TCIPG

Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks

S. Bratus, R. Melgares, R. Speers

Goals

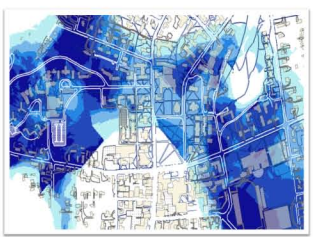
- Provide 802.15.4/ZigBee network operators and asset owners with cheap and simple-to-operate tools for self-assessment.
- Enable exploration of 802.15.4-based network technologies' attack surface.
- Audit ZigBee networks with the ease of 802.11/Wi-Fi "wardriving", both classic Kismet-like interface & Google Earth

Fundamental Questions/Challenges

- **"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 and inject valid and malformed frames.
- To be useful in the field, this functionality requires **cheap**, **commodity devices** rather than special-purpose, lab-only equipment.
- Most attack surface exploration experiments with 802.15.4 require expensive peripherals, such as the Ettus Research USRP. Such equipment is beyond the means and skills of a typical wireless network administrator.
- Administrators must be able to easily observe the **footprint** of their networks and the view it presents to would-be attackers of various levels of sophistication, and be able to explore its responses to crafted and/or malformed traffic. **Exposed and brittle networks must be fixed or protected.**

Tools

- **OpenEar**: an all-channel passive sniffer and network locator, integrated with GPS for easy geolocation; works with up to 16 sniffing devices.
- **zbWarDrive**: active scanner with capability to locate and lock several sniffing devices into channels with observed responses and activity.
- **zbForge**: tool for crafting 802.15.4 frames.
- Contributions to **KillerBee** codebase.



Results

- First generation of tools released http://code.google.com/p/zigbee-security/
  - KillerBee & GoodFET contributions
  - Api-do suite, extending KillerBee
  - Dot15d4 Scapy modules

- **Api-mote** prototype designed, test run manufactured:

- Used in multiple industry assessments, security audits of equipment deployed by major US telecom company. Reportedly used to audit smart grid deployments in the UK.
- Enabled applied ZigBee research at the US Air Force Institute of Technology
- Signaling weakness of 802.15.4 and similar digital radios exposed
  - Presented at USENIX WOOT 2011, other security industry conferences
  - Receieved the BlackHat 2012 Pwnie Award for most innovative research.

Technology Transfer

RIVER LOOP SECURITY

- Founded by TCIPG/Dartmouth alumni Ryan Speers, Ricky Melgares, providing 802.15.4 digital radio security & product assessments http://riverloopsecurity.com/
- Api-do/KillerBee open source tools maintained at http://code.google.com/p/zigbee-security/

Broader Impact

- Tools for exploring network technologies' attack surface lead to security solutions. We aim to accelerate development of solutions.

Future Efforts

- Further development of tools, production of **Api-mote**.
- Porting tools to 900MHz platforms.