A Layered Solution to Cybersecurity

By Erfan Ibrahim, PhD

Center Director, Cyber-Physical Systems Security & Resilience

National Renewable Energy Lab

Golden CO

Erfan.Ibrahim@NREL.gov

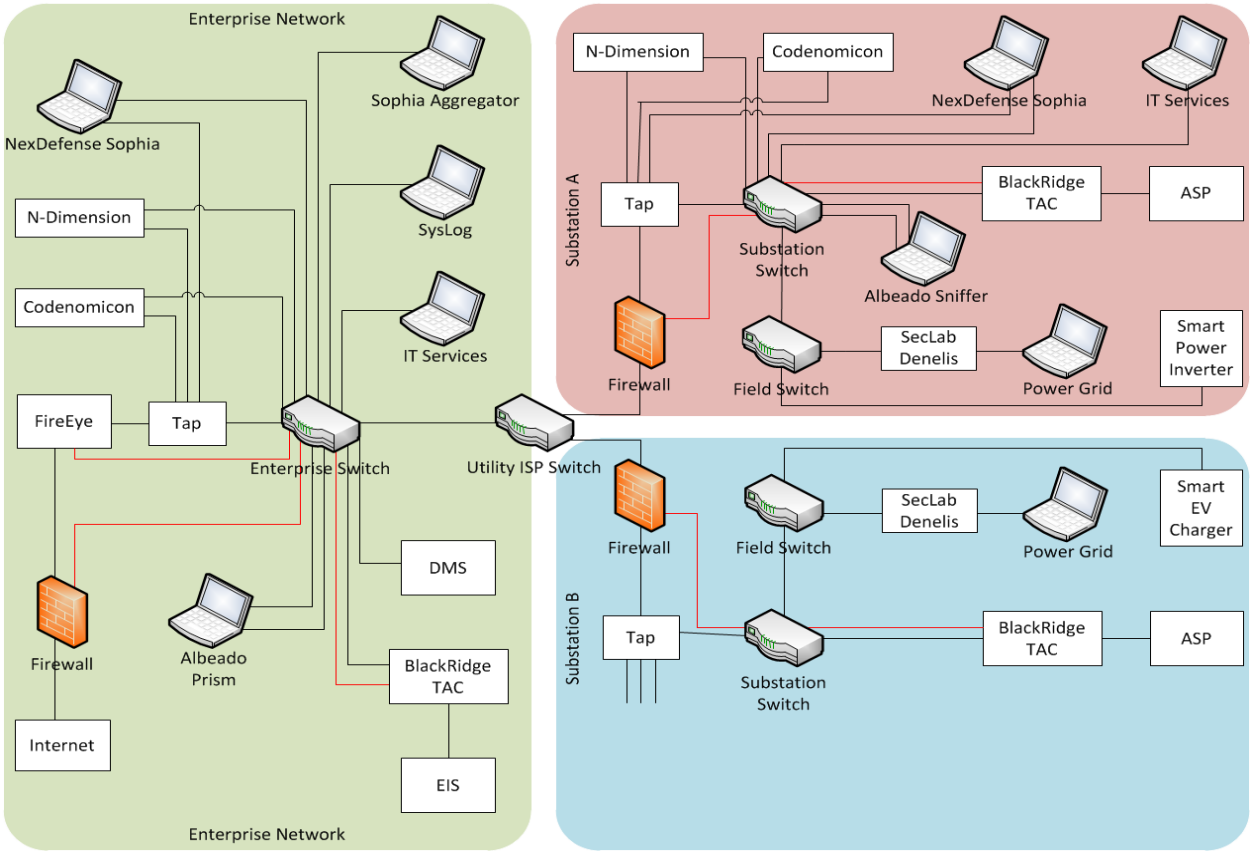
Introduction:

Today's highly internetworked business applications are exposed to a variety of threats—both internal and external. The external threats include natural disasters, amateur hackers and advanced persistent threats from nation states or non-state entities. Internal threats include disgruntled employees, industrial espionage rings, and other nefarious groups that have infiltrated legitimate enterprises. System errors can also cascade into large scale disruptions to business applications. All verticals of the economy that are dependent on information systems for day-to-day operations and business transactions are susceptible to internal and external cyber threats. Since information systems control the functions of many tangible devices at data centers and in the field, the threats can also be physical in nature. The cyber-physical interface has to be protected in both directions to ensure business continuity.

