Purpose-Engineered, Active-Defense Cybersecurity for Industrial Control Systems

Roger Hill, *Veracity Industrial Networks, Inc.*
Rhett Smith, *Schweitzer Engineering Laboratories, Inc.*

Introduction

Software-defined networking (SDN) is revolutionizing the way industrial control system (ICS) networks are engineered, and it is enabling system designers to improve the performance and delivery quality of communications. A primary goal of any control system design is to ensure reliable and safe operations. Cybersecurity is key to this reliability and safety. The programmability of operational technology (OT) SDN networks opens the door for the development of new cybersecurity methods and controls to improve network performance and protection. As part of a project named Chess Master, the U.S. Department of Energy (DOE) has sponsored energy industry stakeholders to research, develop, and commercialize technology that takes advantage of these cybersecurity methods and controls. The Chess Master project is part of the Cybersecurity for Energy Delivery Systems (CEDS) program, which focuses on accelerating the commercialization of advanced cybersecurity technology.

This paper outlines the distinct advantages that OT SDN brings to Ethernet-based ICSs: dramatically improved packet delivery performance under normal and fault event conditions, greater cybersecurity without added complexity, centralized situational awareness, and disruptionless change control that enables safe scalability. The paper also outlines the scope of work for the Chess Master project and the benefits it will bring the energy industry.

The Chess Master project team includes Schweitzer Engineering Laboratories, Inc. (SEL), Veracity Industrial Networks, Inc., Ameren, and Sempra Energy. SEL is the world's leader in microprocessor-based electronic equipment for protecting electric power systems. Veracity is a technology startup specializing in ICS SDN cybersecurity solutions. Ameren is a Fortune 500 company, employing over 8,500 people and providing service to 2.4 million electric customers and more than 900,000 natural gas customers across Illinois and Missouri. Sempra Energy is a San Diego-based Fortune 500 energy services holding company with revenue of more than $10 billion and serving more than 32 million customers worldwide.

Industrial Control Systems

ICSs produce, manage, and monitor processes for the production of goods and services. The organizations that use these systems are constantly looking for ways to reduce workplace injuries and production losses and to increase productivity, system stability, and efficiency. Process improvements and a skilled workforce are key to achieving these goals, but technological advances contribute some of the most significant improvements. It is the responsibility of everyone involved to ensure that technology is safe and secure to protect the operators who work on these systems, the physical process being controlled, and the people these systems serve.

To keep an ICS operating safely and reliably, it must have cybersecurity integrity. However, successful control system cybersecurity is contingent on taking advantage of the core components of the system itself: purpose-built, close-looped, continuously monitored, deterministic, large-scale machines. The best results occur when information technology (IT) security teams work side-by-side with OT control system engineers to design processes and policies that align with standard operating procedures and minimize training burdens. This IT-OT collaboration reduces accidental setting mistakes and oversights.

SDN abstracts the control plane from the data plane and centralizes it in software. Decisions about how to forward packets are made in centralized software (flow controller), and network switches execute the forwarding behavior dictated by the software. This simplifies the switches and allows for a multilayer inspection of each packet at each hop using simple lookup tables in the switch, which are programmed by the flow controller. The key in ICS networks is to provide this traffic engineering capability proactively (i.e., to configure the switches ahead of time for all packets that are authorized on the network and for how to react to network failures).

SDN is an Ethernet technology based on the proven interoperability provided by the IEEE 802.3 standard [1]. Ethernet has become the world's most-used network technology, providing widespread interoperability across manufacturers. Ethernet meets business and critical infrastructure requirements when it is engineered appropriately. However, challenges arise when IT and OT control system traffic are combined on the same network or when the control system networks are scaled to very large systems.

The programmable nature of SDN networks enables them to be purpose-engineered to provide the repeatable results that OT control system engineers demand and the situational awareness and predefined, automated responses to incidents that cybersecurity policies require. By blending these requirements without introducing complexity, SDN allows control system security to reach safety levels at which all packets are inspected and authorized before being delivered to their destinations without trading off performance.

Key Success Criteria for Reliable Cybersecurity

Cybersecurity is critical to the reliability of ICS networks. Cybersecurity spans organizational policies, the procedures followed when people interact with the technology, and the technology itself. Designing and managing a sustainable cybersecurity program that balances all three of these aspects is key to successful long-term security and reliability. The Chess Master team identified five key criteria for ensuring reliable cybersecurity: whitelisting, situational awareness, incident response planning, business benefits, and simplicity.

