Needle in a Haystack?  
Getting to Attribution in Control Systems  

January 2012  
A SANS Whitepaper  

Written by: Matthew E. Luallen  

Control System Event Logging  PAGE 2  
Getting to Attribution  PAGE 5  
Monitor, Analyze, Respond and Attribute  PAGE 11
Control systems are responsible for critical operations and have become increasingly more frequent targets of attack. In July 2011, a known member of Anonymous posted information associated with control system attack vectors, and in October, the information-collecting tool Duqu was identified as collecting critical control system data to be used in attacks against those specific systems. As depicted in a recent series of articles, Duqu may give evidence to a cyberweapon platform that builds attack code using Stuxnet and Duqu as the bullets—bullets that can be directed at specific critical infrastructure such as control systems.

The most critical control systems provide energy, water and transportation. It is those systems we worry about most. Not only do we worry about loss of Intellectual Property (IP) and Personal Identifiable Information (PII), but also we worry about Personnel Loss of Life (PLL).

With these systems increasingly targeted, there is little or no way to assign attribution to attackers who find their way into these systems and attempt to control them. Why? The control system components do not natively log the events of interest, and they lack supplemental controls to create the events. Many devices may not even be programmed to generate the events. The challenge becomes even greater because many cyber assets operate on old and vulnerable code bases.

Working in the realm of cybercontrols creates an interesting situation in which people cannot classify myriad events using their traditional five senses. Therefore, mechanisms for achieving attribution must be implemented across physical, cyber and operational controls using additional tools. Many tools attempt to address the challenge of control system protection; however, very few specifically address the issue of control system cyber attack attribution. Addressing the physical portion of this challenge is commonly referred to as false flag operations.

With proper controls, events can be contained. One such example is the media hyping as a hack what turned out to be misinterpreted operations and VPN activity at the Curren Garden Water District outside of Springfield, Ill. All it takes is proper logging, correlation and event data handling to prevent such hyperbole from spreading. This case highlights the challenges in associating event activity with approved operations to detect problems. Such public-facing events also illustrate the need for well-defined public–private partnerships that could, potentially, lead to the correlation of activity across geopolitical boundaries for deeper insight to where the attack originated.

Control system cyber assets include Programmable Logic Controllers (PLCs); Master and Remote Terminal Units (MTUs/RTUs); traditional laptops, workstations and servers with applications; embedded microcontrollers; sensors; and actuators controlled across wide area and local area communications links. These systems may be dispersed across field sites, control rooms at a processing facilities and control centers, as shown in Figure 1.

Many of these cyber assets do not natively create event logs, but instead rely on separate—and possibly not implemented—control system historian and change management functions to record operational events within the environment. The control system historian and change-monitoring applications typically are added to the environments for troubleshooting control failures and identifying control operations to increase system reliability. These functions are not commonly added to reactively or proactively identify malicious system activity.

As is common in most cases, the only true security occurs at the Human Machine Interface (HMI) workstation using common operating system logs, remote access Virtual Private Networks (VPN) authentication and physical security systems programmed with access restrictions to the facility, control rooms and cabinets housing equipment.
Ultimately, successful event attribution requires a correct classification of time-indexed events of interest as approved or unapproved changes and as accidental or malicious events. These events should include traditional login and access events, physical access events, as well as changes, configuration alterations and other granular attributes. These types of security events far exceed what are traditionally logged and monitored in control systems.

The following two real-world and training control system events highlight the need to extend beyond the traditional event logs and perform accurate system baselining, enhanced security event logging, correlation and analysis.

**Control System Real Event Example (Springfield, Ill., Curren Garden Water District)**

In November 2011, a private report (and subsequent news reports) discussed how a physical water pump at a facility outside of Springfield, Ill., may have been destroyed by hackers outside of the United States. Days later, further analysis indicated the activity originally associated with another country was attributed to a contractor on vacation. The situation highlights the need for extreme accuracy of attribution and the relationships between public and private entities. The challenge appears to have come from directly associating approved control system activity with approved remote access events.

We may never know the full story, but many lessons can be learned from the public versions. Foremost, we must ensure that event logs are available that correlate activity across a ticket-based operations change management system, physical facility access, electronic remote access VPNs, HMI operator logins and control system historians. This level of event logs has an expectation that the control system environment uses unique user IDs for personnel, has physically and electronically controlled cyber assets, and leverages an event-generating defense-in-depth architecture.

