PNNL-28810

VOLTTRON™ Community Security Report

In collaboration with PNNL's Secure Software Central

May 2019

Chance Younkin
Patrick O'Connell

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov**

PNNL-28810

VOLTTRON™ Community Security Report

In collaboration with PNNL's Secure Software Central

May 2019

Chance Younkin
Patrick O'Connell

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Acronyms and Abbreviations

AWS	Amazon Web Services
CIA	Confidentiality, Integrity, Availability
IDDIL-ATC	Identify Assets, Define the Attack Surface, Decompose the System, Identify Attack Vectors, List the Threat Actors, Analysis & Assessment, Triage, Controls
PII	personally identifiable information
PNNL	Pacific Northwest National Laboratory
SSC	Secure Software Central
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SWG	Security Working Group
UI	user interface

Contents

Acronyms and Abbreviations ii
Contents iii
1.0 Introduction 1
2.0 Background 2
3.0 Definition of Terms 3
4.0 Security Working Group 4
5.0 Use Cases 5
5.1 Use Case 1 – PNNL Campus Deployment 6
5.2 Use Case 2 – Flat Topology Deployment 6
5.3 Use Case 3 – Hierarchical Topology Deployment 8
6.0 Guidance for Development 12
6.1 Preliminary Findings 12
6.2 Areas of Non-Security Development 12
7.0 Next Steps 14
8.0 Summary 15
Appendix A – Microsoft STRIDE Model A.1

Figures

Figure 1. Secure Software Central offerings 2
Figure 2. Lockheed Martin's IDDIL-ATC methodology 2
Figure 3. CIA cybersecurity triad 2
Figure 5. Hierarchical topology VOLTTRON deployment 5
Figure 4. Flat topology VOLTTRON deployment 5
Figure 6. Flat topology use case 6
Figure 7. Hierarchical topology use case 9

Tables

Table 1. Flat topology initial findings 8
Table 2. Hierarchical topology initial findings 11

1.0 Introduction

Our nation’s government, corporations, critical infrastructure, and citizens are in harm’s way in a very expensive, never-ending cyber arms race. In less than a decade, cybersecurity spending has risen by over $60 billion. In June 2015, the U.S. Office of Personnel Management saw 21.5 million social security numbers stolen, along with fingerprints, usernames, and passwords[1]—in just one of numerous incidents. The problem persists, the costs keep rising, and the bad guys keep gaining entry. As a result, new and innovative solutions are needed.

To address this problem, the VOLTTRON™ development team partnered with the Pacific Northwest National Laboratory (PNNL) Secure Software Central (SSC) team in a Threat-Based Software Analysis of the VOLTTRON platform. The context for the analysis was PNNL’s campus deployment and the result was a Threat Profile containing critical assets, prioritized threats, and controls for mitigating those threats. The Threat Profile documents controls already in place, controls not yet in place, and recommendations for implementing controls. As a companion to the software, the Threat Profile shows due diligence in cybersecurity risk management.

The success of the first Threat Profile motivated the need to understand VOLTTRON usage in the wider VOLTTRON community. SSC members formed and now moderate the Security Working Group (SWG) to share information, improve the software security processes, and develop Threat Profiles for other use cases.

This Community Security Report outlines the process for developing a Threat Profile, discusses results of the campus deployment Threat Profile, and describes preliminary Threat Findings for two use cases. These findings will be refined and further analyzed to produce full Threats Profiles for both use cases. In addition, the SWG will continue to identify additional use cases for existing and potential platform users (especially utilities) who have different software needs.

[1] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

2.0 Background

The SSC is a PNNL capability that provides both Threat-Based Software Analysis services and Secure Software Development services to software development efforts. (Figure 1). These services document, understand, and mitigate software vulnerabilities based on secure software life-cycle principles and due diligence threat analysis.

Threat-Based Software Analysis – determines and prioritizes threats against the software system and recommends mitigation controls.

Services include threat models, threat findings, and threat profiles.