Whitelisting and SDN

The Chess Master project team has determined that the best way to design and apply a cybersecurity program on a system is to use the system attributes as the core of the program and take advantage of the system's operational aspects. This can only be done with a solid understanding of the system. ICSs are purpose-engineered upfront and are maintained with formal change control management. This allows for the most powerful advantage in the cybersecurity war: whitelist security management.

In this approach, because the devices and what applications each of those devices is running are known, security controls can be designed to drop all other communications and devices. Devices on the ICS are typically embedded, performing a specific task for an extended period of time. Applying security controls is simple when the focus is on what each device should do, creating an enforceable, approved baseline. This approach puts the focus on enabling authorized traffic instead of finding unauthorized traffic and eliminates the need for rapid and ever-evolving signature updates for intrusion detection systems or malware protection. Change management is only needed when devices or applications are added or removed, so safe updates or outages can be scheduled well ahead of time.

SDN aligns well with whitelist security management by enabling the network itself to be proactively traffic-engineered and by enforcing an approved baseline for traffic forwarding. SDN allows multilayer packet inspection in order to ensure that each packet has the approved header information before it is forwarded to its destination. This inspection happens on every hop through the network. Network performance is also improved by using SDN because no ports are blocked by Rapid Spanning Tree Protocol (RSTP) loop mitigation. All ports in an SDN network can be traffic-engineered so that even the physical path planning becomes part of the cybersecurity defensive controls. Networks can be purpose-engineered just like the rest of the ICS to improve performance and whitelist authorized traffic.

Situational Awareness

There is greater situational awareness when the network topology is actively discovered. Operators have a single point from which to see all hosts and network switches on their network and manage all the switches as a single asset. OT SDN breaks from traditional network management systems in that it allows operators to see packet and byte counts throughout the network. This enables them to see where and how the traffic is flowing through the network at any given time and to quickly know the overall health of the network. The removal of the dynamic control plane traffic frees that bandwidth and prioritizes services for operational data, reducing jitter and improving efficiency.

ICSs are continuously monitored via SCADA, distributed control systems (DCSs), energy management systems (EMSs), and process control systems (PCSs). Adding network monitoring is a logical step, but it is critical to ensure that the network monitoring provides information in a way that can be easily integrated into existing systems and procedures. While these systems and procedures vary between organizations, a programmable network infrastructure based on SDN can still be broadly adopted. SDN has the same architecture as SCADA, with the flow controller providing a global view of the network assets and establishing a monitoring and change management platform. The situational awareness SDN provides is greater than that of typical network management software because the packets' paths and matching attributes—as well as the flow byte counts—are known.

Incident Response Planning

ICS operations must have well-established incident response plans and must practice those plans to ensure that all responsible parties understand and can execute them when the need arises. These response plans are typically focused on life safety and production retention, but they also apply to cybersecurity. SDN complements this approach by allowing the establishment of response plans for new or unexpected communication flows and multiple profiles for the entire network. Depending on the business situation, operators can quickly and easily change the operation of the ICS using predetermined responses or operational states.

Business Benefit

Security controls must provide a business benefit. It is good to have negative controls (that is, cybersecurity technology that stops bad things from happening), but it is best when the cybersecurity controls bring positive business returns as well. SDN provides the platform to do just that with more active ports and quick-healing links.

Deployed assets are more efficient with all ports active and able to forward traffic. SDN performs loop mitigation via path planning rather than penalizing the entire system through trunking (as RSTP does). The largest performance advantage of SDN is that commercially available OT SDN switches heal link and switch failures in microseconds, versus RSTP performance that requires milliseconds. This massive performance advantage is maintained regardless of how large the network is, so there are no network size limitations like there are with RSTP. SDN also improves operational efficiency by helping orchestrate device outages for firmware and patch updates that do not disrupt the network.

Simplicity

ICS solutions must be kept simple. SDN provides simplicity by abstracting the control plane complexity out of the deployed switches and centralizing it in the flow controller. This means that the deployed assets have less code in them, which reduces the attack surface and patch management burden. SDN is a multilayer network design that reduces the number of network appliances needed because subnetting is no longer needed. Having fewer devices with less-complicated firmware increases the mean time between failures and reduces operational expenses. The removal of the dynamic control plane also eliminates worries about Bridge Protocol Data Unit (BPDU) spoofing and Address Resolution Protocol (ARP) cache poisoning.

