VOLTTRON™: Security Features and Discussion

BORA AKYOL

Pacific Northwest National Laboratory

VOLTTRON™ 2017

Cyber Security

- Definition of Cybersecurity (Webster)
  - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

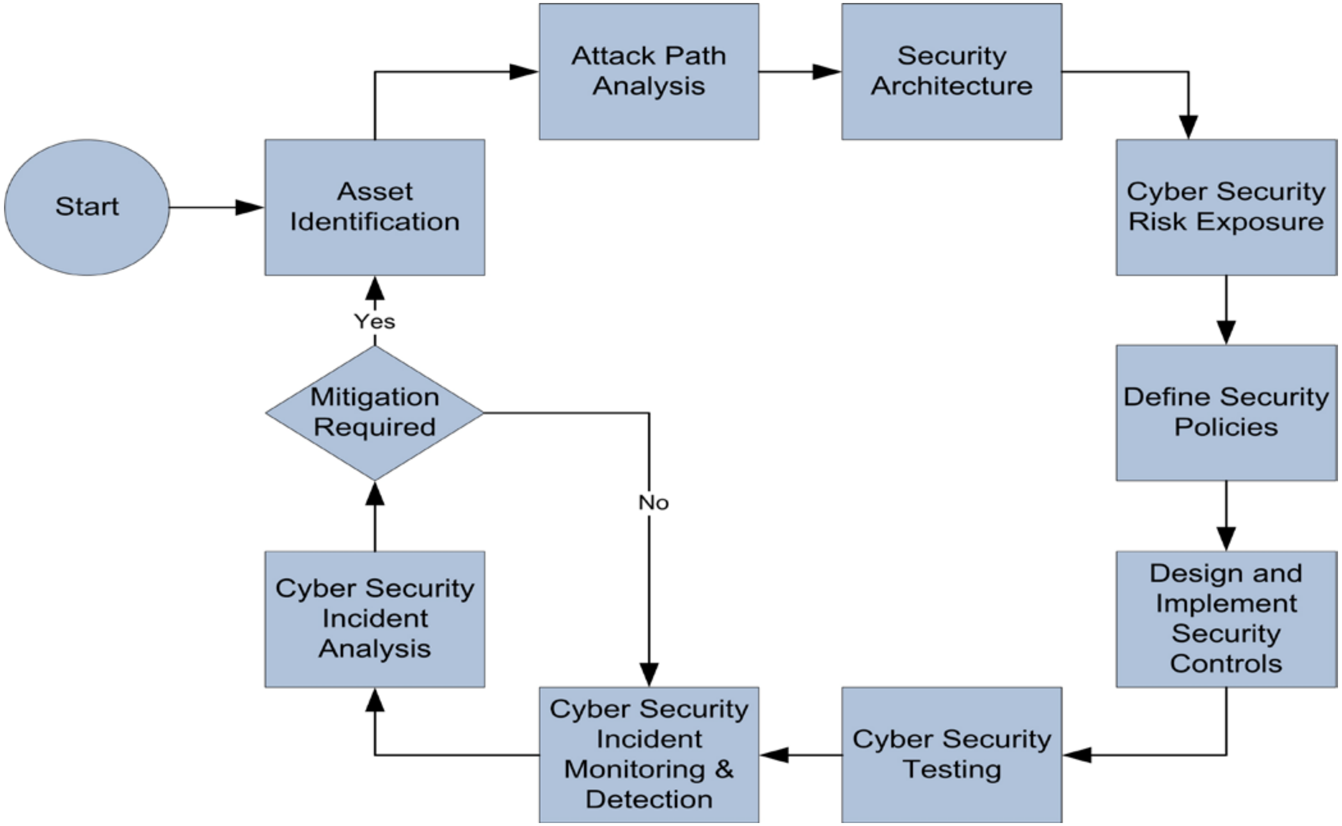
VOLTTRON^{TM} Security Goals

- Protecting the integrity of agent code through cryptographic means
- Protecting agent configuration from manipulation
- Securing communications between VOLTTRON^{TM} platforms and external data sources
- Securing communications between platform instances, including the transfer of agents
- Securing the message bus by controlling who gets to access what topics
- Protecting agents from using excessive system resources to ensure platform stability