This case also includes some interesting security concerns, such as the ability of a contractor physically located in another country being able to access a control system across the Internet using his smartphone. Current geopolitical conditions warrant continuous technical limitations and operational controls placed on communication channels as well as the use of portable devices while key personnel are traveling to areas of potentially less trust.

---

Control System Training Event Example (Tiger Trap)

In September 2011, students and professionals converged at four major universities in Louisiana to participate in the annual cyber Capture the Flag exercise called “Tiger Trap,” sponsored by the FBI InfraGard, the Information Systems Audit and Control Association (ISACA) and control system vendors. The 2011 Tiger Trap included the CYBATI portable control system training kit used at each of the four locations posing as tempting cyber assets belonging to the virtual Chemical Company. Participants were unable to reach the control system environment during the weekend event. However, on the second day, a “rogue insider” compromised the system with a modified mouse, as shown in Figure 2.

![Figure 2. CYBATI-Modified Mouse with USB Hub and Teensy++](image)

Two hours after being inserted, the PowerShell script operated flawlessly on the fully patched Microsoft Windows 7 operator workstation, causing the virtual fluid pump to fail catastrophically. Meanwhile, the HMI tags being swapped with faulty points created false operator readings, so the change in operational state was not immediately depicted in the HMI. After the change was identified, the local operator at the Tiger Trap site did not notify other team members.

In terms of attribution, the participants were successful in using the HMI logs to identify the time of the pump failure. However, because the system was never inventoried to understand what applications, files, attributes, user accounts and devices were connected to it before the attack, there was no way to perform a comparison between the before and after states when the pump was impacted. This example highlights the need to baseline the environment, log and monitor system activity events, and respond as a team if suspected activity is identified.

Other similar incidents include the Polish Tram System unauthenticated track switching administration, the BP Texas Refinery false sensor readings, and the attempts to achieve attribution with PLCs with hard-coded passwords as seen recently with vendors such as Schneider and Siemens. Associate these activities with the described simplicity of crafting Metasploit exploits to turn off, on or even rewrite PLC logic by students involved with DePaul University’s CNS 366/466 Critical Infrastructure and Control Systems Cybersecurity course, and it becomes obvious that there is a serious lack of attribution across the involved systems.

4  [www.theregister.co.uk/2008/01/11/tram_hack](http://www.theregister.co.uk/2008/01/11/tram_hack) (accessed Jan. 9, 2012)
Getting to Attribution

Attribution is necessary to keep individuals and nation states in check within the cyber arms race. Without absolute attribution, the potential for errant finger pointing may just provide the pathway to the next major multinational war.

Attribution is the act of associating an individual or group of individuals with an activity. The level of associated attribution begins by directly associating the event with the threat actors and maybe to additional sponsors of the activity (for example, nation states, organized crime units, competitors and activist groups). Ultimately, attribution involves finding answers to the following seven questions:

1. What occurred within the system?
2. How did the attacker gain a foothold?
3. What vulnerability did the attacker exploit to access the system?
4. What actions did the attacker perform on the compromised system?
5. Is the attack still ongoing?
6. What actions can be performed to reduce the current risk?
7. How can this attack be prevented in the future?

Getting accurate answers to these questions starts with validating existing controls and deficiencies.

Identifying Deficiencies and Validating Controls

Attack tree analysis can serve as a foundation to identify architectural deficiencies. The analysis ultimately dictates what security controls should be implemented to increase the difficulty associated with the sophistication and motivation of the threat agent. For example, it does not make sense to spend $1,000 to protect an asset worth $100.

This is a difficult model for control systems because, by default, no other barrier exists between the safest cyberlocation and the most dangerous. Control system devices trust their environment and have a wide attack surface, as shown in Figure 3 (on next page).
Many control system components lack the most basic security mechanisms and have:

- Limited or no authentication requirements
- Firmware updates that are openly accessible and susceptible to reverse engineering
- No vendor hardening guidelines
- No standard deployments
- Unprotected network communications
- Exposed information on public forums

It is essential that we identify the most pervasive and valuable security controls to protect these and other attack surfaces and monitor them well. A good resource is a thesis developed by a Major at the Air Force Institute of Technology (AFIT) that discusses the Stuxnet attack tree used to gain and install persistent access, exploit network and host vulnerabilities, establish a command and control channel, and then erase the event logs and update the attack logic. The thesis, titled “Evaluating Information Assurance Control Effectiveness on an Air Force Supervisory Control and Data Acquisition (SCADA) System,” recommends the need for the categorical and most influential Information Assurance (IA) controls depicted in Table 1 (on next page).