Challenges

The Chess Master team also identified challenges to using SDN to provide security controls in the manner described. Trust management is the first hurdle to clear. How will the flow controller and cybersecurity applications trust each other? How will the orders that are sent through the network appliances be trusted? How will change control transactions be applied without having an intermediate state where undesired packet forwarding could occur? How can all of this be done without making the product technology or the process to manage the technology overly complicated, increasing potential misconfigurations, or creating overly burdensome training requirements? The Chess Master project will address each of these challenges by defining new cybersecurity controls and how to use them.

Chess Master Project Scope of Work

Chess Master is a two-phase project that will take place over a three-year period. The first phase is to research, develop, test, and commercialize a security validation and policy enforcement application that connects to a flow controller to centrally manage all field networks. The second phase is to field-test and demonstrate the technology in real-world ICS installations and prepare best-practice guides for testing, deployment, and long-term management of the technology.

In order to sustain critical energy delivery functions during a cyber intrusion, ICS operators need the ability to automatically identify and contain affected network areas and to reroute critical information and control flows around them. To effectively do so, ICS operators need a global view of the communications flows. They also need a method to proactively determine the whitelisted communications and how to respond to communications in which adversarial behavior is detected (i.e., non-whitelisted communications).

The Chess Master project builds on the success of the Watchdog and the SDN projects, previous DOE CEDS-sponsored projects that commercialized an SDN flow controller and a substation-hardened SDN switch. The Chess Master team is working with the OpenFlow® protocol to maintain interoperable communications between the flow controller and the SDN switch. The Chess Master project addresses a topic area of interest in the CEDS program: “Continual and Autonomous Reduction of Cyber Attack Surface for Energy Delivery Control Systems.”

The Chess Master project is addressing this by developing a solution that:

- Enables all networks running in unmanned field facilities to be proactively configured and monitored as if they are a single asset to monitor their cybersecurity attack surface.
- Enables a whitelisted security profile of all communications with multilayer match fields and preconfigured and automated response actions, minimizing the attack surface.

- Supports a wide variety of security controls to change the operational profile of the flows allowed on the network based on the threat environment. These controls range from on-demand point-to-point encryption and centralized key distribution to intrusion detection system interfaces and flow packet captures.
- Leverages SDN performance increases while enabling the central architecture to apply the security policy and control platform, all while keeping reliability paramount.
- Improves the ability to identify deviations in network behavior to detect and analyze potential cyber intrusions and respond faster.
- Provides the ability to program security zones (with security whitelisting policies) with profiles for each threat state level.

The Chess Master project will achieve all of these benefits by developing a security northbound application and standardizing the application programming interface (API) between the flow controller and a proposed security state monitoring application. The Chess Master team will research, develop, test, and release the following:

- A security policy enforcer application that runs on the northbound interface of a flow controller (e.g., the SEL-5056 Software-Defined Network Flow Controller).
- A DIN rail-mounted SDN switch for pad-mounted and cabinet-mounted field devices. This will extend the central control and monitoring of field-deployed equipment, specifically control-based communications devices.
- An ICS extension to the OpenFlow standard.
- Visualization tools for situational awareness with associated context metrics to help operators quickly know the threat level and exposed attack surface in all field networks based on flow capture indicators and automated response actions that have been taken.
- Technology and tools to automatically enforce proactively configured security profiles and change between them for different threat state levels with increasing defensive controls.
- Technology and methods to secure field networks with predefined security controls applied based on the applications and services running and the behavioral characteristics of the devices.
- Best practices for system architectures and administrative processes to maximize performance, awareness, and security.
- Techniques to evaluate the resiliency provided by preconfigured backup routes and response mechanisms and suggested methods to improve resiliency.

Test results will detail the advances, benefits, and cost impacts for an organization to transition from traditional network technology to SDN technology with an open-source API and standards-based interoperability testing.

The DIN-rail-mounted OT SDN switch developed by the Chess Master team will enable the Chess Master technology to be deployed across most applications in the energy sector. The team will also commercialize a new write action within the OpenFlow configuration, allowing cryptographic applications on a per-flow basis. This write action will automate the key management and allow the application of encryption and/or authentication to the packets belonging to the flow. It will also allow for the distribution of the keys and the coloring of the packets after they are encrypted so that switches at intermediate hops can quickly match and forward the packets without having to decrypt them.

