Pacific Northwest
NATIONAL LABORATORY

PNNL-29932

VOLTTRON™ Threat Profile for VOLTTRON Version 7.0

Provided by Secure Software Central

May 2020

Ryan Bays
Taylor Edwards
Emma McMahon
Patrick O'Connell
Garret Seppala
Torri Simmons
Sarah Sundgren
Chance Younkin

U.S. DEPARTMENT OF ENERGY

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

Click here to enter a date.

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

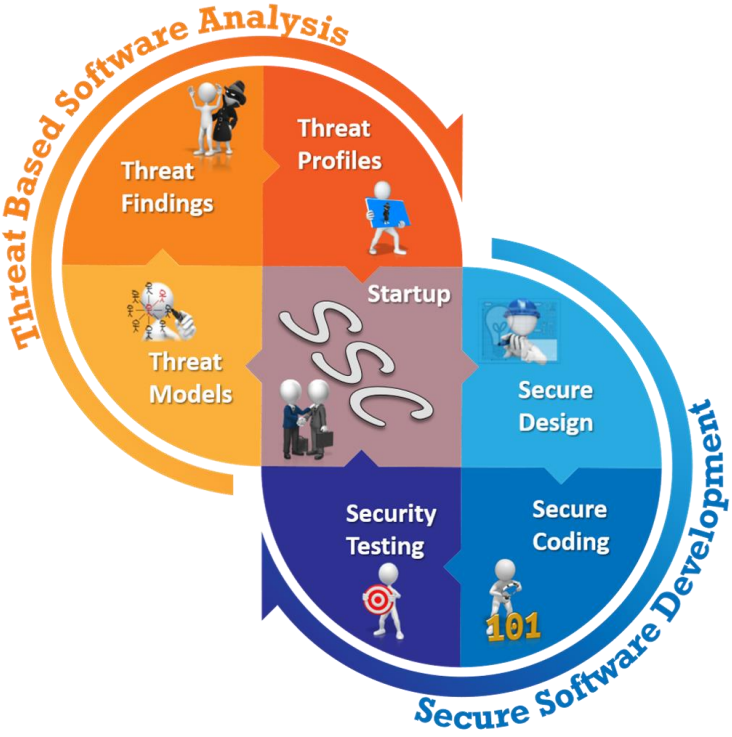
Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

VOLTTRON™ Threat Profile for VOLTTRON Version 7.0

Provided by Secure Software Central

May 2020

Ryan Bays
Taylor Edwards
Emma McMahon
Patrick O'Connell
Garret Seppala
Torri Simmons
Sarah Sundgren
Chance Younkin



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

Pacific Northwest National Laboratory
Richland, Washington 99354

Contents

Diagrams

Figures

Tables

Acronyms and Abbreviations

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
IP	Internet Protocol
JSON	JavaScript Object Notation
PNNL	Pacific Northwest National Laboratory
RabbitMQ	Rabbit Message Queue
ROI	Return on Investment
RPC	Remote Procedure Call
SSC	Secure Software Central
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TMT	Threat Modeling Tool
ZMQ	Zero Message Queue

Summary

The VOLTTRON™ project team at Pacific Northwest National Laboratory (PNNL) has engaged with PNNL's Secure Software Central (SSC) Team to produce this Threat Profile for VOLTTRON Version 7.0. The Threat Profile gives the VOLTTRON team the means to understand the potential threats against VOLTTRON. The objective is to provide the knowledge to mitigate or accept threats based on the impact those threats have on the system. Not all threats must be mitigated, and not all threats can be addressed in a cost-effective way. This Threat Profile provides critical information for making threat-based decisions to increase security at a reasonable cost and to reduce risk.

This VOLTTRON Threat Profile establishes security requirements, justifies security measures, yields actionable controls, and effectively communicates risk to stakeholders. To that end, it can be effectively used by development teams, software architects, and managers.

Through the Threat Profile, threats to the system were categorized, prioritized, and mapped directly to affected system components. The Threat Profile shows mitigations that were already addressed at the time of engagement, as well as those that could be addressed or considered acceptable as-is.

Use cases and threat diagrams were created through engagement between SSC and VOLTTRON. An SSC analysis followed, producing a Threat Findings document. Follow-on engagements with the VOLTTRON team led to the full Threat Profile, which details threat type, threat category, and mitigations for every threat identified. Finally, this detailed Threat Profile table was summarized in a mitigations table that prioritizes and lists every mitigation, implemented or not, with references to the full Threat Profile in 4.0Appendix A. The mitigations map to the threats, which map to components in the diagrams, providing complete coverage of the system from a threat analysis perspective.

This Threat Profile provides the foundation for a thorough understanding of threats for the development team, the testing team, management, stakeholders, and customers of VOLTTRON. It enables decision makers at all levels to improve the security posture of the system. This effort leads to more secure software and better-understood security; the VOLTTRON team is to be commended for their rigorous approach to employing cybersecurity throughout the software development life cycle.

The results of this assessment are summarized in this table:

Threat Type	High Priority	Medium Priority	Low Priority	Total
Spoofing	7	0	1	8
Tampering	11	0	0	11
Repudiation	1	2	3	6
Information Disclosure	2	0	2	4
Denial of Service	0	5	1	6
Elevation of Privilege	14	1	0	15

1.0 Introduction

The VOLTTRON team is engaged with Pacific Northwest National Laboratory's (PNNL's) ***Secure Software Central (SSC)*** Team to provide cybersecurity analyses of the VOLTTRON software. SSC offers both threat-based analysis services and secure software development services, as defined in Figure 1. These services are ultimately used to understand and mitigate threats against and vulnerabilities in software, thus improving overall cybersecurity and informing decision makers. SSC's threat-based analysis produced this document, a ***Threat Profile***, which is composed of threat model diagrams, threat findings, and most importantly, controls that mitigate those threats. This Threat Profile is for VOLTTRON Version 7.0

Threat-Based Software Analysis **–** determines and prioritizes threats against the software system and recommends mitigations. The result is a Threat Profile that contains a threat model, threat findings, and mitigations.

Secure Software Development **–** applies security best practices to the software development life cycle. This includes secure design, secure code review, vulnerability scanning, and security testing.

Figure 1. Secure Software Central services.

1.1 Purpose of the Threat Profile

The Threat Profile establishes security requirements, justifies security measures, yields actionable controls, and effectively communicates risk. To that end, it can be effectively used by development teams, software architects, managers, and stakeholders. For stakeholders and managers, the Threat Profile shows what has been mitigated and what has not been mitigated, thus enabling decision makers to assess priorities based on the actual system and the threats against it. For development teams and software architects, the Threat Profile provides direct and actionable tasking that boosts the cybersecurity of the software product. In addition to providing information, the format of the Threat Profile maps mitigations to threats and threats to the diagram, making it clear where and how the controls are affecting and benefiting the system. This is advantageous for controls and vulnerability assessments that are not threat based and do not stem from system diagrams.

