ZCOVER: Uncovering Z-Wave Controller Vulnerabilities Through Systematic Security Analysis of Application Layer Implementation

Nkuba Kayembe Carlos, Jimin Kang, Seunghoon Woo, and Heejo Lee

Korea University

2025. 06. 25

고려대학교 정보대학
Korea University
College of Informatics

고려대학교 소프트웨어보안연구소
Korea University
Center for Software Security and Assurance

CCSLAB
Computer & Communication
Security Laboratory

1. Smart Home Systems

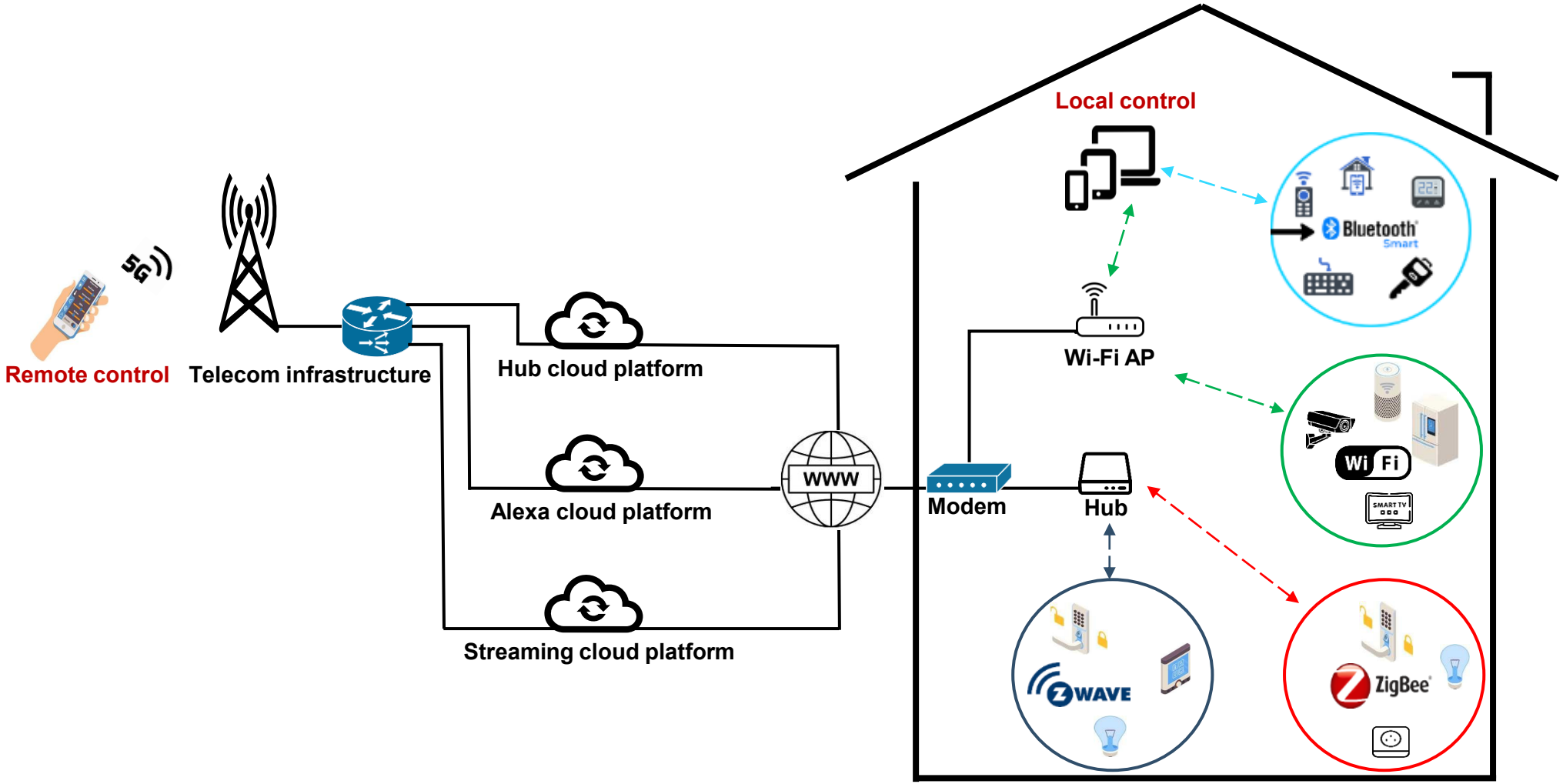
1. Smart Home Systems

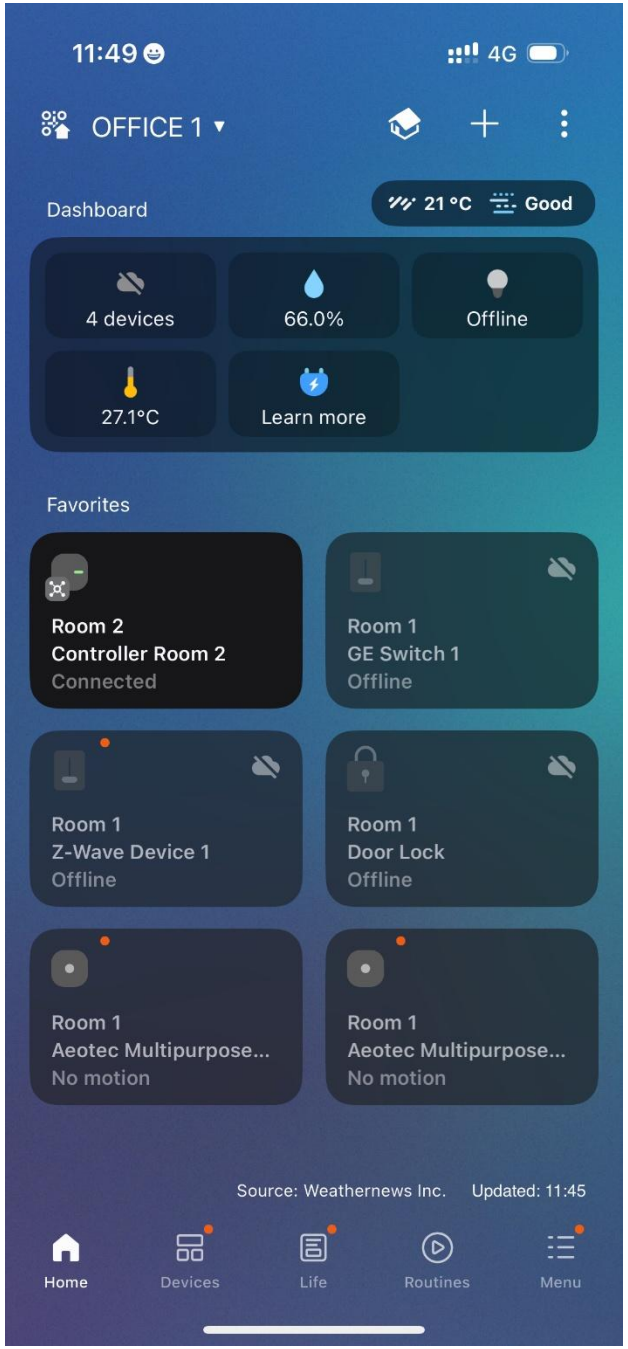
Security, comfort, convenience, and energy efficiency