In addition, this project will provide system operators with a single point from which to set and view field network security policies and validate that they are operational in a simplified manner. Operators will be able to engineer the virtual circuits that communications flows travel on and monitor those communications. In addition, they will be able to preconfigure and automate response actions to events and to undesired network behavior to keep critical systems operational. The technology will provide operators with a quick, visual representation of what happened, which communications were impacted, and how. Integrated security controls will include the following:

- Field network access control (NAC) configuration.
- Verification that NAC configurations satisfy security and compliance policies.
- Specific actions defined for any new communications flow attempts.
- A monitoring window into what traffic is on each network and flow circuit.
- Central management capabilities for whitelisting protocols, applications, and devices on field networks.
- On-demand flow encryption to centrally control when wrapper encryption protocols are applied and stripped, without the burden of key management.
- Configuration of automated defensive measures based on network behavior.

Components of the Chess Master Project

Network Engineering Collaboration Improvements

A key focus for the Chess Master project is operational and engineering efficiency. This efficiency will be realized via a digital peer review process for configuring security zones and security policies. This integrated approach will provide direct collaboration between OT and IT personnel, with all relevant parties receiving change notification alerts in near real time and the ability to accept or make design changes in a simplified, visual manner.

Threat State Model

The Chess Master team is also developing a threat state model that will define distinct threat states for a system. The threat state model is divided into five categories of trust, following the defense readiness model. The development of this model will provide both internal and external triggers, via an API, for transitioning between configurable security levels. The system can be configured to determine whether a human should be alerted to recommend a transition of the state or whether predefined triggers can automatically transition the level. Each level will be assigned a predesigned security policy (what the device is allowed to do) and a security zone plan (what trust level the device is a member of). This will result in a threat-based approach to security policies and defensive measures for a system.

Industry Benefits of SDN

SDN is an architectural networking concept that abstracts the control plane out of the switches and centralizes it in software. This central software manages the fleet of switches in its domain, as shown in Figure 1.

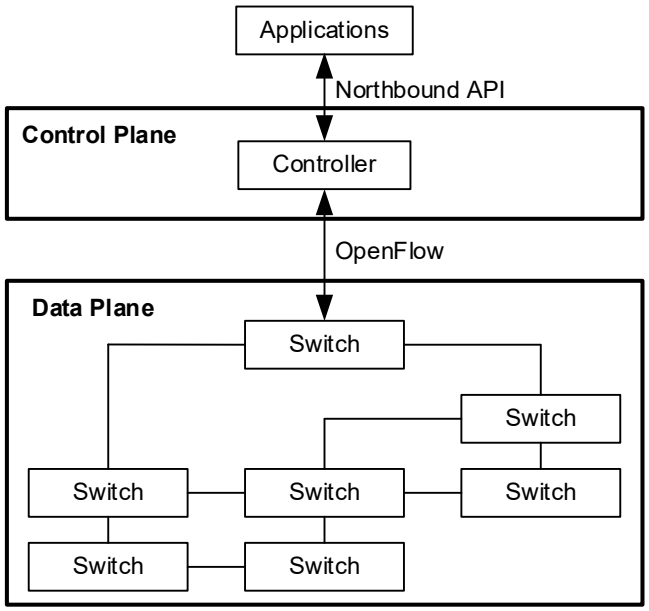

Figure 1 SDN Architectural Overview

The switches become simpler once the control plane is removed. This results in less patch management and fewer errors. The Chess Master project takes advantage of this architectural change to address some of the most challenging cybersecurity issues.

The goal of the Watchdog and SDN research projects was to develop and commercialize an industrially rated SDN switch and flow controller that could support the lengthy lifetimes industrial OT applications require, in many cases ten years or more. These two projects brought together industry experts from academia, a national laboratory, a manufacturer, and multiple power system owners to bring the advanced technology to the market. The results, which exceeded the expectations of the research participants, are making a significant impact in OT networking performance and security around the world [2].

Because SDN is based on interoperable Ethernet technology, network hosts do not have to be altered to work in an SDN network. In fact, the hosts do not know if they are connected to a traditional spanning tree algorithm-based (STA-based) network or an SDN network.

It is important to recognize what the implementation of SDN removes. Pure OpenFlow SDN networks no longer use STAs, so the dynamic topology discovery and loop-mitigation convergence behavior are no longer required. The switches themselves do not have MAC address tables. Instead, they have flow tables that associate the packet with its application at each hop.

It should be noted that OT SDN does not change the OpenFlow architecture of SDN, nor were the OpenFlow standards changed to fit OT systems. However, the way the technology is applied to OT systems is different than how it is applied in IT networks for data centers and carrier industries. Table 1 shows a summary of how SDN is applied to an OT network versus an IT network. Because the standards were not altered, the interoperability between different industry SDN solutions remains, which lays the foundation for rapid innovation.