Possible Solution:

The complex cyber-physical environment in modern enterprises described above cannot be secured with traditional cybersecurity technologies such as firewalls, anti-virus servers, access control lists and username/password alone. A layered approach is needed to secure all seven logical layers of the OSI Basic Reference Model (ISO standard), as well as the semantic and business process layers that ride above them. Typically, security controls are inserted into the protocols only at the application and network layers. Not enough consideration is given to systemic security through intrusion detection technologies that combine in-line blocking with passive observation of network traffic and determine anomalous behavior by comparing actual commands between legitimate nodes with the desired commands between them for each protocol/business application of interest.

The National Renewable Energy Lab's Cyber-Physical Systems Security and Resilience Center has designed, built and tested a testbed in the Energy Systems Integration Facility (see diagram below) that incorporates a 9-layer security model. This testbed consists of electric utility distribution grid management hardware, and includes an enterprise station and two substations, protected by multiple layers of security. This security architecture is applicable to any multi-site information system in any industry vertical that has real time transactions between different end-users, end-systems or a hybrid of the two.



NREL Cyber-Physical Systems Security & Resilience Testbed

Network Description

The testbed consists of an enterprise site with a Cisco ASA 5512x firewall facing the Internet and a Cisco 3850 Layer 2/3 switch. The Cisco 3850 switch has three VLANs configured on it (Information Technology, Operational Technology and Management VLAN). The IT VLAN contains the DNS server, the SMTP server, the FTP Server and the Syslog server. The OT VLAN contains Distribution Management System and Enterprise Information System devices commonly found in the control center of a typical distribution utility. The management VLAN contains the management ports of the cybersecurity technologies, with a logical separation from the production network to limit access to only authorized network administrator staff.

The testbed connects the enterprise site with two substation sites through a mock Internet Service Provider network represented by an ISP switch. Each substation has a Cisco ASA 5512x firewall facing the ISP switch and a Cisco 3850 Layer 2/3 switch behind it representing the Bus Network, and containing the Advanced Substation Platform (substation logic in a box). Each Bus switch is connected to another Cisco 3850 Layer 2/3 switch, representing the Field Network by connecting the field equipment (Electric Vehicle Charger, Electric Storage, and Photovoltaic Simulator–which represents a solar array) to the 2 substations. The testbed uses the Open Shortest Path First (OSPF) routing protocol.

Power Systems Use Case Description:

The testbed supports Distribution Grid Management use cases such as Auto-Sectionalizing and Restoration, Volt-Var Optimization, EV charging with Demand Response, PV smoothing with Electric Storage and Frequency Regulation with Electric Storage. These use cases are supported by the Advanced Substation Platform in each substation via built-in software modules communicating with field equipment via the Modbus TCP protocol. The Advanced Substation Platform in each substation communicates with the Enterprise Information System via a proprietary protocol. The Enterprise Information System communicates with the Distribution Management System via the Distributed Network Protocol version 3 (DNP3). With these power system use cases, this testbed represents the complete ecosystem of a typical distribution utility's IT, OT and Management system.

Cyber-Security Architecture Description:

The testbed is secured by the following controls:

1. The Enterprise firewall is configured for VPN access through role-based access control, requiring unique login credentials for each user, and restricting access to specific nodes of the testbed based on their specific role.
2. Reflexive access control lists are set up to allow OT nodes to send notifications and files to the IT VLAN and receive acknowledgements. But no unilateral communication is allowed from the IT VLAN to the OT VLAN or Management VLAN under any circumstances. This allows IT/OT convergence to occur to support the Distribution Grid Management application, but without compromising the OT VLAN nodes by IT VLAN traffic that may contain inside threats, or viruses and other malware from the Internet.
3. Bi-directional data can be transmitted between the Enterprise station and each substation in the IT VLAN, between the Enterprise station and each substation in the OT VLAN, and between the Enterprise station and each substation in the Management VLAN. However, no data can be sent or received between the two substations.
4. All Cisco Layer 2/3 switches (Bus and Field) are configured with "sticky" specification, which locks the MAC address of legitimate nodes to unique interfaces of the switch. If the device is removed from the interface it cannot be re-attached unless the switch interface is re-enabled. Unauthorized MAC addresses cannot connect to any enabled interface. All unused interfaces on each switch are disabled by configuration to minimize unauthorized access by insider threat.
5. The most recent security patches and software upgrades have been applied on each server, to minimize software vulnerabilities that can be exploited by hackers.
6. Strong authentication—which is difficult to break with password cracking tools—has been enforced on each testbed node.

The testbed uses BlackRidge Transport Access Control (TAC) to provide in-line blocking to protect the Enterprise Information System and the two Advanced Substation Platforms. This system inserts authenticated tokens in the first TCP segment header to ensure that only legitimate users access these nodes. This limits the possibility of distributed denial of service attacks.

In-line blocking is also provided by the SecLab Denelis platform to prevent unauthorized access to field equipment on the Modbus TCP server. The Denelis is a hardware layer filter that strips all header information from each data packet and verifies that the payload consists of only authentic commands from a legitimate source before forwarding it to the

Modbus TCP Server, and vice versa. The SecLab device ensures the physical segregation of the network and will block network layer attacks through packet dis-assembly and assembly.

Four situational awareness tools are connected via taps located on the Enterprise and substation racks.

- The first is Albeado, which provides Business Process Layer security by comparing data at the enterprise and the substation to ensure consistency across multiple data protocols. Data fuzzing would be easily detected with this tool.
- The second is N-Dimension's N-Sentinel which is an enhanced form of the open source Snort Intrusion Detection System, which can decipher power systems protocols—such as DNP3, Modbus TCP and IEC 61850—and identify anomalies in them caused by malware, hacker attack, data fuzzing schemes and system errors. The N-Sentinel appliances are connected via the Internet to the cloud where malware signatures and other threat information is available from the classified side for continuous threat monitoring capability.
- The third is NexDefense which provides network anomaly detection capability by tracking all the simultaneous TCP sessions that are active in the testbed and providing a visualization capability on a computer screen to allow quick and effective identification of unnecessary or unauthorized communications.
- The fourth is AbuseSA from Codenomicon/Synopsys, which also provides near zero day protection from malware and advanced persistent threats through the use of a cloud-based information sharing service.

Additionally there is a file filter provided by SecLab that checks all files from peripheral devices before allowing them to be saved on the testbed server. This is mitigation for Stuxnet type virus proliferation across the air gap.

Codenomicon/Synopsys has a "Static Code Analyzer" tool that inspects software code as it is being developed to identify vulnerabilities resulting from poor coding techniques. Codenomicon/Synopsys also has AppCheck, which performs the same function as Static Code Analyzer on third party software and also verifies that there are no "back door" routines in the software that can be exploited in a production environment. Finally, Codenomicon/Synopsys also has "Defensics" which is a powerful data fuzzing tool to test how resilient applications are to dealing with adulterated data.

Conclusion:

Two months of pen testing from inside and outside the testbed did not result in a successful exploit or compromise of any system. The NREL cyber-physical systems security and resilience testbed has therefore demonstrated the value of layered security in protecting against a variety of threat vectors (internal and external to an organization), and proven that "off the shelf" cybersecurity technologies today combined with sound cybersecurity management principles can successfully protect enterprise from these threats. The assistance that enterprises need today is in developing a sound cybersecurity architecture based on business applications running across multiple sites, and on profiles of end users, to minimize vulnerabilities that can be exploited. NREL Cyber-Physical Systems Security & Resilience Team is uniquely qualified to provide this support, given its experience with the Distribution Grid Management testbed, and years of practical experience in the electric utility industry.