Examining security flaws in ZigBee

Evan Nichols, EECS 700
Zigbee

- Personal Area Networks (PAN) standard
  - builds on IEEE 802.15.4 standard
  - low-cost, low-power
  - Star, Tree, Mesh networks
  - developed by Zigbee Alliance

- Four Layer Stack
  - Physical Layer (PHY)
  - Medium Access Control Layer (MAC)
  - Network Layer (NWK)
  - Application Layer (APL)
Security

- Network and Application Support Sublayer (APS)
  - “Open trust” model

- Encryption Keys
  - Network Key - 128-bit, shared among all devices
  - Link Key - 128-bit, shared only between two devices (only used by APS)

“Trust in the security architecture ultimately reduces to trust in the secure initialisation and installation of keying material and to trust in the secure processing and storage of keying material.”

- Two Exceptions
  - non-preconfig device joins: single key sent unprotected to enable encryption
  - physical access to “limited capability” items - light switch, temperature sensor
Application Profiles

“Agreements for messages, message formats, and processing actions that enable developers to create an interoperable, distributed application employing application entities that reside on separate devices.”

- Allow applications to send commands, request data, process commands and requests
- **ZigBee Home Automation Public Application Profile (HAPAP)**
  - Includes Startup Attribute Sets (SAS)
    i. Default Trust Center Link Key
    ii. Default Link Key Join - 0x01 - TRUE
      1. enables the use of the default link key join as a fallback case at startup time
Putting it Together

“There are two possible ways to acquire the network key. One is for the current network key to be transported using the default TC Link Key in the case where the joining device is unknown or has no specific authorization associated with it.”

- Default TC Key introduces high risk
- If attacker sniffs a device join using the default TC link, active network key is compromised, entire network communication is at risk
- Example: ZigBee Light Link (ZLL) profile
  - ZLL Master Key Leaked on Reddit, Twitter
  - Knowing Master Key allows for attacker to intercept and acquire network key
2 Examples

**User Level**

1. Send noise on the target Zigbee channel, jam communication
2. User notices jam, re-pairs the device
3. Attacker sniffs transmitted network key

**Fake Network**

1. Attacker sends “reset to factory defaults” command to lightbulb
2. Wait for bulb to search for Zigbee networks and join
3. **Bulb will connected to the first network available without any user interaction**

[Detailed Example of Hacking Philips HUE Wireless Lighting System](#)
Conclusion

- Zigbee’s security features are strong, but is at risk for Home Automation Systems
  - Issues to address
    1. Device Tampering - tamper-resistant nodes to disallow pulling keys from device memory
    2. Key Transport - disallow use of default TC key since it is public knowledge
    3. Key Establishment - distribute master keys via “out-of-band” channels (e.g. sticker)
    4. Key Rotation - periodically updated network key
Further Reading/Links

  - slides
  - video