Table 1
OT SDN vs. IT SDN

Key Attribute	OT SDN	IT SDN
Network state	Persistent	Dynamic
Network control	Purpose-engineered	Traffic-reactive
Controller purpose following switch deployment	Monitor	Control
Security	Deny-by-default	Forward-by-default
Fault-healing speed	Link detect	Flow setup time
Network management	Proactively planned	Fault-reactive

In OT SDN, all primary and failover paths are planned in advance to achieve the predictable and repeatable behavior desired for ICSs. This proactive traffic engineering informed how the DOE research team applied SDN to OT networks. For simplicity, only OpenFlow 1.3 switches were used instead of hybrid STA/SDN switches. This maximized performance, minimized the cost of ownership, and reduced the attack surface of the switch. In ICSs using SDN, all communications to and from each device are purpose-engineered. The switches store the flow, group, and meter entries such that the network performance is not dependent on the flow controller being online, eliminating a potential single point of failure. The rate of change in an OT network is very low; changes are only needed when devices are added or removed, or when new applications requiring new network delivery requirements are enabled. This works well with the proactively traffic-engineered, whitelisted model of OT SDN.

The Chess Master project builds on the commercially released OT SDN technology by developing new security capabilities that will allow operators to manage the security state by policy and quickly change between those policies as required by the state of the system. The project will provide security orchestration for the OT flow controller via complete network visibility, situational awareness, programmable security zones, and security policy management with whitelisting for all assets on the network (see Figure 2).

The Chess Master project will create an integrated threat management platform that can be coordinated centrally and executed in a distributed manner by policy in SDN-enabled switches, such as the SEL-2740S Software-Defined Network Switch. There is no need for ports to be dedicated as mirror ports because SDN allows packets to be sent to the controller based on the programming of the switch. The northbound interface of the flow controller extracts the relevant data needed to perform comprehensive analytics as well as core security capabilities. This distributed approach enables the dynamic isolation of assets in security zones with predefined security policies that are established by system users to reduce recovery time.

Cyber threat experts and analysts, as well as system operators, will have a centralized platform to engineer their networks and define how the networks will react to events like link loss or unauthorized packets. Operators can visualize, monitor, and manage the planned recovery by controlling and managing all forensic investigations from one place. The power of visualizing the effects ahead of an attack helps avoid missteps and accelerates the triage and recovery process.