1.2 Categorizing and Prioritizing Threats

Categorizing threats helps identify, organize, and prioritize threats in any system—this holds true for the VOLTTRON software that is being developed. To optimize the analysis process, streamline the engagements, and aid in mitigation implementations, SSC utilizes Microsoft's

Spoofing – when a process, file, website, network address, etc. is not what it claims to be
Tampering – the act of altering the bits in a running process, data in storage, or data in transit
Repudiation – involves an adversary denying that something happened
Information Disclosure – when the information can be read by an unauthorized party
Denial of Service – when the process or data store is unable to service incoming requests
Elevation of Privilege – when an adversary gains increased capability on a system or network

Figure 2. Microsoft's STRIDE model described.

STRIDE model (see Figure 2). There are many categorization models, but STRIDE best lends itself to PNNL's processes, and tools are available to partially automate and expedite the initial analysis processes. SSC uses Microsoft's Threat Modeling Tool, which is based on the STRIDE model. The tool provides initial results, and the SSC team provides expertise to consolidate the threats.

Prioritizing threats is also critical to the process of developing a Threat Profile. With a list of mitigations, each with their own cost, level of effort, and consequences, it is necessary to understand which ones are most important and why. For a Threat Profile, priorities start with the standard CIA (Confidentiality, Integrity, and Availability) Triad, as used in Figure 3. The terms are defined simplistically as follows:

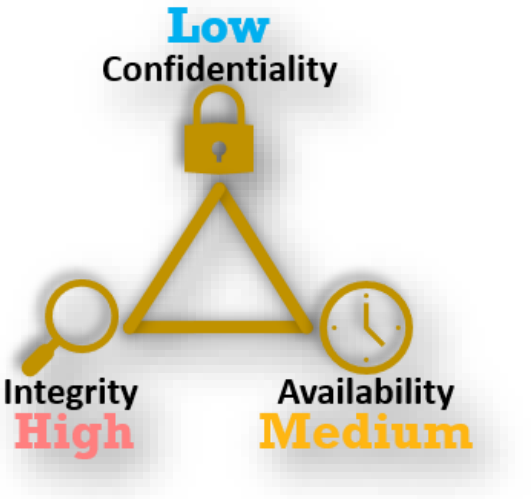


Figure 3. VOLTTRON priorities.

Confidentiality – keep the data secret.

Integrity – make sure the data is correct.

Availability – make the data available.

These terms are important considerations when prioritizing threats, but using the triad necessitates that one of the three must be ranked as the most important. Figure 3 shows the VOLTTRON priorities for this Threat Profile.

1.3 Types of Mitigation

Mitigations identified in this Threat Profile fall into three categories:

Physical – This is the traditional type of security in which valuable assets are guarded with guns, guards, and gates. However, physical security is becoming blended with cybersecurity in many ways because computers and networks are linked with gates, locks, and other access protection devices.

Technical – This refers to cybersecurity technology that is applied to typically (but not always) digital assets. Multi-factor authentication is a good example of a technical mitigation for access control.

Operational/Administrative – This is a method of following policy or procedural practices to implement security.

While these three types are not identified directly in the Threat Profile, it is important to note that most of the mitigations fall into the technical category, although both physical and operational do occur.

2.0 Threat Model

An SSC threat model is a set of use cases, a set of threat cases, and a set of system diagrams. Use cases are descriptions of how the system operates from a user's viewpoint. They are invaluable for deriving system diagrams, which are the framework for the Threat Findings and Threat Profile documents. Threat cases are just like use cases, but from the perspective of an adversary, threat cases are used primarily to help derive and understand mitigations.

The diagram(s) in this section represent the VOLTTRON system and were derived through engagements between the SSC team and the VOLTTRON team. They contain some assumptions based on a mutual understanding about how the system will be designed and implemented.

2.1.1 Understanding Trust Boundaries

The most important aspect in performing threat-based analysis is knowing what trust boundaries are and where they are located. Interactions that cross trust boundaries are the most likely place for an adversary to inflict damage on a system. Figure 4 and Figure 5 show the VOLTTRON trust boundaries and explain what they are and where they are. These trust boundary hierarchies are maintained throughout the threat diagrams.

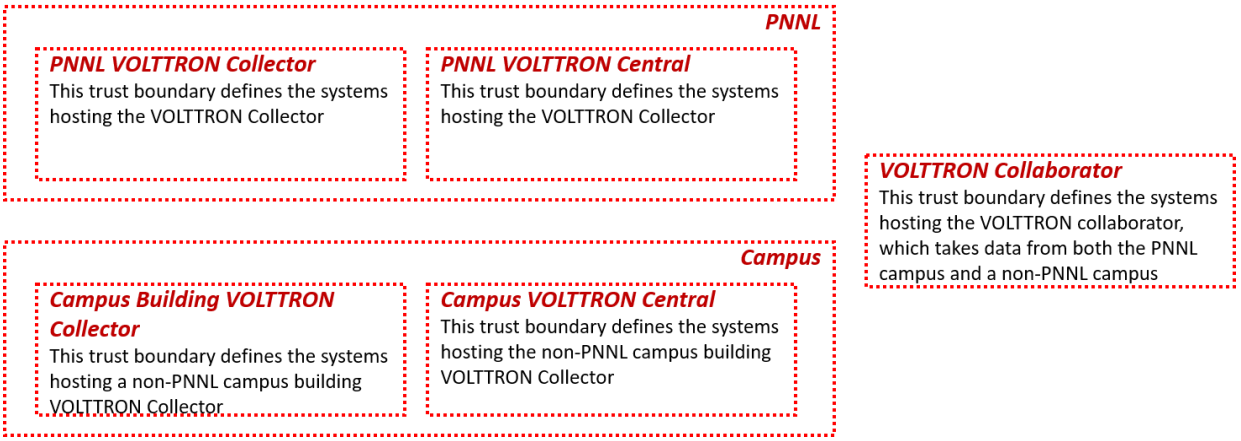


Figure 4. VOLTTRON intercampus deployment trust boundaries.

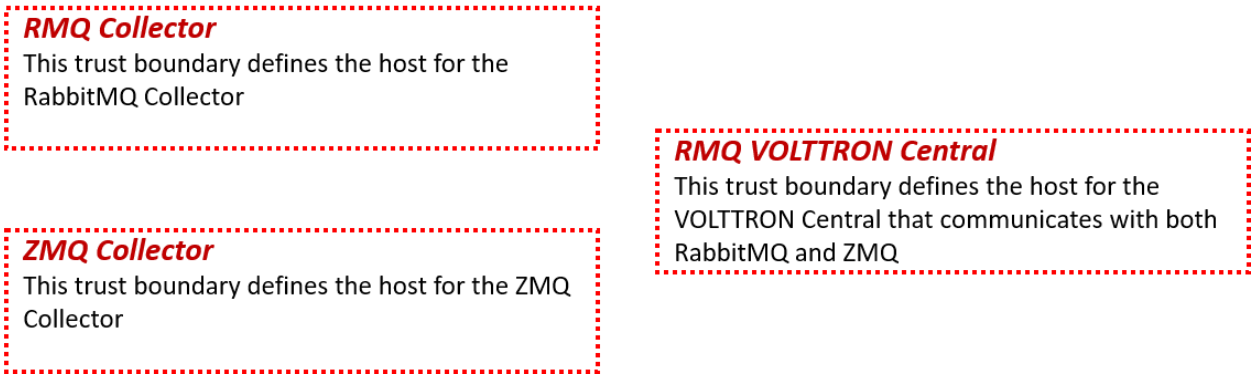


Figure 5. RabbitMQ and ZMQ legacy compatibility trust boundaries.

