INL/EXP-24-79459-Revision-0

Zapiary: Creating Visibility in IOT Networks

August 2024

Claire E. Westby

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-24-79459-Revision-0

Zapiary: Creating Visibility in IOT Networks

Claire E. Westby

August 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Zapiary: Creating Visibility in IOT Networks

Claire Westby | University of Idaho | D520 | Mentor: Rita Foster, Manuel Vazquez Jr

Abstract

Zigbee[1] and **Z-Wave**[2] are the main networking protocols used by low-power Internet of Things **(IOT)** devices. These protocols use low frequencies. Mesh architecture, and unique address formats that make them not compatible with traditional network traffic tools like IX-Discovery Tools[3]. **Zapiary** is a software that takes CSV files with Zigbee and Z-Wave traffic and generates Structured Threat Information eXpression **(STIX)**[4] JSON bundles illustrating communication happening within IOT networks. The bundles can then be viewed within Structured Threat Intelligence Graph **(STIG)**[5] or used within **AI/ML** models to provide **deeper visibility into nodes** that make up the network and the ability to **trend the mesh network over time.**

Problem

No program available to visualize and analyze the traffic for most of our IOT devices due to their usage of Zigbee and Z-Wave networking protocols. We needed to increase visibility into IOT networks and automate Codified Attack Surface (CAS) creation to better understand the network and security functionalities of these devices.

STIX & STIG

STIX is a language created to easily share cyber threat and infrastructure information in JSON code. STIX bundles can then be visualized using STIG. Having network information in this format allows for the creation of standardized codified models of the network architecture that can be visualized in STIG or analyzed as structured data.

Image 1: STIX object in JSON code

```
"type": "network-traffic",
"spec_version": "2.1",
"id": "network-traffic--28339a47-fd2a-585e-b5a3-3e51357b3c1c",
"end": "2023-08-08T17:19:27.068896Z",
"is_active": false,
"src_ref": "ipv4-addr--862397b6-4732-5956-9e3f-2e0a51093831",
"dst_ref": "ipv4-addr--fe20356f-b83e-570a-8c67-0dca67b46ffd",
"protocols": [
    "ZigBee ZDP",
    "Permit Join Request"
]
```

Impact

- Zapiary creates visibility into IOT device communication through graphing and visualization of network traffic that is currently difficult to analyze.
- It standardizes the traffic into one language to make protocols of varying frequencies the ability to be analyzed together.

Zigbee vs Z-Wave

Zigbee

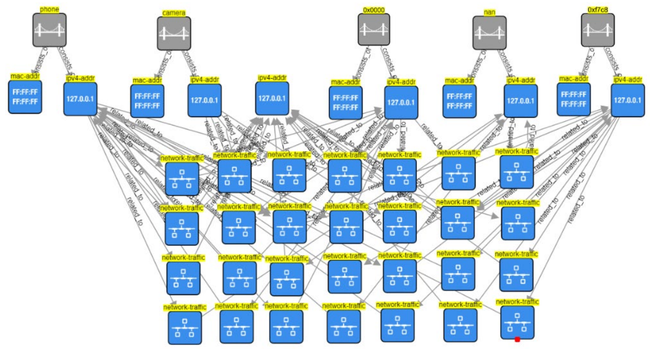
- IEEE 802.15.4-based and open source
- Utilizes 2.4GHz and 915MHz frequencies
- Addresses devices using 16-bit Network Addresses and 64-bit MAC Addresses
- Used more widely and more resources available.
- Significantly faster: 250 kbps vs 100 kbps of Z-Wave

Z-Wave

- Proprietary technology by the Z-Wave Alliance
- Uses 908.42MHz frequency
- Addresses devices using 32-bit Network IDs for the whole network and 8-bit Node IDs for individual devices
- Has stronger security
- Longer range: 100 ft vs 35 ft of Zigbee