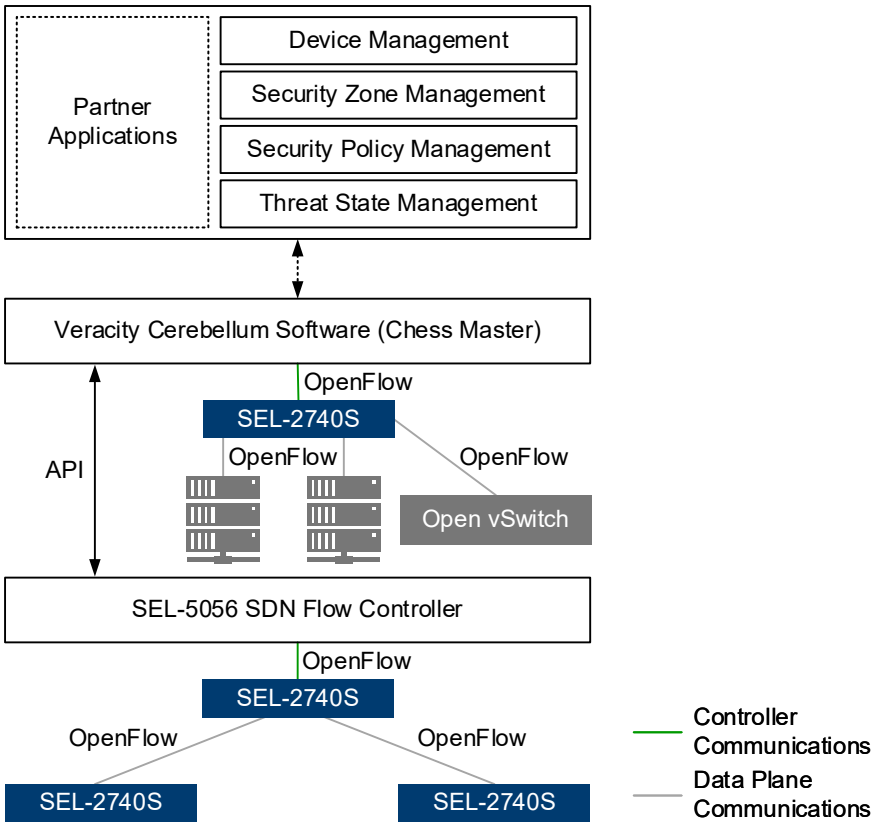

Figure 2 Chess Master Project Architecture

Chess Master System Training Mode

The project team is developing a training mode for operators to learn and characterize the network environment and create a baseline network behavior model. Using SDN capabilities, the switches will be programmed during the training mode to replicate the ICS network traffic to a central security orchestrator and network analytics platform. The team is also researching ways to identify communications patterns among these industrial assets, to determine the types of assets (e.g., remote terminal unit [RTU], programmable logic controller [PLC], or human-machine interface [HMI]), and to determine the baseline communications for the ICS network.

Discovery of Networked Nodes During Training

One of the most critical challenges within ICS networks today is gaining visibility into what devices are on the network, what the communications partners of each device are, and what protocols are required for the machine-to-machine communications. The security state monitoring software will provide a module for identifying, managing, and determining the baseline of each asset within the system. The software will also provide a historical record of active devices on the network as well as devices that are no longer active. The historical record will aid in incident response during an investigation by providing a complete visual record of which assets were connected. The user interface for the software will provide a graphical network view with a time-based slider, allowing the user to scroll through time or enter a specific time range. The key to success is making the software easy to use, merging the physical and cyber events into an easy-to-understand visual representation of what is happening at any given time, and identifying when monitored network behavior deviates from the approved, whitelisted baseline.

Critical Infrastructure Risk Planning

Energy infrastructure requires planning ahead to mitigate risks in a way that prevents system failure or the shutdown of critical parts of the infrastructure. This creates a challenge for system operators and cyber experts who must plan for various situations to ensure the operational continuity of critical infrastructure.

The Chess Master project will provide a new paradigm for managing, planning, programming, and preprovisioning ICS networks. Just as software developers program for exceptions and error paths in their code, the Chess Master security state monitoring software will provide the ability to program for exceptions to normal network traffic behavior.

Security Zone

A security zone is a collection of assets (e.g., PLCs, RTUs, and SCADA) that function together based on communications flows that are grouped to form a logical enclave or zone. The grouping of these assets and their communications flows within an isolated zone creates a trusted region to keep the critical infrastructure in good health and operational by protecting it from unauthorized communications. It is very important for ICSs to have such trusted regions to keep critical assets functioning, even during adversarial activity. The ability to design and provide dynamic security zones for different threat levels gives operators a powerful tool to visually plan and manage the security needs of the ICS before an attack or cyber incident.

Security Operational States

A security operational state is a set of rules to describe what the communications are allowed to do in a facility. One or more operational states can be associated with a security zone or across zones based on the cyber threat situation or the system-wide scope.

Security Policy

The Chess Master security state monitoring software will allow an operator to build different operational states to develop a security management policy. Different policies can be programmed for different threat levels.

A security policy describes how security is managed for critical infrastructure and how treatment changes as the threat level changes. A comprehensive policy workflow shifts the paradigm on security management from reactive analytics and detection to preplanned, preprovisioned design for management under different situations.

Security Building Blocks

SDN provides a unique perspective on network security implementation. Security functions are the lowest-level constructs needed to implement security policies, which are based on the higher-level constructs of security zones and security profiles. The Chess Master security orchestrator separates these higher-level constructs into simple, low-level building blocks and then orchestrates their execution in the SDN-enabled switches using the OT flow controller. The primary objective of the orchestrator is to apply the security building blocks to realize the security objectives described by the higher-level constructs. The security orchestrator also coordinates the dynamic transition of security policies and profiles necessitated by changes in threat levels. The security functions presented to the northbound interface of the flow controller enable the software to convert the policies into sets of configurations. Figure 3 shows the management of these security zones and the addition of cryptography to a flow.

