Securing Medical Devices and Industrial Control Systems

Palo Alto Networks and Aruba Networks Integration

Technical Security Solution Brief

As the number of network attached devices continues to grow, so do the gaps in proper identification and security. Medical devices and SCADA/ICS systems present significant problems to network security with antiquated software and specialized communication. With the help of integration efforts by Palo Alto Networks and Aruba Networks, Sun Management can help reduce the cyber attack surface.

by Mike Bermudez
Sun Management, Inc.
04 June 2015

Overview

Remote Monitoring and Control; Automated Alerting and Response; Centralized Data Collection and Visibility. These are just a few modern benefits of the Internet of Things (IoT) that is already an integral part of the current Medical and Industrial sectors. Latest technology trends suggest that these devices will only become more network aware, self-sufficient, and have the ability to intelligently and autonomously interact with other devices and their environment.

"We marveled at our own magnificence as we gave birth to AI".[1]

As with many technological achievements, the allure of the "shiny new toy" starts to dull and the darker side of humanity begins to explore vulnerabilities and discovers ways to leverage new capabilities outside of the originally conceived and designed construct. Organizations are currently faced with a network security problem resulting from a large number of devices that are attached to the network, but don't have the capacity to keep pace with the latest system patches, and cannot tolerate service outages.

Medical Problems

Medical Treatment Facilities currently host an alarming number of devices that communicate using an IP network, many of which were never originally designed to do so, and have been retrofitted with modules to translate between IP and their native communication protocols. This enables, for example, devices such as pulse and blood gas sensors to transmit data to monitoring stations and wireless mobile devices so that healthcare professionals can remotely monitor patient vital signs. Critical devices, like pacemakers, drug infusion pumps, and defibrillators may not directly interact with a corporate network, but there is evidence to suggest that the systems that support these devices have reach-back to such networks and can be used as a "pivot-point" in a cyber attack.[2] Even planning and management systems contain information that could be used to map and target specific medical devices, when compromised. These problems are often compounded by the fact that many hospital networks are connected to third-party provider networks that can be used as attack vectors or malware delivery paths.

"We are aware of hundreds of medical devices that have been infected by malware." – Bill Maisel, senior FDA official, 2013[3]

Industrial Dilemma

Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) employ technologies that are used by facilities like Nuclear Power Stations, Waste Treatment Plants, Oil Refineries, and Chemical Plants. These systems provide monitoring and control for the equipment and machinery operating is such facilities. SCADA and ICS systems are also found in most office buildings controlling elevators, physical access, and HVAC units. Although best practices call for physical and logical isolation of these systems from corporate networks, the reality is that misconfiguration, poor management, and convenience sometimes allow this gap to be bridged and leaves these infrastructure control systems vulnerable. In recent years, we have seen the ramifications of such vulnerabilities in cyber attacks like Stuxnet, Operation Aurora, and Energetic Bear. In these cyber campaigns vulnerabilities in SCADA and supporting systems were exploited, leading to data loss, and in some cases, physical destruction of property. Furthermore, new trends in access and remote management are showing how a large number of legacy Human Machine Interfaces (HMI) are being replaced by mobile devices that operate over a shared network infrastructure.[4]

"With great power comes great responsibility"[5]

Although many of the technological advancements that allow devices to collaborate and communicate more effectively have led to operational efficiency and better access to care, they present an increasing number of vulnerabilities that can leave organizations open to exploitation and attack. Security Administrators are presented with a number of challenges when attempting to secure these devices and systems, including:

- Device mobility and turnover
- Expensive firmware and hardware upgrades
- Exceedingly lengthy tech refresh cycles
- Antiquated and proprietary software with no patch support
- Vendor cost of reconfiguring hosted systems
- Intolerance of downtime for critical systems

We Have the Technology

Aruba Networks ClearPass Policy Manager (CPPM) helps solve these problems by identifying wired and wireless devices on the network, collecting information about them, and creating device fingerprints. Fingerprinting can be accomplished using any switched or wireless network vendor (agnostic) via a number of communication methods including:

- DHCP Fingerprinting
- TCP Fingerprinting
- Authentication (RADIUS, TACACS+, etc.…)
- SNMP

ClearPass stores and maintains a comprehensive database of device fingerprints. Aruba Networks is constantly updating this database to capture changes in protocol communication, device updates and upgrades, and new devices. ClearPass administrators have the ability to create new fingerprints for unknown devices and assign custom attributes.

Once devices are identified, the information collected by ClearPass can be shared with Palo Alto Networks firewalls via the Palo Alto XML API. The following attributes are currently available to be passed to Palo Alto firewalls:

- Source IP Address
- Hostname
- Domain/Username (when user authentication is performed)
- MAC Address (when no user authentication occurs)
- Device Type or Operating System

The Palo Alto firewalls receive these attributes and store them in Dynamic Tags and Address Groups, User Identification (User-ID) databases, and Host Information Profiles (HIP). This grouping of objects allows firewall administrators to create extremely granular security policies that control network traffic in a Least-Privileged, Zero Trust security model. Furthermore, the attribute information collected and shared by Aruba ClearPass is dynamically updated and passed to the Palo Alto firewalls in real-time to keep the security policies up-to-date with changing network elements.

