Honey, I’m Home!!
Hacking Z-Wave Home Automation Systems

Behrang Fouladi, SensePost UK
Sahand Ghanoun
Home
Automation
Central Control
Central Control

- Entry Control
- Lighting
- HVAC
- Home Security
- Smart Appliances
- Sensors
- CCTV
- Home Entertainment System
Convenience

Energy Management

Remote Monitoring & Control

Accessibility

Security
5 million
Z-Wave devices to be shipped in 2013
How Does It Work?
Wireless

AES-128
ZigBee®
Control your world

WPA/WPA2

AES-128
Z-wave

EO
Bluetooth®
KillerBee: Practical ZigBee Exploitation Framework
Joshua Wright. 2009.

Pen Testing Over Power Lines
Dave Kennedy, Rob Simon. 2011.

Zigbee Wardriving Kit
Travis GoodSpeed. 2012.
Why Z-Wave?
According to Z-Wave Alliance...

80% of US home security market is Z-Wave

Proprietary protocol

Wireless home security tops homeowners’ wishlist

No public research so far...
Z-Wave Protocol
Z-Wave Protocol Stack

- **Application**
  - Device specific commands & parameters

- **Security**
  - Encryption, Anti-replay and MAC

- **Network**
  - 32-bit Home ID
  - 8-bits Node ID
  - Mesh Network
  - Topology Discovery
  - Automatic Healing

- **Transport**
  - Error Detection & Retransmission
  - Acknowledgment

- **Physical**
  - 868.42 (EU) / 908.42 (US) MHz
  - 9.6/40/100 Kbps
RF Configurations

FSK Modulation

9.6/40 kbps

868.42/40 MHz (EU)

±20 KHz

Manchester/NRZ
Texas Instruments CC1110

Sub-1 GHz RF transceiver SoC
Supports Z-Wave configurations
Communication via serial

*SmartRF Studio Tool*
RTFM!
ITU-T Rec. G.9959

We identified **inconsistencies** with the actual implementation!
Z-Wave Frame Format

- **PHY Frame**
  - Preamble
  - SoF
  - MAC Data Frame *(variable length)*
  - EoF

- **Singlecast MAC Frame**
  - Home ID
  - Source ID
  - Frame Ctrl.
  - Length
  - Dest. ID
  - Data Payload
  - Checksum

- **Application Frame**
  - Header
  - Command Class
  - Command
  - Param 1
  - Param 2
  - Param n
Packet needed to do network discovery
I Like to Move It!!
Live Demo
Z-Wave Security
Message Freshness: 64-bit Nonce

Encryption: AES-OFB

Data Authentication: AES-CBCMAC

Custom Key Establishment Protocol

128-bit Random Network Key: $K_n$

128-bit Cipher & MAC Keys: Derived From $K_n$
Custom Key Establishment Protocol
Get ready for key establishment

Ready

Nonce request

Nonce value

Encrypted network key – $K_n$

Nonce request

Nonce value

Encrypted message (new key is set)

Encrypt & MAC by $K_0$

Encrypt & MAC by $K_n$
Get ready for key establishment

Ready

Nonce request

Nonce value

Encrypted network key – $K_n$

Nonce request

Nonce value

Encrypted message (new key is set)

Encrypt & MAC by $K_0$

Encrypt & MAC by $K_n$
Protocol Vulnerabilities
Passive attack:
Intercept and decrypt the “set key” message

Happens at system installation time in “low power transmission” mode
Passive attack:
Intercept and decrypt the “set key” message

Happens at system installation time in “low power transmission” mode

Not very interesting!
With “whom” key is being established?
With someone who knows...

temporary key value

and...

...key derivation functions
\[ K_0 = \text{byte}[16] \{0\} \]

\[ K_c = AES - ECB_{K_n}(Passwd_c) \]

\[ K_m = AES - ECB_{K_n}(Passwd_m) \]
\[ C = AES - \text{OFB}_{K_c}(\text{IV}, P) \]

\[ MAC = AES - \text{CBCMAC}_{K_m}(\text{IV}, \text{SH} \parallel \text{SRC} \parallel \text{DST} \parallel \text{LEN} \parallel C) \]
Unauthorized Key Reset

Attack?
Honey, I’m Home!!
Live Demo
Hmm... Now What?
Critical vulnerability... needs an urgent fix!

Short-term fix (OTA)

*Check current key state before it’s set*

Actual fix (Next Gen)

*Public key cryptography and authentication*
More technical detail in our White Paper

code.google.com/p/z-force
Thank You!

Behrang Fouladi
behrang@sensepost.com
@BehrangFouladi

Sahand Ghanoun
research@sahand.net
@Sahand__