Stateful Contextually-Aware Access Control for ICS

Nancy Cam-Winget
Distinguished Engineer
Cisco Systems

Paul Didier
Solutions Architect
Cisco Systems

Presented at the ODVA
2014 Industry Conference & 16th Annual Meeting
March 11-13, 2014
Phoenix, Arizona, USA

Abstract:

Industrial Control Systems (ICS) stay abreast with the Internet revolution by improving their productivity and efficiency through the use of standard networking technology that enables remote access and mobile systems. With trends to improve production by leveraging supply chains to a global scale and outsourcing services for improved efficiency, management and security, care must be taken to ensure that the very services and devices entering the ICS whether remotely or thru a mobile environment do not further introduce or are introduced to security vulnerabilities.

This paper will describe how the use of stateful and contextually-aware access control systems can aide in both the visibility as well as the enforcement of when and how devices can access and control ICS functions.

Keywords:

Role-Based Access Control (RBAC), Deep Packet Inspection (DPI), Machine-to-Machine (M2M), Internet Protocol (IP), Network Visibility, Context Awareness, Stateful Contextually-Aware Policy

Definition of terms:

Contextually-aware access control: a network device may affect access control based on a given context. In a traditional network environment, this is typically enforced by firewall software which can filter TCP and UDP packets based on application layer controls; as security solutions evolve, the notion of context-based access control can span not just firewalls, but other policy evaluation and enforcement points.

Deep Packet Inspection: a network device may inspect beyond the packet header to gain more information to better affect access control and to further build a session context.

Network Visibility: the means to have awareness of who (humans and devices), what (applications) and how the communications are traversing through the network.

Role-Based Access Control: access control is based on a device or human's role.

 ©2014 ODVA, Inc.

Introduction

Evolving trends to improve productivity and efficiency in Industrial Control Systems (ICS) bring challenges to both safety and security. As ICS environments make use of IP as well as non-IP enabled devices with the need to also grant access to employees, partners and contractors either remotely or at the site, appropriate access controls to manage where and how both the M2M devices and humans can access resources becomes a necessity. In such an evolving complex ICS environment, uniquely identifying M2M devices from human-driven devices (e.g. a HMI) and the humans attached to them, their location, their means of access and their assigned roles becomes a necessity to affect the right access control and ensure, for instance, that humans are compliant to only manage devices assigned to them as well as to ensure safety and security of the overall ICS environment. To make such distinctions, mechanisms and tools to facilitate this network visibility and affect the required access controls are described in this paper.

1. Why is Contextual Awareness needed?

Security professionals in an ICS environment are faced with more complex deployments and sophisticated adversaries and the tools available to them. There is an evolving breed of attackers that are far more patient and willing to take a methodical approach to penetrate devices within a network in order to maintain a persistent foothold for purposes of either stealing or breaching intellectual property, breaching safety practices or causing physical harm. It is no longer sufficient to know "who" or "what" is in the network, but to be contextually aware of "who" and "what" is in the network, "how" and "what" they are accessing the network as well and "when" and "where" they are accessing resources.

As attackers learn to adapt their tools to infiltrate and bypass established intrusion prevention signatures, they also leverage established software techniques to install malware which can be triggered by them at their own will (and time) and enable them to take control of the ICS environment. These and other techniques used to obfuscate communications between the device and command and control networks provide challenges to find and address such breaches. The first step in approaching such attacks is to be able to continually monitor, assess and be contextually aware of "when", "where", "who" and "what" is flowing through the network, e.g., be stateful and contextually aware.

1.1 Building Contextual-awareness through Network Visibility

Network visibility is the means by which network elements, systems, IT (and OT) and security organizations can gain information about who, what, when, where and how information flows through the network. Several techniques and technologies exist to address and provide network visibility, from as simple as identifying who is on the network (e.g. logging a MAC address) to defining how the "who" in the network is *behaving* (e.g. building behavioral and reputational models[7]).

Visibility can begin at the instance a device enters the network. As an example, Figure 1 demonstrates a scenario where NW1, acting as a network access element, can begin to build network visibility by constructing a *context* based on observed events:

1. NW1 acting as a network access edge element, is the first network control point to control access to *things* and *humans*. Whether it is through a (switch) port-link up or an IEEE 802.11 association request [6] or an IEEE 802.1X authentication [5], NW1 can create or update a record into its *context* table (see Table 1) indicating that a new network presence, identified by the MAC address is attempting to access the network as well as the time it initiated the connection.
2. NW1 may also determine how the device initiated the connection, e.g. through a wired port, an IEEE 802.11 association request or through a remote connection and update the corresponding record entry.
3. NW1 can further proxy authentication mechanisms like IEE 802.1X [5] to further extract the username or the *role* assigned (e.g., employee, contractor, guest or an explicit assigned job function) and update the record entry.
4. As NW1 is also in the direct traffic path, it can further inspect the actual network packets to and from a device (e.g., affect deep packet inspection) to determine either or both the device type and the types of applications being accessed from or to the device.