---

Figure 3. Control System Attack Surfaces

Copyright © 2012 – CYBATI www.cybati.org
The appropriate categorical IA controls must be integrated into the control system environment to create the events to analyze. This important step is necessary to assure substantiating evidence is available to attribute the events to a specific source.

**Incorporating Enhanced Control System Event Analysis**

Security is a constant process professionals follow to assure the appropriate use of assets. Well-trained professionals must continuously monitor, analyze, respond to and attribute these events to protect the assets. The process involves the organization integrating a variety of internal and external physical, cyber and operational controls and sensors to deter, defend and detect events. System baselines must be developed to identify normal and approved system activity. A typical starting point is to inventory operational procedures and their use of cyber assets. The next step is to identify common cyber-to-cyber Internet Protocol (IP) communication patterns, user and administrative logins, application usage, physical access, existing hardware and software, portable devices and remote access. These steps serve as an excellent start to baselining cybersystems and are required for any form of event analysis.

---

**Table 1. Recommended Controls**

<table>
<thead>
<tr>
<th>Management Controls</th>
<th>Operational Controls</th>
<th>Technical Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>Awareness and training</td>
<td>Audit and accountability</td>
</tr>
<tr>
<td>Certification, accreditation and security assessments</td>
<td>Configuration management</td>
<td>Identification and authentication</td>
</tr>
<tr>
<td>System and service acquisition</td>
<td>Incident response</td>
<td>Password authentication</td>
</tr>
<tr>
<td></td>
<td>Intrusion detection and prevention</td>
<td>Role-based access control</td>
</tr>
<tr>
<td></td>
<td>Malicious code detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patch management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System and information integrity</td>
<td></td>
</tr>
</tbody>
</table>
Asset Owners and Operators

Although several traditional control system components, such as processing servers, HMIIs and even embedded controllers, have been and continue to be replaced with common IT operating platforms, there is still difficulty in altering any of the components available as OEMs or their configuration to support security enhancements. This leaves most asset owners and operators with the need to bolt on security, leveraging passive detectors, augmented applications and homegrown tools that must also be maintained and updated. Table 2 provides guidance for achieving attribution with internal systems.