2.1.2 VOLTTRON Threat Diagrams

The conventions used in the threat diagrams below help distinguish and categorize the different components of the system as follows:

Circles – represent running processes or VOLTTRON agents.

Squares – represent physical devices, data storage devices, or web browsers.

Arrows – represent interactions between components or between a person and a component. Arrows are labeled so that they can be identified in the system diagrams and have mitigations that map directly to the interactions within the system.

Red dotted boxes – represent trust boundaries between components of the system.

Red dashed lines – represent internet boundaries between VOLTTRON and external components.

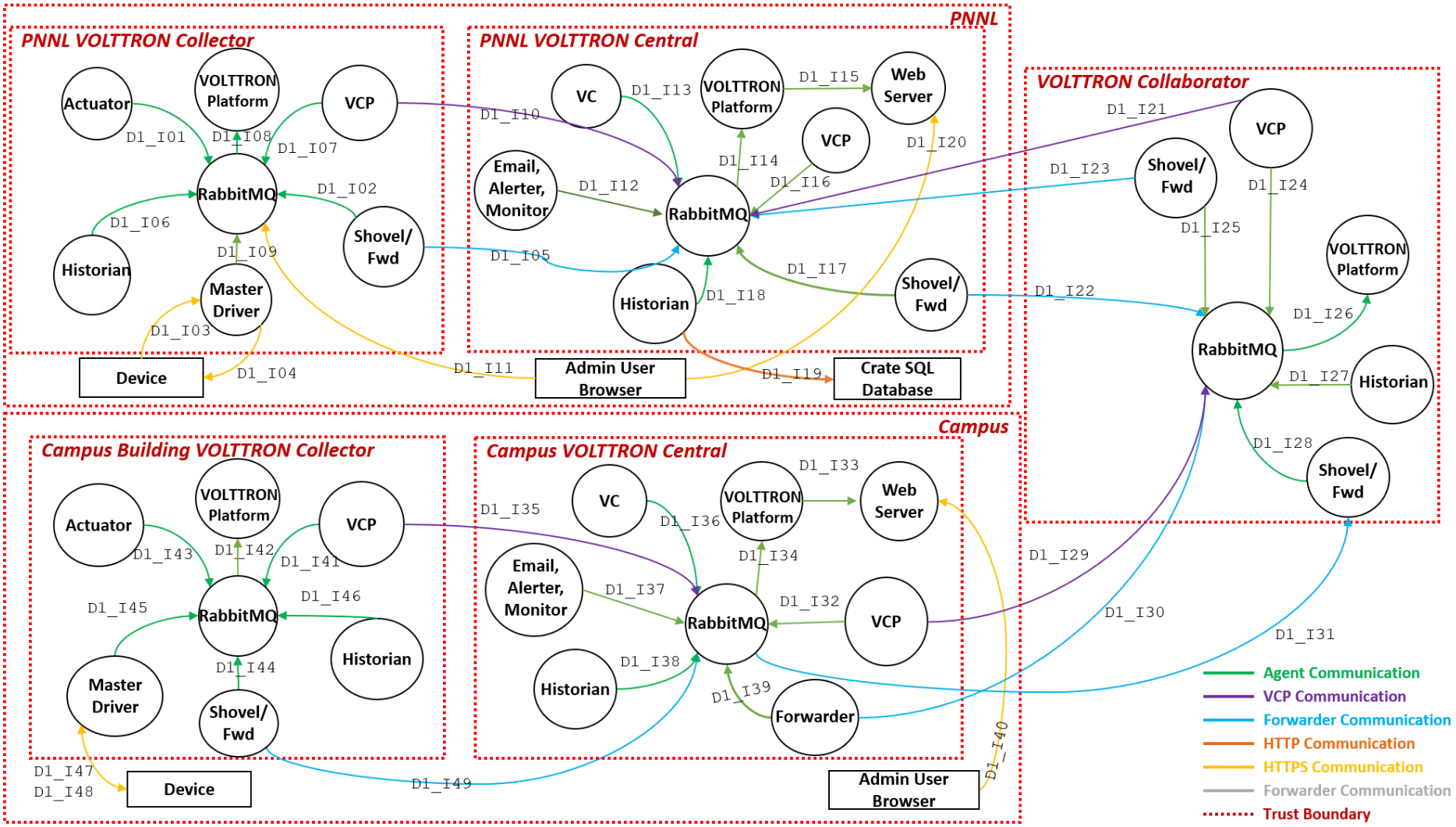


Diagram 1. RabbitMQ shovel.