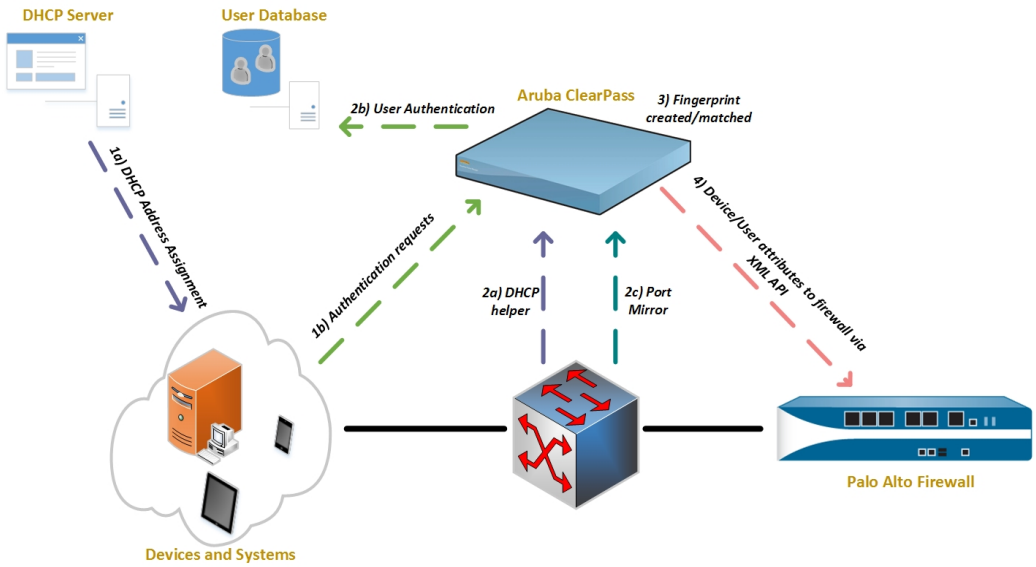
Device identification, fingerprinting, and sharing of attribute information is done to correctly map devices to the appropriate network traffic. Palo Alto Networks can then apply industry-leading Layer 7 Application Identification (App-ID) and Threat Protection (Content-ID) mechanisms to further control and secure the network.

Palo Alto Networks currently has a number of Application and Threat signatures that have been developed to specifically identify proprietary network communication (e.g. HL7, Modbus, DNPv3) and protect against vulnerabilities and malware that target specialized medical devices and ICS systems, as well as the components and infrastructures that support these systems.

In addition to known traffic and threats, Palo Alto Networks WildFire service offers detection and prevention capabilities for unknown or 0-Day threats.

- cip-ethernet-ip
- cygnet-scada
- dnp3
- elcom-90
- iccp
- iec-60870-5-104
  - 104asdu-process-monitor
- ieee-c37.118-synchrophasor
- modbus
  - modbus-base
  - modbus-write-multiple-coils
  - modbus-write-file-record
  - modbus-read-write-register
  - modbus-write-single-coil
  - modbus-write-single-register
  - modbus-write-multiple-registers
  - modbus-read-input-registers
  - modbus-encapsulated-transport
  - modbus-read-coils
  - modbus-read-discrete-inputs
  - modbus-mask-write-register
  - modbus-read-fifo-queue
  - modbus-read-file-record
  - modbus-read-holding-registers
- opc
- osisoft-pi
- siemens-factorylink

Example Workflow



Forensics and Incident Response

In addition to proactive security through visibility and granular control, the Aruba/Palo Alto integration produces detailed data that can be extremely useful for Enterprise Traffic Analysis, Network Forensics, and Incident Response. Through the use of Palo Alto Networks Application Command Center (ACC) and detailed logging information, analysts and administrators can create customized summary reports, generate and forward alerts using various delivery methods, and search for specific events to provide contextual evidence of potential security breaches. Aruba ClearPass can store information indicating device interactions with the network (e.g. authentication events; IP address assignments; changes in network posture) and update external logging and monitoring systems.

Summary

Using advanced visibility, comprehensive control, and centralized monitoring features can greatly enhance the network security posture of an organization. The integrated solution between Aruba Networks ClearPass and Palo Alto Networks Next-Generation Firewalls can provide these capabilities to help secure current network deployments and position organizations to proactively address evolving threats.

Additional Resources

http://www.arubanetworks.com/pdf/partners/SO_PaloAltoNetworks.pdf

http://www.arubanetworks.com/pdf/products/SO_ClearPass.pdf

http://www.arubanetworks.com/clearpass-case-studies

https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/technology-solutions-briefs/aruba.pdf

https://www.paloaltonetworks.com/solutions/industry/scada-and-industrial-control.html

https://www.paloaltonetworks.com/solutions/industry/healthcare.html

http://researchcenter.paloaltonetworks.com/2015/04/nss-labs-releases-latest-next-generation-ips-report-palo-alto-networks-achieves-superior-security-efficacy

http://researchcenter.paloaltonetworks.com/2015/04/palo-alto-networks-now-a-four-time-gartner-magic-quadrant-leader

---

[1] The Matrix. Dir. Andy Wachowski and Larry Wachowski. Warner Bros. Pictures, 1999. Film.
[2] http://www.wired.com/2014/06/hospital-networks-leaking-data
[3] http://www.wsj.com/articles/SB10001424127887324188604578543162744943762
[4] http://innovativecontrols.com/blog/rise-mobile-devices-and-scada-remote-access
[5] Spider-Man. Dir. Sam Raimi. Columbia Pictures, 2002. Film.