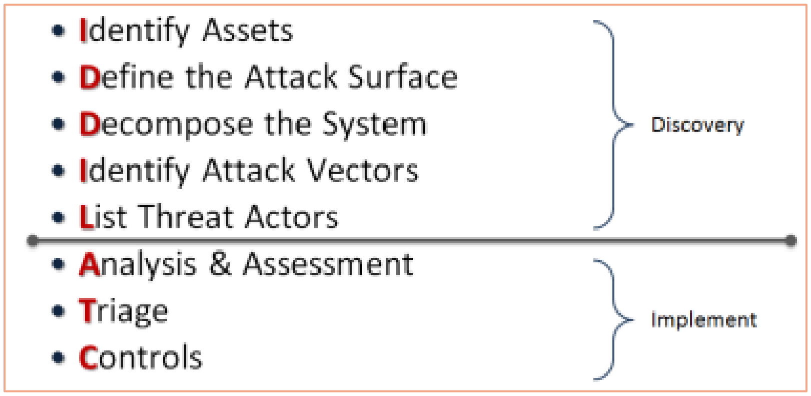
Secure Software Development – provides security methods to the full software life cycle.

Services include secure design, secure code review, and security testing.

Figure 1. Secure Software Central offerings

The Threat-Based Software Analysis provides system diagrams, categorized and prioritized threats, possible attack paths, and mitigation controls against those attack paths. This is represented in a Threat Profile, which was completed for the VOLTTRON campus deployment.

The SSC team uses portions of Lockheed Martin's IDDIL-ATC methodology (Figure 2) to analyze threats for the VOLTTRON system in a campus environment. For the threat model, the team used Microsoft's STRIDE threat categorization model (Appendix A) and Threat Modeling Tool 2016 to identify and categorize threats. Finally, the team used the commonly known CIA triad (Confidentiality, Integrity, Availability) shown in Figure 3 to prioritize the order in which threats should be addressed.



- Identify Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors
- Analysis & Assessment
- Triage
- Controls

Figure 2. Lockheed Martin's IDDIL-ATC methodology

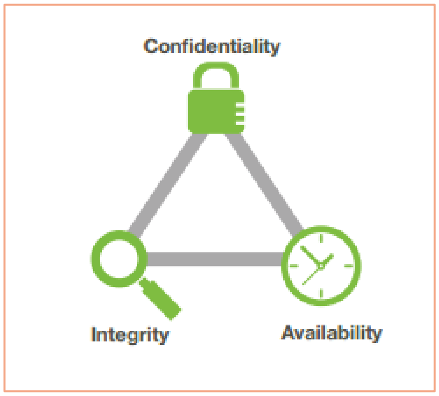


Figure 3. CIA cybersecurity triad

3.0 Definition of Terms

The following are common terms used in this report:

- **Control –** VOLTTRON's control capability is exercised by applications in the deployment to effect changes in set points, damper position, or another controllable point on a device.
- **Data Collection –** VOLTTRON is configured to collect data from devices, publish it to the internal message bus, and store the data in a local or remote storage solution (database, file, etc.).
- **Flat Topology –** All VOLTTRON instances are effectively peers at the same level of the hierarchy. Data storage is performed directly by the platform collecting the data to a local or remote resource.
- **Hierarchical Topology –** Deployed VOLLTRON instances use a tiered topology in which collectors do not store data locally but instead forward to a central VOLTTRON instance which then writes the data. This approach is especially useful in cases where the collectors are on an isolated network.
- **Threat Findings –** An initial threat assessment that contains a threat model diagram, a list of critical assets, a list of categorized and prioritized threats, and a list of resultant conditions should a compromise occur (e.g., "what could go wrong" information).
- **Threat Profile –** A Threat Findings document with an attack path column and a controls column added to the Threat Findings table (e.g., "what to do about it" information).

4.0 Security Working Group

VOLTTRON has an active open source community focused on discussing development issues, requested features, and bug fixes. With the development of the Threat Profile and the SSC capability, the VOLTTRON Security Working Group (SWG) has branched off from that. The purpose of the SWG is to discuss use cases, review Threat Profiles, help prioritize security issues, and provide feedback to the SSC. This valuable communication will improve the value of Threat Profiles, and allow SSC to develop customized Threat Profiles based on newly identified use cases from the community.

The members of the VOLTTRON community most active in the SWG include a renewable development company, building energy management companies, and a university that is part of the Clean Energy Transactive Campus project. The SWG gathers via teleconference and is planning a workshop for August 29-30, 2019 at the Eclipse VOLTTRON Users Meeting.

Anyone with an interest in joining the VOLTTRON SWG should contact the Secure Software Central lead, Chance Younkin (chance.younkin@pnnl.gov) or Jereme Haack (Jereme.haack@pnnl.gov).