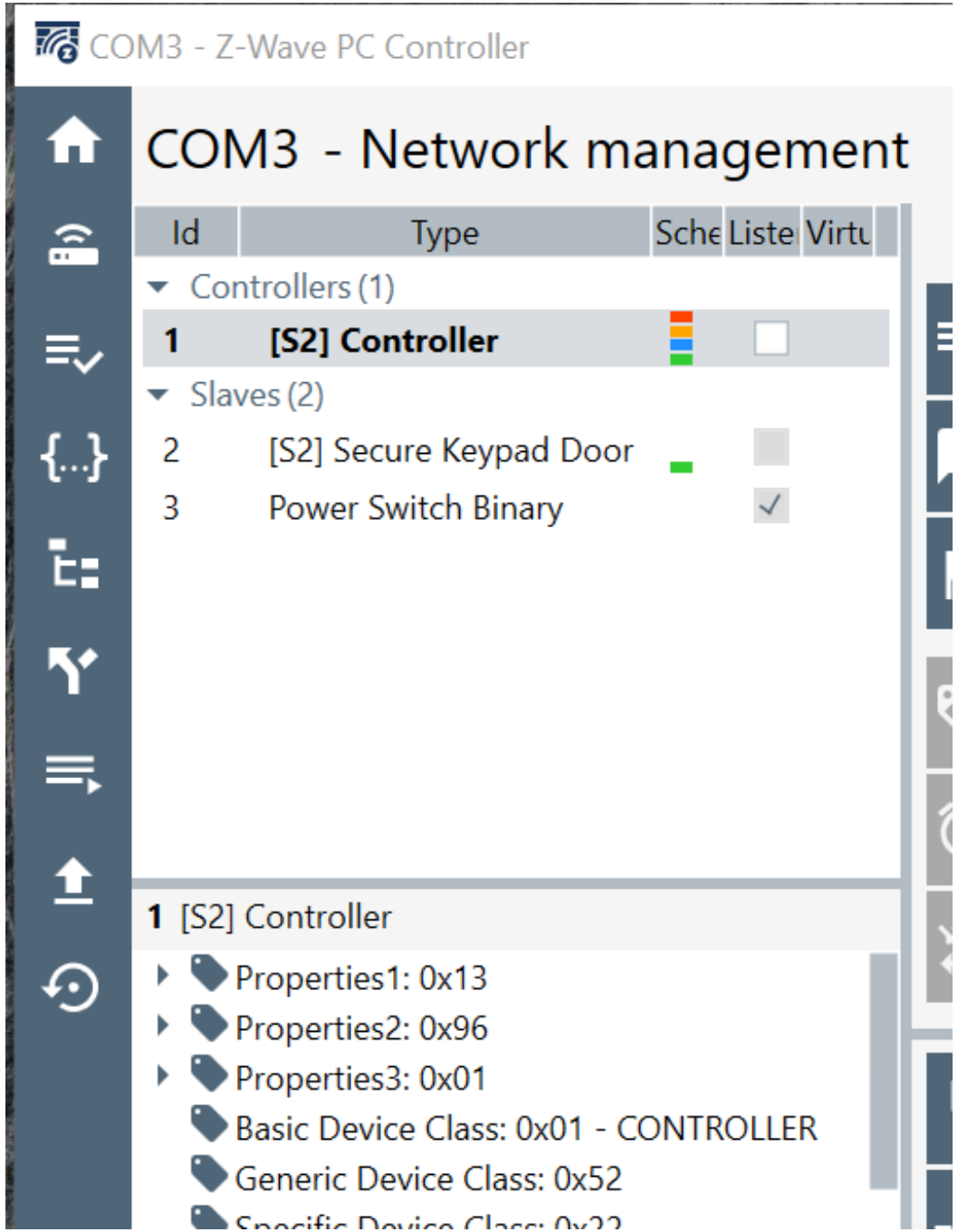
- Interconnected devices and technology to enhance efficiency, security, and convenience by allowing residents to control and automate various aspects of their home through the Internet

1. Smart Home Systems

Smart home may include several IoT devices using different protocols




11:49
4G
OFFICE 1
Dashboard
21 °C
Good
4 devices
66.0%
Offline
27.1°C
Learn more
Favorites
Room 2
Controller Room 2
Connected
Room 1
GE Switch 1
Offline
Room 1
Z-Wave Device 1
Offline
Room 1
Door Lock
Offline
Room 1
Aeotec Multipurpose...
No motion
Room 1
Aeotec Multipurpose...
No motion
Source: Weathernews Inc.
Updated: 11:45
Home
Devices
Life
Routines
Menu


COM3 - Z-Wave PC Controller
COM3 - Network management
Id
Type
Sche
Liste
Virtu
Controllers (1)
1 [S2] Controller
Slaves (2)
2 [S2] Secure Keypad Door
3 Power Switch Binary
1 [S2] Controller
Properties1: 0x13
Properties2: 0x96
Properties3: 0x01
Basic Device Class: 0x01 - CONTROLLER
Generic Device Class: 0x52

1. Smart Home Systems

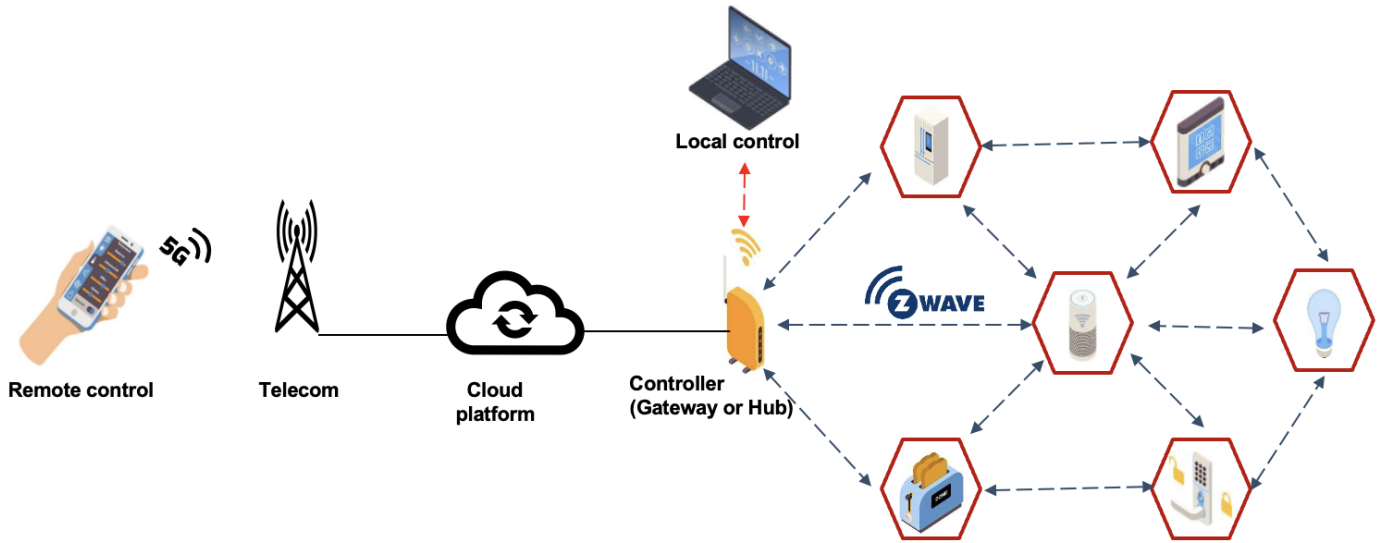
Z-Wave protocol

- Prominent protocol used in smart homes (e.g., USA)
- Mesh network using low-energy radio waves
- Use sub-Gig frequencies: no interference from Wi-Fi or other 2.4 GHz technologies
- Extends range as devices can be repeaters
- Commonly used for several sensors (light, thermostats, alarms, door locks, energy and water management)

1. Smart Home Systems

Z-Wave transport encapsulation scheme

- **CS8/CRC-16**
  - Data is **unencrypted** and relies on basic checksums
- **Security 0 (S0)**
  - S0 uses AES-128 but is vulnerable to MITM due to a fixed key during pairing
- **Security 2 (S2)**
  - S2 improves security with ECDH-based key exchange



1. Smart Home Systems

Z-Wave smart home setup

1. Smart Home Systems

Z-Wave alliance

- Z-Wave alliance includes more than 800 companies developing over 4,500 certified and interoperable products with over 100 million sold devices

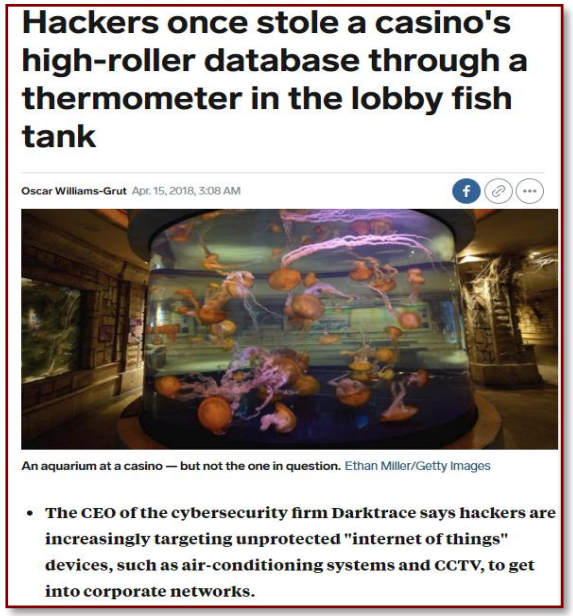
https://z-wavealliance.org/z-wave-alliance-member-companies/