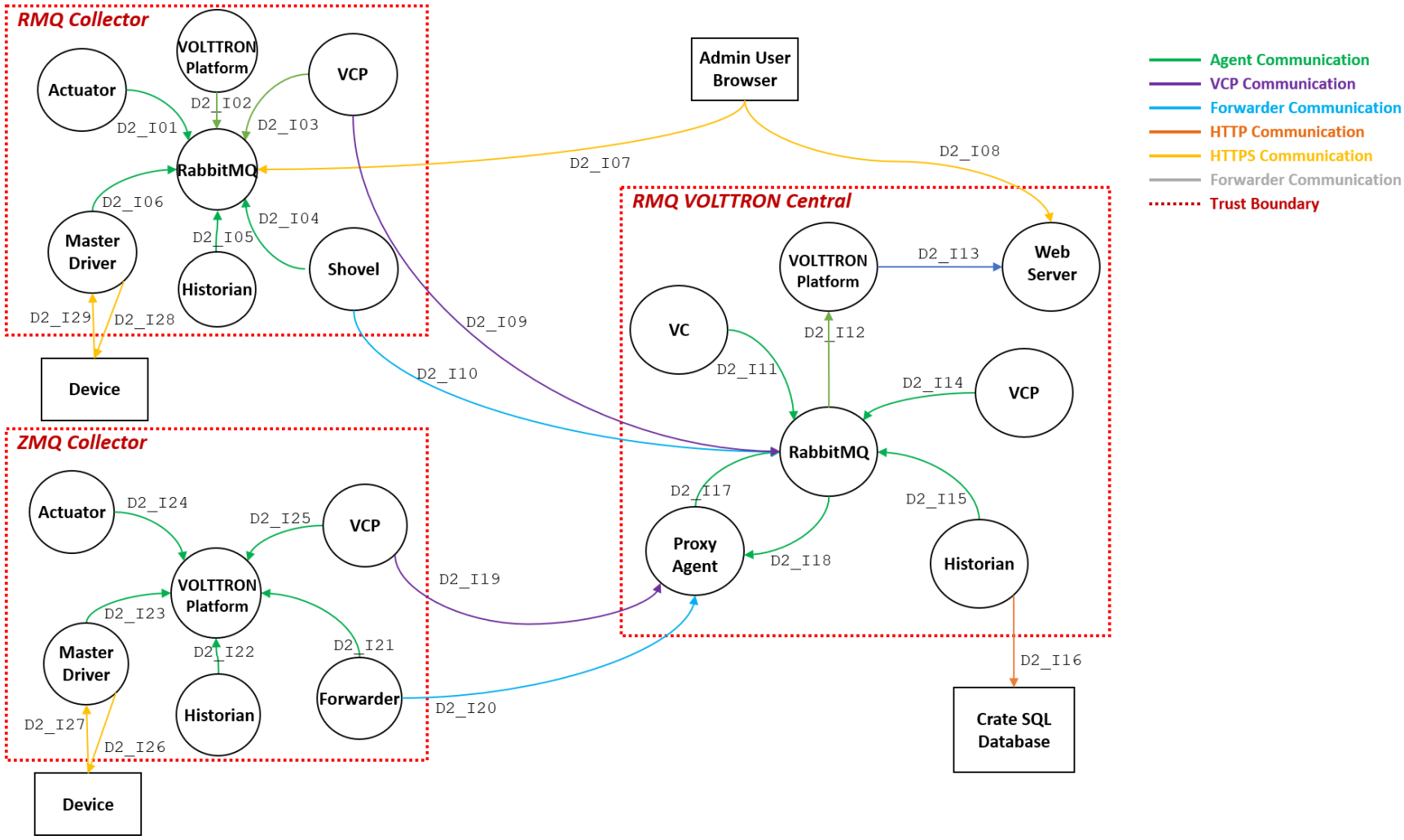


Diagram 2. RabbitMQ mixed legacy.

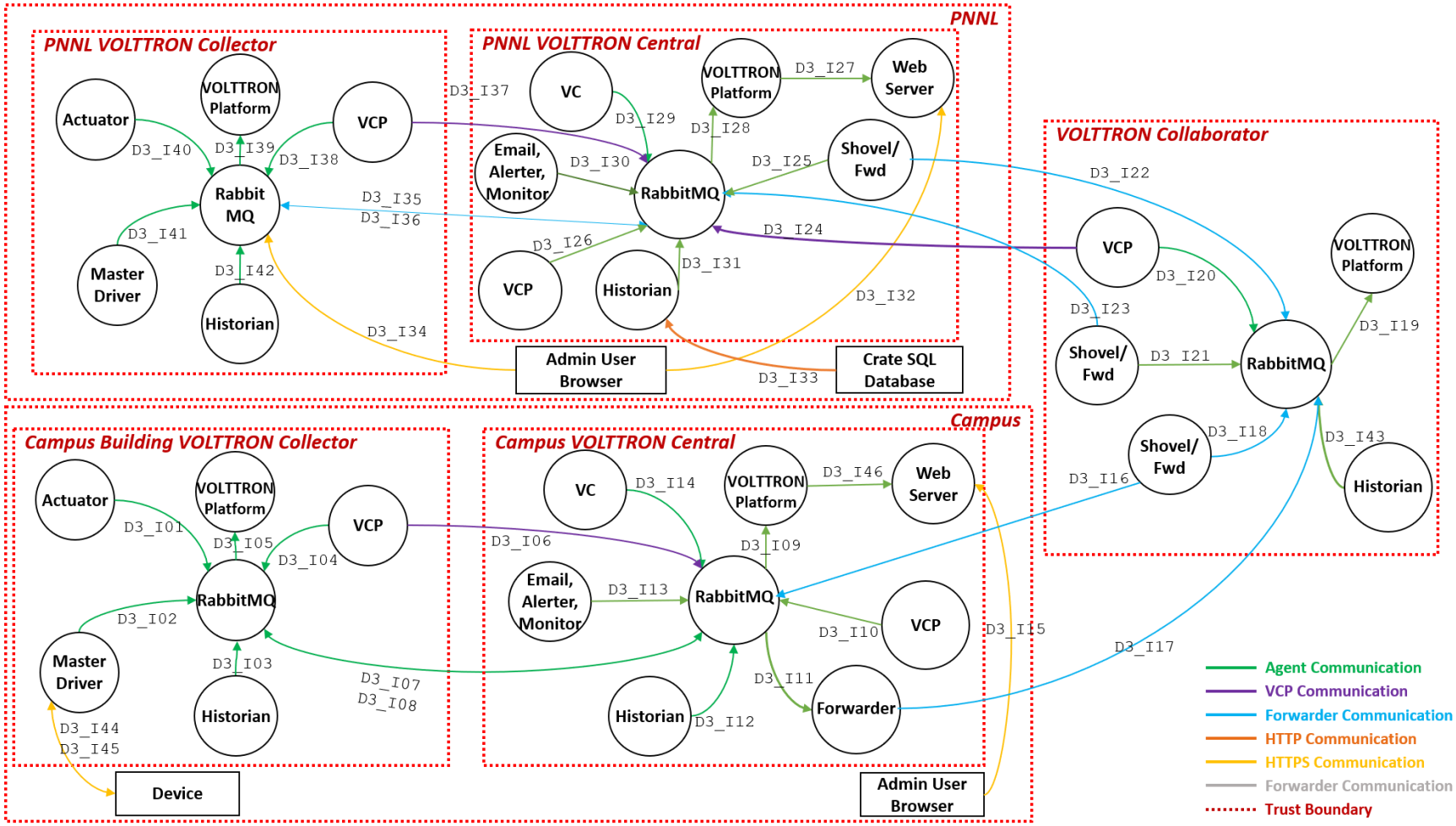


Diagram 3. RabbitMQ federation.

3.0 Mitigations Table

Threat Findings build on the Threat Model by adding threat categorization, project-based prioritization of threats, and the threats themselves. The Threat Profile builds on the Threat Findings document and is completed by filling in mitigations. Mitigations are the main objective and describe what will be done to prevent, deter, or minimize the threat.

3.1 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.

3.2 Mitigations

The mitigations shown in Table 1 are the controls that are either in place or could be put in place depending on risk tolerance, priorities, and budget. The ***Mitigations*** column describes the control, and the ***Threat Table Rows*** column refers to corresponding rows in the Threat Profile Table (

Table 2). Note that mitigations in bold were identified for consideration during the mitigation engagement in April 2020. All non-bold mitigations are already captured by the current system design, implementation, or both.

