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.
- Create a reference commodity assessment and self-assessment platform and tools.

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.

Research Results

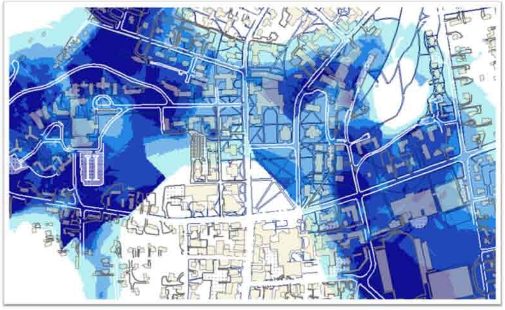
- First generation of tools released: http://code.google.com/p/zigbee-security/
- Tools presented to wireless security researchers and auditors at several practitioner conferences.
- Tools used in assessments (according to feedback received).
- Signaling weakness of 802.15.4 and similar digital radios exposed and presented at USENIX WOOT 2011, San Francisco.

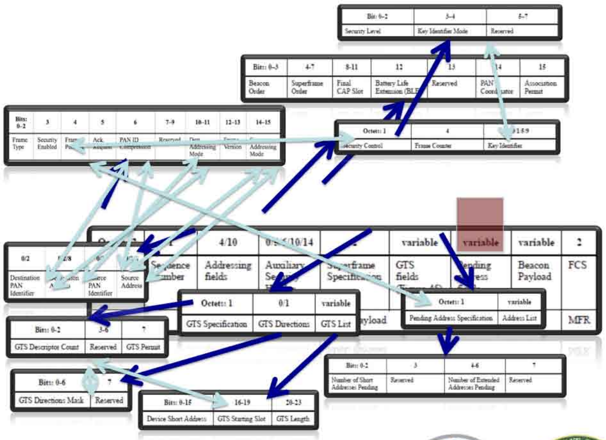
Broader Impact

- Tools for exploring network technologies' attack surface lead to security solutions. We aim to accelerate development of solutions.
- Attack surfaces of Smart Grid networking technologies must be vigorously explored by asset owners, vendors, and independent researchers to avoid wide deployment of vulnerable implementations and/or protocols.

Future Efforts

- Further development of tools.
- Integrated support for the PPI geolocation standard.
- Porting tools to 900MHz platforms.




Bits: 0-2 | 3-4 | 5-7
Security Level | Key Identifier Mode | Reserved
Bits: 0-3 | 4-7 | 8-11 | 12 | 13 | 14 | 15
Beacon Order | Superframe Order | Final CAP Slot | Battery Life Extension (BLE) | Reserved | PAN Coordinator | Association Permit
Bits: 0-2 | 3 | 4 | 5 | 6 | 7-9 | 10-11 | 12-13 | 14-15
Frame Type | Security Enabled | Frame Pending | Ack Request | PAN ID Compression | Reserved | Dest. Addressing Mode | Frame Version | Source Addressing Mode
Octets: 1 | 4 | 0/1/5/9
Security Control | Frame Counter | Key Identifier
Octets: 2 | 1 | 4/10 | 0/5/6/10/14 | 2 | variable | variable | variable | 2
Sequence Number | Addressing fields | Auxiliary Security Header | Superframe Specification | GTS fields | Pending Address fields | Beacon Payload | FCS
Payload
MFR
0/2 | 0/2/8 | 0/2 | 0/2/8
Destination PAN Identifier | Destination Address | Source PAN Identifier | Source Address
Octets: 1 | 0/1 | variable
GTS Specification | GTS Directions | GTS List
Octets: 1 | variable
Pending Address Specification | Address List
Bits: 0-2 | 3-6 | 7
GTS Descriptor Count | Reserved | GTS Permit
Bits: 0-6 | 7
GTS Directions Mask | Reserved
Bits: 0-15 | 16-19 | 20-23
Device Short Address | GTS Starting Slot | GTS Length
Bits: 0-2 | 3 | 4-6 | 7
Number of Short Addresses Pending | Reserved | Number of Extended Addresses Pending | Reserved

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org
University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University