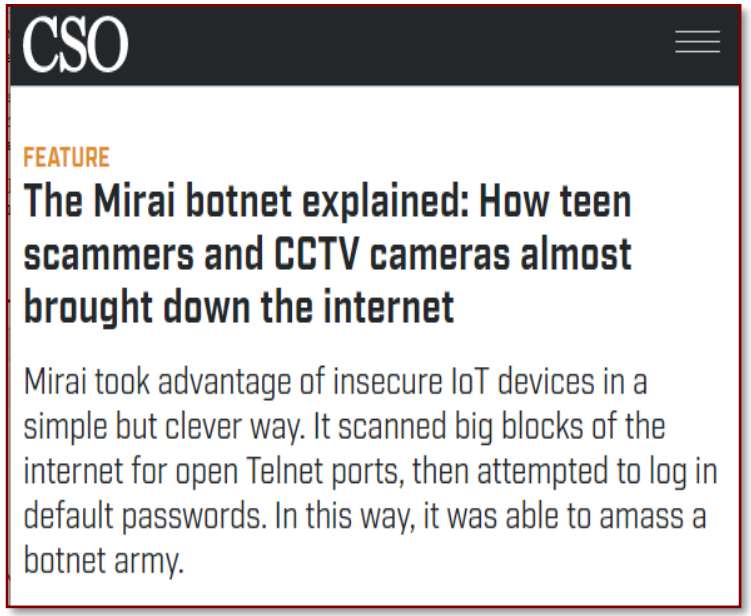
2. Security Issues

2. Security Issues

Vulnerabilities in **smart devices are hard to patch and mitigate**

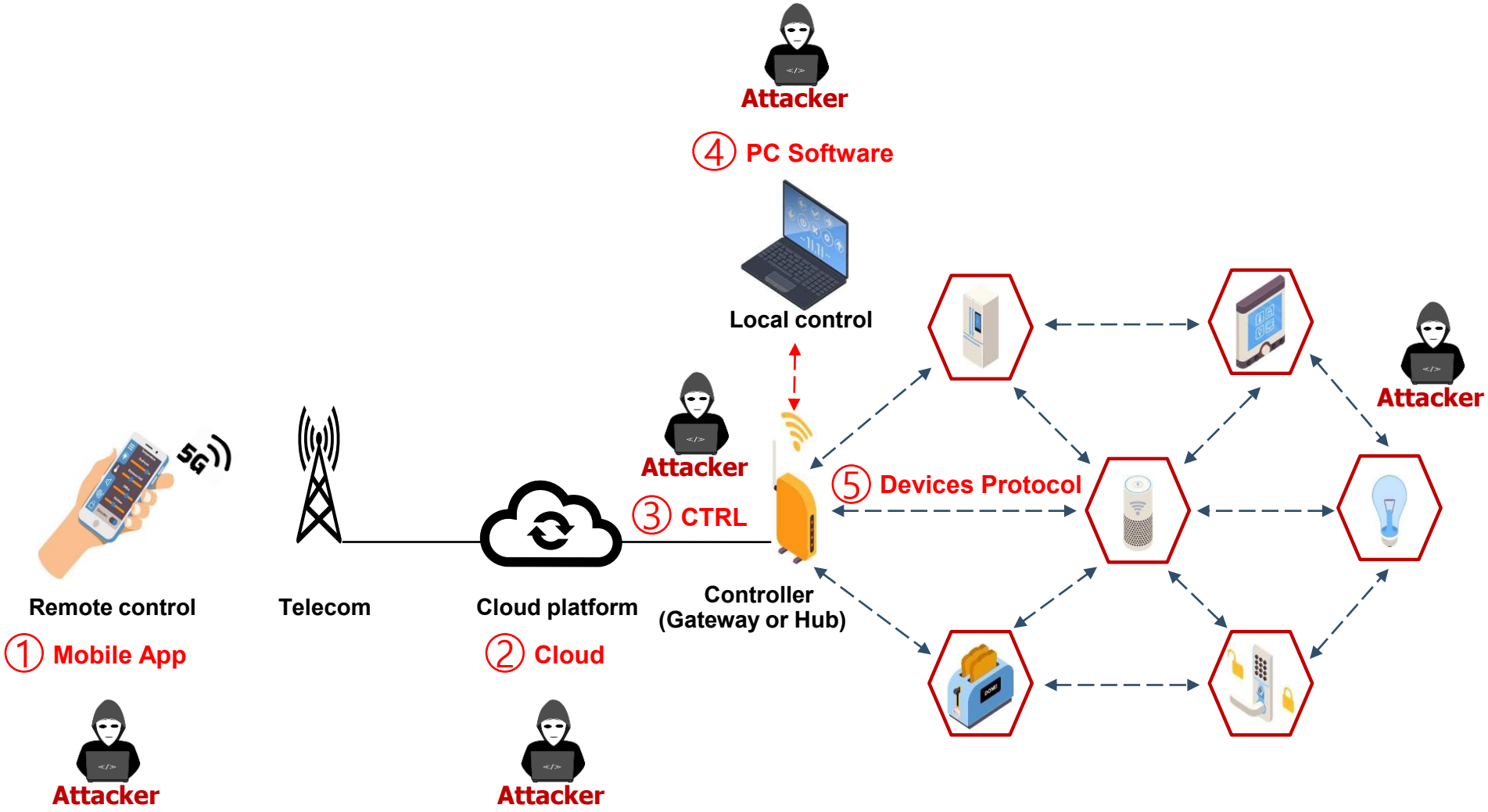
- As smart homes devices are control over the Internet; thus, vulnerabilities in devices could be exploited by hackers to attack also **traditional IT systems**





2. Security Issues

Attack vectors in smart home



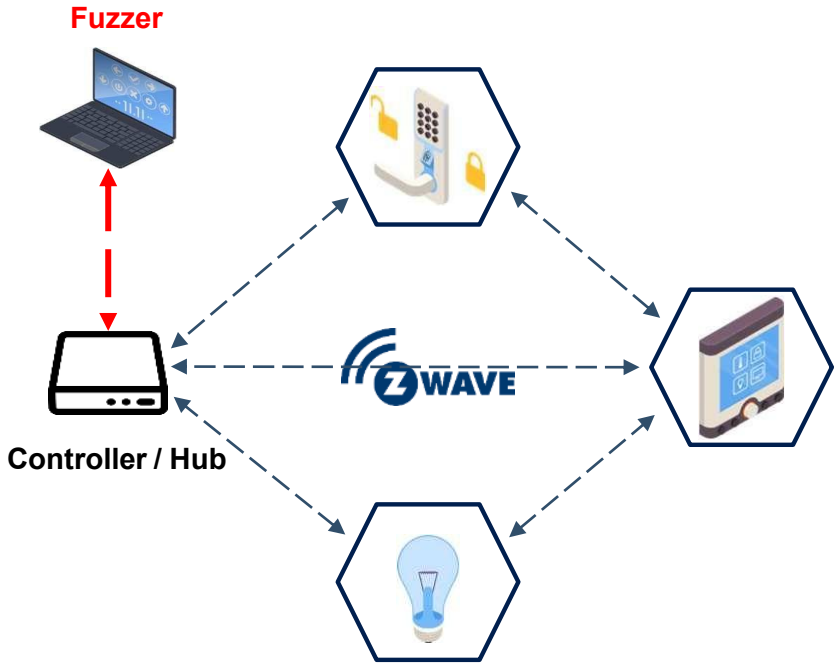
3. ZCOVER

- Find vulnerabilities in main Z-Wave controller to help manufacturers mitigate the risk and protect end-users
- ZCOVER looks at the correctness of controller implementations' handling of application layer payload

3. ZCOVER

ZCOVER checks how controllers handle application-layer payloads

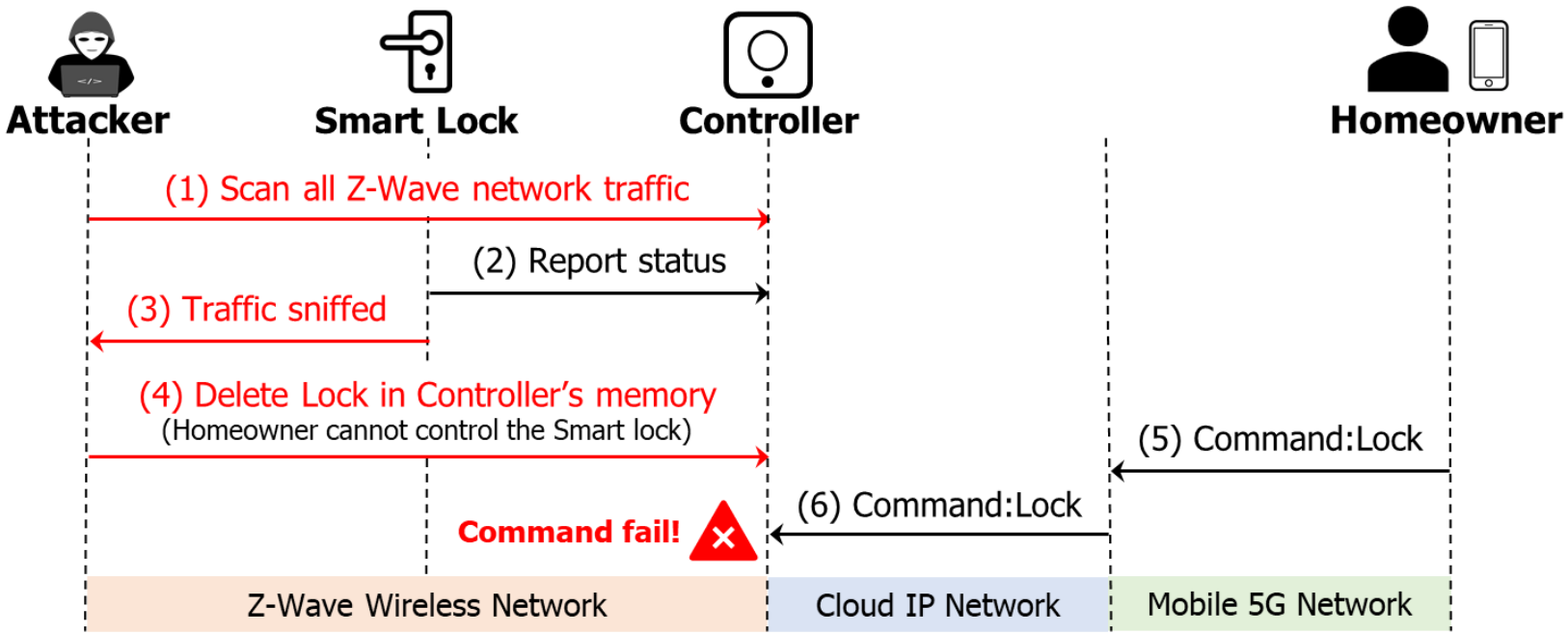
- **Fuzz the controller as an outsider**
  - Mimic an external attack (high impact)
  - No need to encryption key
  - We just test implementations of controller's application layer