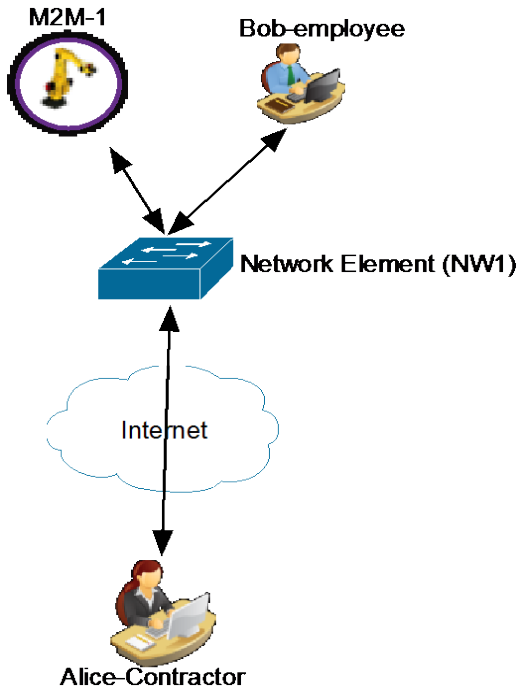

Figure 1 Building Contextual Awareness at the Network Edge

Thus, as M2M devices, HMIs and remote users join the network through an access device such as NW1, *contextual awareness* based on the events it controls can thus be constructed as shown in Table 1.

Who	Role	Device Type	MAC address	How	Access Time
M2M-1	assembly	Robot Arm	00:00:bc:01:02:03	wired	7:00 AM PST
Bob	employee	HMI	00:26:b9:10:20:30	wired	9:00 AM PST
Alice	contractor	IBM Laptop	00:24:d7:9F:88:b5	remote	1:00 PM PST

Table 1 Contents of NW1 Contextual Awareness Database

In this particular example, the context table is populated based on the steps affected by NW1 as a device or human on a device requests access to the network and NW1's configured policy to provide the different levels of access controls. A simple sample set of policies can be defined as:

Policy Name	Policy Rule	Policy Action
M2M	Any M2M device, inside the network	Full Access
Employees	Any employee on any HMI	Full Access
Contractors	Any contractor on any HMI, inside the network	Limit Access

The information in the context database is defined by NW1's configured policy rules as defined above. Note that the Policy Rules expression defines the attributes (e.g. device type and a type of *role* for the human) that lead to an access control (or policy) action. Note however, that there can be other devices dedicated to building network visibility beyond those described by the Policy Rules above.

Other network visibility tools may involve dedicated sensors that are typically co-located or connected (as co-processors, modules or systems) to a network element or the network infrastructure to further inspect, analyze and aggregate information and further enrich awareness to be both stateful and contextual. For instance, the example shown in Table 1 keeps *stateful* information relative to the devices that have attached through the one particular network element, NW1. Technologies already exist to provide in-depth visibility of users, devices, applications and

their behavioral patterns [1][2][3][4]. Leveraging these network visibility tools enables the required stateful, contextually-aware access controls required to secure and maintain ICS safety.

2. Affecting Stateful-Contextually Aware Access Controls

With the use of network visibility tools such as those described in the previous section, an ICS environment can begin to segment the network via specific access controls and VLAN assignments and define the appropriate rules to affect security and safety. Standard technologies already exist to aide in the detection of malware, as well as provide role-based access controls [2] and are deployed in enterprise networks today to address some aspects of network security, e.g. malware and identity based access control respectively. However, an ICS environment requires that both security and safety be maintained. For example, vulnerable HMIs or computer systems in a manufacturing plant can be remediated through existing patch management systems; however, these patches should only be done without risk of forcing a full system shutdown or imposing safety concerns. Thus, there should be a means to define the appropriate access controls by which remediation can occur to minimize security risks and allay safety concerns.

In using a network infrastructure such as that shown in Figure 2, contextual-aware policies and controls can be defined both at the enterprise as well as down in the manufacturing area (e.g. lower Levels 0-3 of the Purdue Model). A stateful, contextually-aware policy system at Levels 0-3 allows network elements to affect finer grain controls that can be tailored to a specific device on a particular cell zone and facilitate the means to address both security and safety.