5.0 Use Cases

VOLTTRON use cases to date revolve around architecture topology and usage. In some instances, the topology is a flat topology, as shown in see 4. In this case, VOLTTRON data is sent straight from the VOLTTRON collector to a database. In other cases, the topology is hierarchical, as shown in 5. In this case, collection agents receive data and forward it to a central VOLTTRON instance that then stores data in a database.

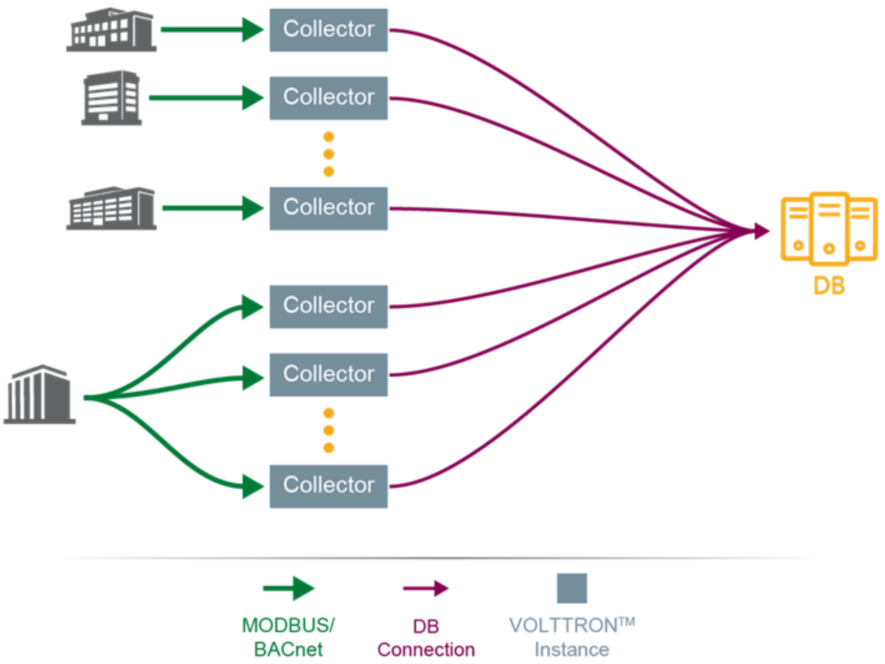


Figure 5. Flat topology VOLTTRON deployment

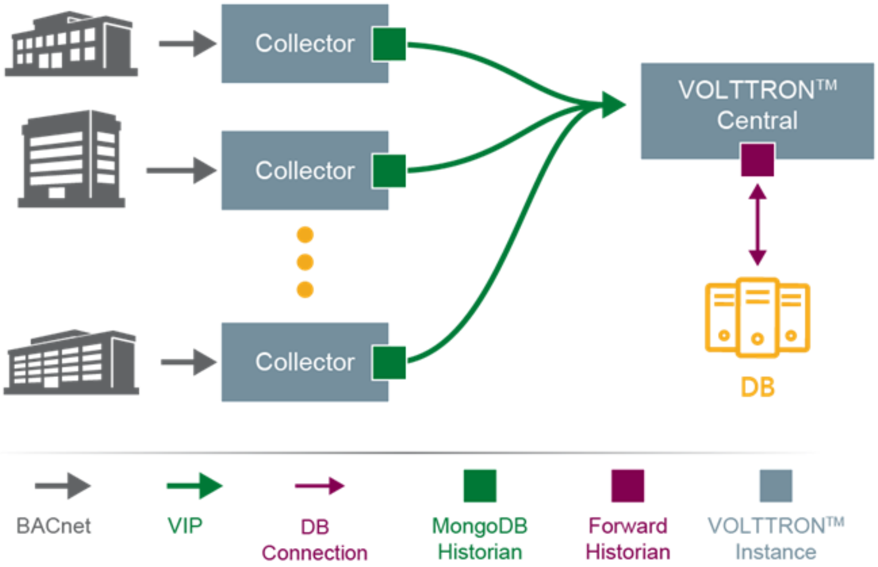


Figure 4. Hierarchical topology VOLTTRON deployment

Usage is categorized as either Data Collection or Control. In the collection case, VOLTTRON is used to collect data only and make it available for use. In the control case, VOLTTRON can be used to physically control the state of devices. In some cases, a deployment is for both data collection and control.