Cybersecurity Risk Management

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*



Start
Asset Identification
Attack Path Analysis
Security Architecture
Cyber Security Risk Exposure
Define Security Policies
Design and Implement Security Controls
Cyber Security Testing
Cyber Security Incident Monitoring & Detection
Cyber Security Incident Analysis
Mitigation Required
Yes
No

VOLTTRON^{TM} Security

- Platform hardening guidelines for securing underlying Linux system
- Multi-platform Message Bus
  - Encrypted communication between VOLTTRON^{TM} instances
  - Authorization required for agents to communicate with the VOLTTRON^{TM} message bus
  - Pub/sub topics can be restricted to authorized agents
- Platform Security and Monitoring
  - Access to VOLTTRON^{TM} instances restricted to approved hosts
  - System for forwarding crucial log files for analysis
  - Alerts can trigger emails to administrators
  - Monitor and alert on pub/sub topics for interruptions and unexpected values
- Agent Security
  - Role based access to agent capabilities
  - Agents execute in separate process from platform

VOLTTRON^{TM} Platform Hardening Requirements

- Physical Security
- Low Level Device Security
- Boot Security
- Security Updates
- Securing System Access
- Trimming Attack Surface
- Limiting Incoming & Outgoing Network Traffic
- Monitoring system integrity
- Monitoring System State & Resources
- Monitoring and Replicating System Logs

Platform Hardening must be Comprehensive to be Successful

- Hardening includes:
  - Physical security. Limit who has access to the device. Locked room, locked cabinet with no physical access is preferred. Enable chassis intrusion detection and reporting if possible.
  - Low-level device security. Password protect the BIOS. Ensure periodic updates to keep the BIOS secure. Disable devices that are not needed via the BIOS.
  - Boot security. Restrict boot devices. Disable auto-booting of external devices. Secure the boot loader. Require a password to boot anything other than default kernel.
  - For critical applications, use of a FIPS certified cryptographic module is highly recommended to secure private key material.

Platform Hardening (cont'd)

- Security Updates are required. Configure the system to install the security updates automatically and reboot (if possible) at a particular time. Use the Actuator Agent to reserve the update time window (e.g. 1:30AM on Saturday morning) to prevent other control agents from running.
- Managing system access. Disable all clear text remote system access. No remote root login. Disconnect idle SSH sessions. No FTP, no TELNET, RSH etc.
- Managing users and usernames. Limit number of user accounts. Use two factor authentication if possible. Scan for weak passwords, utilize Linux PAM to strengthen the login process.
- Control incoming and outgoing network traffic
  - Use built-in host-based firewall
  - Rate limit incoming connections to discourage brute force attacks
  - Disable unwanted services.
- Check file system for unexpected changes using Tripwire or similar tool.
- Scan for exploits in the file system using tools such as rkhunter etc.

System Monitoring is a Key Requirement for Security

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by **Battelle** *Since 1965*

- Monitor system state and resources using a tool such as Xymon or Big Brother as well as VOLTTRON^{TM} Central. Set alerts to notify the administrators if anomalous use of resources is detected.
- Watch system logs and export logs off the system.
  - Logwatch or journalwatch is great for getting daily summaries of system activity.
  - Sending system logs to a remote syslog collector such as Splunk allows long term analysis and trending of data.
  - When logs are available on a remote server, we can inspect the logs even when the local system is compromised
- Use an active intrusion sensor such as PSAD to look for intrusion attempts.