Table 2. Internal Event Analysis for Enhanced Attribution

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Cyber, Operational, or Physical Control</th>
<th>Example Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>System and Service Acquisition</td>
<td>Perform strict change management of cyber asset, personnel and physical asset provisioning and decommissioning.</td>
<td>Enable correlation rule to associate new cyber asset connections with purchase orders and physical facility equipment access.</td>
</tr>
<tr>
<td>Configuration and Patch Management</td>
<td>Cyber: Track configuration modifications and validate reporting of changes. Monitor and associate applicable vendor notifications for software security updates.</td>
<td>Associate approved changes within a specific timeframe to electronic modifications and physical access to facility.</td>
</tr>
<tr>
<td></td>
<td>Operational: Track facility contracts to identify pending operational and asset changes.</td>
<td>Correlate trouble tickets with patch management and administrative updates of cyber assets.</td>
</tr>
<tr>
<td></td>
<td>Physical: Monitor restricted access areas such as control system component cabinets, operator control rooms and communications equipment.</td>
<td></td>
</tr>
<tr>
<td>Continuous Vulnerability Assessment</td>
<td>Cyber: Monitor device-to-device ISO layer 3 protocol, configure IDS to alert for devices that shouldn’t be talking to each other. Integrate deep packet inspection and inline prevention to limit control system protocol behavior.</td>
<td>Correlation between onsite and offsite historian of cyber, physical and operational events.</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention</td>
<td>Monitor system state and usage (CPU, memory, storage, halt, shutdown, reboot, I/O control and alarms), as well as application and hosts for granular system modifications.</td>
<td>Identify necessary cyber asset communications during process startup and shutdown with associated work schedule operators and supporting operations based upon Human Resources hourly work plans.</td>
</tr>
<tr>
<td>System and Information Integrity</td>
<td>Operational: Monitor the process control system startup and shutdown and I/O alarms and control. Monitor/control portable electronic devices and media maintained by personnel.</td>
<td>Enable operational procedures to require and enforce personnel to declare cyber assets at the physical facility entrances and limit remote access based upon geopolitical domain and remote system trustworthiness.</td>
</tr>
<tr>
<td>Malicious Code Detection</td>
<td>Physical: Monitor operator access to facilities as well as for personal portable media devices and electronic equipment. Also monitor wireless spectrum communication channels and physical modifications in secured facilities.</td>
<td></td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Cyber: Monitor operator, administrative and remote access logins separately.</td>
<td>Enable correlation rules to identify users badged in to facility logging in via remote access (i.e., identifies account sharing or rogue access).</td>
</tr>
<tr>
<td></td>
<td>Operational: Monitor established procedures to ensure no sharing of credentials while understanding the safety considerations.</td>
<td>Enable correlations identifying GPS locations of vehicles performing services to field sites and work order records.</td>
</tr>
<tr>
<td></td>
<td>Physical: Monitor facility entrance/exit; door entry/exit; cabinet open/close; live video surveillance.</td>
<td>Manage administrative physical and cyber access using operational procedures and SCADA controls/alerts (i.e., develop control system HMI points with physical and cybernotifications and control).</td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td>Cyber: Enable unique, need-to-know user logins for all control system personnel.</td>
<td>Enable correlation rules based upon responsibilities of anomalous user activity (e.g., administrative access to two systems within a day when the administrator or system account has never performed this task).</td>
</tr>
<tr>
<td></td>
<td>Operational: Perform continuous personnel background screening and access needs analysis.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical: Limit physical access to facilities based upon need to know.</td>
<td></td>
</tr>
</tbody>
</table>
As depicted in part of Table 2, the ultimate organizational goal is to establish a model of continuous vulnerability assessments. For more information about this process, check out the author’s recent article, “Cyber Security Vulnerability Assessment.”

Other components are necessary to support internal event logging and analysis, such as the following:

- Centralized reference clock to timestamp events
- Onsite and offsite logging systems to receive and archive the event logs
- Communication channels across physical, cyber and operational event processing systems, such as physical security, operations and cybersecurity systems that limit the creation of additional exposures (for example, one-way diode communication devices)

Note that it is also common for organizations to use the initial implementations of controls and event analysis to create an approved activity baseline. If an organization has never performed event analysis, it is also common to find a few systems that are being used in ways not approved by the organization, either internally or externally. Therefore, having a response team with a well-defined mission for escalating and responding to the information associated with the identified activities is important.

External Analysis

External event analysis helps develop awareness of the changing threat landscape that may potentially lead to intrusion. It is important to establish relationships with external entities and sources across cyber, operational and physical domains, as shown in Table 3.

<table>
<thead>
<tr>
<th>Cyber</th>
<th>Operational</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish and maintain relationships with local law enforcement and resources, along with commercial and government response entities. Develop reporting procedures for specific circumstances.</td>
<td>Establish peer groups among industry stakeholders.</td>
<td>Subscribe to a physical threat notification service associated with your physical asset locations.</td>
</tr>
<tr>
<td>Subscribe to vulnerability notification and analysis service associated with your organization’s cyber assets and supporting firmware and software.</td>
<td>If contractually allowed, monitor open source intelligence regarding business and personal activities (e.g., online social media and local traditional media).</td>
<td>Maintain situational awareness of current local security conditions around facilities and social activism.</td>
</tr>
<tr>
<td>Maintain situational awareness through regional CERT activity and vendor notifications.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3. External Event Analysis

---

Physical Backups

Reports pertaining to the Kleen Energy Power Plant explosion in Middletown, Conn., on Feb. 7, 2010 do not discuss any cyberforensics efforts. Yet, witnesses stated, “the explosion took place when workers switched on the plant's energy generating systems during a test.” The Kleen Energy plant control system leveraged a Siemens control system at a time when Stuxnet was known to be roving the Internet. However, even if the team had the means to investigate further, the analysis may have been unsuccessful because most cyber assets were lost in the explosion. This example highlights the need for backup procedures, such as offline logging historians and explosion/electronic magnetic pulse resistant control system event recorders placed directly within I/O and other field devices.