3. ZCOVER

Threat model

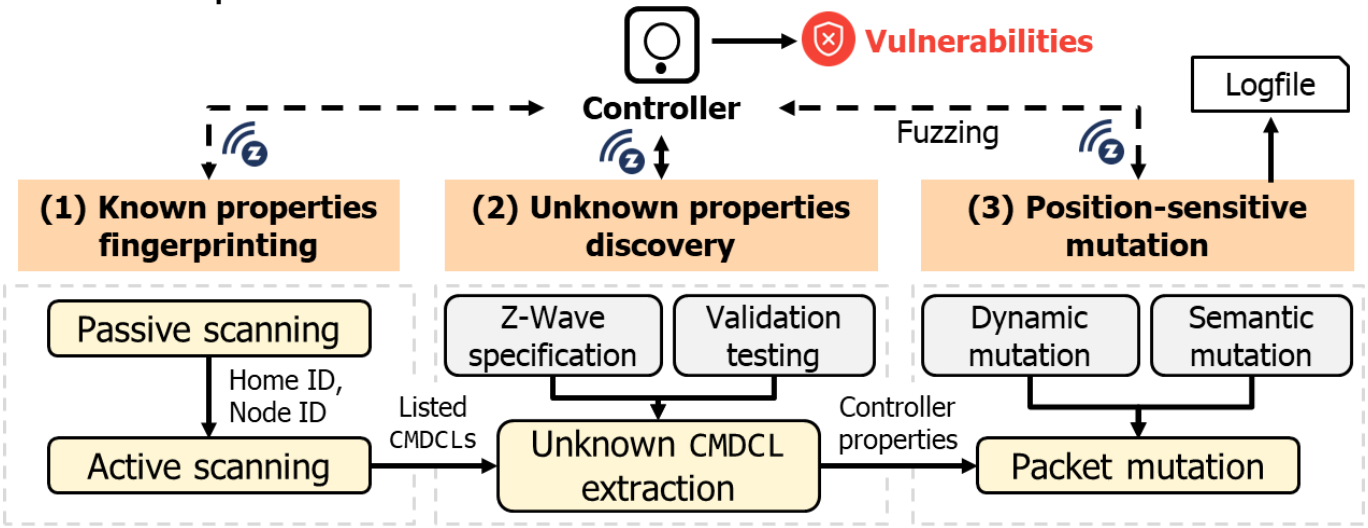
- **Attacker**
  - Sniffs the Z-Wave network to get needed information (e.g., home ID)
  - Sends malicious Z-Wave packet to delete the controller's internal memory of devices



3. ZCOVER

Overview

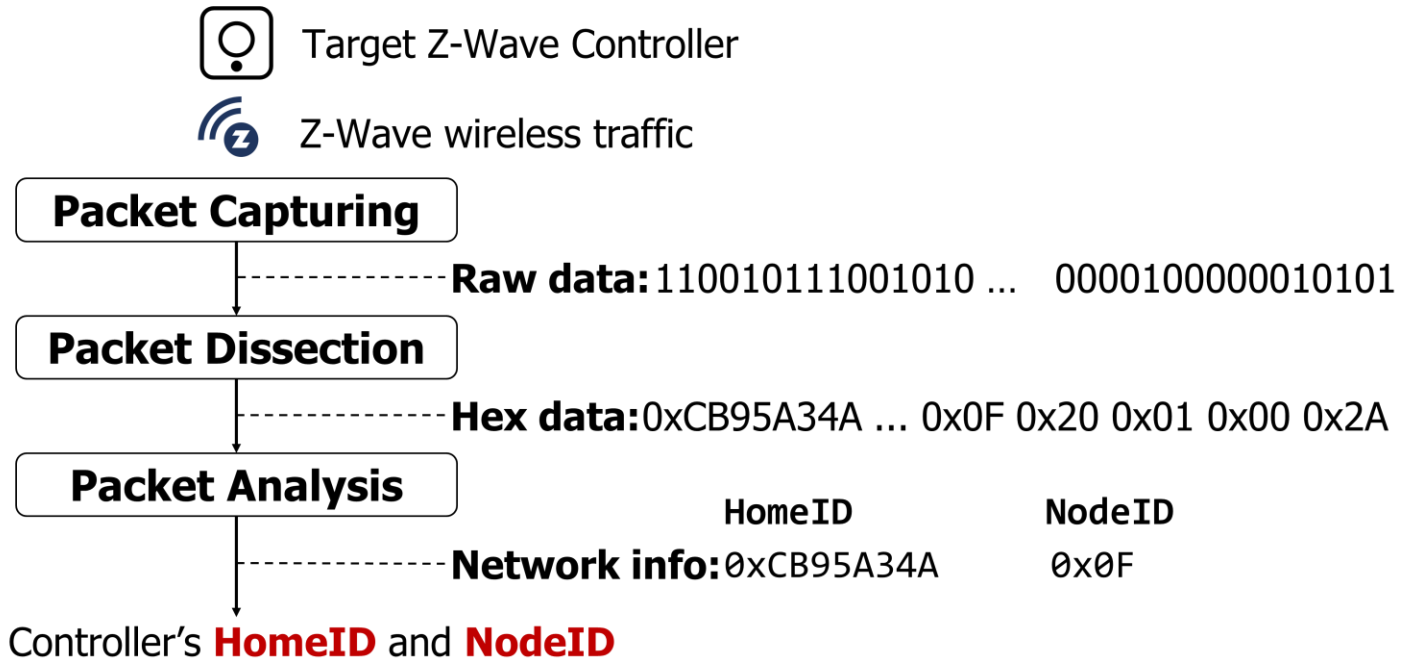
- **Known properties fingerprinting**
  - Sniffs Z-Wave traffic from a target controller to get network information such as home ID
  - Conducts device reconnaissance to retrieve **public known properties** such as listed supported CMDCLs
- **Unknown properties discovery**
  - Uses specification to **uncover hidden** or **unlisted CMDCLs** based on the controller's classification
- **Position-sensitive mutation**
  - Sends the extracted properties to the mutator, which generates test cases by mutating payloads based on CMDCL structure and packet semantics