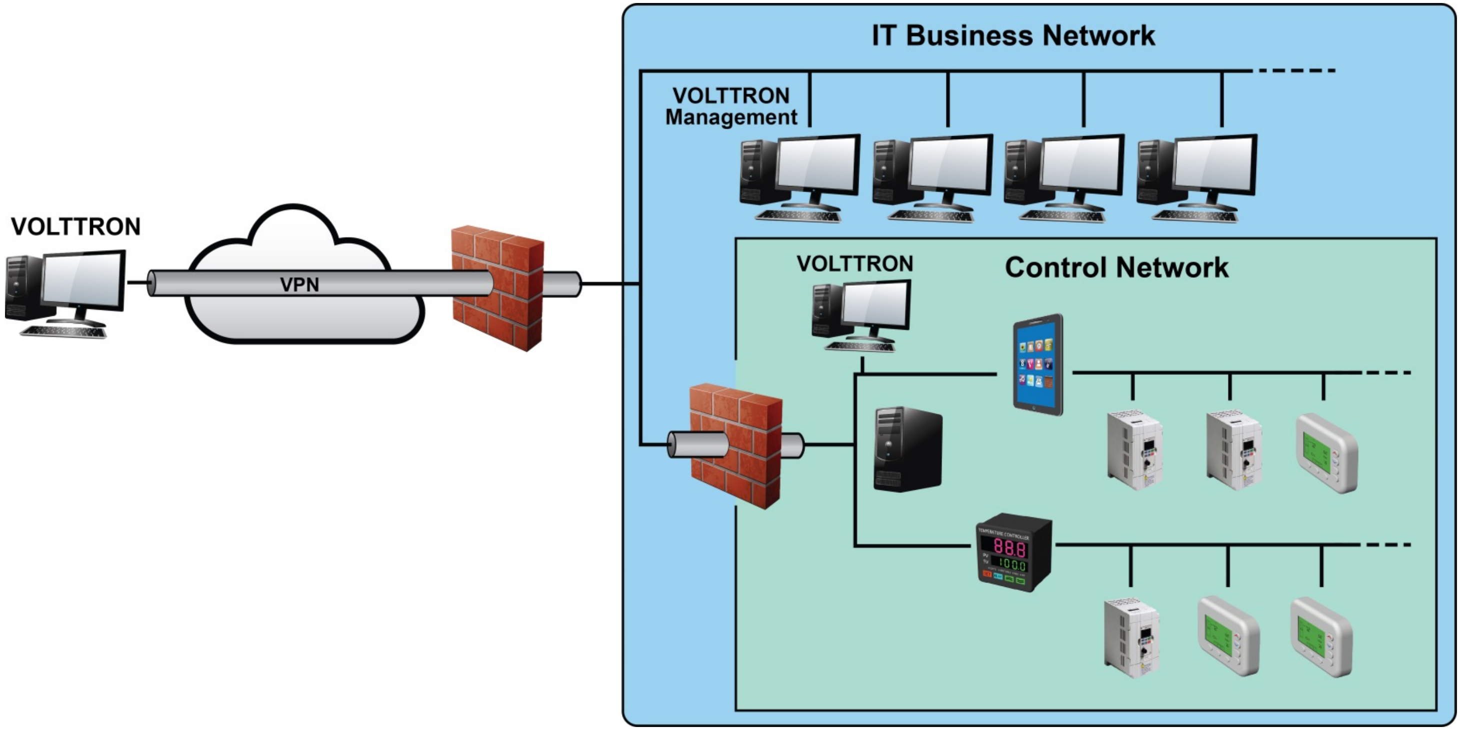
Example Logwatch Output

```
################## Logwatch 7.4.0 (05/29/13) ####################
        Processing Initiated: Mon Jul  6 06:25:02 2015
        Date Range Processed: yesterday
                              ( 2015-Jul-05 )
                              Period is day.
        Detail Level of Output: 5
        Type of Output/Format: mail / text
        Logfiles for Host:
##################################################################
--------------------- Cron Begin ------------------------
Commands Run:
    User root:
          cd / && run-parts --report /etc/cron.hourly: 24 Time(s)
       test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily ): 1 Time(s)
       test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly ): 1 Time(s)
---------------------- Cron End -------------------------
--------------------- Kernel Begin ------------------------

1 Time(s): hv_storvsc vmbus_0_2: cmd 0x85 scsi status 0x2 srb status 0x86
1 Time(s): hv_storvsc vmbus_0_2: stor pkt ffff88028e2daf40 autosense data valid - len 20
1 Time(s): storvsc: Add. Sense: Invalid command operation code
1 Time(s): storvsc: Sense Key : Illegal Request [current]
---------------------- Kernel End -------------------------
--------------------- pam_unix Begin ------------------------
cron:
    Sessions Opened:
       root: 26 Time(s)
---------------------- pam_unix End -------------------------
```