Zapiary

Image 2: Network architecture generated by Zapiary



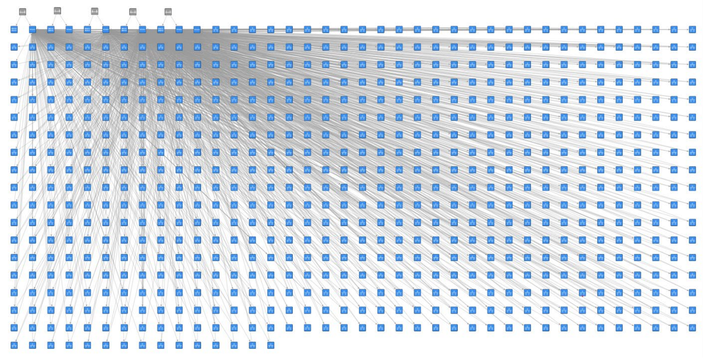


Image 3: All Zigbee network traffic generated by Zapiary

1. Takes a CSV file with traffic captured from IOT devices using Zigbee and Z-Wave networking protocols. Creates Infrastructure objects for each unique node in the network.
2. Generates address objects and relationships for each node.
3. Creates network traffic objects and relationships either for the first instance or every packet in dataset.
    1. Due to the mesh architecture, there will be traffic shown for each hop that is made between physical devices before reaching its destination.

Challenges

- Address Formats
- Sniffing Traffic[6][7]

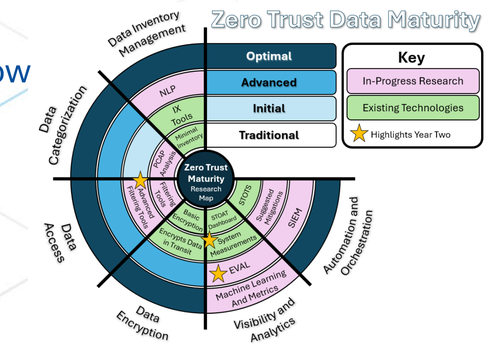
Image 4: Zigbee traffic in a .csv file

No.	Protocol	MAC Src	MAC Dst	NWK Src	NWK Dst	Src 64	UTC date	Info
1	ZigBee	0x9328	0xffff	0x9328	0xfffc	f0:82:c0:ff:fe:76:2b:7c	19:21.0	Link Status
2	ZigBee	0xd810	0xffff	0xd810	0xfffc	38:5b:44:ff:fe:a5:19:68	19:21.8	Link Status
3	ZigBee	0x0000	0xffff	0x0000	0xfffc	00:0d:6f:00:17:f2:15:85	19:26.8	Link Status
4	ZigBee ZDP	0x0000	0xffff	0x0000	0xfffc	00:0d:6f:00:17:f2:15:85	19:27.1	Permit Join Request

Zero Trust for IIOT

- The Zero Trust for Industrial IOT project's main goal is to increase visibility into IOT devices.
- Zapiary provides the ability to understand and analyze how devices are using these protocols to make informed decisions about the security of these devices.

Image 5: Evaluation based on Department of Homeland Security CISA's Zero Trust Maturity Model[6] with extra focus placed on visibility.



References
[1] C. Wang, T. Jiang, and Q. Zhang, *ZigBee Network Protocols and Applications*. CRC Press, 2016.
[2] Silicon Labs, "Z-Wave Dev Documents - v1.0.1 - Z-Wave Silicon Labs," *docs.silabs.com*. https://docs.silabs.com/z-wave/1.0.1/z-wave-docs/overview (accessed Jul. 23, 2024).
[3] idaholab, "idaholab/IX-DiscoveryTools," *GitHub*, Jun. 20, 2024. https://github.com/idaholab/IX-DiscoveryTools (accessed Jul. 23, 2024).
[4] OASIS, "Introduction to STIX," *Github.io*, 2016. https://oasis-open.github.io/cti-documentation/stix/intro.html
[5] idaholab, "idaholab/STIG," *GitHub*, Aug. 27, 2019. https://github.com/idaholab/STIG
[6] Silicon Labs, "Instruction Z-Wave Zniffer User Guide," 2022. Accessed: Jul. 23, 2024. [Online]. Available: https://www.silabs.com/documents/public/user-guides/INS10249-Z-Wave-Zniffer-User-Guide.pdf
[7] V. Alemasov, "homewsn/whsniff," *GitHub*, Jul. 23, 2024. https://github.com/homewsn/whsniff (accessed Jul. 23, 2024).

www.inl.gov INL/EXP-24-79459

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy | Idaho National Laboratory