Pacific Northwest
NATIONAL LABORATORY

PNNL-28204

VOLTTRON™ Threat Profile

May 2019

Chance Younkin
Patrick O'Connell

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

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-28204

VOLTTRON™ Threat Profile

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
RDC	Renewable Development Company
RPC	Remote Procedure Call
SSC	Secure Software Central
SSH	Secure socket shell
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SWG	Security Working Group
UI	user interface
XSS	cross-site scripting

Contents

Figures

Tables

1.0 Introduction

The VOLTTRON™ team engaged Pacific Northwest National Laboratory's (PNNL's) Secure Software Central (SSC) team to provide various cybersecurity analyses on the VOLTTRON software. The SSC offers both threat-based software analysis and secure software development services (Figure 1). These services document, understand, and mitigate software vulnerabilities based on secure software life-cycle principles and prioritized threats.

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 offerings

This document contains all three threat-based software analysis offerings (i.e., threat model, threat findings, and most importantly, the threat profile). Together, these analyses provide system diagrams and a list of categorized and prioritized threats. The third offering, threat profile, includes possible attack paths and mitigation controls for the threats.

The SSC team used portions of Lockheed Martin's IDDIL-ATC methodology (Figure 2) to perform threat analysis 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 cybersecurity triad (Confidentiality, Integrity, Availability) (Figure 3) to prioritize the order in which threats should be addressed.

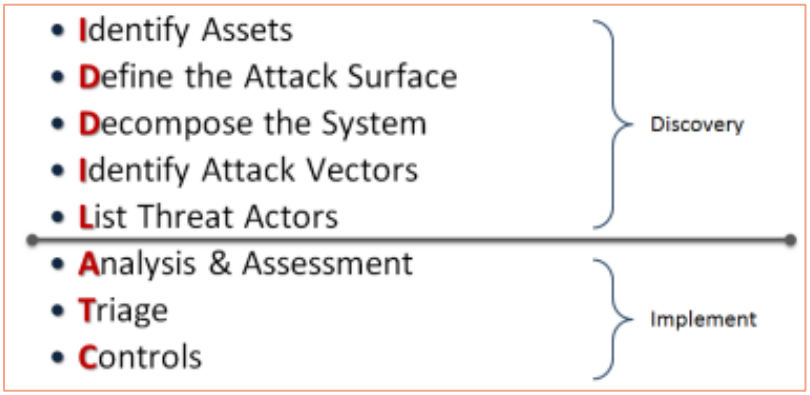

Figure 2. Lockheed Martin's IDDIL-ATC methodology

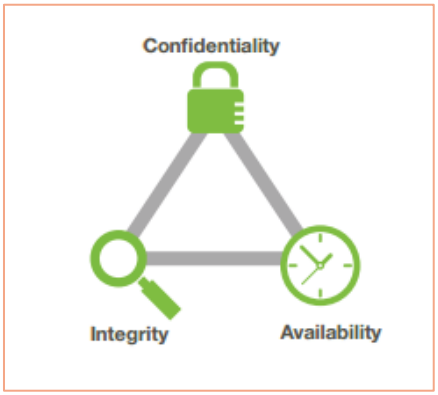

Figure 3. CIA triad

2.0 Threat Model

The VOLTTRON threat model contains a list of threat actors who could be motivated to attack the VOLTTRON software. This list provides context by showing the threats, who might instigate an attack, and why. Further, the model contains a system diagram that illustrates interactions between subsystems and data flow.

2.1 Threat Actor List

Table 1 lists the types of threat actors that should be considered when securing the VOLTTRON system.

Threat Actor	Why they would do it...
Insider	To use the available data to their advantage or for personal gain.
Outsider with intent to harm VOLTTRON or steal VOLTTRON data	Actor with malicious intent who wants to ruin the reputation of VOLTTRON or its users.
Outsider trying to get into other systems	Actor using VOLTTRON as an entry point to gain access to larger networked items—potentially causing larger problems.
Outsider trying to sabotage buildings on which VOLTTRON's sensors are installed	Actor trying to control switches, valves, etc. using VOLTTRON.

Table 1. Threat actors considered and their motivations

2.2 VOLTTRON Diagrams

Figure 4 depicts how communication is achieved with typical VOLTTRON hardware for the Campus Deployment Use Case. The circles in the diagram represent various elements of the system such as a computer system, a database, a web browser, or a person. The arcs in the diagram represent interactions between those elements of the system.