3. ZCOVER

Passive scanning

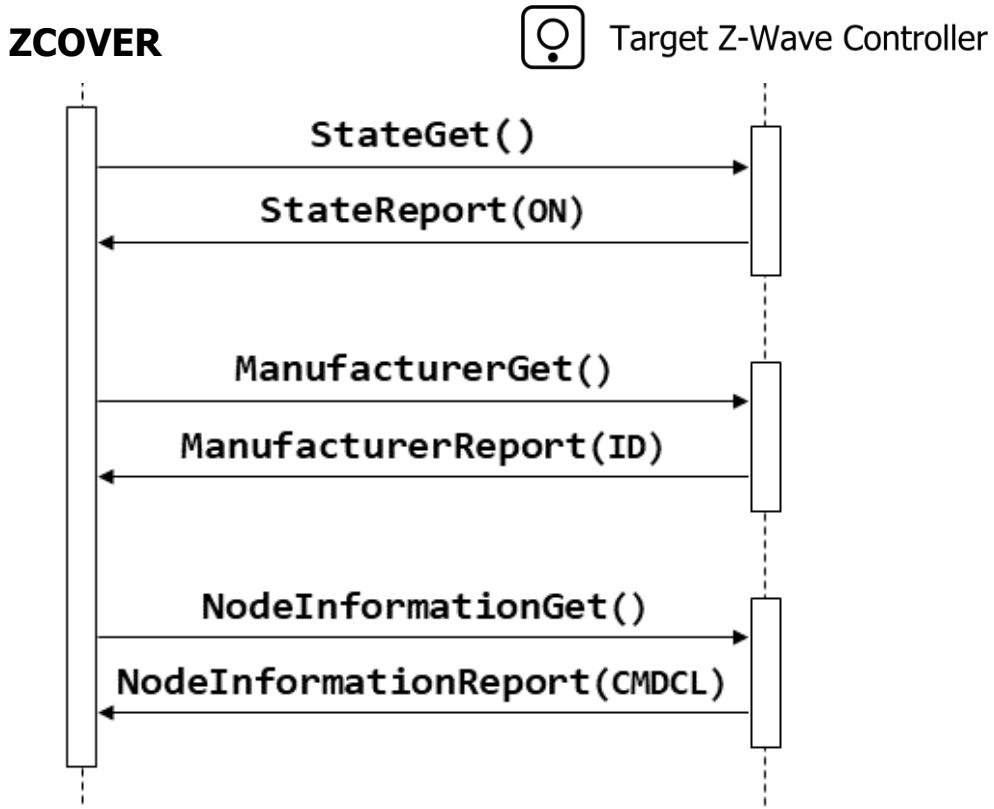
- Retrieve the Z-Wave home ID and devices node ID



3. ZCOVER

Active scanning

- Retrieve the Z-Wave devices and hidden properties



3. ZCOVER

Unknown properties discovery

- **ZCOVER identifies proprietary (i.e., hidden) CMDCLs of the target Z-Wave controller**
  - Often undocumented and known only to manufacturers under a NDA
  - If poorly implemented, these unlisted CMDCLs can be exploited by attackers

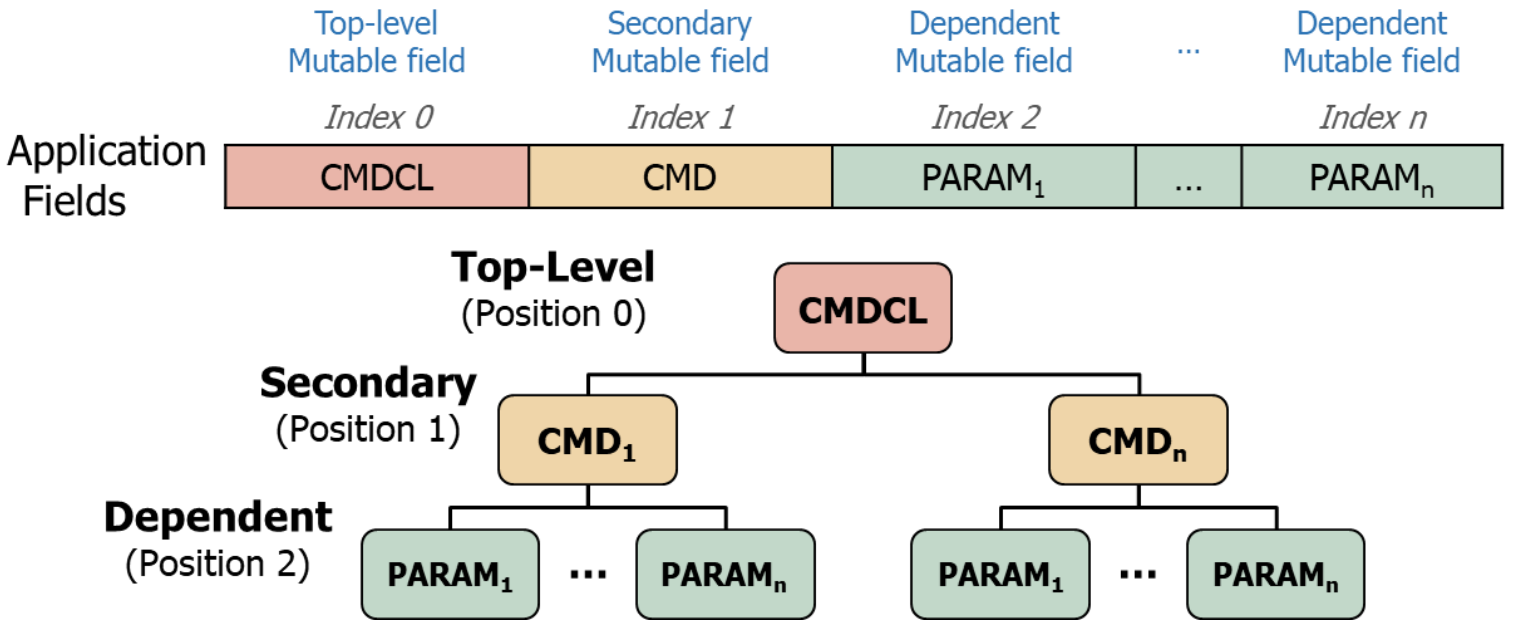
- **Step 1) Leveraging public Z-Wave specification**
  - Understanding this specification is crucial for identifying deviations and potential unlisted proprietary properties related to the controller

- **Step 2) Systematic validation testing**
  - Follows a sequential approach, evaluating **CMDCLs from 0x00** to the **upper limit** of the identified CMDCL list
  - Uncovered two **additional proprietary CMDCLs (0x01 and 0x02)** that were absent from the official Z-Wave specification

3. ZCOVER

Position-sensitive mutation

- Consider the **hierarchical structure** of the Z-Wave **application layer**



3. ZCOVER

Position-sensitive mutation

- Ensures **valid test packets** that maximize **fuzzing effectiveness** and **avoid rejection**

CD F8 A1 43	01	5108	0D	18	25	01	FF	49
Home ID	SRC	FC	LEN	DST	CMDCL	CMD	PARAM	CRC
F	F	F	D	F	M_A	M_A	M_A	D

[Z-Wave frame example: SWITCH ON]

CD F8 A1 43	C8	5108	Added	01	25	0D	0F FF	Added
Home ID	SRC	FC	LEN	DST	CMDCL	CMD	PARAM	CRC

[Sample of mutated Z-Wave frame testing the application layer]

4. Evaluation

- Evaluate several devices from different vendors
- Found critical vulnerabilities

4. Evaluation

Tested devices details information

IDX	Brand name	Device type	Model (year)	Encryption support*
D1	ZooZ	Controller	ZST10 (2022)	Yes
D2	SiLab	Controller	UZB-7(2019)	Yes
D3	Nortek	Controller	HUSBZB-1 (2015)	Yes
D4	Aeotec	Controller	ZW090-A (2015)	Yes
D5	ZWaveMe	Controller	ZMEUUZB1 (2015)	Yes
D6	Samsung	Controller	ET-WV520 (2017)	Yes
D7	Samsung	Controller	STH-ETH-200 (2015)	Yes
D8	Schlage †	Door Lock	BE469ZP (2019)	Yes
D9	GE Jasco †	Smart Switch	ZW4201 (2016)	No

*Encryption support: whether or not the device supports data encryption.
† Slave devices D8 & D9 are added to create a realistic smart home.

4. Evaluation

Discovered 15 zero-day vulnerabilities and 13 CVEs assigned by US. MITRE and SiLabs

TABLE III: Zero-day vulnerability discovery results of ZCOVER. For ethical reasons, full packet payloads are not disclosed.

Bug ID	Affected devices	CMDCL	CMD	Description	Duration	Root cause	Confirmed
01	D1 - D7	0x01	0x0D	Memory corruption in existing device properties.	Infinite*	Specification	CVE-2024-50929
02	D1 - D7	0x01	0x0D	Fake device insertion into controller's memory.	Infinite	Specification	CVE-2024-50920
03	D1 - D7	0x01	0x0D	Remove valid device in the controller's memory.	Infinite	Specification	CVE-2024-50931
04	D1 - D7	0x01	0x0D	Overwriting the controller's device database.	Infinite	Specification	CVE-2024-50930
05	D6 and D7	0x01	0x02	DoS on smartphone app.	Infinite	Specification	CVE-2024-50921
06	D1 - D5	0x9F	0x01	Z-Wave PC controller program crash.	Infinite	Implementation	CVE-2023-6640
07	D1 - D7	0x5A	0x01	Service interruption during the attack.	68 sec	Specification	CVE-2023-6533
08	D1 - D7	0x59	0x03	Service interruption during the attack.	67 sec	Specification	CVE-2024-50924
09	D1 - D7	0x7A	0x01	Service interruption during the attack.	63 sec	Specification	CVE-2023-6642
10	D1 - D7	0x86	0x13	Service interruption during the attack.	4 sec	Specification	CVE-2023-6641
11	D1 - D7	0x59	0x05	Service interruption during the attack.	62 sec	Specification	CVE-2023-6643
12	D1 - D7	0x01	0x0D	Remove the device's wakeup interval value.	Infinite	Specification	CVE-2024-50928
13	D1 - D5	0x73	0x04	Dos on the Z-Wave PC controller program.	Infinite	Implementation	✓
14	D1 - D7	0x01	0x04	Z-Wave controller service disruption.	4 min	Specification	✓
15	D1 - D7	0x7A	0x03	Service interruption during the attack.	59 sec	Specification	✓

*Infinite: Users cannot control their devices. ✓: Vendors acknowledged the reported bugs.