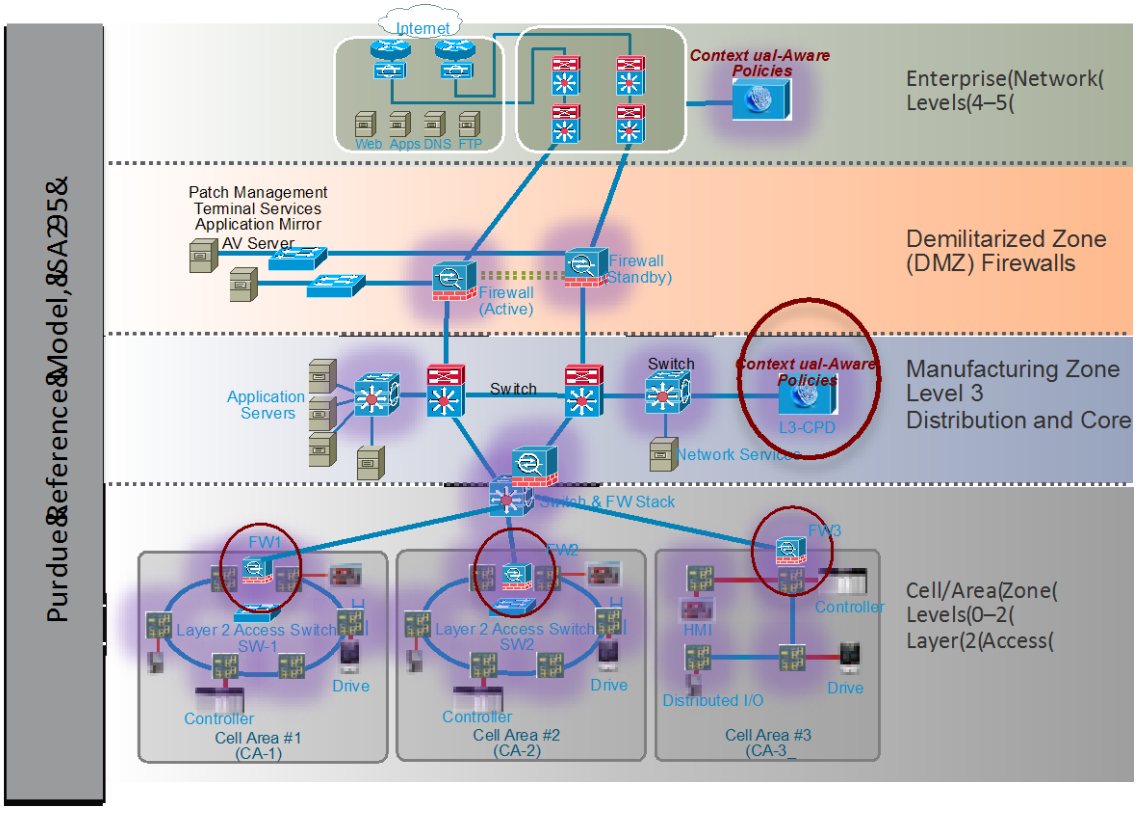

Figure 2 Using Contextual-Aware Policies and Enforcement at Levels 0-3

 ©2014 ODVA, Inc.

In the current example, a policy addressing both security and safety can be defined as:

Disallow any software updates if any device is active within a cell zone

Note that the policy statement requires that both real-time, dynamic state and contextual awareness be maintained to determine how access controls are to be affected:

- Contextual: a logical grouping of a Cell Area and the devices currently participating in a particular Cell Area is required and can be achieved by sensors that are collecting network visibility information either at Levels 2 or 3. In this example, a *contextually-aware* aggregator is instantiated in Level 3 for this purpose.
- Statefulness: awareness of what devices are currently active (e.g. if there is any network traffic, or general activity) need to be maintained.

In this example, the Cell Area grouping and its context would be defined and stored at the Level 3 contextually-aware policy device (L3-CPD). The switches and firewalls in Level 2 communicate with the L3-CPD to provide the telemetry needed by L3-CPD to build its stateful context as:

Group	Who	Role	Device Type	MAC address	Access Time	Activity Status
CA-1	M2M	assembly	Controller	00:00:bc:01:02:03	7:00 AM PST	active
CA-1	Bob	employee	HMI	00:26:b9:10:20:30	7:00 AM PST	inactive
CA-2	M2M	assembly	PLC	00:00:bc:01:02:13	7:00 AM PST	inactive
CA-2	Admin	employee	HMI	00:26:b9:10:20:31	7:00 AM PST	inactive
CA-3	Admin	employee	HMI	00:26:b9:10:20:40	7:00 AM PST	inactive
CA-3	M2M	assembly	Controller	00:00:bc:01:02:23	7:00 AM PST	active

Table 2 Stateful Contextually Aware Table

L3-CPD builds its stateful contextual awareness database either as it is classifying attributes in during policy evaluation (as described in Section 1.1). It can also query other systems for information to analyze and aggregate into its database. For instance, to determine "Activity Status", L3-CPD may span information beyond a device being "connected to the network", by having the firewalls (FW1, FW2 and FW3) provide information on the type of network traffic flowing, e.g. traffic accessing data resources or other m2m devices or receiving control type functions may trigger an "active" status. Note that stateful information, e.g. "Activity Status" requires that L3-CPD do continuous monitoring, analysis and evaluation to ensure the database is up to date.