Table 1. Mitigations Table

	Mitigations	Threat Table Rows
HIGH		
1	Prevent using secure network policy. *Assumption A2	1,2,4,13,8,45
2	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates. Agents only send messages to the RabbitMQ instance they have established certificate trust with.	3,5,6,7,32,33
3	Assure you reassemble data before filtering it, and confirm you explicitly handle these sorts of cases. Implement Internet Protocol Security (IPSEC) for communication crossing outside of VOLTTRON trust boundary. Only accept connections from instances that possess legitimate certificates. **Look into return on investment (ROI) of input validation capability.**	8

	Mitigations	Threat Table Rows
4	Assure the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2	9,10,11,15,50
5	**Rate limit the messages allowed to be sent to RabbitMQ**. Drop and do not process malformed JavaScript Object Notation (JSON) messages. **Use threshold agents as a detection for potential data tampering.**	12,14
6	Verify the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2	9,10,11,15
7	Implement HTTPS. **To protect system from compromised browser, implement controlled and defined access for configuration changes.**	16
8	Implement timestamps in messages.	17
9	XSS has been thought of based on https://securityheaders.com/?q=vc.pnnl.gov%2F&followRedirects=on and https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/.	18
10	Alternate log specifically for auditing purposes. Verify logging around relevant portions of code.	19,36,37,47,48
11	Use VOLTTRON Platform to generate root self-signed certificate; distribute client certificates to agents for authenticating to RabbitMQ. RabbitMQ only accepts connections from valid certificates. This is a standard technique for authenticating to RabbitMQ.	20,25
12	When possible, do not store data on device for longer than needed for transmission.	21
13	**In hardening guide, recommend using a standard and patchable web server as a proxy to the VOLTTRON Platform web server.** Scan for default password hashes and request password changes or disable account. Perform periodic vulnerability assessments on deployed web server. **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.** Monitor and log privileged activity on the VOLTTRON Platform by web services. **Implement protection against directory traversal.**	22,26,27,28
14	Agent processes run as a separate user than the VOLTTRON platform. **Only device driver can publish to the device topic (implemented but not currently deployed).** **Limit Remote Procedure Calls (RPC) to the control agent by capability (implemented but not currently deployed).** Agents run in a user space distinct from the VOLTTRON Platform.	23,24

	Mitigations	Threat Table Rows
	Use discretionary controls for agents to use privileges. **Verify (actively check) agent and platform processes are not running as a privileged user.**	
15	**Monitor agents for detection of anomalous behavior.** **Prescribe limits on messages sent to agent.** **Only accept expected messages (input validation).** Perform periodic static code analysis on source code base for common vulnerabilities.	29,30,34
16	Configure RabbitMQ to only accept data from authenticated sources. RabbitMQ does not process data. It just places messages (that are expected from validated sources) on a bus. Shovel agent has restricted permissions to RabbitMQ. Only the topics that VOLTTRON Central has configured can be forwarded by the Collector to RabbitMQ.	31,35,43
MEDIUM		
17	No third-party agents allowed on the central platform. Historian has a persistent cache that matches storage on collection box. PNNL supplies network security controls that VOLTTRON deployment leverages. *Assumption A1 Secure socket shell (SSH) account access to SSH is not through keys, but through PNNL account via Kerberos. Integrity of VOLTTRON agents is confirmed and verified before being registered. Rate limit the messages allowed to be sent to the message bus. **Run VOLTTRON Platform as a service.** **Set resource limits on agents.** **Set the limit core to zero (ulimit -c 0) for the start-up shell for VOLTTRON Platform process.** **Retire log files by size; limit the size of log files.** **Set Internet Protocol (IP) tables to rate limit new and/or distinctive connections.**	38,51
18	Set a cache size limit for the historian as a configuration.	39
19	Configure automatic agent recovery.	40,41
20	**Implement heartbeat monitoring for RabbitMQ.** **Implement quick recovery from crash or low-responsive operation of RabbitMQ.**	42
21	**Monitor RabbitMQ for detection of anomalous behavior.** **Restrict communication between RabbitMQ instances to prescribed topics.**	44
LOW		
22	Encrypt using non-vulnerable version of TLS.	49

4.0 Conclusion

This VOLTTRON Threat Profile identifies threats that are mapped to specific system components. It also provides mitigations for each distinct threat–asset pairing. The outputs are actionable controls and facilitate an understanding of risk that informs decision makers who are most concerned with optimizing impact or cost. The contents of this Threat Profile inform threat-based decisions for increasing security at a reasonable cost and for reducing risk.

This threat-based software analysis illustrates the due diligence of the VOLTTRON team. In seeking an external assessment of their software, the team is assuring that VOLTTRON provides a secure and reliable capability in its operating environment.

The VOLTTRON Threat Profile provides a foundation for a thorough understanding of possible threats for the development team, the testing team, management, stakeholders, and partner stakeholders of VOLTTRON. It enables decision makers at all levels to improve the security posture of the VOLTTRON platform. This effort leads to more secure software and better-understood security. The VOLTTRON team is to be commended for their rigorous approach to employing cybersecurity throughout the software development life cycle.

Appendix A Threat Profile Table

A.1 Why the Details are Here

The mitigation table (Table 1) is organized such that the actionable controls are front-and-center in an easy-to-identify, easy-to-follow table. Because of the number of threats and amount of information in the Threat Profile, the details are laid out fully in this appendix. The details for all the threats, the mapping of those threats to categories, example threats, and associated mitigations are documented here for reference. The intent is that for those directly involved in decision-making or implementation, the mitigations can be seen immediately, with easy references to this appendix in the mitigation table (Table 1). Mitigations are the main objective and describe what will be done to prevent, deter, or minimize the threat.

A.2 Interpreting the Labels

The labels captured in parentheses in the Threat column of the Threat Profile below refer to the diagrams above. The label refers to an interaction (arrow) in the diagram, thus showing which interaction and which components the threat corresponds to. For example, a label such as `D3_I15` refers to Diagram 3, Interaction 15. If you find Diagram 3 above, the arrow labeled `I15` will be the interaction corresponding to the threat. This strategy enables the tracking of a mitigation, the threat it addresses, and the area of the diagram that indicates where the threat could occur. Thus, the table provides complete traceability from mitigation to threat to interactions between components.

Note that bold items in the Mitigations column are mitigations that have yet to be implemented and are therefore potential issues that should be addressed. Non-bold items are either already in place, expected to be addressed outside of direct VOLTTRON scope, or represent a risk that is accepted by the VOLTTRON team. Whether bold or not, the description provides the detail needed to explain the situation for the purposes of due diligence, traceability, or risk management.

A.3 The Detailed Threat Profile Table

Table 2 below lists threat type, priority, threat, and mitigation. The mitigations are identical to those listed in Table 1.