4. Evaluation

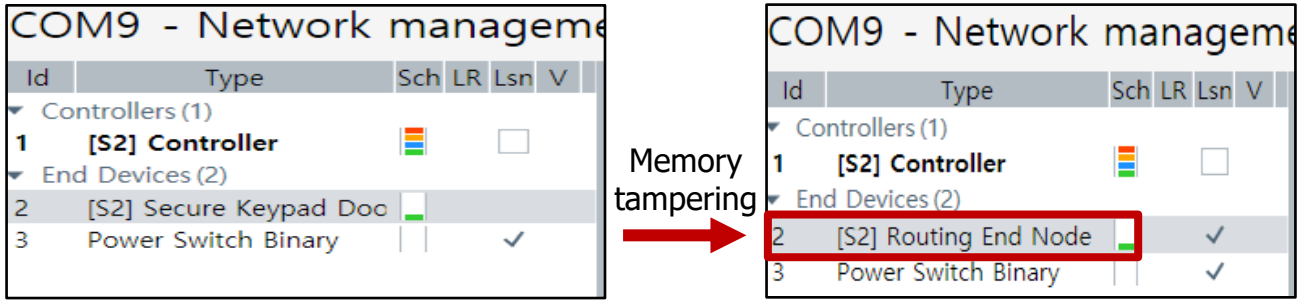
Changing properties of saved devices

- **Exploit Z-Wave specifications and implementation flaws**
  - **<u>CMDCL: 0x01, CMD: 0x0D</u>**

    → This CMDCL should undergo encryption for processing;
    However, we discovered its acceptance of non-encrypted Z-Wave packets

- **Attack impact**
  - Homeowner cannot control affected devices

```
## Memory tampering: Changing existing devices properties
## Vulnerable CMDCL x01 x0D New Node Registered
## Target Node is x02 after \x01\x0d\
test = generate_packet(homeID,
                       "\x41\x01", '\xc8','\x01',
                       "\x01\x0d\x02"+"\xcb\x59\xe0\x28\x07\x54\x8b\xc8")
for _ in range(2):
    d1.RFxmit(invert(test))
    time.sleep(0.25)
```



4. Evaluation

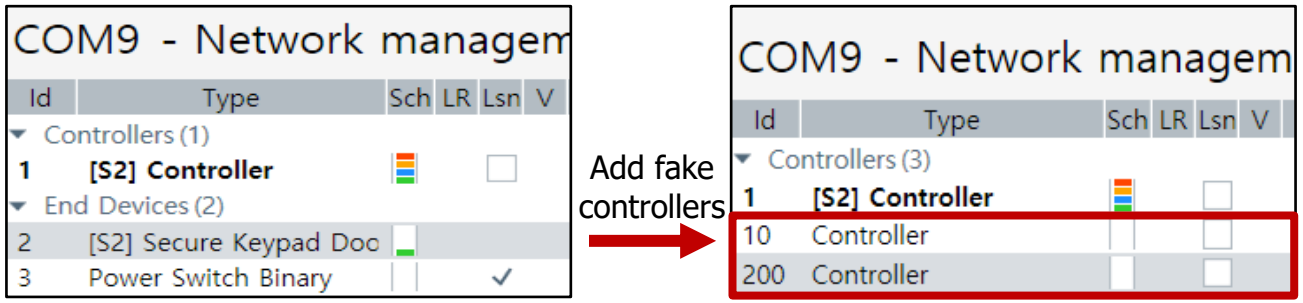
Inserting rogue secondary controllers in main controller memory

- **Exploit Z-Wave specifications and implementation flaws**
  - **CMDCL: 0x01, CMD: 0x0D**

    → These rogue devices can compromise security by serving as entry points for attackers, intercepting and manipulating data, and causing system instability or malfunction

- **Attack impact**
  - Retrieve network internal configurations

```
## Memory tampering: Inserting Rogue Devices
## Fake node ID 0x0A= 10 Insertion
test = generate_packet(homeID, "\x41\x01", '\xc8','\x01',
                               "\x01\x0d\x0a"+"\x0d\x9a\x48\x7c\x5e\xec\x04")
for _ in range(2):
    d1.RFxmit(invert(test))
```



4. Evaluation

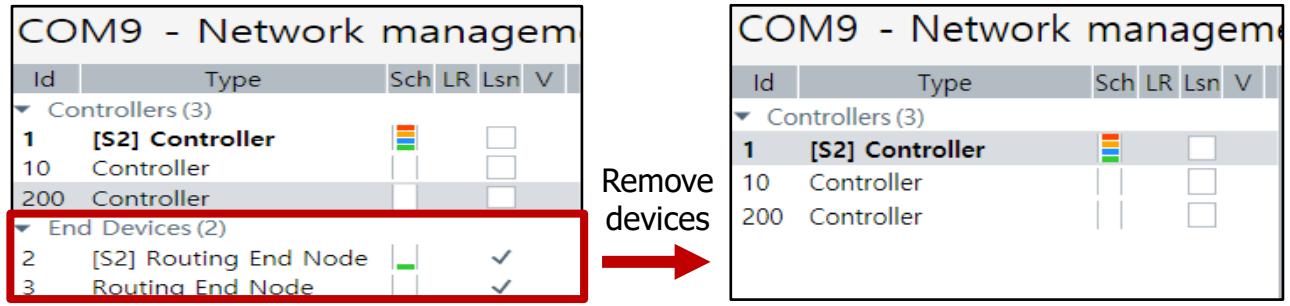
Memory tampering attack: erasing devices in controller memory

- **Exploit Z-Wave specifications and implementation flaws**
  - **<u>CMDCL: 0x01, CMD: 0x0D</u>**

    → Removing a valid device from the smart home controller memory can significantly impact functionality, security, and user experience

    → This necessitates re-configuring settings and routines, leading to user inconvenience and frustration

- **Attack impact**
  - Homeowner cannot use its devices



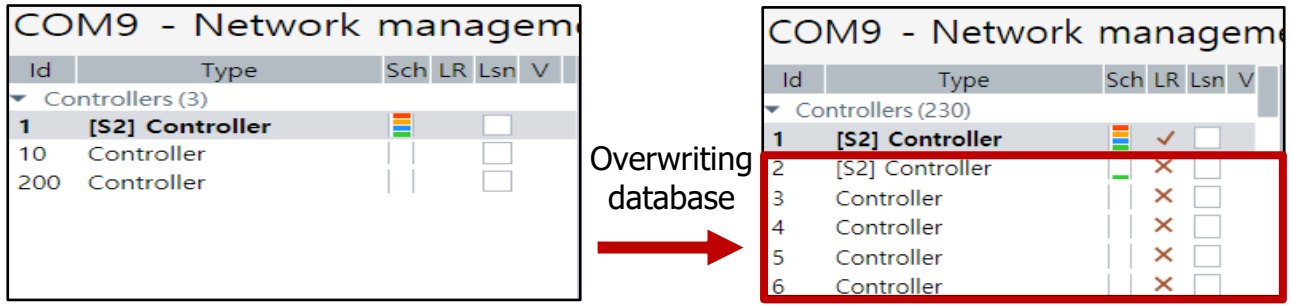
4. Evaluation

Overwriting the controller's device table database with fake devices

- **Exploit Z-Wave specifications and implementation flaws**
  - **<u>CMDCL: 0x01, CMD: 0x0D</u>**
- **Attack impact**
  - Erase all pre-configured automations and scenes

    → This leads to loss of device configurations and disrupts automation, causing inconsistent behavior and service interruptions

    → Without backups, critical data may be permanently lost, making recovery difficult and time-consuming
- **Require a factory reset and reconfiguration of all devices and automations**



4. Evaluation

Short demo video

- **Z-Wave network with 3 devices**
  - S2 controller **ID 1**
  - S2 secure keypad door lock **ID 2**
  - Power switch **ID 3**