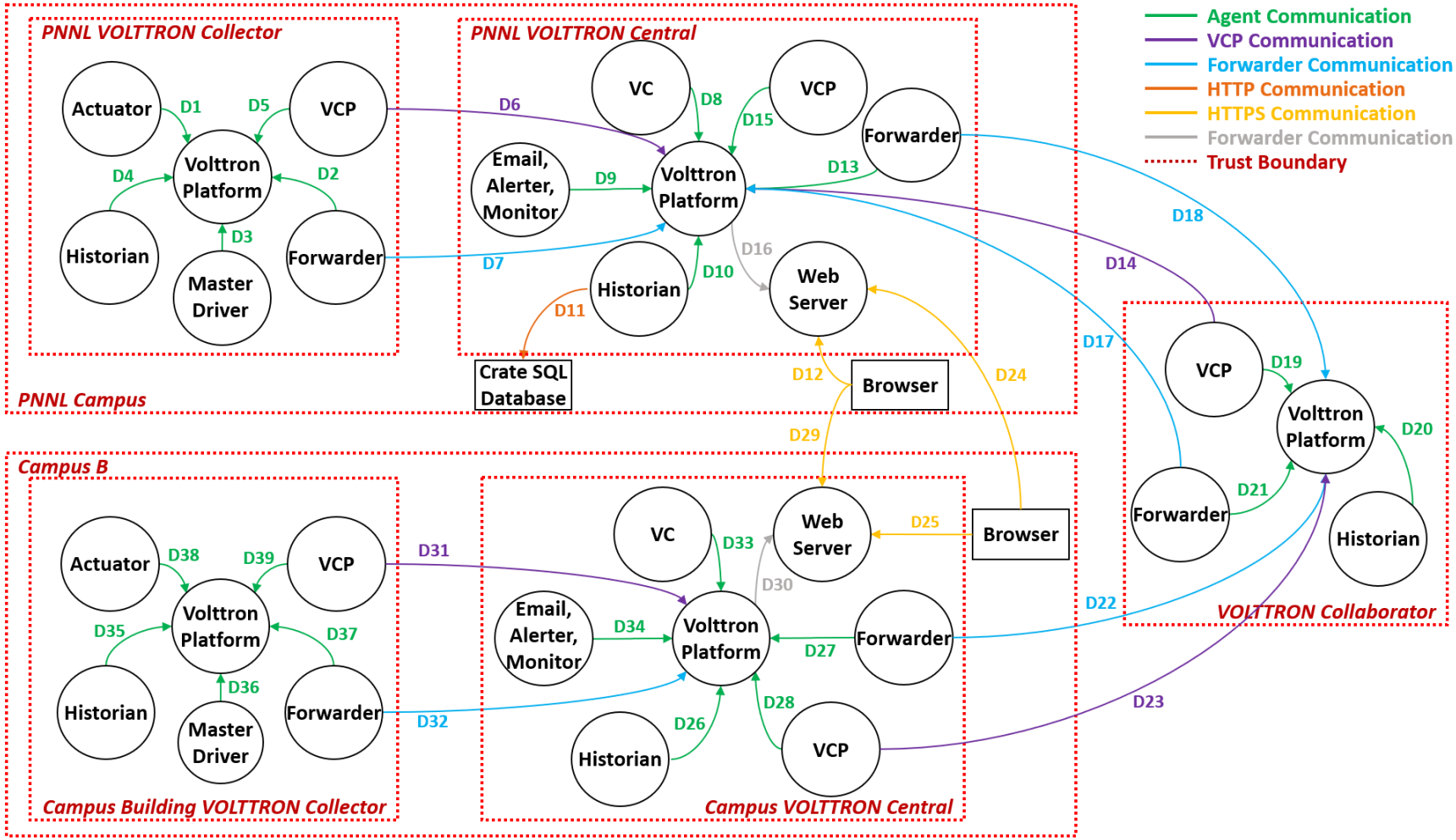

Figure 4. VOLTTRON deployed in a campus environment

3.0 Threat Profile

3.1 Description of Process

The VOLTTRON Threat Profile is derived from the diagram in Figure 4. The VOLTTRON team initially prioritized the discovered threats based on Confidentiality, Integrity, and Availability (CIA). The CIA triad (Figure 5) shows how the VOLTTRON team chose the initial priorities. Table 2 represents the Threat Profile, which is based on assets that need to be protected from the threat actors listed in Table 1, and contains a STRIDE-categorized list of threats.

Figure 5. VOLTTRON CIA priorities

3.2 During analysis with SSC, priorities in Table 2 were adjusted based on feedback from the VOLTTRON development team. For each asset/threat in Threat Profile Table

, the possible attack vectors and controls are listed. Within the table:

- Numbers listed in the “Consequences” column map to the diagram in Figure 4.
- Numbers in the “Controls” column map to the attack vectors listed.
- Bold items in the “Controls” column are solutions that still need to be implemented to mitigate the potential vulnerability. Non-bold items are either already in place or the risk is accepted by the VOLTTRON team.
- Whether bold or not, the description provides the detail to explain the situation.