Table 2. Threat Profile table

	Threat Type	Threat	Mitigations
HIGH			
1	Spoofing	Device may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of Device. (D3_I44,D2_I28,D2_I26,D1_I48)	Prevent using secure network policy. *Assumption A2
2	Spoofing	Device may be spoofed by an attacker, and this may lead to incorrect data delivered to Master Driver. (D3_I45, D2_I27,D2_I29,D1_I47)	Prevent using secure network policy. *Assumption A2
3	Spoofing	Forwarder may be spoofed by an attacker, and this may lead to unauthorized access to RabbitMQ. (D1_I31)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates.
4	Spoofing	Historian may be spoofed by an attacker, and this may lead to unauthorized access to Crate SQL Database. (D3_I33, D2_I16,D1_I19)	Prevent using secure network policy. *Assumption A2
5	Spoofing	RabbitMQ may be spoofed by an attacker, and this may lead to information disclosure by Forwarder. (D1_I31)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates.
6	Spoofing	RabbitMQ may be spoofed by an attacker and this may lead to information disclosure by Shovel/Forwarder. (D3_I17, D3_I23,D3_I22,D3_I16)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates.
7	Spoofing	Shovel/Forwarder may be spoofed by an attacker and this may lead to unauthorized access to RabbitMQ. (D3_I17, D3_I23,D3_I22,D3_I16)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates.
8	Tampering	Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100	Assure you reassemble data before filtering it, and assure that you explicitly handle these sorts of cases.

	Threat Type	Threat	Mitigations
		bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Assure you reassemble data before filtering i, and that you explicitly handle these sorts of cases. (D2_I10,D1_I44,D1_I49)	Implement IPSEC for communication crossing outside of VOLTTRON trust boundary Only accept connections from instances that possess legitimate certificates. **Look into ROI of input validation capability.**
9	Tampering	Data flowing across 26_IPsec_CF may be tampered with by an attacker. This may lead to corruption of Device. Verify the integrity of the data flow to the data store. (D2_I26)	Verify the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2
10	Tampering	Data flowing across 28_IPsec_CF may be tampered with by an attacker. This may lead to corruption of Device. Verify the integrity of the data flow to the data store. (D2_I28)	Verify the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2
11	Tampering	Data flowing across 44_Fed_CF_IPsec may be tampered with by an attacker. This may lead to corruption of Device. Verify the integrity of the data flow to the data store. (D3_I44)	Verify the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2
12	Tampering	Data flowing across Control Flow may be tampered with by an attacker. This may lead to a denial of service attack against RabbitMQ, an elevation of privilege attack against RabbitMQ, or an information disclosure by RabbitMQ. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. (D3_I17, D1_I31)	**Rate limit the messages allowed to be sent to RabbitMQ**. Drop and do not process malformed JSON messages. **Use threshold agents as a detection for potential data tampering.**
13	Tampering	Data flowing across Crate Comm may be tampered with by an attacker. This may lead to corruption of Crate SQL Database. Verify the integrity of the data flow to the data store. (D3_I33,D2_I16,D1_I19)	Prevent using secure network policy. *Assumption A2
14	Tampering	Data flowing across Generic Data Flow may be tampered with by an attacker. This may lead to a denial of service attack against RabbitMQ, an elevation of privilege attack against RabbitMQ, or an information disclosure by RabbitMQ. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. (D3_I16)	**Rate limit the messages allowed to be sent to RabbitMQ**. Drop and do not process malformed JSON messages. **Use threshold agents as a detection for potential data tampering.**

	Threat Type	Threat	Mitigations
15	Tampering	Data flowing across IPSEC may be tampered with by an attacker. This may lead to corruption of Device. Verify the integrity of the data flow to the data store. (D1_I48)	Verify the integrity of the data flow to the data store. Implement encryption when possible. Prevent using secure network policy for devices with unencrypted connections. *Assumption A2
16	Tampering	If a dataflow contains JSON, JSON processing and hijacking threats may be exploited. (D3_I15,D2_I08,D1_I40)	Implement HTTPS. **To protect system from compromised browser, implement controlled and defined access for configuration changes.**
17	Tampering	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity. (D3_I05,D3_I09,D3_I07,D3_I11,D3_I19,D3_I08,D2_I10,D2_I04,D2_I17,D2_I12,D1_I34,D1_I44,D1_I49)	Implement timestamps in messages. These are all internal agent communications.
18	Tampering	The web server "Web Server" could be a subject to a cross-site scripting attack because it does not sanitize untrusted input. (D3_I15,D2_I08,D1_I40)	XSS has been thought of based on https://securityheaders.com/?q=vc.pnnl.gov%2F&followRedirects=on and https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/. **Implement protection against directory traversal.**
19	Repudiation	Master Driver claims that it did not receive data from a source outside the trust boundary. (D3_I45, D2_I27,D2_I29,D1_I47)	Alternate log specifically for auditing purposes. Verify logging around relevant portions of code.
20	Information Disclosure	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. (D3_I11,D3_I19,D3_I09,D3_I08,D3_I05,D3_I07,D2_I12,D2_I17,D1_I34)	Use VOLTTRON Platform to generate root self-signed certificate; distribute client certificates to agents for authenticating to RabbitMQ. RabbitMQ only accepts connections from valid certificates. This is a standard technique for authenticating to RabbitMQ.
21	Information Disclosure	Improper data protection of Device can allow an attacker to read information not intended for disclosure. Review authorization settings. (D3_I45,D2_I27,D2_I29,D1_I47)	When possible, do not store data on device for longer than needed for transmission.
22	Elevation Of Privilege	Admin User Browser may be able to remotely execute code for Web Server. (D2_I08)	**In hardening guide, recommend using a standard and patchable web**

	Threat Type	Threat	Mitigations
			server as a proxy to the VOLTTRON Platform web server. Scan for default password hashes and request password changes or disable account. Perform periodic vulnerability assessments on deployed web server. **Verify that public interface (vc.pnnl.gov) cannot inject JavaScript into the VOLTTRON Central process server and that the server cannot execute JavaScript as a mediator.** Monitor and log privileged activity on the VOLTTRON Platform by web services. **Implement protection against directory traversal.**
23	Elevation Of Privilege	An attacker may pass data into Master Driver to change the flow of program execution within the Master Driver to the attacker's choosing. (D3_I45,D2_I29,D2_I27,D1_I47)	Agent processes run as a separate user than the VOLTTRON Platform. **Only device driver can publish to the device topic (implemented but not currently deployed).** **Limit RPC calls to the control agent by capability (implemented but not currently deployed).** Agents run in a user space distinct from the VOLTTRON Platform. Use discretionary controls for agents to use privileges. **Verify (actively check) agent and platform processes are not running as a privileged user.**
24	Elevation Of Privilege	An attacker may pass data into Proxy Agent to change the flow of program execution within Proxy Agent to the attacker's choosing. (D2_I19,D2_I20)	Agent processes run as a separate user than the VOLTTRON platform. **Only device driver can publish to the device topic (implemented but not currently deployed).** **Limit RPC calls to the control agent by capability (implemented but not currently deployed).** Agents run in a user space distinct from the VOLTTRON Platform. Use discretionary controls for agents to use privileges. **Verify (actively check) agent and platform processes are not running as a privileged user.**
25	Elevation Of Privilege	An attacker may pass data into RabbitMQ to change the flow of program execution within RabbitMQ to the attacker's choosing. (D3_I07,D3_I17,D3_I16,D3_I06,	Use VOLTTRON Platform to generate root self-signed certificate; distribute