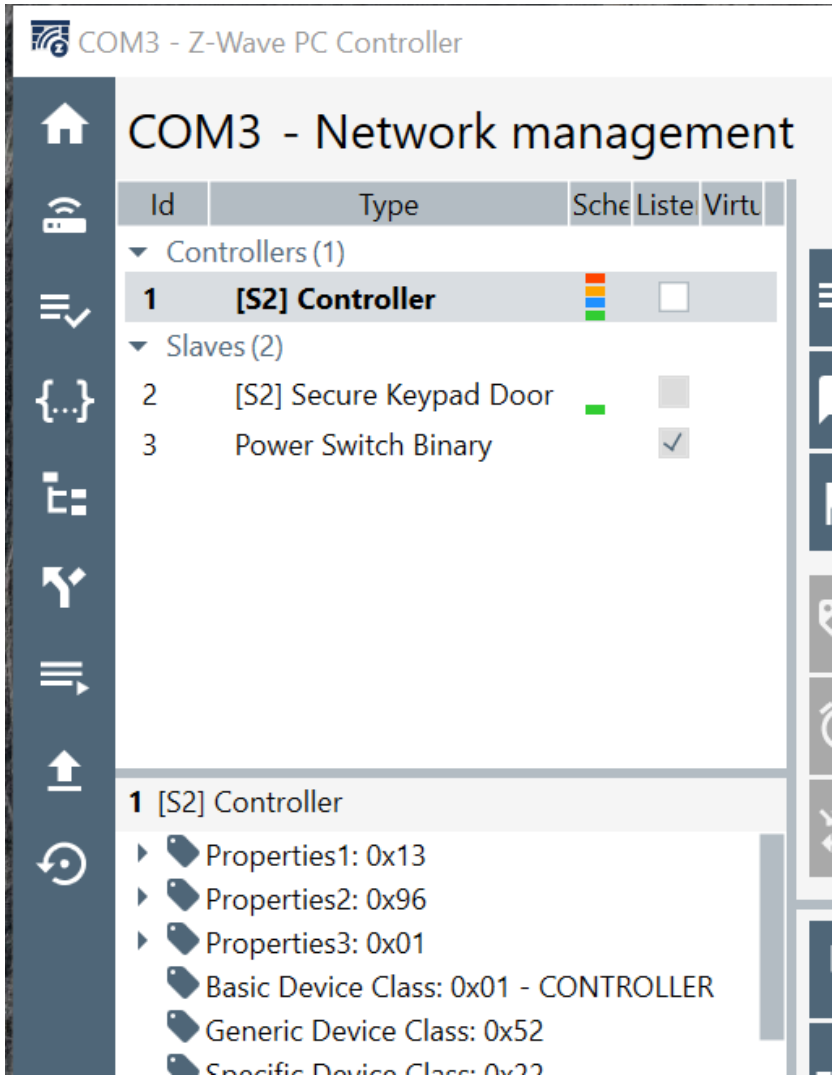
- **Attacker**
  - Raspberry pi
  - Yardstick dongle transceiver
  - Small keyboard
  - No need of Internet to launch the attack
  - Attack range: ~70m and can be extended with RF amplifiers

4. Evaluation

Normal network vs Attacked network

- **Z-Wave network with 3 devices**
  - S2 controller **ID 1**
  - S2 secure keypad door lock **ID 2**
  - Power switch **ID 3**

- **Attack type: Memory corruption**
  - Insertion of **rogue node 10**
  - **Device 3 properties** change
  - **Delete device 2** in memory
  - **Override** device **DB table**

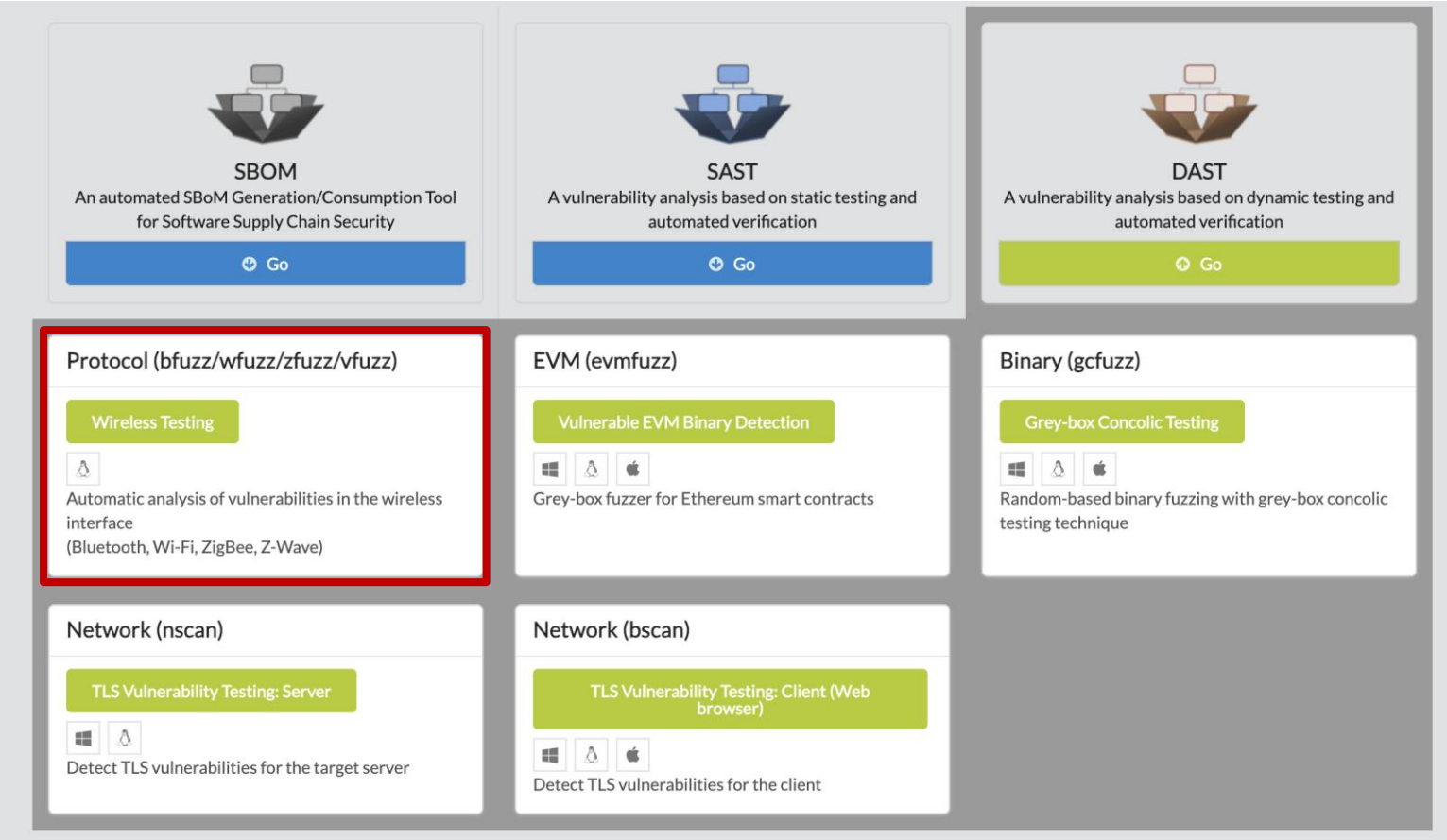


5. Availability

- Evaluate several devices from different vendors
- Found critical vulnerabilities