2.1 Aggregated Stateful Contextual Awareness

To enforce the sample policy described above and evaluate the determination of "any device is active", aggregated context expanding on data shown in Table 1 are required; both dynamic state of the devices and their relative group membership must be maintained. As shown in Table 2, new attributes to a contextual record are added to describe the "Group" membership as well as each individual's activity status.

Several mechanisms exist today to determine "Group" membership:

- Identity Management systems such as Lightweight Directory Access Protocol (LDAP) or Microsoft's Active Directory allow for group membership definitions to map identities (humans, devices, computers, etc.) to defined groups.
- Network elements, in the policy definitions may also allow for pre-configuration of established groupings either through IP address ranges or abstract groupings (Table 2.)

- Group memberships can also be formed dynamically by sensors that are configured to cluster or "group" network session flows (by MAC addresses or IP addresses) based on configured criteria. For example, a sensor may cluster or group all session flows that have accessed Skype to belong to a "computer" group.

To establish "activity status", L3-CPD needs to collect information from several network elements, analyze and evaluate the data to determine if a particular device is "active". For example, an HMI device transmits and receives data both to coalesce reports to present to a human as well as to allow the human to affect control of other devices. A definition of "activity" for an HMI may be defined as "active" only when there is human intervention involved; network control or management traffic and application data transmitted and received for purposes of report production do not force an "active" status, but all other types of functions or application layer traffic would trigger a positive "active" status. To determine this "activity status", L3-CPD could make such a determination by collecting all network traffic from the Level 2 firewalls to inspect and analyze, or it could instruct the Level 2 firewalls to inspect their traffic and trigger an event to L3-CPD when there is any ICS control or configuration traffic as well as any access to non-ICS applications (e.g., Skype, Microsoft Word, etc).

2.2 Enforcement of Stateful Contextually Aware Policies

Policies must be dynamically enabled and disabled as the network infrastructure responds to the state changes and context updates it observes. To affect the general policy of: *"Disallow any software updates if any device is active within a cell zone"*, the Level 3 Contextually-Aware Policy engine can affect policies to be enforced, disabled or updated at the Level 2 switches and firewalls. In particular, two policies (Table 3) are defined and configured at the Level 2 firewalls:

Policy Name	**Policy State**	**Policy Action**	**State Parameters**		**DPI parameters**
			Grouping	**Group-State**	
Allow-Remediation	Disabled	Allow	Cell-Zone	inactive	Allow only the permitted traffic between devices, including control and configuration commands
Block-Remediation	Enabled	Limit	Cell-Zone	active	Disallow ICS protocol commands that control and configure devices

Table 3 FW1 and FW3 Stateful Contextual Aware Policy Definitions

As L3-CPD evaluates from a broader view of "Cell Area" grouping, and the state within that grouping, it determines what policies must be affected by the different firewalls. In the example and current contextual state defined in Table 2, only Cell Area 2 is inactive; L3-CPD instructs the respective firewalls of the right policy to enable, disable or both. That is, L3-CPD would communicate with FW1 and FW3 to reflect the policy table shown in Table 3 while FW2 would be instructed to "Enable" the "Allow-Remediation" policy while setting "Disabled" the "Block-Remediation" policy.

3. Conclusion

This paper describes how stateful contextual awareness can be established and leveraged to provide both improved network visibility as well as stateful contextually-aware policy definitions. By establishing such awareness, steps to improve security and safety can be addressed:

- Detect and Block at the edge: by learning the device type and role of the device (or human), the access edge can act as the first tier discriminator for providing the first level of contextually-aware access control tier
- Protecting through the Network: with the use of stateful contextual awareness, the network can further refine and limit where, when and what devices and how resources can be accessed.

References:

[1] Bradford Networks Whitepaper, “Network Visibility”, http://www.bradfordnetworks.com/whitepaper-network-visibility
[2] Cisco Systems Whitepaper, “Identity Based Networking Systems: MAC Security”, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html#wp9000231
[3] Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 191–192
[4] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007 ISBN 978-0-471-74300-2, pp. 203–209
[5] IEEE 802.1X, http://standards.ieee.org/getieee802/download/802.1X-2004.pdf
[6] IEEE 802.11, http://standards.ieee.org/getieee802/download/802.11-2012.pdf
[7] Nguyen, H. T., Zhao, W. and Yang, J., “A Trust and Reputation Model based on Bayesian Network for Web Services”, ICWS, pp.251-258, 2010 IEEE International Conference on Web Services, 2010

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2014 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org.
CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP Safety, CIP Sync, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.