5.1 Use Case 1 – PNNL Campus Deployment

The PNNL Campus is the first use case put through the SSC Threat-Based Software Analysis. This use case represents the hierarchical topology and uses VOLTTRON for both data collection and control. The full Threat Profile[2] was developed and released to the community and is available for review and feedback.

5.2 Use Case 2 – Flat Topology Deployment

The VOLTTRON user community has instances that use the Flat Topology Deployment. RDC was chosen as the first “community-based” example for the flat topology use case. The SWG and RDC are producing a Threat Profile for this use case. The SSC team worked with SWG members to develop initial diagrams (Figure 6), which led to preliminary findings detailed in Table 1.

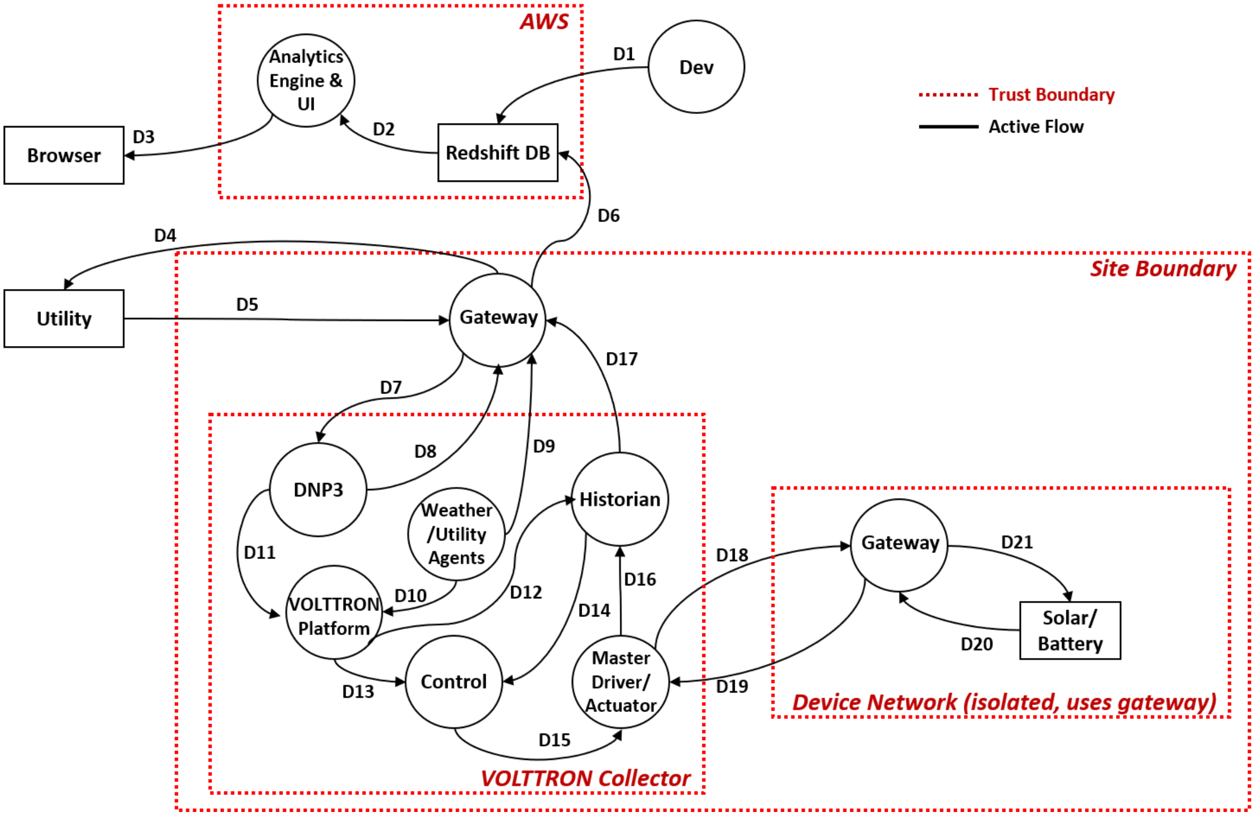


Figure 6. Flat topology use case

[2] The PNNL Campus Threat Profile can be obtained by contacting Jereme Hack (Jereme.haack@pnnl.gov).

