TCIPG

802.15.4/ZigBee Security Tools

Active Fingerprinting of IEEE 802.15.4/ZigBee Devices

Ira Ray Jenkins, Rebecca Shapiro, and Sergey Bratus

GOALS

- Overall:
  - Provide IEEE 802.15.4/ZigBee network operators and asset owners with cheap and simple-to-operate tools for self-assessment.
  - Enable the exploration of the attack surface of IEEE 802.15.4-based network technologies.
- Specifically:
  - Actively fingerprint (identify based on characteristic responses to malformed frames) IEEE 802.15.4/ZigBee digital radio chips and firmware for self-audits and the detection of rogue nodes.

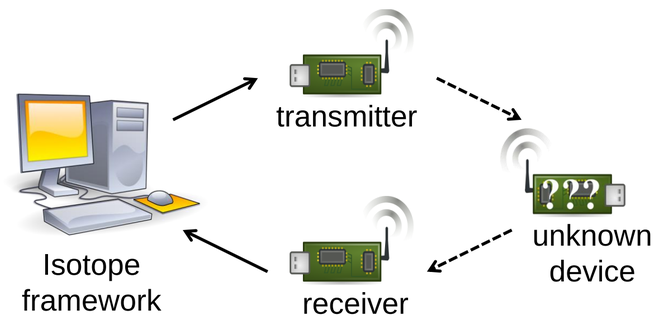
FUNDAMENTAL QUESTIONS/CHALLENGES

- Mission-critical services and infrastructure rely on communications networks, like IEEE 802.15.4/ZigBee, for monitoring, control, and automation.
- Network administrators must be able to easily observe the footprint of their networks, understand the view it presents to would-be attackers of various levels of sophistication, and explore network responses to crafted and/or malformed traffic. **Exposed and brittle networks must be fixed and protected.**
- **"Security does not get better until tools for practical exploration of the attack surface are made available"** —Joshua Wright, the author of the first open-source ZigBee security toolkit, *KillerBee*.
- Practical network attack surface exploration requires capabilities to locate networks, capture frames on multiple channels, and craft/inject both valid and malformed frames.
- To be useful in the field, that functionality requires **affordable commodity devices** rather than special-purpose, lab-only equipment.
- Fingerprinting allows us to observe network responses to malformed traffic, identify trusted nodes, and explore potential vulnerabilities in both the PHY layer and firmware implementations.

We can fingerprint IEEE 802.15.4/ZigBee radio chips and their open-source firmware, in an active manner, by observing responses to specially crafted malformed frames.

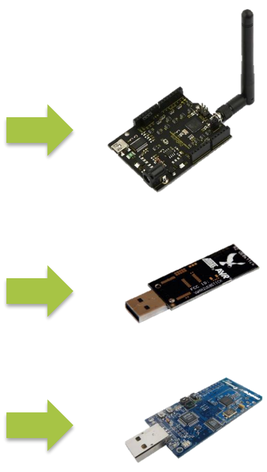
RESEARCH PLAN

- Identify possible fingerprinting techniques.
- Develop fingerprinting framework, Isotope.
- Experimentally verify unique fingerprints.



Fingerprinting Framework

Device	Radio	Firmware
zigduino	**atmega128rfa1**	Contiki
		GoodFET
		TinyOS
		Arduino
rzusbstick	**at86rf230**	Chibi
		Contiki
		Raven (GoodFET)
tmote sky	**cc2420**	Contiki
		GoodFET
		TinyOS



Hardware and Firmware Utilized

Symbols: 8	2	2		variable
Preamble	SFD	Frame length (7 bits)	Reserved	PSDU
SHR		PHR		PHY payload

IEEE 802.15.4 Physical Frame

- Smallest transmittable piece of data is a symbol, or 4 bits.
- Preamble: 32 bits or 8 symbols of 0x0.
- Start of Frame Delimiter (SFD): 0xA7.

FINGERPRINTING TECHNIQUES

Several methods were implemented to slightly alter the standard physical frame:

Variable Preamble	SFD	Length	Payload

Physical frame with variable preamble length

- Vary the number of preamble 0x0 symbols.

0x0s ➔ 0xFs	SFD	Length	Payload

Physical frame with Franconian Notch

- Modify the standard 8 preamble symbols from 0x0s to 0xFs.

Preamble	0xFs	SFD	Length	Payload

Physical frame with Franconian Bridge

- Insert a variable number of 0xF symbols between the preamble and SFD.

