TCIPG Trustworthy Cyber Infrastructure for the Power Grid | tcipg.org

802.15.4/ZigBee Security Tools

Overview and Problem Statement

Mission-critical services and infrastructure, such as the power grid, are increasingly dependent upon communications networks, like IEEE 802.15.4 and ZigBee, to facilitate monitoring, control, and automation. Network administrators must be able to easily observe the footprint of their networks, understand the view they present to would-be attackers of various levels of sophistication, and explore potential responses to crafted and/or malformed traffic. Exposed and brittle networks must be fixed and protected.

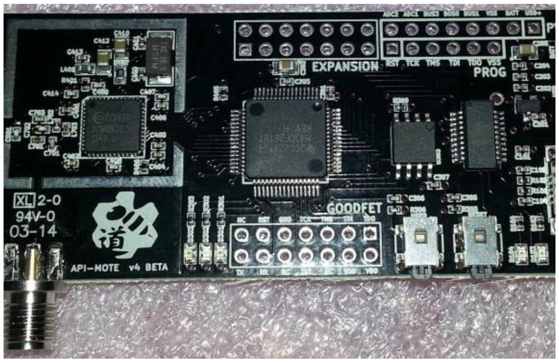
Active fingerprinting is the identification of digital radio devices through exploitation of unique characteristics, introduced by the analog circuitry and firmware implementations, in response to malformed traffic. Fingerprinting allows us to observe network responses to malformed traffic, identify trusted nodes, and explore potential vulnerabilities in both the PHY layer and firmware implementations. In addition to producing a digital radio peripheral and utilities for the passive mapping of 802.15.4/ZigBee digital radio deployments, such as smart meter networks, we have developed techniques for the active fingerprinting of nodes in such networks. Active fingerprinting is both faster and more accurate than traditional passive techniques currently used in self-assessments.

Research Objectives

- 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 IEEE 802.15.4-based network technologies' attack surface.
- Actively fingerprint IEEE 802.15.4/ZigBee digital radio chips and firmware for self-audits and the detection of rogue nodes.
- **Smart Grid Application Area:** IEEE 802.15.4/ZigBee is the networking technology of choice for SCADA systems, home automation, and smart meter connectivity.

Technical Description and Solution Approach

- The IEEE 802.15.4 standard was used to develop multiple standard-frame mutations that might be effective for fingerprinting.
- Low-cost hardware based on commodity components was designed and developed to inject crafted frames into 802.15.4 networks.



Preamble: 00000000	SFD: 0xA7	Length (<512)	Payload

Standard 802.15.4 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

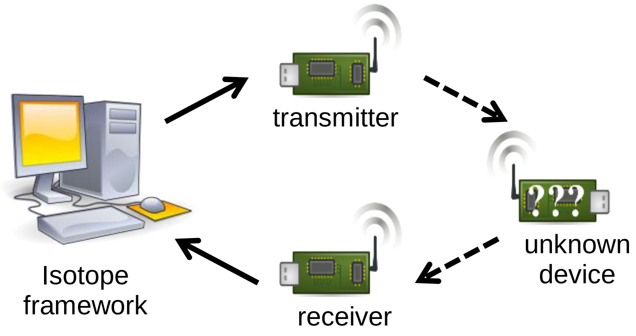
  - Insert a variable number of 0xF symbols between the preamble and SFD

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

- A Python framework, codenamed *Isotope*, was developed to facilitate the active fingerprinting of multiple commodity IEEE 802.15.4/ZigBee-compliant network radio devices. Malformed frames are transmitted to an unknown device; potential responses are recorded and later analyzed for a potential fingerprint.



IEEE 802.15.4/ZigBee Fingerprinting Framework

Results and Benefits

- Fingerprinting framework, Isotope, introduced; results published at the ACM WiSec 2014 conference.
- Partnerships and External Interactions: Enabled applied ZigBee research at the Air Force Institute of Technology; made contributions and improvements to Joshua Wright's KillerBee; provided 802.15.4 extensions to Scapy; developed extensions to Api-do with River Loop Security's APImote device.
- Demonstrated new threats for 802.15.4/ZigBee, including feasibility of **targeted attacks** on selected makes of radio chips and **evasion** of Wireless Intrusion Prevention Systems (WIPS).
- **Technology Readiness Level:** Beta; tools in ongoing development; more experimental results to come.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Ira Ray Jenkins, jenkins@cs.dartmouth.edu

Industry Collaborators

- Travis Goodspeed, travis@radiantmachines.com
- Ryan M. Speers & Ricky Melgares, River Loop Security, team@riverloopsecurity.com