3.3 Assumptions

Some of the identified controls were out of scope for this assessment but were however trusted to perform their duties as advertised and are depended upon by other listed controls. When this is the case, those threat controls will reference one of the following assumptions:

A1. The greater campus infrastructure provides standard IT access control policies.

A2. The greater campus infrastructure provides standard IT network security using network segregation, firewalls, and NAT routing.

A3. The greater campus infrastructure provides authentication through Kerberos, which in the campus deployment is considered a trusted implementation of user-based authentication and clear access revocation paths.

3.4 Threat Profile Table

Asset	Threat Type	Priority	Consequences	Attack Vector	Controls
Historian Agent Storage System (formerly Crate DB)	Denial of Service	Medium	• An external agent prevents access to a data store on the other side of the trust boundary (D11) • An external agent interrupts data flowing across a trust boundary in either direction. (D11) • An external agent triggers excessive resource consumption for SQL Database (D11)	AV1. Actor with access to PNNL network and subnet (where Crate is located) makes resource-intensive queries to Crate DB. AV2. Actor with access to PNNL network and subnet (where Crate is located) logs onto Crate host and shuts down Crate DB. AV3. Actor with access to PNNL network and subnet (where Crate is located) disrupts network connection between historian and Crate DB. AV4. Actor with access to VOLTTRON central platform deploys agent that overwhelms the VOLTTRON platform message bus, preventing messages from moving to the historian and out to Crate DB.	1. No third-party agents allowed on the central platform. (AV4) 2. Historian has a persistent cache that matches storage on collection box. (AV2, AV3) 3. PNNL supplies network security controls that VOLTTRON deployment leverages. (AV3) *Assumption A1 4. Secure socket shell (SSH) account access to Crate DB host machine is permitted to VOLTTRON team members. (AV1, AV2) 5. SSH access is not through keys, but through PNNL account via Kerberos. (AV1, AV2, AV3) 6. Integrity of VOLTTRON agents is confirmed and verified before being registered. (AV4)
	Repudiation	Low	• Historian claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	AV5. Another agent or actor writes to the database without historian's knowledge.	1. Use PKI encryption for signing data stored by the historian. (AV5)
	Spoofing	Low	• Historian Database may be spoofed by an attacker, which could lead to data being written to the attacker's target instead of Crate DB. Consider using a standard authentication mechanism to identify the destination data store. • Historian may be spoofed by an attacker and this may lead to unauthorized access	AV6. Actor takes over IP address of the Crate DB.	1. Prevent using secure network policy. (AV1) *Assumption A2

			to Crate SQL Database. Consider using a standard authentication mechanism to identify the source process.		
VOLTTRON Platform	Elevation of Privilege	High	• An attacker may pass data into the VOLTTRON Platform to change the program execution flow within the VOLTTRON Platform to the attacker's choosing. (D1-D5, D8-D16, D19-D23, D25-D29, D31-D39) • Agents may be able to remotely execute code for the VOLTTRON Platform. (D1-D5, D8-D16, D19-D23, D25-D29, D31-D39)	AV7. Actor with publish access to message bus passes data that change calculations. AV8. Actor with publish access to message bus passes Remote Procedure Call (RPC) data to cause the VOLTTRON Platform to call agent RPC functions (for agents with that functionality exposed). AV9. Actor with publish access to message bus passes RPC data to cause the VOLTTRON Platform to call VOLTTRON platform control agent service functions. AV10. Actor with access to message bus could issue command to VOLTTRON platform control agent to shut down. AV11. Actor with control of malicious agent can modify VOLTTRON home, which contains sensitive and privileged files. AV12. Actor with control of malicious agent has agent spawn a shell.	1. **Agent processes run as a separate user than the VOLTTRON platform.** (AV11) a. Possible implementation: Whitelist commands using pattern matching that can be executed using sudo. **2. Only device driver can publish to the device topic (implemented but not currently deployed). (AV7)** 3. **Limit RPC calls to the control agent by capability (implemented but not currently deployed). (AV8, AV9, AV10)** 4. Agents run in a user space distinct from the VOLTTRON Platform. **(AV12)** 5. **Verify (actively check) agent and platform processes are not running as a privileged user. (AV12)**
	Denial of Service	High	• VOLTTRON Platform crashes, halts, stops, or runs slowly; in all cases violating an availability metric (VOLTTRON Platform nodes) • An external agent interrupts data flowing across a trust boundary in either direction. (D6, D7, D17, D18, D22, D31, D32)	AV13. Actor, software defect, or configuration error causes a high number of messages to cross the bus and lead to instability across the platform. AV14. Actor or software defect kills the VOLTTRON platform process. AV15. Actor or software defect causes the spawning of orphaned agents. Can also be caused by the unexpected and repeated shutdown of the VOLTTRON Platform. AV16. Actor sends the "kill-11" command enough times to consume resources with core dumps.	1. Rate limit the messages allowed to be sent to the message bus (AV13) 2. Run VOLTTRON Platform as a service. (AV14) 3. Set resource limits on agents. (AV15) 4. **Set the limit core to zero (ulimit -c 0) for the startup shell for VOLTTRON Platform process. (AV16)** 5. **Retire log files by size; limit the size of log files. (AV17)** 6. Set a cache size limit for the historian as a configuration. (AV18) 7. **Set IP tables to rate limit new and/or unique connections. (AV19)**