	Threat Type	Threat	Mitigations
		D3_I24,D3_I23,D3_I22,D3_I08,D2_I09,D2_I10,D1_I49,D1_I30,D1_I23,D1_I29,D1_I35,D1_I22,D1_I31)	client certificates to agents for authenticating to RabbitMQ. RabbitMQ only accepts connections from valid certificates. This is a standard technique for authenticating to RabbitMQ.
26	Elevation Of Privilege	An attacker may pass data into the Web Server to change the flow of program execution within the Web Server to the attacker's choosing. (D3_I15,D2_I08,D1_I40)	**In hardening guide, recommend using a standard and patchable web server as a proxy to the VOLTTRON Platform web server.** Scan for default password hashes and request password changes or disable account. Perform periodic vulnerability assessments on deployed web server and hosted capabilities (pages). **Verify that public interface (vc.pnnl.gov) cannot inject JavaScript into the VOLTTRON Central process server and that the server cannot execute JavaScript as a mediator.** Monitor and log privileged activity on the VOLTTRON Platform by web services. **Implement protection against directory traversal.**
27	Elevation Of Privilege	Browser may be able to remotely execute code for Web Server. (D3_I15,D1_I40)	**In hardening guide, recommend using a standard and patchable web server as a proxy to the VOLTTRON Platform web server.** Scan for default password hashes and request password changes or disable account. Perform periodic vulnerability assessments on deployed web server and hosted capabilities (pages). **Verify that public interface (vc.pnnl.gov) cannot inject JavaScript into the VOLTTRON Central process server and that the server cannot execute JavaScript as a mediator.** Monitor and log privileged activity on the VOLTTRON Platform by web services. **Implement protection against directory traversal.**
28	Elevation Of Privilege	Cross-site request forgery (CSRF, or XSRF) is a type of 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	**In hardening guide, recommend using a standard and patchable web server as a proxy to the VOLTTRON Platform web server.**

	Threat Type	Threat	Mitigations
		the vulnerable website. In a simple scenario, a user is logged in to website A using a cookie as a credential. The other browses to website B. Website B returns a page with a hidden form that posts to website A. Because the browser will carry the user's cookie to website A, website B now can take any action on website A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g., by session cookie, integrated authentication, or IP whitelisting. The attack can be carried out in many ways, such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable website that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) that is known only to the legitimate website and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations. (D3_I15,D2_I08,D1_I40)	Scan for default password hashes and request password changes or disable account. Perform periodic vulnerability assessments on deployed web server and hosted capabilities (pages). **Verify that public interface (vc.pnnl.gov) cannot inject JavaScript into the VOLTTRON Central process server and that the server cannot execute JavaScript as a mediator.** Monitor and log privileged activity on the VOLTTRON Platform by web services. **Implement protection against directory traversal.** Use HTTPS.
29	Elevation Of Privilege	Device may be able to remotely execute code for Master Driver. (D3_I45,D2_I27,D2_I29,D1_I47)	**Monitor agents for detection of anomalous behavior.** **Prescribe limits on messages sent to agent.** **Only accept expected messages (input validation).** Perform periodic static code analysis on source code base for common vulnerabilities.
30	Elevation Of Privilege	Forwarder may be able to remotely execute code for Proxy Agent. (D2_I20)	**Monitor agents for detection of anomalous behavior.** **Prescribe limits on messages sent to agent.** **Only accept expected messages (input validation).** Perform periodic static code analysis on source code base for common vulnerabilities.
31	Elevation Of Privilege	Forwarder/Shovel may be able to remotely execute code for RabbitMQ. (D1_I49,D1_I22, D2_I10, D3_I17,D3_I16,D3_I22,D3_I23)	Configure RabbitMQ to only accept data from authenticated sources. RabbitMQ does not process data. It just places messages (that are expected, from validated sources) on a bus. Shovel agent has restricted permissions to RabbitMQ. Only the topics that VOLTTRON Central has configured can be

	Threat Type	Threat	Mitigations
			forwarded by the Collector to RabbitMQ.
32	Elevation Of Privilege	Proxy Agent may be able to impersonate the context of RabbitMQ to gain additional privilege. (D2_I17)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates. Agents only send messages to the RabbitMQ instance they have established certificate trust with.
33	Elevation Of Privilege	Shovel/Forwarder may be able to impersonate the context of RabbitMQ to gain additional privilege. (D3_I11)	Implement authentication of connection between RabbitMQ instances. Only accept connections from instances that possess legitimate certificates. Agents only send messages to the RabbitMQ instance they have established certificate trust with.
34	Elevation Of Privilege	VCP may be able to remotely execute code for Proxy Agent. (D2_I19)	**Monitor agents for detection of anomalous behavior.** **Prescribe limits on messages sent to agent.** **Only accept expected messages (input validation).** Perform periodic static code analysis on source code base for common vulnerabilities.
35	Elevation Of Privilege	VCP may be able to remotely execute code for RabbitMQ. (D3_I06,D3_I24,D2_I09,D1_I29,D1_I35)	Configure RabbitMQ to only accept data from authenticated sources. RabbitMQ does not process data. It just places messages (that are expected from validated sources) on a bus. Shovel agent has restricted permissions to RabbitMQ. Only the topics that VOLTTRON Central has configured can be forwarded by the Collector to RabbitMQ.
MEDIUM			
36	Repudiation	Proxy Agent claims that it did not receive data from a source outside the trust boundary. (D2_I20, D2_I19)	Alternate log specifically for auditing purposes. Verify logging around relevant portions of code.
37	Repudiation	RabbitMQ claims that it did not receive data from a source outside the trust boundary. (D3_I07,D3_I06,D3_I22,D3_I24,D3_I16,D3_I08,D2_I09,D2	Alternate log specifically for auditing purposes.