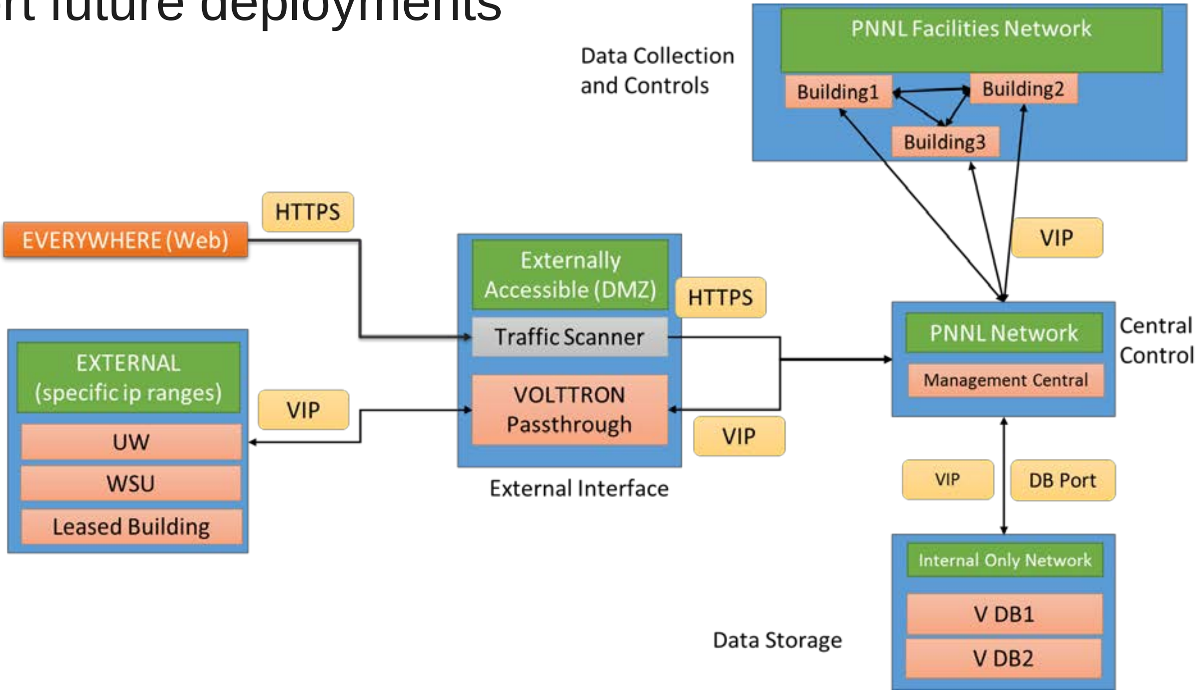
An Example Best Practice for Securing Building Control Networks

- VOLTTRON^{TM} cannot secure an inherently insecure protocol/network.
- Deployment can help minimize exposure



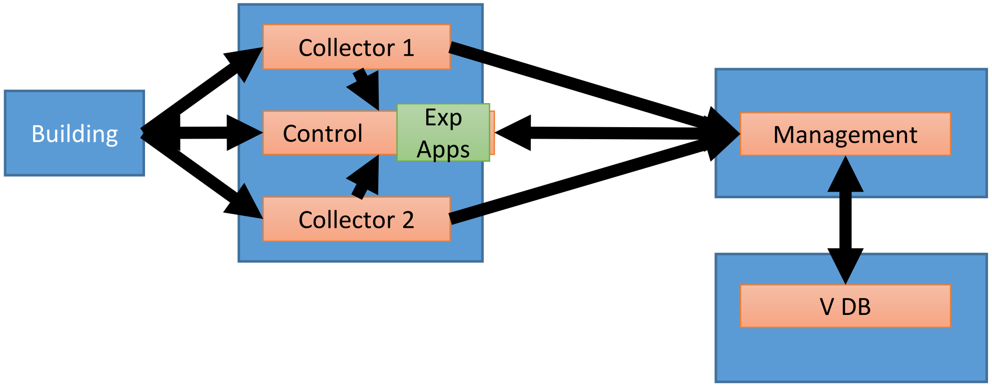
CETC Infrastructure

- Separate networks to ensure security of buildings, data, and platforms
  - External traffic sent through scanners
  - No direct access to building controllers, databases, or VOLTTRON^TM Management platform
- Developing deployment blueprints and enhancing VOLTTRON^TM services to support future deployments



