques, impact, and defenses
   - Analogues to wired networks
   - Examples and demos
3. How to apply this information

HISTORICAL BACKGROUND

EVOLUTION OF NETWORK SECURITY

https://frostedpress.files.wordpress.com/2016/09/4286297.png

Packet sniffing in the

1990s

Protocols:

802.3

802.5

$8,000+ (in 1990s dollars)

NETWORK GENERAL PACKET SNIFFER

Installed on a Dolch lunchbox computer

http://s202976374.onlinehome.us/ebay/test_equip/analyzers/Dolch_PAC_64_05.jpg

PROPRIETARY

$8,000+ (in 1990s dollars)

NETWORK GENERAL PACKET SNIFFER

Installed on a Dolch lunchbox computer

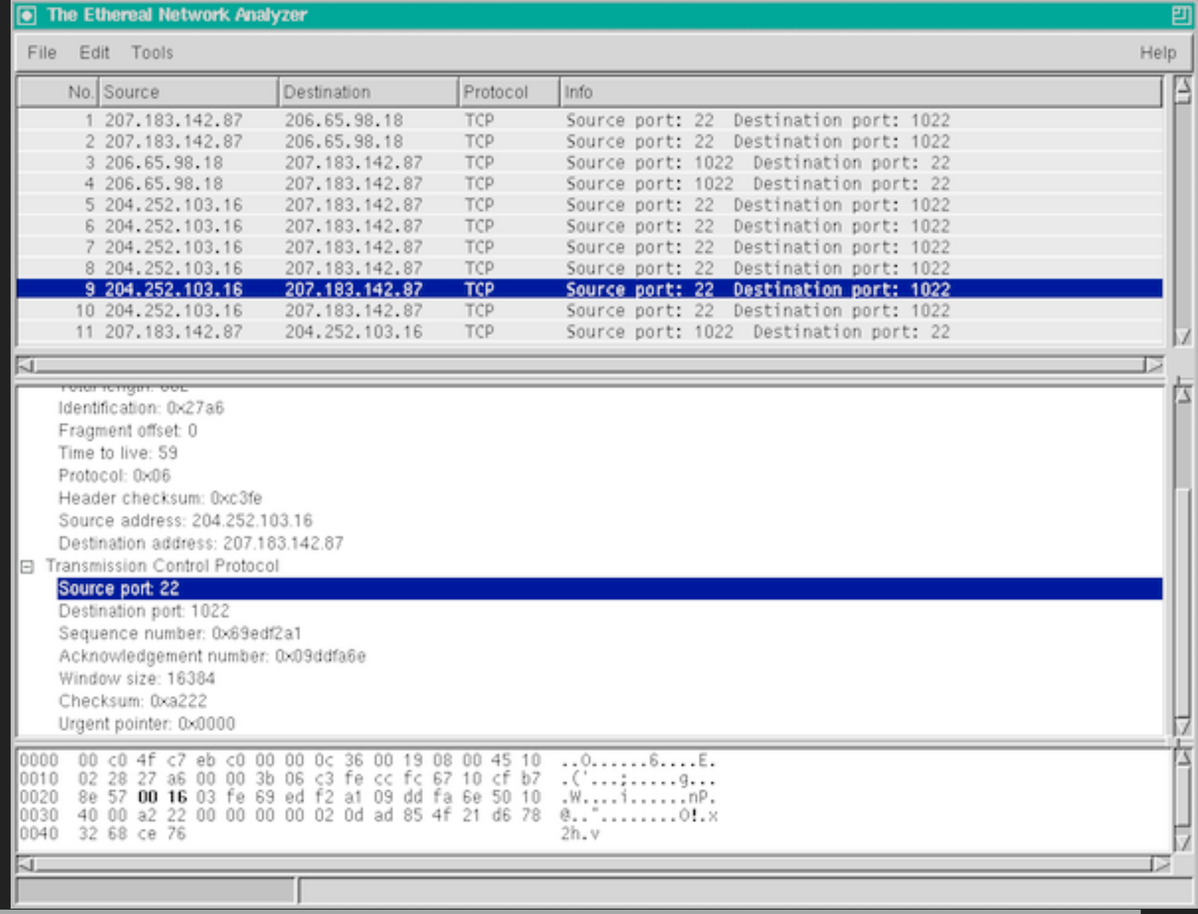
http://s202976374.onlinehome.us/ebay/test_equip/analyzers/Dolch_PAC_64_05.jpg