Monitor, Analyze, Respond and Attribute

The greatest expense is associated with the ongoing operations of analyzing events of interest and responding to incidents, so it's important to have a chain of authorized personnel and associations in place to respond to escalated incidents (see Figure 4).

**Monitor**

Current and maintained system documentation is the cornerstone to the success of incident response. All cyber, physical, operational and environmental changes made to the facilities, control system I/O, operating systems, hardware configurations and device drivers must be identified and documented as to the necessity of the change and who approved and performed the modification. This correlation activity begins manually at first, but eventually it can be intelligently programmed at the device level using host-based controls and centrally monitored with a Security Information and Event Management (SIEM) or other similar solution. The correlated activities help the investigator understand and identify configuration changes that have been performed and determine whether the events of interest were due to approved, unapproved or undocumented modifications.

**Analyze**

Analyzing events of interest requires a wide knowledge base and business acumen. The NIST SP 800-61—Computer Security Incident Handling Guide, the DHS white paper—“Developing an Industrial Control System Cybersecurity Incident Response Capability,” and CPNI’s Good Practice Guide on Establishing a Response Capability can serve as foundational resources. Analysts need to understand how to appropriately classify the activities and associate them with business operations and technology.

**Respond**

Incident response is a combination of the analysis results of control point events, the capabilities of the investigative team and their authority to make timely and appropriate decisions. The response should be based upon organizational risk and vary from issuing an advisory or alert to escalating the response to modify business operations. Possible responses may be as simple as applying a security patch, revoking a user account or blocking an IP address, or something that opens the business to more risk, such as isolating cyber asset communications and even disabling process control systems. Therefore, the team should consist of process control engineers, IT and corporate security representatives, as well as business management, internal audit, legal and public relations team members.

Conclusion

Control system components are difficult to protect and monitor because many components inherently trust the environment and do not natively create security events. Therefore, bolt-on hardware and combined cyber, physical and operational techniques must be used to protect the control system. SCADA and other control systems span large geographic areas, geopolitical domains and communication networks, thus increasing the challenges and requiring external partnerships and combined cyber, physical and operational approaches to security.

The primary components of a solid security posture that allows for event analysis and attribution include the following:

1. Know your cyber assets, their communication requirements, usage procedures and physical location.
2. Incorporate strict change management procedures with limited trusts within the control system environment.
3. Define, continuously monitor and analyze correlated cyber, physical and operational controls internally and externally.
4. Establish internal incident response teams with authority to respond and external partnerships with law enforcement, vendors and other asset owners to manage escalating events.

Well-trained personnel with authority to respond must be available to address security concerns in a timely and appropriate manner, leveraging both internal resources and external partnerships. These mechanisms must be defined prior to an event occurring.
Other Resources


"The Problem Isn’t Attribution; It’s Multi-Stage Attacks.” Proceedings of the Re-Architecting the Internet Workshop, ReARCH ’10, 2010.


*TSA Pipeline Security Guidelines*. Transportation Security Administration, April 2011.


Matthew E. Luallen is cofounder and president of CYBATI, a critical infrastructure and control system cybersecurity consulting, awareness and training company. He has written, consulted and trained extensively on process control and SCADA security issues and continues to work with electric utilities in the U.S. and Canada on the NERC CIP reliability standards. He has also presented on ICS cybersecurity within critical infrastructures to the FBI InfraGard, FBI, ISA, NERC RROs, USSS, NNSA, DOE National Labs, U.S. Army Central Command, FAA, European Union, RCMP, and at the request of specific asset owners. Mr. Luallen holds a bachelor’s degree in industrial engineering from the University of Illinois-Urbana, a master’s degree in computer science from National Technological University and is a 12-year Cisco Certified Internetwork Expert (CCIE). He serves as adjunct faculty for DePaul University’s capstone cybersecurity and control system courses, as a certified instructor for Cisco Systems and as a certified instructor for the SANS Institute. He is also the author of a new hands-on, control system cybersecurity course promoted by CYBATI.