Asset	Threat Type	Priority	Consequences of Compromise
Analytics Engine and User Interface (UI)	Elevation of Privileges	High	An adversary can gain unauthorized access to resources in the Amazon Web Services (AWS) organization. The adversary can be either a disgruntled internal user or someone who has stolen the credentials of an AWS organization. (D3)
	Elevation of Privileges	High	An adversary may perform malicious activities by leveraging vulnerabilities in the AWS resource configuration. (D3)
	Spoofing	High	An adversary may perform malicious activities using stolen AWS privileged user credentials. (D3)
Solar/battery Devices	Tampering	High	An adversary may launch malicious code into the solar/battery and execute it. (D21)
	Elevation of Privileges	High	An adversary may exploit unpatched device firmware. (D20)
	Elevation of Privileges	High	An adversary may access the admin interface or privileged services such as Wi-Fi, SSH, file shares, FTP etc., on a device. (D20)
	Elevation of Privileges	High	An adversary may use unused features or services on Gateway such as UI, USB port etc. Unused features increase the attack surface and serve as additional entry points for the adversary. (D20)
	Information Disclosure	Low	If solar/battery transmits sensitive (personal) data but does not protect its confidentiality sufficiently, adversaries may potentially steal it by eavesdropping. (D20)
	Information Disclosure	Low	In cases such as a stolen device or if the device is sold, (e.g., if the device is a consumer Internet-of-Things device), an adversary may potentially gain access to device owners' sensitive data. (D20)
	Repudiation	High	An adversary may probe a device's security posture by performing malicious activities (such as physical tampering of the device components or injecting malicious code) and go unnoticed. (D20)
	Spoofing	High	An attacker may extract cryptographic key material from the solar/battery, either at the software or hardware level, and subsequently access the system with a different physical or virtual solar/battery under the identity of the solar/battery from which the key material was taken. A good illustration is a remote control (a popular prankster tool) that can turn on any TV. (D20)
	Tampering	High	An adversary who has control over a device may inject malicious code into telemetry data. All downstream systems that trust the data sent by the device could potentially be compromised. (D20)
	Tampering	High	An adversary may tamper data transferred by devices through wireless protocols. (D20)
	Tampering	High	An adversary may leverage known vulnerabilities and exploit a device if the firmware of the device is not updated. (D20)
	Tampering	High	If sensitive information such as cryptographic key material is stored insecurely, an adversary may tamper the software running on the device and potentially extract the information. (D20)
	Tampering	High	An adversary may launch offline attacks made by disabling or circumventing the installed operating system or made by physically separating the storage media from the device in order to attack the data separately. (D20)
Redshift DB and Data	Elevation of Privileges	High	An adversary can gain unauthorized access to AWS resources. The adversary can be either a disgruntled internal user or someone who has stolen the AWS credentials. (D1)

	Elevation of Privileges	High	An adversary may perform malicious activities by leveraging vulnerabilities in the AWS resource configuration. (D1)
	Information Disclosure	Low	Personally identifiable information (PII) may be retrieved from data store and used to identify the user to whom the data refers. (D1)
	Information Disclosure	Low	An adversary may eavesdrop traffic to Redshift DB and launch man-in-the-middle attacks. (D1)
	Information Disclosure	Low	An adversary may gain access to sensitive data in Redshift DB. (D1)
	Repudiation	Low	An adversary may repudiate (deny) performing an action on Redshift DB. (D1)
	Spoofing	High	An adversary may spoof Dev if no or non-standard authentication mechanisms are in place. (D1)
	Spoofing	High	An adversary may perform malicious activities using stolen AWS privileged user credentials. (D1)
	Elevation of Privileges	High	An adversary can gain unauthorized access to AWS resources. The adversary can be either a disgruntled internal user or someone who has stolen AWS credentials. (D1)
	Elevation of Privileges	High	An adversary may perform malicious activities by leveraging vulnerabilities in the AWS resource configuration. (D1)
	Information Disclosure	Low	PII may be retrieved from data store and used to identify the user to whom the data refers. (D1)
	Information Disclosure	Low	An adversary may eavesdrop traffic to Redshift DB and launch man-in-the-middle attacks. (D1)
	Information Disclosure	Low	An adversary may gain access to sensitive data in Redshift DB. (D1)
	Repudiation	Low	An adversary may repudiate (deny) performing an action on Redshift DB. (D1)
	Spoofing	High	An adversary may spoof Gateway if no or non-standard authentication mechanisms are in place. (D6)
	Spoofing	High	An adversary may perform malicious activities using stolen AWS privileged user credentials. (D6)

Table 1. Flat topology initial findings

5.3 Use Case 3 – Hierarchical Topology Deployment

The VOLTTRON user community also has instances that use the Hierarchical Topology Deployment. SES Consulting was chosen as the example for the hierarchical topology use case. The SSC team worked with SWG members to develop initial diagrams, which led to preliminary findings detailed in Figure 7 and Table 2.