Packet sniffing in

1998

$0

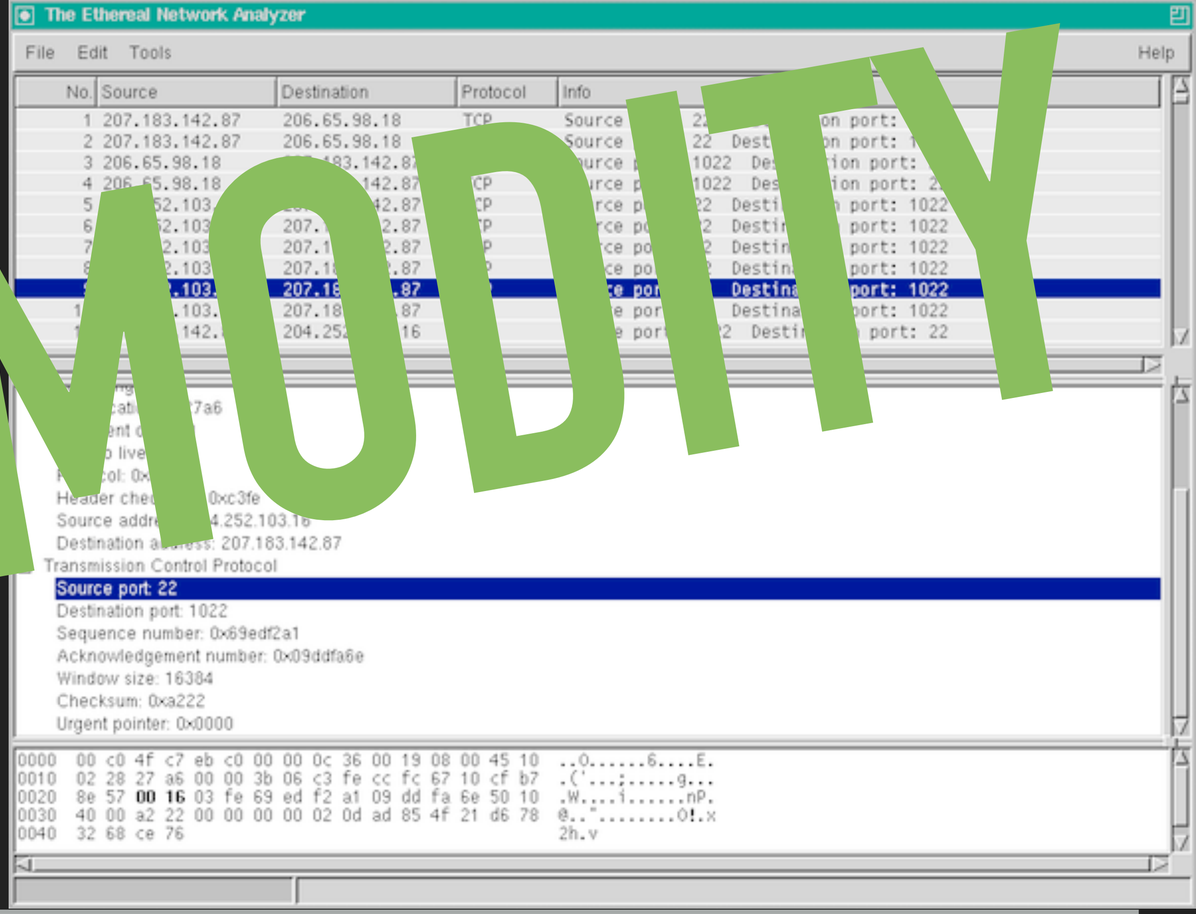
ETHEREAL // WIRESHARK



https://blog.wireshark.org/wp-content/uploads/2013/10/ethereal-0.2.0.png

$0

COMMODITY



ETHEREAL // WIRESHARK

https://blog.wireshark.org/wp-content/uploads/2013/10/ethereal-0.2.0.png

Packet sniffing since the

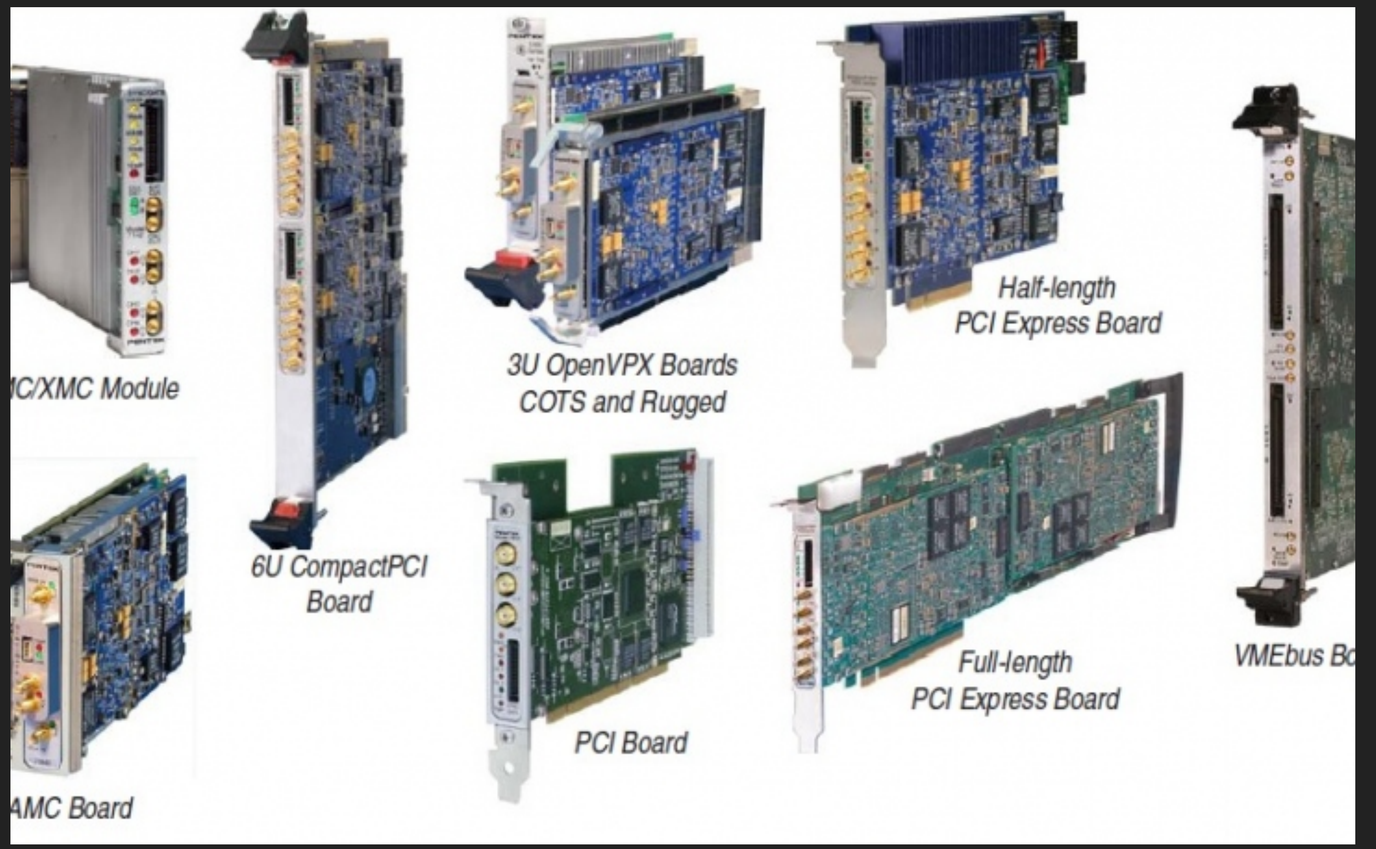
2000s


802.15.4
6LoWPAN
nRF24
Protocols:
EDGE
RSPA
GPS
DECT
Bluetooth
Z-Wave
NB-IoT
CDMA
LTE
WiMax
802.11
LoRa
GSM
Bluetooth LE
SIGFOX
802.16