	Threat Type	Threat	Mitigations
		_I10,D1_I49,D1_I30,D1_I23,D1_I29,D1_I35,D1_I22, D1_I31)	Verify logging around relevant portions of code.
38	Denial Of Service	An external agent interrupts data flowing across a trust boundary in either direction. (D3_I45,D3_I44,D3_I33,D3_I15,D3_I07,D3_I17,D3_I16,D3_I06,D3_I22,D3_I24,D3_I23,D3_I08,D2_I28,D2_I26,D2_I29,D2_I16,D2_I27,D2_I20,D2_I09,D2_I08,D2_I19,D2_I10,D1_I19,D1_I40,D1_I49,D1_I30,D1_I23,D1_I29,D1_I35,D1_I22,D1_I31,D1_I47,D1_I48)	No third-party agents allowed on the central platform. Historian has a persistent cache that matches storage on collection box. PNNL supplies network security controls that VOLTTRON deployment leverages. *Assumption A1 Secure socket shell (SSH) account access to SSH access is not through keys, but through PNNL account via Kerberos. Integrity of VOLTTRON agents is confirmed and verified before being registered. Rate limit the messages allowed to be sent to the message bus. **Run VOLTTRON Platform as a service.** **Set resource limits on agents.** **Set the limit core to zero (ulimit -c 0) for the start-up shell for VOLTTRON Platform process.** **Retire log files by size; limit the size of log files.** **Set IP tables to rate limit new and/or unique connections.**
39	Denial Of Service	An external agent prevents access to a data store on the other side of the trust boundary. (D3_I45,D3_I33,D3_I44,D2_I29,D2_I26,D2_I27,D2_I16,D2_I28,D1_I19)	No third-party agents allowed on the central platform. PNNL supplies network security controls that VOLTTRON deployment leverages. *Assumption A1 Rate limit the messages allowed to be sent to the message bus. Set a cache size limit for the historian as a configuration.
40	Denial Of Service	Master Driver crashes, halts, stops, or runs slowly; in all cases violating an availability metric. (D3_I45,D2_I29,D2_I27,D1_I47)	Configure automatic agent recovery.
41	Denial Of Service	Proxy Agent crashes, halts, stops, or runs slowly; in all cases violating an availability metric. (D2_I20,D2_I19)	Configure automatic agent recovery.
42	Denial Of Service	RabbitMQ crashes, halts, stops, or runs slowly; in all cases violating an availability metric. (D3_I07,D3_I17,D3_I16,D3_I06,D3_I22,D3_I24,D3_I23,D3_I08,D2_I09,D2_I10,D1_I49,D1_I30,D1_I23,D1_I29,D1_I35,D1_I22,D1_I31)	**Implement heartbeat monitoring for RabbitMQ.** **Implement quick recovery from crash or low-responsive operation of RabbitMQ.**
43	Elevation Of Privilege	Forwarder may be able to remotely execute code for RabbitMQ. (D1_I30,D1_I23,D1_I31)	Configure RabbitMQ to only accept data from authenticated sources.

	Threat Type	Threat	Mitigations
			RabbitMQ does not process data. It just places messages (that are expected from validated sources) on a bus. Shovel agent has restricted permissions to RabbitMQ. Only the topics that VOLTTRON Central has configured can be forwarded by the Collector to RabbitMQ.
44	Elevation Of Privilege	RabbitMQ may be able to remotely execute code for RabbitMQ. (D3_I07,D3_I08)	**Monitor RabbitMQ for detection of anomalous behavior.** **Restrict communication between RabbitMQ instances to prescribed topics.**
LOW			
45	Spoofing	Crate SQL Database may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of Crate SQL Database. (D3_I33, D2_I16,D1_I19)	Prevent using secure network policy. *Assumption A2
46	Repudiation	Device claims that it did not write data received from an entity on the other side of the trust boundary. (D3_I44, D2_I28,D2_I26,D1_I48)	Accept risk of threat; no mitigation feasible because device logging is out of scope.
47	Repudiation	Crate SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. (D3_I33, D2_I16, D1_I19)	Alternate log specifically for auditing purposes. Verify logging around relevant portions of code.
48	Repudiation	Web Server claims that it did not receive data from a source outside the trust boundary. (D3_I15,D2_I08,D1_I40)	Alternate log specifically for auditing purposes. Verify logging around relevant portions of code.
49	Information Disclosure	Data flowing across Control Flow may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. (D3_I17,D1_I31, D3_I16)	Encrypt using non-vulnerable version of TLS.
50	Information Disclosure	Data flowing across Crate Comm may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. (D3_I33,D2_I16,D1_I19)	Prevent using secure network policy for devices with unencrypted connections. *Assumption A2
51	Denial Of Service	Web Server/VOLTTRON Platform crashes, halts, stops, or runs slowly; in all cases violating an availability metric. (D3_I15,D2_I08,D1_I40)	Run VOLTTRON Platform as a service.

Appendix B The Secure Software Central Process in Brief

The Secure Software Central (SSC) Team uses portions of Lockheed Martin's IDDIL-ATC methodology (Figure B.1) to perform threat analysis. The SSC optimizes IDDIL-ATC for more cost-effective, time-efficient results that lead to immediately actionable controls. Using the Lockheed Martin nomenclature, SSC actually begins with ***Decompose the System***. To accomplish this, SSC requests that ***Usage Narratives*** be written by members of the project team. The narratives provide the SSC team with valuable context in simple, non-jargon terms. With this context, the next step is to develop a set of use cases and data flow diagrams that represent the system. Generally, the assets and the attack surface can be identified using these diagrams, thus addressing ***Identify Assets*** and ***Define the Attack Surface***. From there we attempt to ***List Threat Actors***, but this is not yet a rigorous exercise. The use cases, threat cases, and data flow diagrams represent the ***SSC Threat Model***, which is the foundation for developing the Threat Profile.

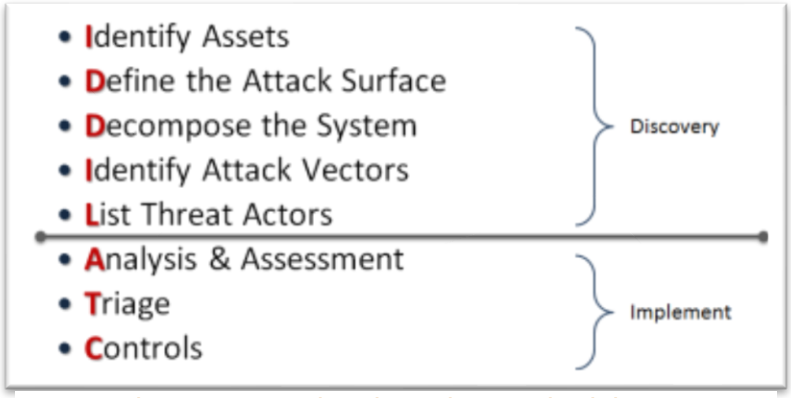


Figure B.1. Lockeed Martin's methodology.

SSC asks the project team to set an initial expectation of threat priority based on Confidentiality, Integrity, and Availability (CIA). The CIA Triad (see Figure 6) is a commonly used cybersecurity model.

Figure B.2. CIA Triad.

The SSC team uses the data flow diagrams as input to Microsoft's Threat Modeling Tool (TMT). The TMT is a free download that comes with standard threat templates used by SSC. The TMT reads the diagrams and uses the templates to provide initial ***Analysis and Assessment*** as well as ***Triage*** results. The TMT also uses Microsoft's STRIDE model (Figure 2) to categorize threats. The initial results from the TMT are then analyzed by SSC subject matter experts to complete the ***SSC Threat Findings*** for review by the project team.

With the Threat Findings in hand, SSC goes back to the project team to collaboratively analyze and determine mitigations (***Controls***). When this exercise is complete, the SSC team organizes the information into the final product, the ***SSC Threat Profile***.

Pacific Northwest National Laboratory

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

www.pnnl.gov