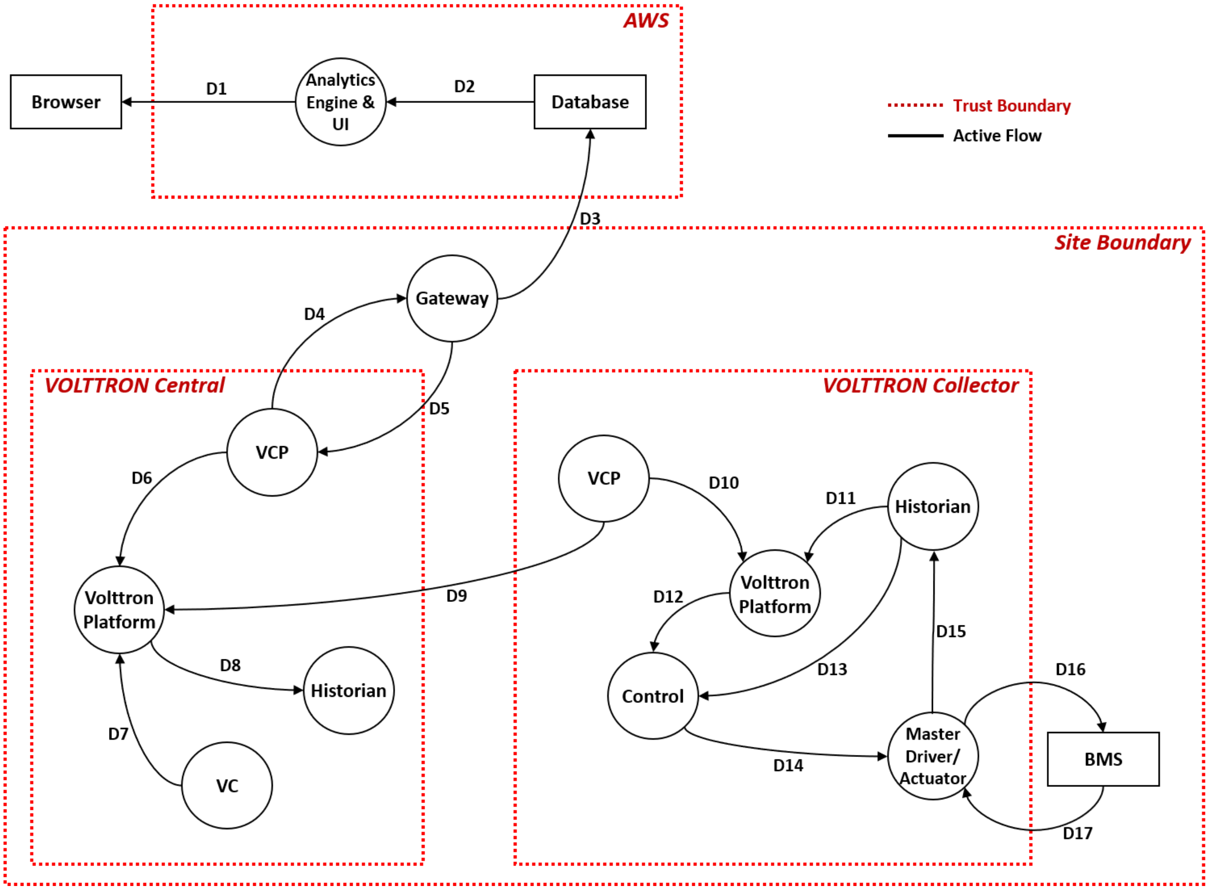


Figure 7. Hierarchical topology use case

Asset	Threat Type	Priority	Consequences of Compromise
Analytics Engine and UI	Elevation of Privileges	High	An adversary can gain unauthorized access to resources in an AWS organization. The adversary can be either a disgruntled internal user or someone who has stolen AWS credentials. (D1)
	Elevation of Privileges	High	An adversary may perform malicious activities by leveraging vulnerabilities in the AWS resource configuration. (D1)
	Spoofing	High	An adversary may perform malicious activities using stolen AWS privileged user credentials. (D1)
Database	Elevation of Privileges	High	An adversary can gain unauthorized access to resources in an AWS organization. The adversary can be either a disgruntled internal user or someone who has stolen AWS credentials. (D3)
	Elevation of Privileges	High	An adversary may perform malicious activities by leveraging vulnerabilities in the AWS resource configuration. (D3)
	Information Disclosure	Low	PII information may be retrieved from data store and used to identify the user to whom the data refers. (D3)
	Information Disclosure	Low	An adversary may eavesdrop traffic to Redshift DB and launch man-in-the-middle attacks. (D3)
	Information Disclosure	Low	An adversary may gain access to sensitive data in Redshift DB. (D3)
	Repudiation	Low	An adversary may repudiate (deny) performing an action on Redshift DB. (D3)

	Spoofing	High	An adversary may spoof Gateway if no or non-standard authentication mechanisms are in place. (D3)
	Spoofing	High	An adversary may perform malicious activities using stolen AWS privileged user credentials. (D3)
BMS	Elevation of Privileges	High	An adversary may exploit unpatched device firmware. (D17)
	Elevation of Privileges	High	An adversary may access the admin interface or privileged services such as Wi-Fi, SSH, file shares, FTP etc., on a device. (D17)
	Elevation of Privileges	High	An adversary may use unused features or services on a Master Driver/Actuator such as UI, USB port etc. Unused features increase the attack surface and serve as additional entry points for the adversary. (D17)
	Tampering	High	An adversary may leverage known vulnerabilities and exploit a device whose firmware is not updated. (D17)
	Tampering	High	An adversary may launch offline attacks by disabling or circumventing the installed operating system or by physically separating the storage media from the device to attack the data separately. (D17)
	Tampering	High	An adversary may launch and execute malicious code into the Building Management System (BMS). (D16)
BMS Data	Information Disclosure	Low	If BMS transmits sensitive (personal) data but does not protect its confidentiality sufficiently, adversaries may potentially steal it by eavesdropping. (D17)
	Tampering	High	An adversary may tamper data transferred by devices through wireless protocols. (D17)