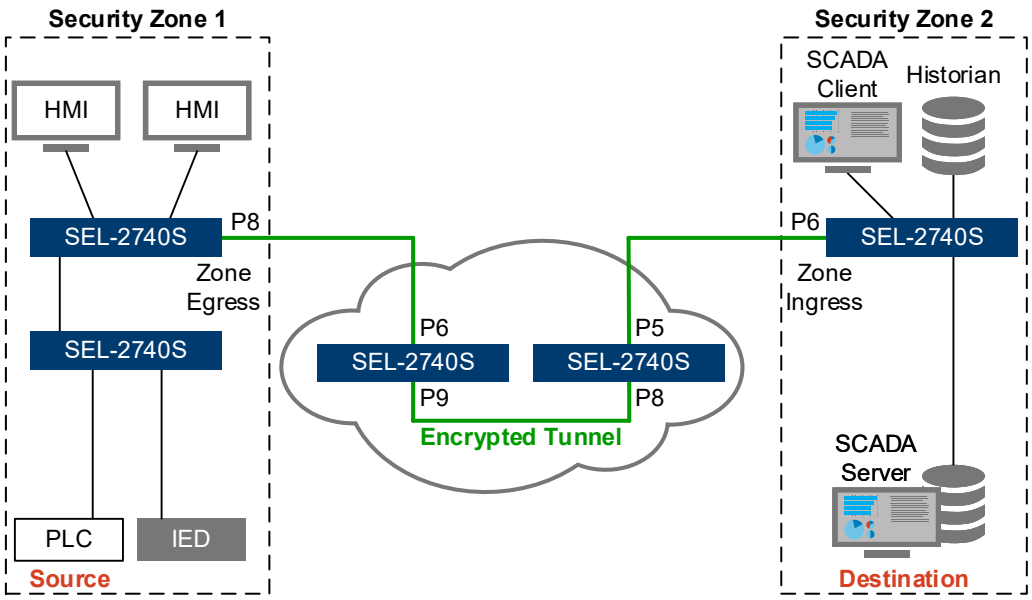

Figure 3 Chess Master Operational Monitoring and Protection

New Paradigm for Detection During Reconnaissance Stage of the Cyber Kill Chain

Most network detective controls focus their efforts on detecting the installation of malware as early in the cyber kill chain as possible. This can allow an adversary to be present on the network for 12–18 months before they are detected. To truly reduce the attack surface, a new paradigm is required. SDN provides the foundation necessary to detect intrusion at the Reconnaissance phase (see Figure 4).

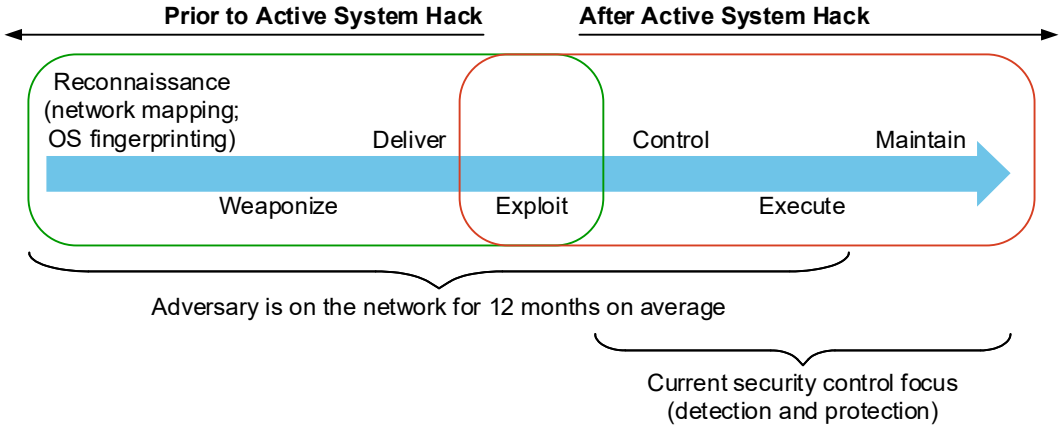

Figure 4 Example Cyber Kill Chain

An adversary needs to understand the network and know what operating systems (OSs) and other software are used on targets in order to move into the Deliver or the Weaponize stages. The Chess Master project will provide a generic prevention mode to protect the network against an adversary attempting to learn the network by using rogue scans. All ARP traffic for the critical infrastructure is relayed to the Chess Master analytics platform, and the orchestrator provides proxy ARP services to the assets marked as critical. MAC addresses and IP addresses are masked for traffic external to security zones for critical infrastructure. All multicast and broadcast traffic outside the security zone is blocked.

For example, if the system detects ARP scanning, and the scan request is attempting to identify the IP addresses used within a specific subnet, the system can provide false or non-used IP addresses in response. The system can be preprogrammed to generate different responses so that an adversary cannot create a map of the network. If an adversary uses specific OS fingerprinting techniques, the system can be preprogrammed to send false OS information in response. If the adversary cannot create a map of the network, nor identify the OSs of networked devices, moving forward to weaponization is prevented.