5. Availability

IOTCUBE.NET is an open-source framework for security analysis

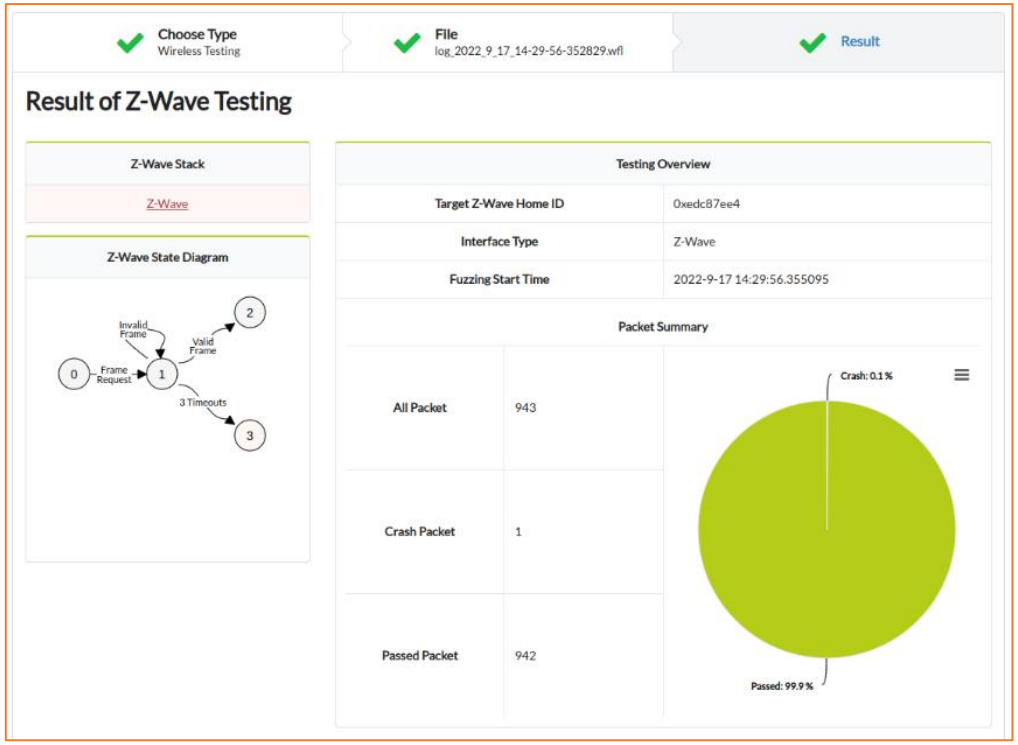


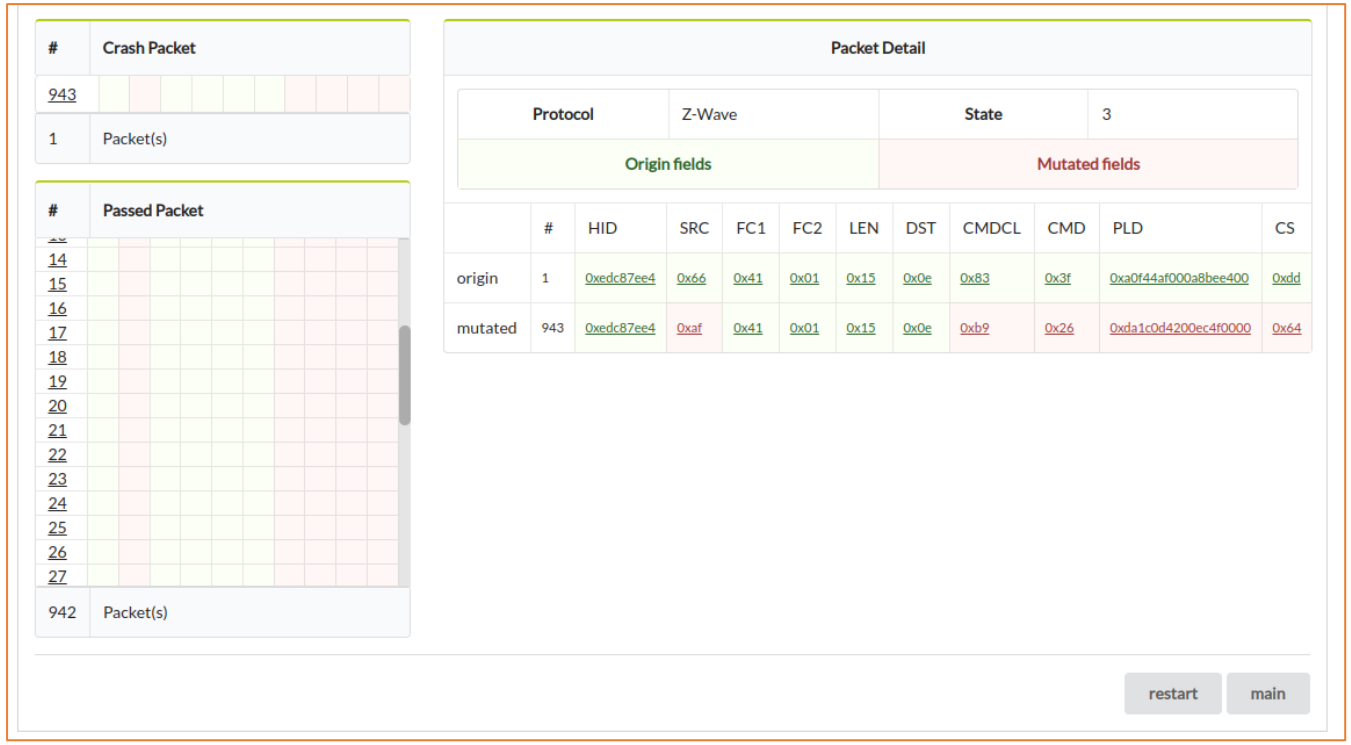
https://iotcube.net/

5. Availability

IOTCUBE.NET is an open-source framework for security analysis

- Better UI and easy debug visualization
- Drop the log file to see details





5. Availability

ZCOVER is open-source and available online

- **Web link**
  - https://ccs.korea.ac.kr/pds/Vulnerabilities_in_ZWave.html
  - https://github.com/CNK2100/ZCOVER_PUBLIC
- **CVE link**
  - https://github.com/CNK2100/2024-CVE/blob/main/README.md
- **Proof-of-concept attack scenarios**
  - https://drive.google.com/file/d/1LBycOFbQThFxuGedefVfNqNa0TbTE0R0/view
  - https://drive.google.com/file/d/1aZMcGRUVtweYkWlcHzWRsl1jhp1nSBYs/view

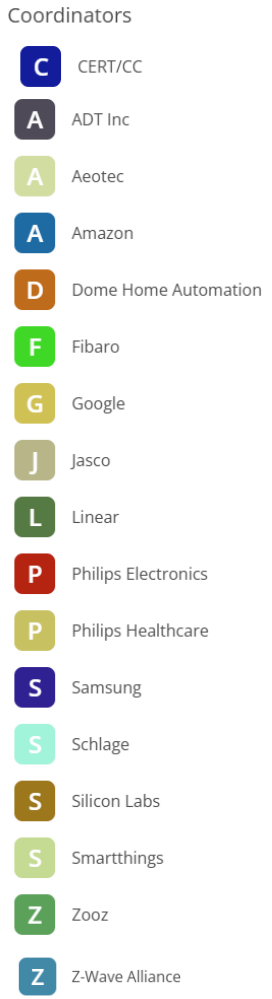
6. Countermeasures

- Worked with 19 vendors to mitigates found vulnerabilities

6. Countermeasures

We worked with US CERT/CC and MITRE with 19 vendors to fix found vulnerabilities

- **To address the discovered vulnerabilities, S2 devices should block malicious payloads via updated specifications**
- **For legacy devices (OTP), smart home should use lightweight IDS (e.g., ZMAD) to alert on discovered attacks**
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10148964
- **We collaborate with SiLabs and vendors**
  - Mitigation plans and SDK updates were confirmed, and our findings will be reflected in the next Z-Wave specification update
  - SiLabs issued two Security Advisory (A-00000502, A-00000505), which can be accessible after creating a free account
    - → https://community.silabs.com/s/alert/a45Vm00000000knIAA/a00000502
    - → https://community.silabs.com/s/contentdocument/069Vm000002020u



7. Lesson Learned & Final Thoughts

7. Lesson Learned & Final Thoughts

IoT security needs to be a priority as devices are increasing significantly

- **100+ million of Z-Wave devices are vulnerable**
- **Security should be high priority in IoT device development**
  - Firmware update is difficult and impossible on legacy devices
  - Vendors should stop security by obscurity practice but adopt best security practices using well-established cryptographic algorithms, protocol, and security measures
- **Flaws mitigations are difficult to implement**
  - Require a joint effort from both the protocol designer and the IoT manufacturer
- **Z-Wave protocol should disable insecure portions of legacy functionalities**
  - Issue with backward compatibility
- **Vendors should restrict vulnerable CMDCL on Z-Wave devices**
- **Smart home users should be aware of the security risks of IoT devices**

7. Lesson Learned & Final Thoughts

References

- C. K. Nkuba, J. Kang, S. Woo, and H. Lee, ”ZCOVER: Uncovering Z-Wave Controller Vulnerabilities Through Systematic Security Analysis of Application Layer Implementation“, IFIP International Conference on Dependable Systems and Networks (DSN), 2025.
- C. K. Nkuba, S. Woo, H. Lee and S. Dietrich, "ZMAD: Lightweight Model-Based Anomaly Detection for the Structured Z-Wave Protocol," in IEEE Access, vol. 11, pp. 60562-60577, 2023, doi: 10.1109/ACCESS.2023.3285476.
- **IoTCube**, Wireless Testing, Online: https://iotcube.net/process/type/bf1
- **Center for Software Security and Assurance (CSSA)**, Online: https://cssa.korea.ac.kr/
- **Computer & Communication Security Laboratory (CCS Lab)**, Online: https://ccs.korea.ac.kr/

Q&A

Thank you very much for your attention and your time!

Nkuba Kayembe Carlos

- **Email:** carlosnkuba@korea.ac.kr
- **LinkedIn:** https://www.linkedin.com/in/carlos-nkuba/
- **Center for Software and Security Assurance:** https://cssa.korea.ac.kr/
- **Computer and Communication Security Laboratory:** https://ccs.korea.ac.kr/
- **Korea University:** https://www.korea.edu/

고려대학교 정보대학
Korea University
College of Informatics

고려대학교 소프트웨어보안연구소
Korea University
Center for Software Security and Assurance

CCSLAB
Computer & Communication
Security Laboratory