	Tampering	High	If sensitive information such as cryptographic key material is stored insecurely, an adversary may tamper the software running on the device and potentially extract the information. (D17)
VOLTTRON Collector	Repudiation	Low	An adversary may probe a device's security posture by performing malicious activities (such as physical tampering of the device components or injecting malicious code) and go unnoticed. (D17)
	Spoofing	High	An adversary may deploy a fake instance of cloud gateway and pose as a legitimate one. (D17)
	Spoofing	High	An attacker may extract cryptographic key material from BMS, either at the software or hardware level, and subsequently access the system with a different physical or virtual BMS under the identity of the BMS from which the key material was taken. A good illustration is a remote control (a popular prankster tool) that can turn on any TV. (D17)
	Tampering	High	An adversary who has control over a device may inject malicious code into telemetry data. All downstream systems that trust the data sent by the device could potentially be compromised. (D17)
VOLTTRON Central	Denial of Service	Medium	An adversary may launch Denial-of-Service attacks on the VOLTTRON platform. (D9)
	Elevation of Privileges	High	An adversary may gain unauthorized access to sensitive data in the VOLTTRON platform due to excessive privileges. (D9)

	Elevation of Privileges	High	An adversary may gain unauthorized access to the VOLTTRON platform due to no or insufficient network-level segregation. (D9)
	Repudiation	High	An adversary may repudiate (deny) performing an action on the VOLTTRON platform. (D9)
	Spoofing	High	An adversary may spoof VOLTTRON Central Platform (VCP) if no or non-standard authentication mechanisms are in place. (D9)
	Tampering	High	An adversary may inject malicious inputs into the VOLTTRON platform and impact downstream processes. (D9)
	Information Disclosure	Low	An adversary may eavesdrop traffic to the VOLTTRON platform and launch man-in-the-middle attacks. (D9)
VOLTTRON Data	Information Disclosure	Low	An adversary may gain access to sensitive information through error messages. (D9)
	Information Disclosure	Low	An adversary may gain access to sensitive data in the VOLTTRON platform. (D9)
	Information Disclosure	High	An adversary may break weak cryptographic implementations or steal cryptographic keys and gain access to sensitive data. (D9)

Table 2. Hierarchical topology initial findings

6.0 Guidance for Development

These initial Threat Findings identify both preliminary security focus areas for further VOLTTRON development and non-security-based focus areas. The completed VOLTTRON PNNL Campus Threat Profile provides guidance on some of these findings. For the flat and hierarchical use cases, a full Threat Profile will be completed for each and reviewed with the community to verify and prioritize the findings.