				AV17. Actor triggers the VOLTTRON Platform to log enough events to consume resources, causing system instability. AV18. Actor triggers historian cache to consume resources, causing system instability. AV19. Actor attempts to connect with invalid credentials to the VOLTTRON Platform as if it were an external agent, which generates a enough errors to consume resources and cause system instability.	
	Repudiation	Low	• The VOLTTRON Platform claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. (D6, D7, D17, D18, D22, D31, D32)	AV20. Actor publishes false data while logging is not at a level to record it.	1. Alternate log specifically for auditing purposes. (AV20)
VOLTTRON Web Server	Tampering	Medium	• If a dataflow contains JavaScript object notation, JavaScript object notation processing and hijacking threats may be exploited. (D12, D24, D25, D29) • The web server 'Web Server' could be a subject to a cross-site scripting (XSS) attack because it does not sanitize untrusted input. (D12, D24, D25, D29)	AV21. Actor performs XSS attack.	1. XSS has been thought of based upon https://securityheaders.com/?q=vc.pnnl.gov%2F&followRedirects=on and https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/. (AV21)
	Repudiation	Low	• Web Server claims it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. (D12, D24, D25, D29)	AV22. Actor sends data or performs actions that do not appear in the log due to logging level or incomplete logging in the code.	1. Verify logging around relevant portions of code. (AV22) 2. Provide an alternate log specific to this (Apache log). (AV22)

Denial of Service	Medium	• Web Server crashes, halts, stops, or runs slowly; in all cases violating an availability metric. (Web Server nodes) • An external agent interrupts data flowing across a trust boundary in either direction. (D12, D24, D25, D29)	AV23. Actor attempts repeated failed logins attempting to bog down the web server.	1. Blacklist IP address for a period of time. (AV23)
Elevation of Privilege	High	• Browser may remotely execute code for Web Server. (D12, D24, D25, D29) • An attacker may pass data into Web Server to change the program execution flow within Web Server to the attacker's choosing. (D12, D24, D25, D29) • Cross-site request forgery is an attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. (D12, D24, D25, D29)	AV24. Actor obtains valid login or exploits vulnerability to gain illegitimate access. AV25. Actor with read-only web logon escalates privilege to admin web logon. AV26. Actor uses agent to request unprotected access to the file system via web server. AV27. Actor uses cross-site request forgery to inject JavaScript into trusted connection with web server to execute on the VOLTTRON Platform.	1. **Use a standard and patchable web server. (AV24, AV25)** 2. **Scan for default password hashes and request password changes or disable account. (AV24)** 3. **Perform periodic vulnerability assessments on deployed web server. (AV24, AV25)** 4. **Permission for newly deployed agents to request exposure to a passwordless web server must be explicitly requested and granted. (AV26)** 5. **Verify that public interface (vc.pnnl.gov) cannot inject JavaScript into the VOLTTRON Central process server and that server cannot execute JavaScript as a mediator. (AV27)** 6. Monitor and log privileged activity on the VOLTTRON Platform by web services. (AV24, AV25, AV26, AV27) 7. Use PNNL infrastructure (F5 and Apache proxy) to protect against common threats and to provide visibility for cyber defenders. (AV24, AV25, AV26, AV27)

Table 2. Profile based on assets to be protected

4.0 Conclusion

This threat-based software analysis shows the VOLTTRON team's due diligence to seek external assessment of their software, ensuring to the best of their abilities that VOLTTRON provides a secure and reliable function in its operating environment. By beginning with possible threats, actionable controls against those threats can be prioritized and implemented. The profile also provides knowledgeable security requirements and justification for taking security measures. Lastly, when controls are too costly or too difficult to implement, the risk of not addressing those controls is understood and can be communicated easily to stakeholders.

Appendix A – The Microsoft STRIDE Model[1]

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

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

PNNL-28204

Pacific Northwest National Laboratory

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

www.pnnl.gov