Preventing Data Loss During Collection

- Multiple platforms collect from the same source
  - Alternate collection (even/odd minutes)
  - If a collector goes down, the other(s) increase collection frequency
- Separate platform for issuing control commands and running experimental agents
  - Gets data from collectors
  - Avoids worst case of application interfering with data collection



Summary of VOLTTRON^{TM} Security Features

- Built on Linux to take advantage of its many built-in security features, such as powerful file system permissions, user management, Linux capabilities configuration, control groups, and a highly secure firewall
- When VOLTTRON^{TM} accesses remote resources is done as securely as possible, utilizing the highest version of TLS/SSL protocols and with the largest key size available to both endpoints. Within VOLTTRON^{TM}, OpenSSL is used for TLS/SSL encrypted links. The system's OpenSSL libraries are kept as up-to-date as possible to prevent vulnerabilities such as HeartBleed.
- For multi-platform communication, VOLTTRON^{TM} uses remote ØMQ sockets using CurveZMQ elliptical curve encryption. Keys must be configured for links to be encrypted.
- Code is peer reviewed for correctness and security

Summary of VOLTTRON Security Features (cont'd)

- VIP is used for all internal, inter-agent, and inter-platform communications providing encryption, when appropriate, authentication, authorization, and attribution.
- Linux control groups (cgroups) CPU and memory subsystems are used to limit excessive processor and memory usage.
- Platform control (Unix domain) socket utilizes a mixture of file permissions and access control lists to limit access to authorized users.
- Code is peer reviewed for correctness and security.
- Agent code and packages are signed and verified using RSA encryption with x509 certificates. Unsigned code is not executed unless explicitly allowed by the administrator.

PNNL Role in Securing VOLTTRON$^{\text{TM}}$ Going Forward

VOLTTRON^{TM} Security Needs Served by PNNL

- Cyber security evangelism
- Cyber security clearing house
- Cyber security testing
- Convenor of cyber security working group as part of VOLTTRON^{TM} Foundation

Cyber Security Evangelism

- Act as the voice of VOLTTRON^{TM} Foundation when it comes to cyber security
- Evangelize VOLTTRON^{TM} cyber security related to building and power grid cyber security
- Maintain relationships with and participate in standards developing organizations (e.g. OpenFMB, SGIP)
- Present at conferences and workshops industry wide

Cyber Security Clearing House

- Serve as a clearing house (and verification entity) for all VOLTTRON$^{\text{TM}}$ cyber security bugs
- Responsible for validating and releasing cyber security patches for VOLTTRON$^{\text{TM}}$
- Interface with entities that use or develop on VOLTTRON$^{\text{TM}}$ for all cyber security related topics
- Maintain a security related web site for disseminating information
- Be the first responders for VOLTTRON$^{\text{TM}}$ cyber security incidents

Cyber Security Testing

- Develop and maintain a cyber security validation suite for VOLTTRON^{TM} based systems
- Serve as an independent and unbiased cyber security validator
- Communicate all potential cyber security issues to the cyber security clearing house

Cyber Security Working Group

- Convenor of the cyber security working group of VOLTTRON^{TM} Foundation
- Maintain cyber security agenda going forward
- Maintainer of the VOLTTRON^{TM} cyber security architecture, attack path analysis and risk management controls
- Responsible for cyber security working group schedule and deliverables
- Maintain relationships with and participate in standards developing organizations

QUESTIONS?

- VOLTTRON Resources
  - Wiki: https://github.com/VOLTTRON/volttron/wiki
  - Email: volttron@pnnl.gov
  - Bi-weekly office hours