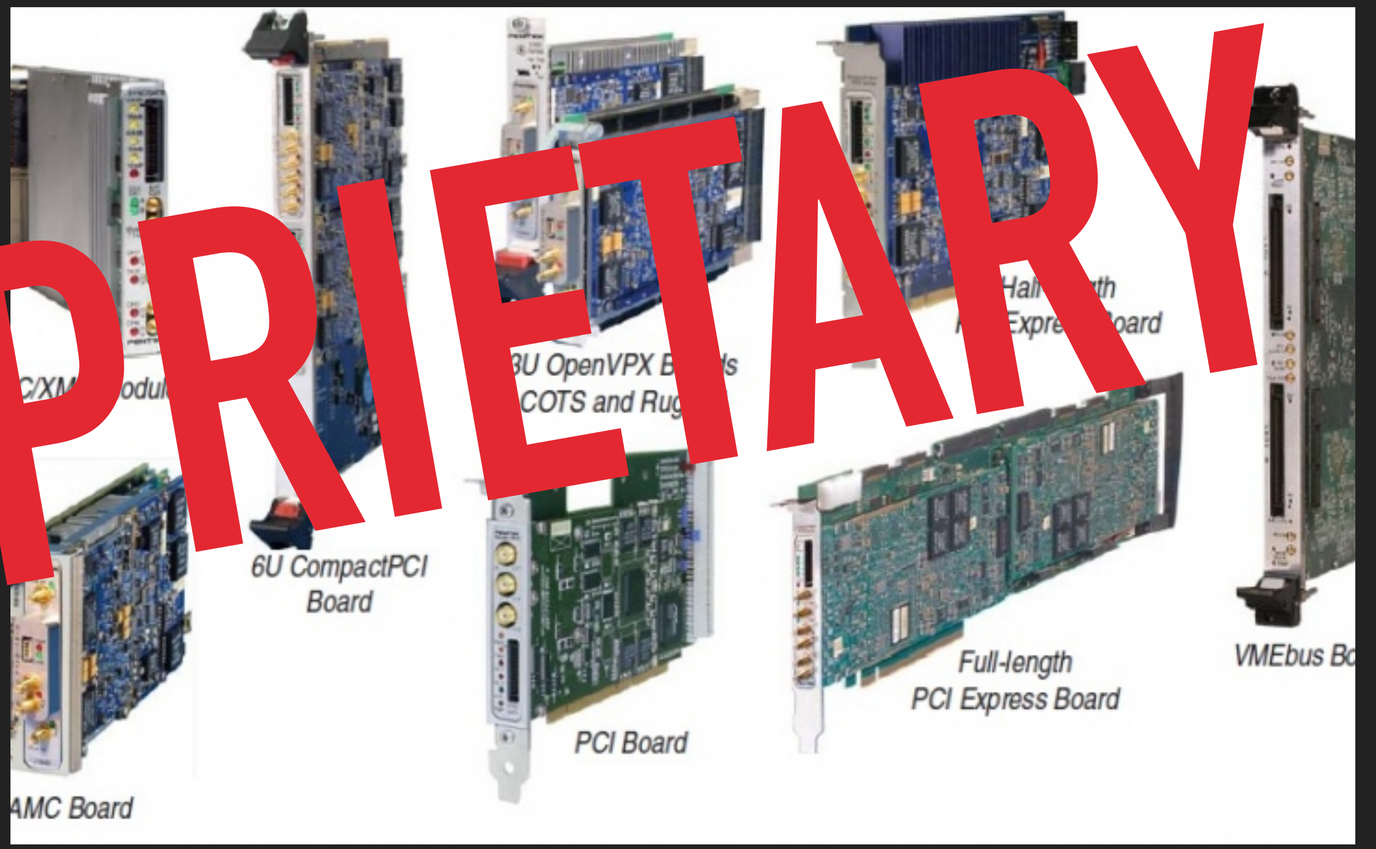
TONS OF WIRELESS

>>$100K

EARLY SDRS



PROPRIETARY

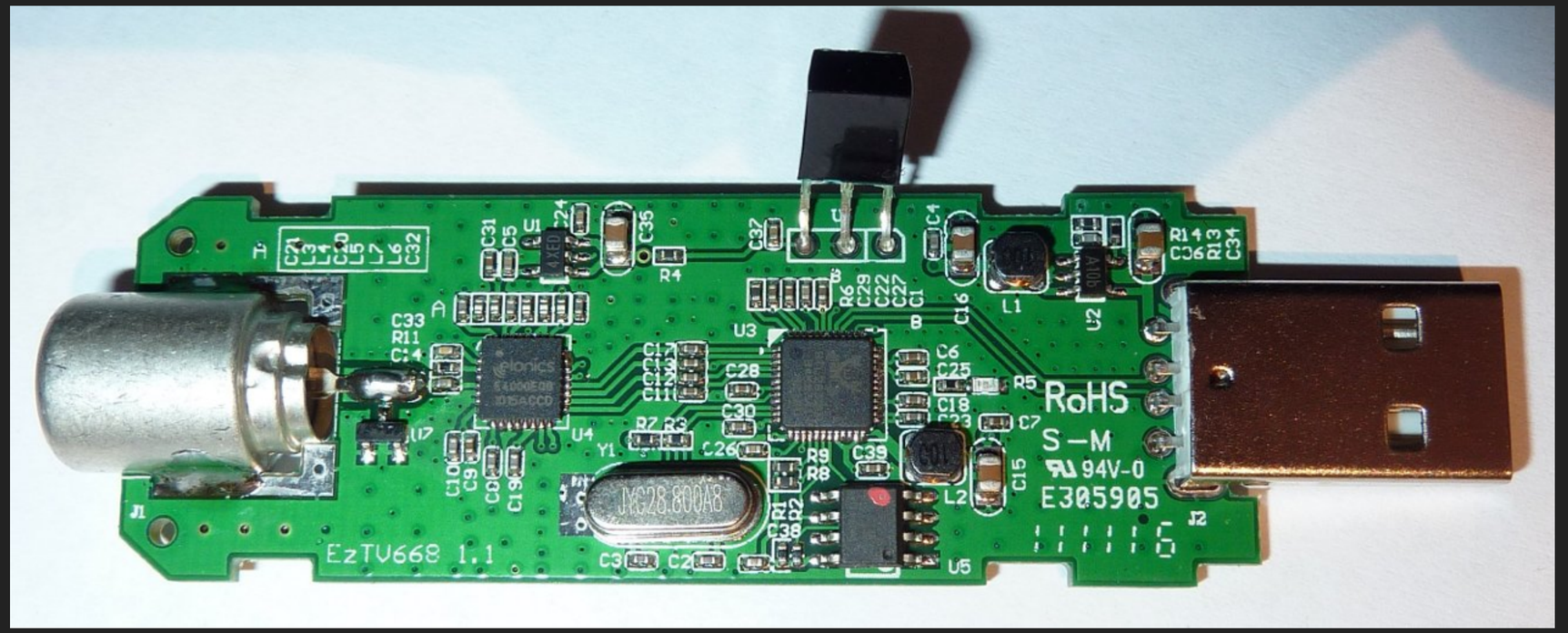


>>$100K

EARLY SDRS

Wireless sniffing in

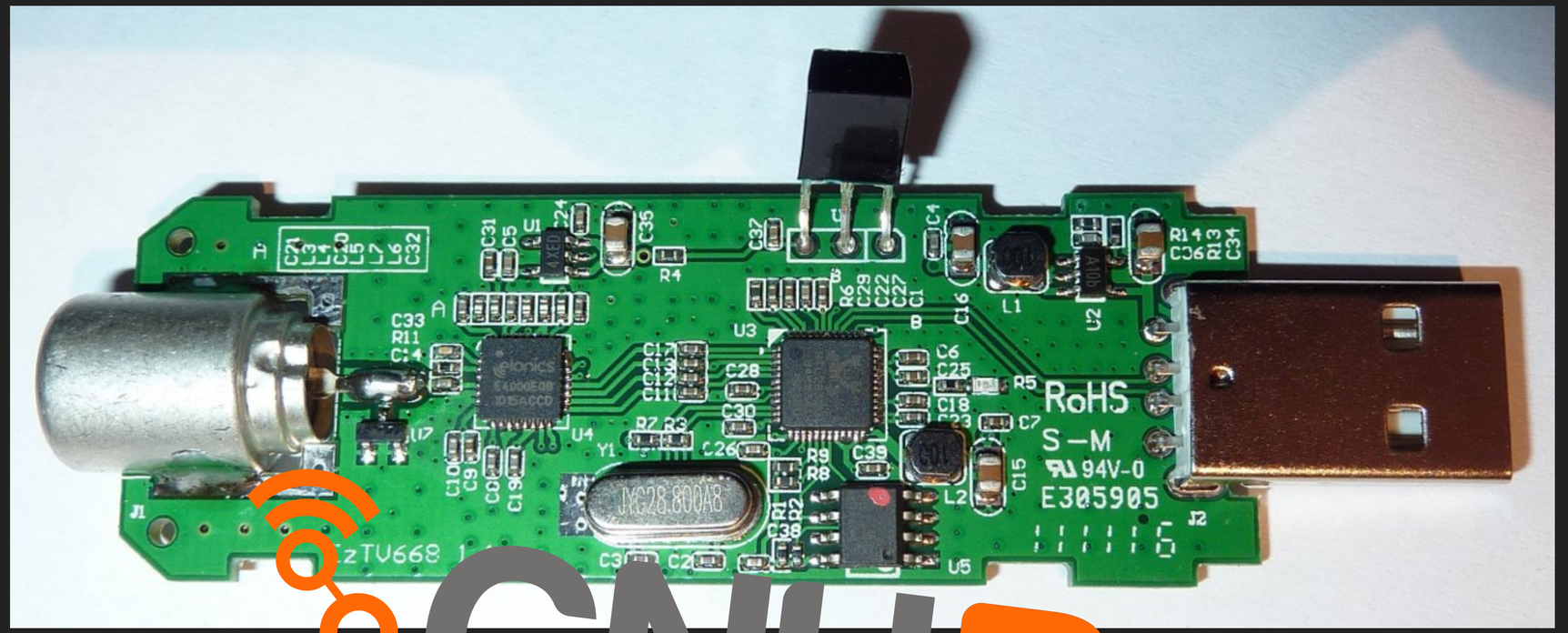
2012



$8

RTL 2832 USB STICK

(not pictured: promiscuous mode driver)



GNU Radio

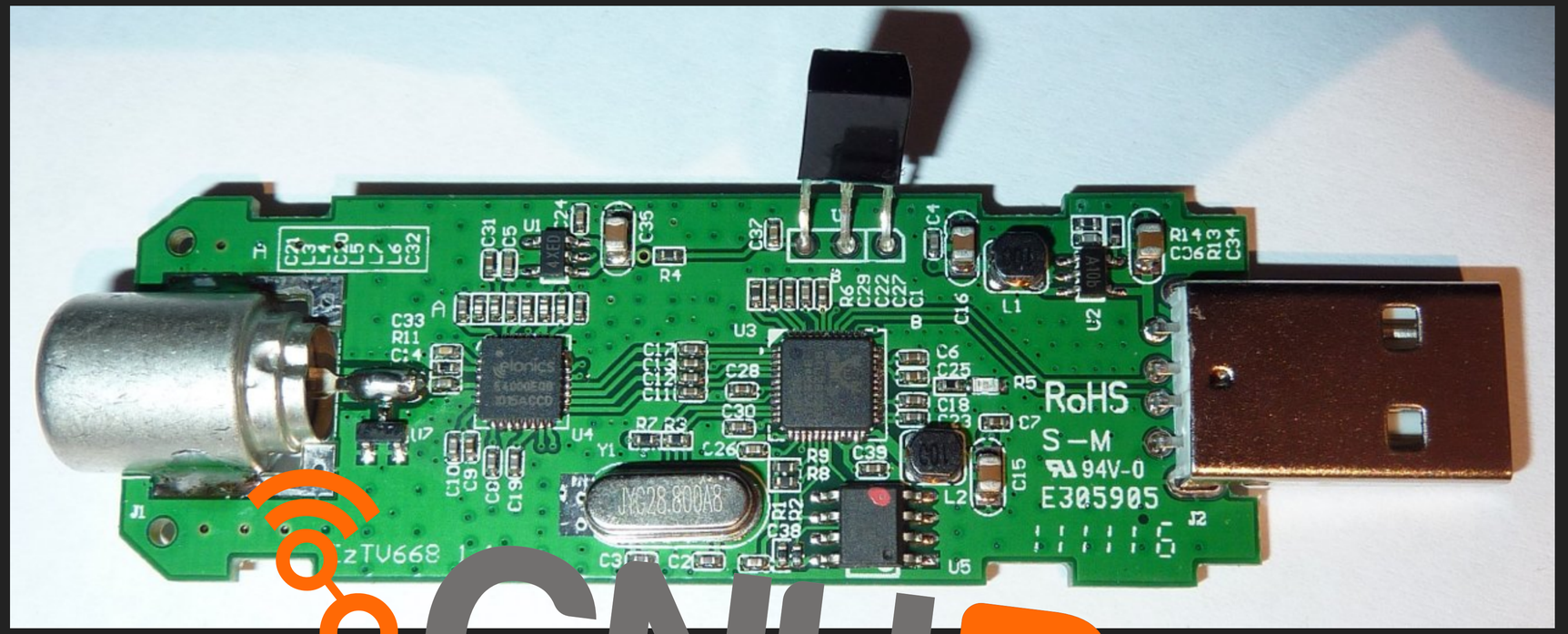
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

$8

RTL 2832 USB STICK

+ Free Software

(not pictured: promiscuous mode driver)



$8

GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

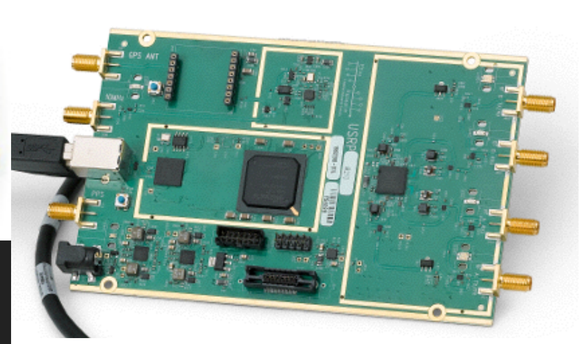
RTL 2832 USB STICK

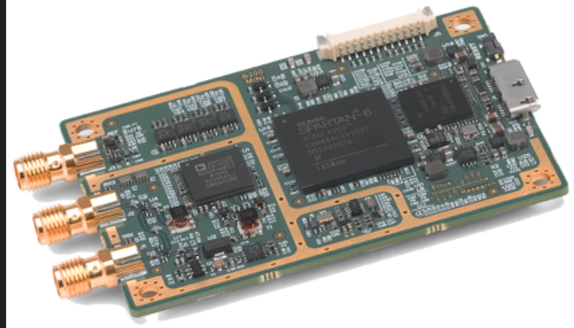
+ Free Software

(not pictured: promiscuous mode driver)

Wireless sniffing in

2017





$8 -> $1150

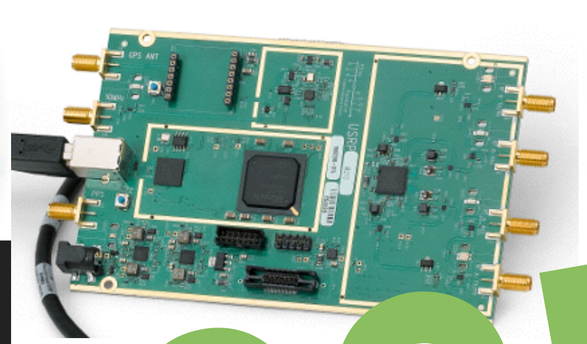
ALL THE SDRS

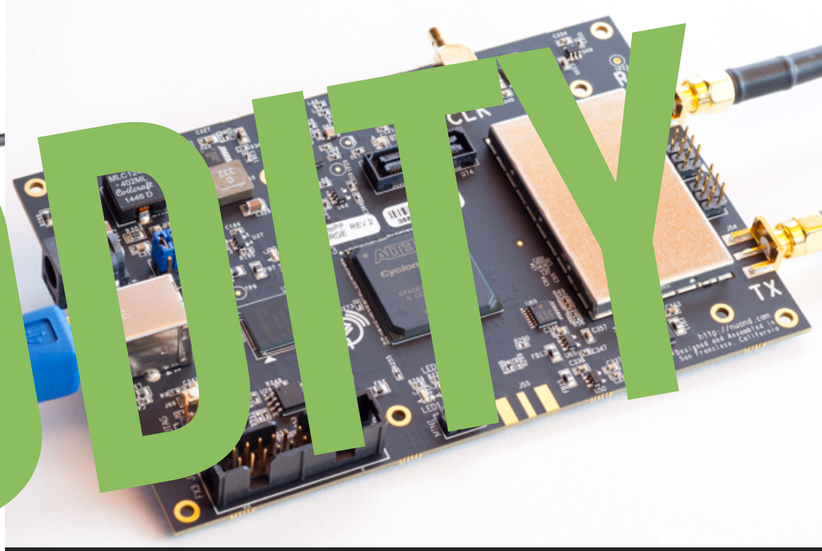
+ Free Software

GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

https://www.ettus.com/content/images/USRP_B200mini_Front_Diagonal_Large.png
http://www.nooelec.com/store/media/catalog/product/cache/1/image/1200x/040ec09b1e35df139433887a97daa66f/n/e/nesdr_mini_1b.jpg
https://cdn.itead.cc/media/catalog/product/i/m/im141027001_5__1.jpg
https://cdn.sparkfun.com//assets/parts/9/9/5/3/13001-04.jpg
https://www.ettus.com/product/details/UB210-KIT
https://www.nuand.com/blog/wp-content/uploads/2013/05/DSC0063.png





COMMODITY

$8 -> $1150

GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

ALL THE SDRS

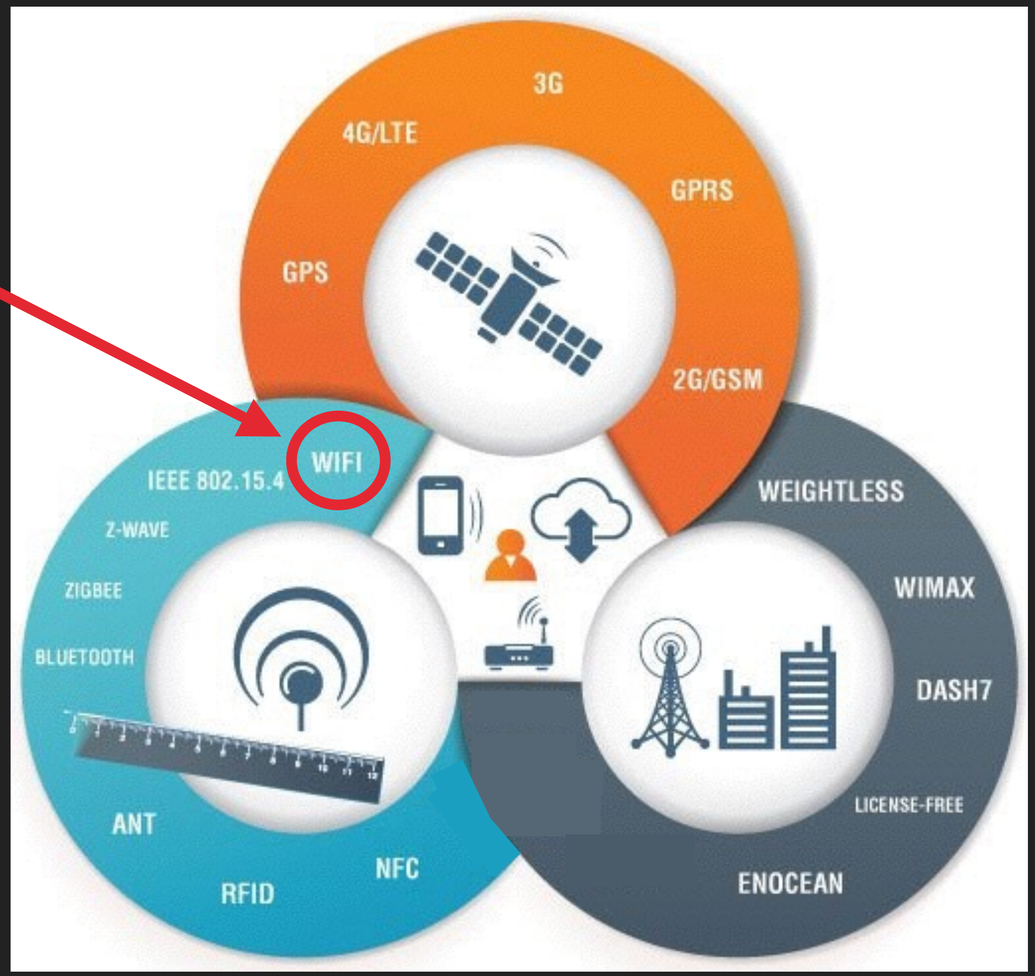
+ Free Software

https://www.ettus.com/content/images/USRP_B200mini_Front_Diagonal_Large.png
http://www.nooelec.com/store/media/catalog/product/cache/1/image/1200x/040ec09b1e35df139433887a97daa66f/n/e/nesdr_mini_1b.jpg
https://cdn.itead.cc/media/catalog/product/i/m/im141027001_5__1.jpg
https://cdn.sparkfun.com//assets/parts/9/9/5/3/13001-04.jpg
https://www.ettus.com/product/details/UB210-KIT
https://www.nuand.com/blog/wp-content/uploads/2013/05/DSC0063.png

WIRELESS IN 2017

- 802.11 is just one piece of the puzzle

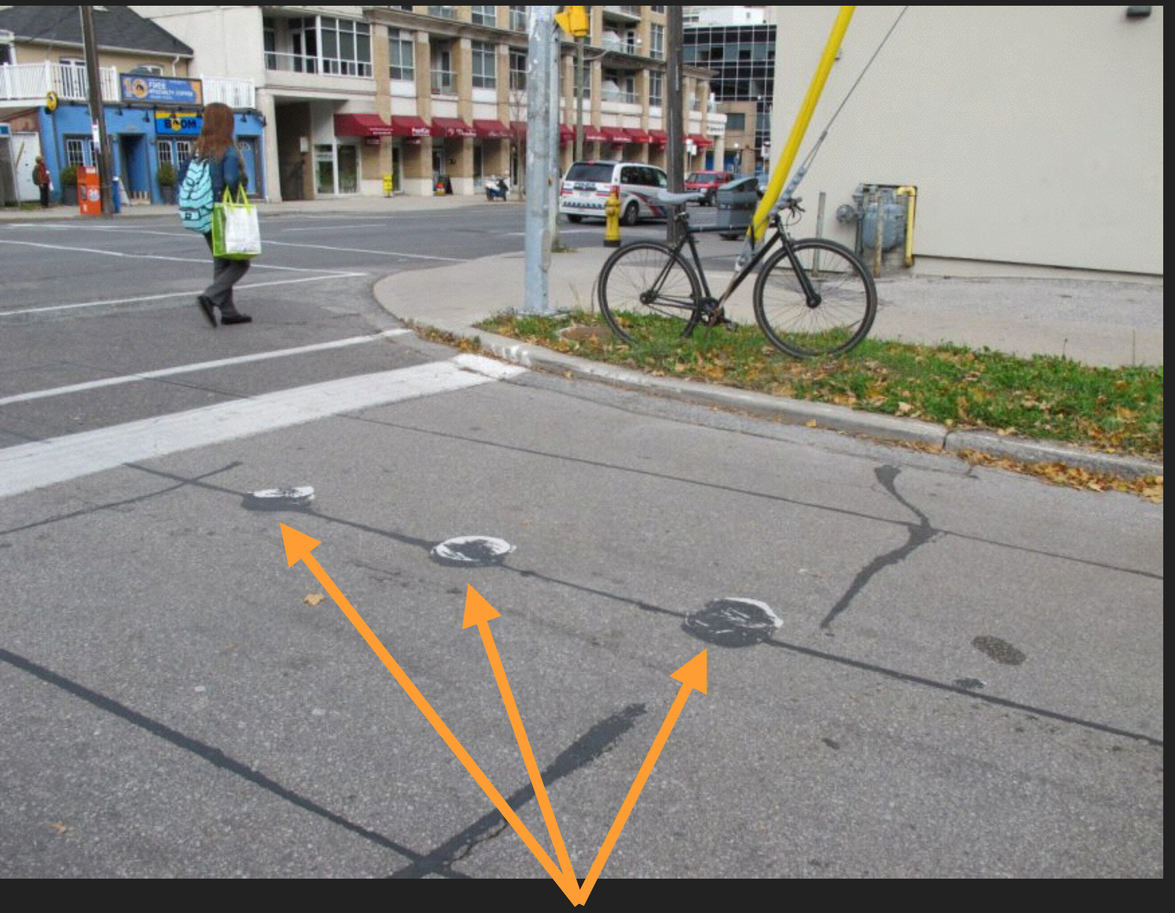
- Explosion of IoT and Mobile means…
  - There's a PHY for every use case
  - Embedded systems are everywhere



http://postscapes.com/internet-of-things-technologies

EMBEDDED == DESIGN BY COMPROMISE

(or is it Compromised by Design?)



Literal embedded systems

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

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

https://www.thestar.com/content/dam/thestar/yourtoronto/the_fixer/2013/11/08/cyclists_cant_trip_the_light_if_the_sensor_doesnt_work/the_fixer.jpg.size.custom.crop.867x650.jpg

Industry reliance on

SECURITY THROUGH OBSCURITY

means...

[PIÑATAS]

CLASSIFYING RF ATTACK METHODS

METHODS OF EXPLOITATION

CLASSIFYING RF ATTACK METHODS

- For each attack category, we'll show:
  1. Method: how the attack is performed
  2. Impact: what the attack enables
  3. Analogue: equivalent attack on wired/IP network, if one exists
  4. Limitations: mitigations, whether incidental or intentional
  5. Example: relevant examples of this type of attack
  6. Proof: demo

RF ATTACK CATEGORIES

1. Sniffing
2. Wardriving
3. Replay
4. Jamming
    - 4.1. Smart Jamming
    - 4.2. MAC Layer Reservation
5. Evil Twin
6. Firmware Updates
7. PHY Layer Targeting

RF ATTACK CATEGORIES

1. Sniffing
2. Wardriving
3. Replay
4. Jamming
    - 4.1. Smart Jamming
    - 4.2. MAC Layer Reservation
5. Evil Twin
6. Firmware Updates
7. PHY Layer Targeting

RF ATTACK CATEGORIES

1. Sniffing
2. Wardriving
3. Replay
4. Jamming
    - 4.1. Smart Jamming
    - 4.2. MAC Layer Reservation
5. Evil Twin
6. Firmware Updates
7. PHY Layer Targeting

DENIAL OF SERVICE // NETWORK STATE DISRUPTION

JAMMING

JAMMING OVERVIEW

- Method
  - Transmit noise or conflicting traffic within target network's RF channel (same frequency)
- Impact
  - Blocks traffic on network
  - Network state disruption
- Wired Analogue
  - Denial of Service

JAMMING APPLIED

- Limitations
  - Jam detection mechanisms
  - Self-denial: difficult to simultaneously jam and monitor network traffic
- Example
  - Home security system jamming

JAMMING DEMO

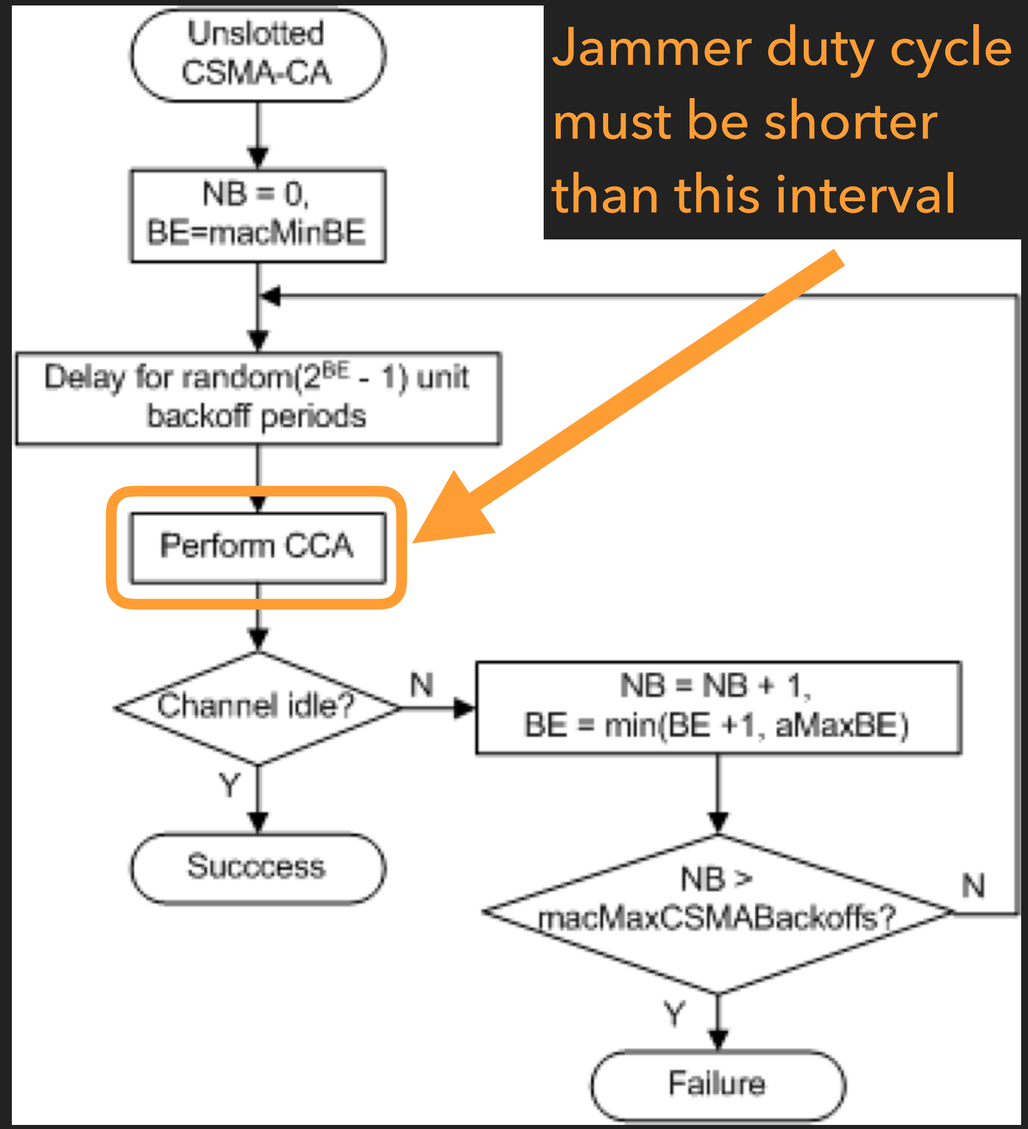
- Honeywell home security system
- 345 MHz on-off keying protocol
  - Transmit wideband noise at 345 MHz
  - Device jam detection mechanisms will detect after several seconds, so…

EVADING DETECTION 😏

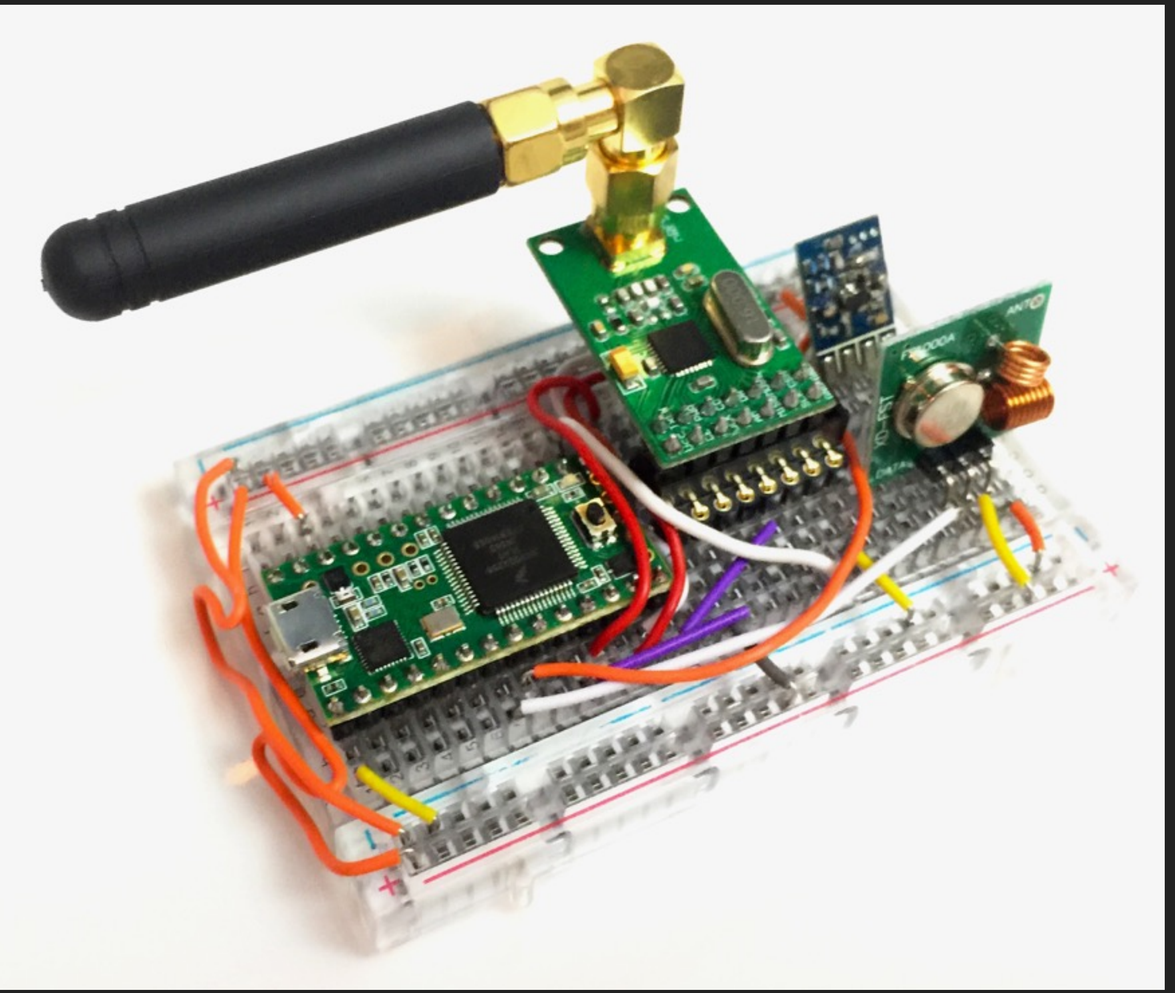
SMART JAMMING

DUTY CYCLED JAMMING

- Problem: Hardware radios implement “clear channel” detection features to avoid talking over other radios
  - Polling CCA is a zero marginal cost jam detector
- Solution: pulse jammer on and off at appropriate rate to evade jam detection functions
- Examples: Matt’s done this to defeat 802.15.4 jam detection, but doesn’t know of any public examples



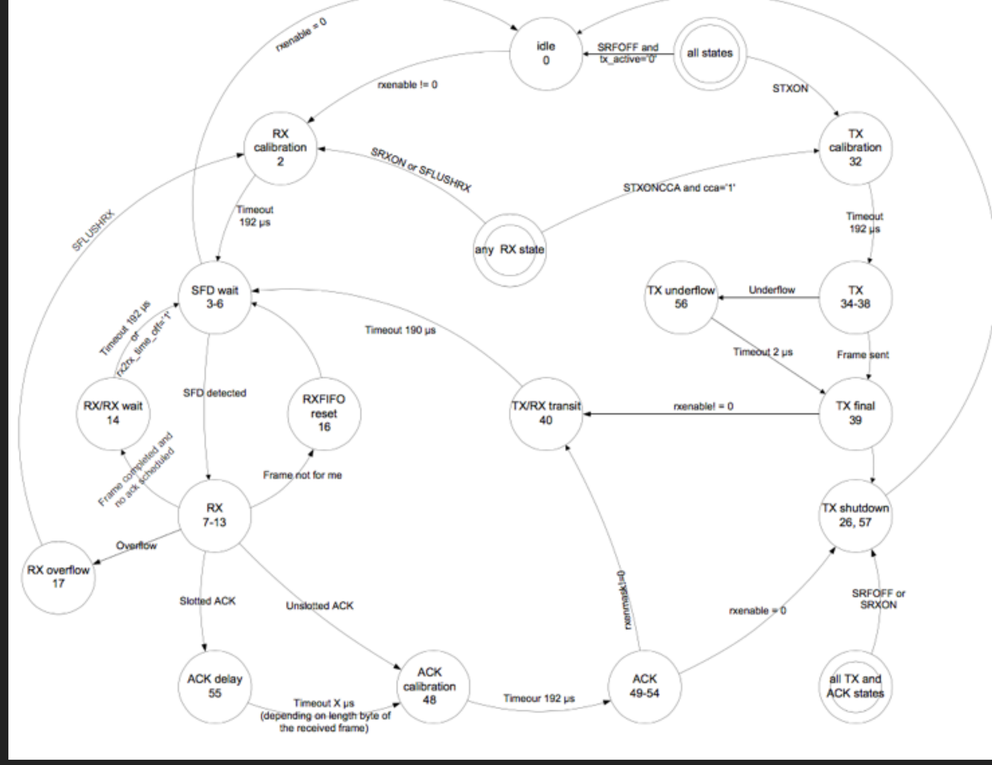
http://www.mdpi.com/sensors/sensors-11-03852/article_deploy/html/images/sensors-11-03852f1-1024.png



REFLEXIVE JAMMING

- Problem: Continuously jamming makes offensive network monitoring hard
  - Jamming denies both the attacker and the defender
- Solution: detect beginning of frame and reflexively jam to target either specific packets or trailing checksums
- Examples: Samy Kamkar's RollJam (left), reflexive jamming built into Killerbee// 802.15.4 ApiMote

https://www.wired.com/wp-content/uploads/2015/08/rolljam3.jpg



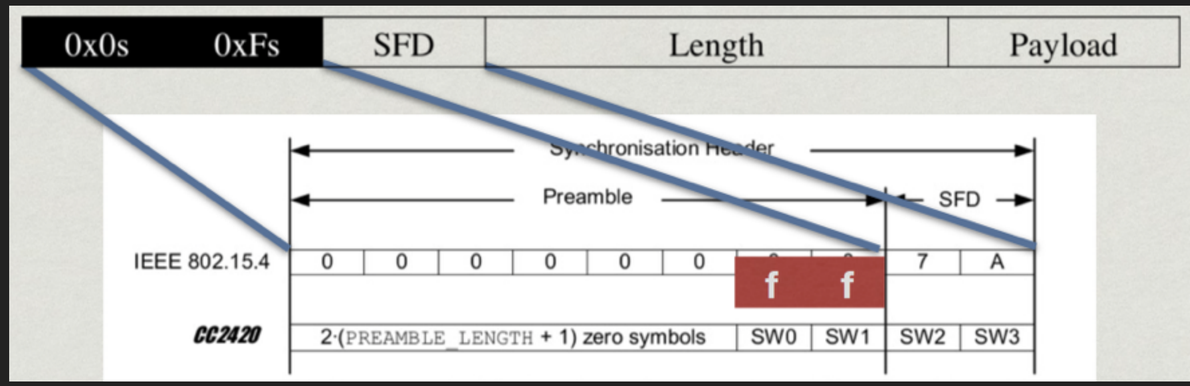
ESCALATION // IDS EVASION // DEVICE FINGERPRINTING

PHY LAYER SELECTIVE TARGETING

http://www.ti.com/lit/ds/symlink/cc2520.pdf

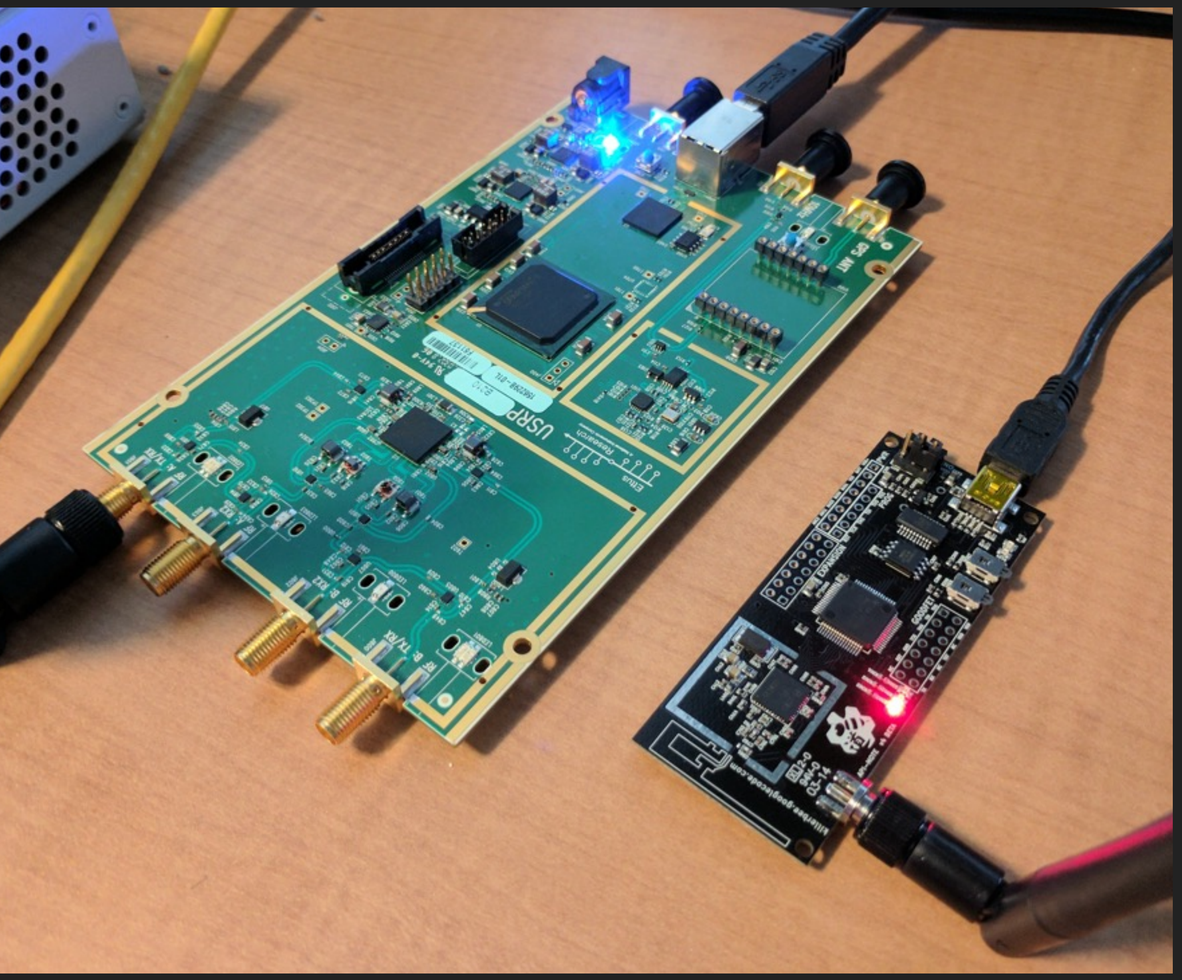
PHY SELECTIVE TARGETING OVERVIEW

- Method
  - Chipsets implement PHY standards differently – various degrees of error tolerance
  - Send standards-noncompliant transmissions that exploit corner cases in specific PHY state machines
- Impact
  - Targeted receiver evasion (IDS evasion)
  - Device fingerprinting
- Wired Analogue
  - Same (demonstrated on 802.3 chipsets)
  - Far more practical in RF domain



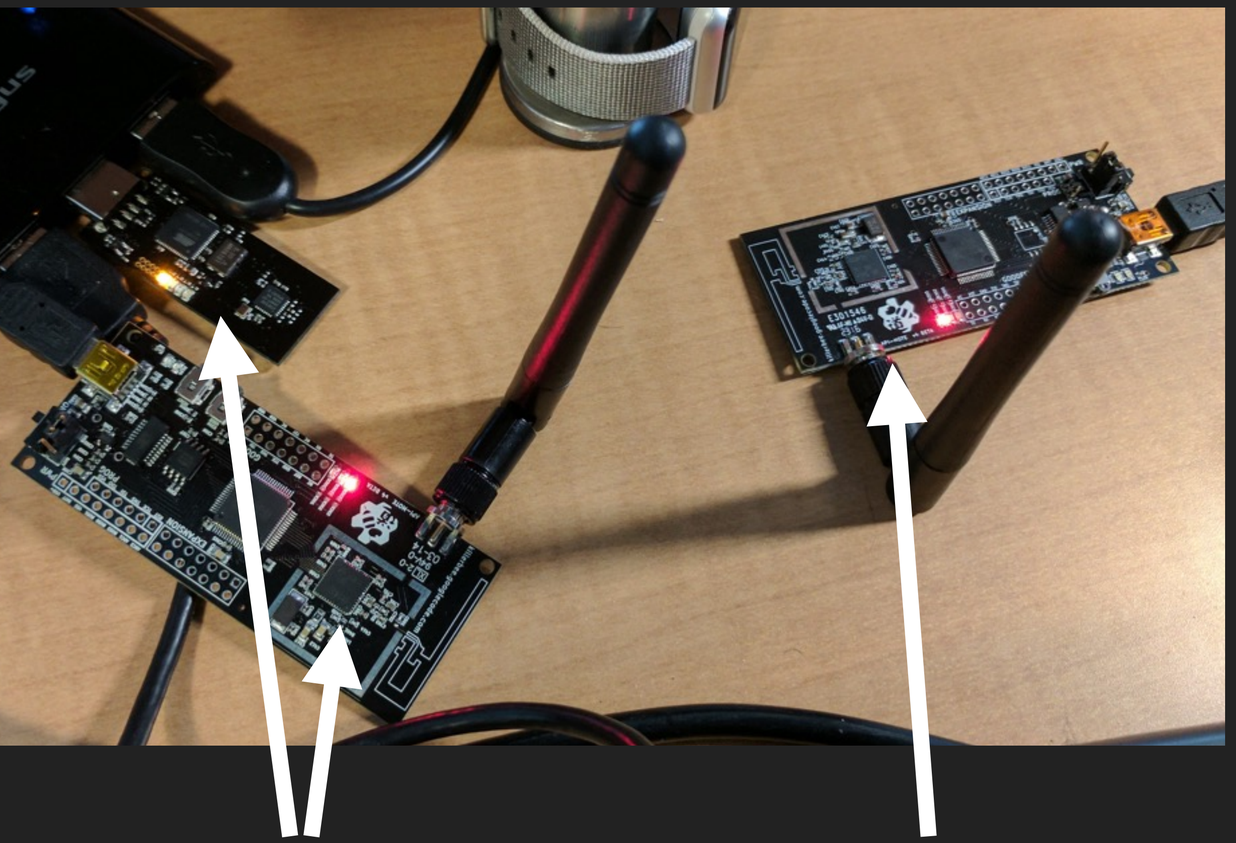
Preamble	RZUSB Observed	ApiMote Observed
00 00 00 00	672	1000
00 00 00 ff	991	0
00 00 ff ff	990	0
00 ff ff ff	855	1
ff ff ff ff	4	0

https://www.troopers.de/wp-content/uploads/2013/11/TROOPERS14-Making-and_Breaking-an_802.15.4_WIDS-Sergey_Bratus+Javier_Vazquez+Ryan_Speers.pdf