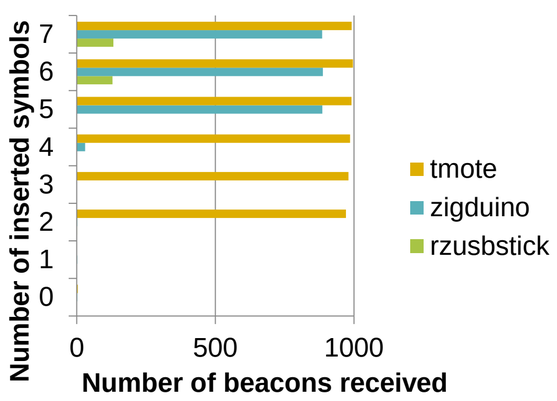
Preamble	SFD (bad)	0xFs	Preamble	SFD	Length	Payload

Physical frame with Cumberland Gap

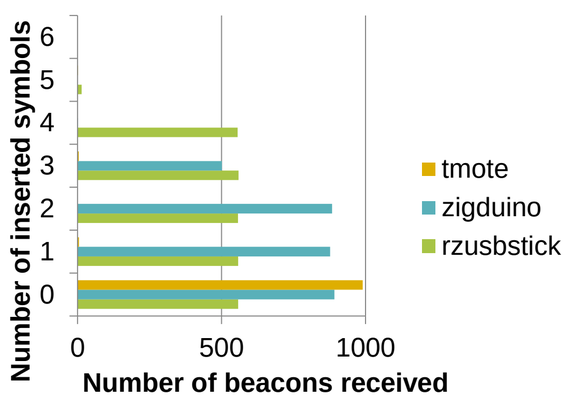
- Transmit a bad SFD followed by a variable number of 0xF symbols and then a valid frame.

RESEARCH RESULTS

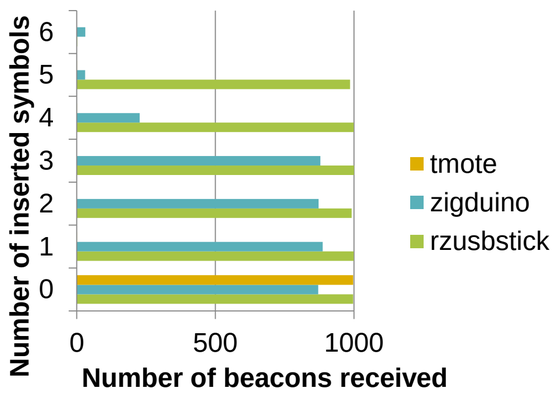
Variable preamble with GoodFET firmware



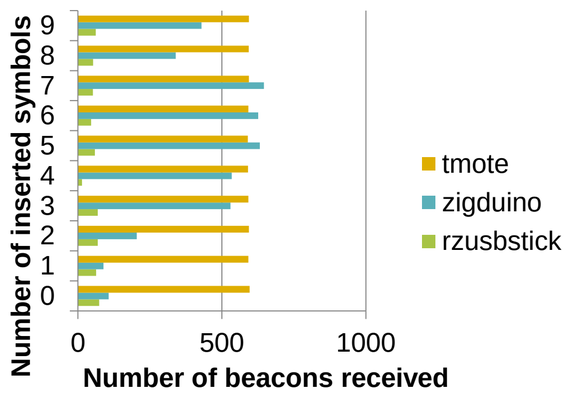
Franconian Notch with GoodFET firmware



Franconian Bridge with GoodFET firmware



Cumberland Gap with GoodFET firmware



We can distinguish between devices of different makes.

BROADER IMPACT

- We set the current standards for open-source, open-platform, low-cost security tools for 802.15.4. Our **APImote** tool is used by many security industry researchers.
- We exposed significant security issues with the 802.15.4 PHY protocol and suggested practical mitigation.
  - We also demonstrated ineffectiveness of other proposed mitigations.
- Our research demonstrated new attack vectors for digital radio PHY.

INTERACTION WITH OTHER PROJECTS

riverloopsecurity.com

River Loop Security

- Founded by Dartmouth/TCIPG alumni Ryan Speers and Ricky Melgares, providing IEEE 802.15.4 digital radio security and product assessments.

Api-do/KillerBee

- Result of previous Dartmouth/TCIPG activity on IEEE 802.15.4/ZigBee security.
- Tools for assessing security of IEEE 802.15.4/ZigBee deployments.

code.google.com/p/killerbee
code.google.com/p/zigbee-security/

FUTURE EFFORTS

- Refinement and extension of existing tools.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T