Further capabilities can be designed into the system so that scanning or fingerprinting requests are redirected to a logical network that is sandboxed and is, in reality, a honeynet populated with low- and high-interactive honeypots. This provides a unique opportunity to identify the tactics, techniques, and procedures of the adversary. SDN itself provides security controls that block pivoting, network manipulation, and reconnaissance tactics [3].

Energy Sector Application

The Chess Master project takes advantage of the core attributes of an ICS for defensive cybersecurity controls. Today's integrated and automated ICSs repeatedly perform specific tasks in real time for safety and operational reliability. The Chess Master team recognizes that a proactively engineered environment using whitelisting will allow more advanced security controls to be applied. With the commercialization of energy sector SDN technology, the foundation is in place to apply this advanced automation and security policy enforcement centrally and safely.

Conclusion

SDN provides OT networks with greater performance, stronger cybersecurity, and better situational awareness that traditional networking solutions. The Chess Master team is developing technology that takes advantage of the OT SDN infrastructure to more efficiently manage the cybersecurity of the system. These new controls simplify the management, strengthen the controls, reduce the attack surface, and support the reliable operation of energy systems.

The resulting technology will enable greater situational awareness, allowing for strong system-wide security policy enforcement and near real-time baselining. Having complete network visibility and control; threat-based security zones and policies; and read, read-write, or unidirectional control over network flows represents a compelling advancement in an environment where simple visibility at the control layer is not readily available.

When using an SDN architecture, value-added applications can be applied to the system without operational downtime or impacts to reliability. This is because the Chess Master application is an abstracted northbound interface to the flow controller that does not involve firmware upgrades to field devices.

SDN technology removes traditional network restrictions, allows networks to be purpose-engineered, and achieves performance that redefines what is possible. Programmable network infrastructure allows the creation of new best-known methods to deliver information between applications and services. It is rare to come across technology that improves the system performance in technical, procedural, and policy aspects without breaking existing functionality, but SDN has achieved this.

SDN technology allows OT network engineers to purpose-engineer their networks to support even the most demanding applications for operating, controlling, and monitoring critical infrastructure. It allows system owners to centrally monitor and deploy managed change control services without the risk of application disruption. It provides near real-time centralized reporting on the ports and services running on any network, potentially removing the time and cost of deploying crews to manually check this information.

These cybersecurity advances will require network engineers to rethink what a subnet is and how packets should be filtered through each hop. The problems faced by large networks using STAs are not present in SDN, opening up even more possibilities and calling into question network architecture best-known methods for routers and subnetting. The Chess Master project is positioned to bring more advanced security controls to market that will also help improve reliability through better network performance and simplify the technology in the system at the same time.

References

[1] IEEE Standard 802.3, IEEE Standard for Ethernet.

[2] R. Bobba, D. R. Borries, R. Hilburn, J. Sanders, M. Hadley, and R. Smith, “Software-Defined Networking Addresses Control System Requirements,” April 2014. Available: https://selinc.com.

[3] M. Hadley, D. Nicol, and R. Smith, “Software-Defined Networking Redefines Performance for Ethernet Control Systems,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2017.

Biographies

Roger Hill is the founder and Chief Technology Officer at Veracity Industrial Networks, Inc. Roger has over 20 years of industrial control systems (ICSs) experience in many different industrial segments. Before joining Veracity, Roger worked for Siemens as the global head of technology management in their plant security services business. He has led organizations in the validation of security controls and in penetration testing of controls within SCADA security test beds, as well as in the development of models to employ within security programs for ICSs. Roger is a subject matter expert in ICSs, including programmable logic controllers, programmable automation controllers, drives, motion controls, human-machine interfaces, SCADA, and distributed control systems.

Rhett Smith is the senior product manager for the wired networks department in research and development at Schweitzer Engineering Laboratories, Inc. (SEL). He was the principal investigator and project director for the Watchdog and SDN projects sponsored by the U.S. Department of Energy. In 2000, he received his B.S. degree in electronics engineering technology, graduating with honors. Before joining SEL, he was an application engineer with AKM Semiconductor. Rhett is a Certified Information Systems Security Professional (CISSP).

Making Electric Power Safer,
More Reliable, and More Economical

Schweitzer Engineering Laboratories, Inc.
Tel: +1.509.332.1890 | Email: info@selinc.com | Web: www.selinc.com