PHY SELECTIVE TARGETING APPLIED

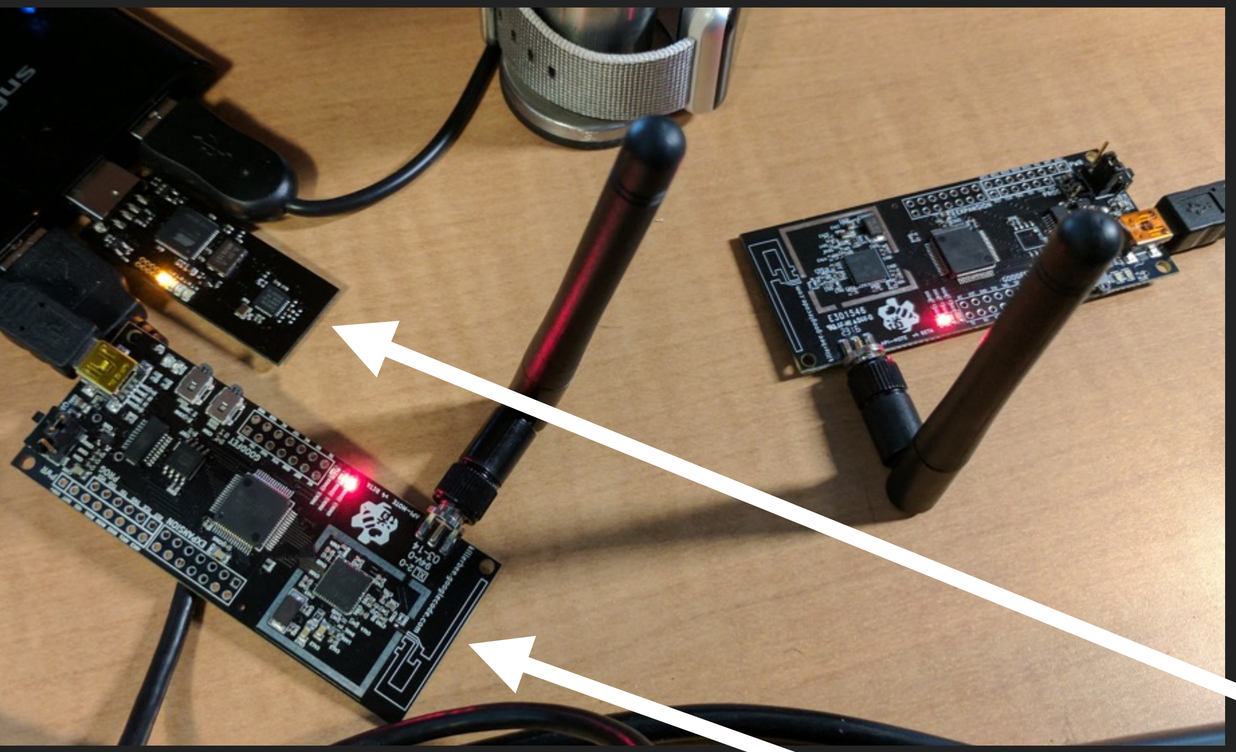
- Limitations
  - Network participants must be on different chipsets
  - Not all chipsets are vulnerable
- Example
  - 802.15.4 receiver evasion



PHY SELECTIVE TARGETING DEMO

- Selectively evasive 802.15.4 packets
- Transmitter: ApiMote w/ CC2420
- Receivers: ApiMote w/ CC2420
  RZUSB stick w/ AT86RF230
- Both receivers receive everything, until they don't... 😏

*cheers to David Dowd, River Loop Security, Travis Goodspeed, and Dartmouth for original research



PHY SELECTIVE TARGETING DEMO

- 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

*cheers to David Dowd, River Loop Security, Travis Goodspeed, and Dartmouth for original research

CHARACTERIZING WIRELESS ATTACK METHODS

CONCLUSIONS

WIRELESS ATTACK METHODS SUMMARY

	Analogue	Complexity	Ease of Mitigation
Sniffing	Unique!	Easy	Hard
Wardriving	Port Scanning	Easy	Hard
Replay	[same]	Easy	Moderate
Jamming	Denial of Service	Easy	Hard
Link Layer Congestion	Unique!	Moderate	Moderate
Evil Twin	ARP Spoofing	Hard	Moderate
Firmware Attack	Malware	Hard	Moderate
PHY Abuse	[same]	Hard	Hard

NON-EXHAUSTIVE LIST

[OBVIOUSLY]

AS ATTACKERS...

- Look for low-hanging fruit first
  - Unencrypted comms, replay attacks, cleartext key exchanges, etc.
  - Complexity goes up in a hurry

- Lean on your existing wired/IP network skill set
  - Analogues exist!

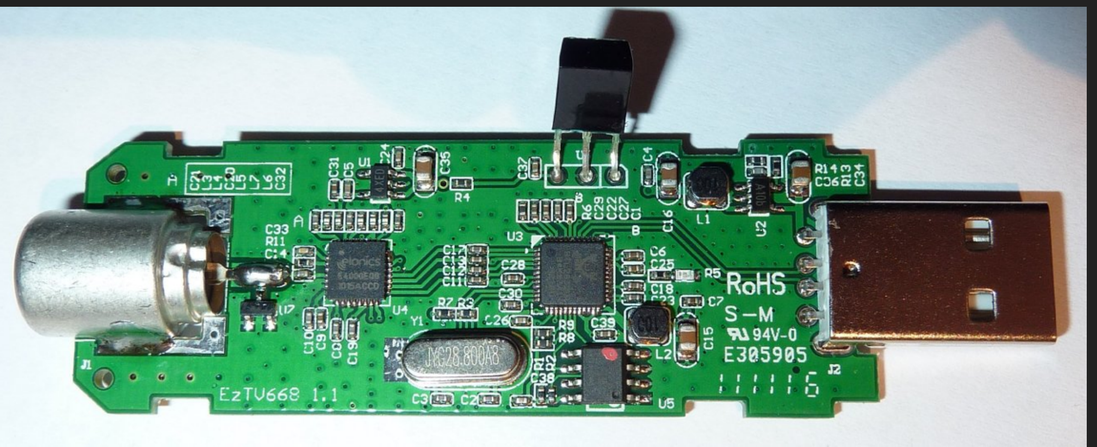
AS ATTACKERS... CONTINUED

- Leverage Open Source Intelligence (OSINT):
  - FCC regulatory filings
  - Data sheets
- It will make your life easy

- Marc gave an entire talk on this at HITB2016AMS

AS DEVELOPERS…

- This is the Golden Age of RF Hacking
  - Software Defined Radio has been commodity for >5 years
  - Every RF PHY is in scope now



TIME TO OWN YOUR AIRWAVES

ADDITIONAL RADIO RESOURCES

- "So You Want to Hack Radios" series (all about RF Physical Layers)
  - Shmoocon: https://www.youtube.com/watch?v=L3udJnRe4vc
  - Troopers: https://www.youtube.com/watch?v=OFRwqpH9zAQ
  - HITB2017AMS Commsec: https://www.youtube.com/watch?v=QeoGQwT0Z1Y
- Matt's LoRa research
  - 33c3: https://media.ccc.de/v/33c3-7945-decoding_the_lora_phy
- Marc's OSINT techniques
  - HITB2016AMS Commsec: https://www.youtube.com/watch?v=JUAiav674D8
- Dallas siren attack research
  - White paper: https://www.bastille.net/blogs/2017/4/17/dallas-siren-attack

ACKNOWLEDGEMENTS

- Balint and Logan from Bastille's Threat Research Team
- Bastille at large
- GNU Radio community!

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

THANKS

github.com/BastilleResearch

marc@Bastille.net
@marcnewlin

matt@Bastille.net
@embeddedsec

QUESTIONS?

github.com/BastilleResearch

marc@Bastille.net
@marcnewlin

matt@Bastille.net
@embeddedsec