6.1 Preliminary Findings

6.1.1 VOLTTRON Central Agent

VOLTTRON Central Agent security and registration is vital to maintain the security of the hierarchical deployment. This need is similar to the PNNL Campus Deployment, and the Threat Profile will guide its development.

6.1.2 Cloud Resource Interaction

Both community use cases involve interaction with cloud resources. VOLTTRON cannot control the security of that endpoint, but the SSC can make recommendations for ensuring security. Any code developed to interact with these resources (by the community or the VOLTTRON development team) must do so as securely as possible and with no communication conducted in the open.

6.1.3 Security Logs for Forensic Analysis

Transferring security-related logs from remote collector instances is necessary to perform forensics if the computer hosting VOLTTRON is compromised. This facility exists in VOLTTRON, but the community should be instructed on its use. This will become a topic for a future SWG meeting.

6.1.4 Community Web Resources

If the community develops use cases in which control actions can be input through their web resources down to the VOLTTRON-connected devices, special security considerations must be taken to maintain safe operations. SSC will monitor community usage to ensure this is communicated and controlled as much as possible through the platform.

6.2 Areas of Non-Security Development

The collected use cases also suggest several priorities not necessarily covered by the security review. These are outlined below.

6.2.1 Resilient Agents

As deployments expand to hundreds or thousands of instances, a capability must exist for agents to automatically recover from an error if possible. Agents could automatically restart numerous times after sending an alert. If they consistently fail, they will raise a higher-level alert and cease to prevent overloading the system.

6.2.2 Simple Deployment

Ease of deployment is essential to a company using the platform at scale. Many companies are growing their own tools and capabilities to integrate VOLTTRON deployment into their business process. These processes should be understood, and care should be taken to ensure that updates to add security to the platform do not break their processes unless absolutely necessary.

6.2.3 Visibility into System Status

VOLTTRON can send alerts to inform administrators of off-normal conditions. SSC can communicate this to the community to communicate how this can best be used or modified for them to increase systems' security posture and reliability.

7.0 Next Steps

Throughout Fiscal Year 2019, the SSC team will continue to develop the flat and hierarchical use cases. The above Threat Findings will be revised as the diagrams are updated and then developed into Threat Profiles. The SSC will continue to moderate the SWG, ensuring that VOLTTRON community needs drive the software security work. The primary focus will be to establish valid representative use cases from which Threat Profiles will be developed. The Threat Profiles will be released to appropriate community members to serve as actionable fixes, security requirements, or risk acceptance criteria. In addition to developing Threat Profiles, SSC will solicit feedback and incorporate new ideas into the SSC process.

8.0 Summary

The VOLTTRON development team and the SSC team have an established relationship and a process that enhances security awareness for the VOLTTRON community. By establishing the PNNL Campus Threat Profile, VOLTTRON has shown due diligence when it comes to developing software with security in mind throughout the development life cycle. The Threat Profile yields actionable controls, creates security requirements in proper context, provides justification for taking security measures, and communicates risk for actions not taken. Ultimately, VOLTTRON has taken the necessary steps to protect the reputation of the VOLTTRON community, its users, and PNNL.

Appendix A – Microsoft STRIDE Model[3]

Threat Type	Definition	Example
Spoofing	Impersonating something or someone else	Pretending to be an administrator, enterprise, or file
Tampering	Modifying the data or code	Modifying a Dynamic Link Library on disk or DVD, or a packet as it traverses a network
Repudiation	Claiming to have not performed an action	“I didn’t send that email.” OR “I didn’t modify that file.”
Information Disclosure	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site
Denial of Service	Denying or degrading service to users	Crashing windows or a web site; sending a packet and absorbing seconds of CPU time
Elevation of Privilege	Gain capabilities without proper authorization	Allowing a remote internet user to run commands; advancing from a limited user to admin

[3] Adapted from https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

PNNL-28810

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov