Auditing 6LoWPAN networks
Using Standard Penetration Testing Tools

Adam Reziouk
Arnaud Lebrun
Jonathan-Christofer Demay
The 6LoWPAN protocol

• IPv6 over Low power Wireless Personal Area Networks

• Header compression flags
  • Addresses factoring (IID or predefined)
  • Predefined values (e.g., TTL)
  • Fields omission (when unused)
  • Use of contexts (index-based)
  • UDP header compression (ports and checksum)

• Packet fragmentation
  • MTU 127 bytes Vs 1500 bytes
  • 80 bytes of effective payload
What’s the big deal?
The IEEE 802.15.4 standard

- **PHY layer and MAC sublayer**
- **Multiple possible configurations**
  - Network topology
  - Data transfer model
- **Multiple security suites**
  - Integrity, Confidentiality or both
  - Encryption key size (32, 64 or 128)
- **Multiple standard revision**
  - 2003
  - 2006 and 2011
Deviations for the standard
The ARSEN project

• **Advanced Routing between 6LoWPAN and Ethernet Networks**

• **Detect the configuration of existing 802.15.4 infrastructure**
  • Network topology
  • Data transfer model
  • Security suite
  • Standard revision
  • Standard deviations

• **Handle packet translation**
  • Compression/decompression
  • Fragmentation/defragmentation
  • Support all possible IEEE 802.15.4 configurations
Based on Scapy-radio

```python
>>> pckt = Dot15d4FCSS() / Dot15d4Data() / ZigbeeNwk()
>>> pckt.show()

>>> 
```
Two main components

• **The IEEE 802.15.4 scanner**
  - Build a database of devices and captured frames
  - The devices that are running on a given channel
  - The devices that are communicating with each other
  - The types of frames that are exchanged between devices
  - The parameters that are used to transmit these frames

• **The 6LoWPAN border router**
  - TUN interface
  - Ethernet omitted
  - Scapy automaton
New Scapy layers

- **Dot15d4.py**
  - Several bug fixes
  - Complete 2003 and 2006 support

- **Sixlowpan.py**
  - Uncompressed IPv6 support
  - Complete IP header compression support
  - UDP header compression support
  - Fragmentation and defragmentation support
Demonstration
Thank you for your attention