IoT Threat Environment

An overview of the IoT threat landscape with risk-based security program recommendations

Introduction

Business and operational teams are responding to security and compliance challenges as networks evolve from closed systems to Internet-enabled operational technology (OT) connectivity. Facilities continue to be networked and Internet of Things (IoT) endpoints proliferate as the technology opens new opportunities for increased efficiency and operational effectiveness. Yet extensive legacy hardware and software that are not designed to address security dominate existing systems. These legacy systems were often deployed before security requirements were a mainstream issue and often cannot be readily patched or upgraded to support modern security controls. Meanwhile, with this backdrop, energy, manufacturing, smart cities, and transportation are facing ever more sophisticated, widespread and persistent threats, and the potential for significant economic damage and real world physical impact such as process shutdown, power grid interruption and physical injury.

In this paper we’ll review security incidents and vulnerability trends to build an empirical model of the threat environment. We’ll discuss lessons learned from these incidents, highlight common threats and identify attack patterns. This information describes a risk-based approach to threat modeling and effective security program management, which in turn helps to enable cost-effective deployment of security controls that prioritize critical security risk mitigation while also achieving regulatory compliance. In this way business and OT leaders can achieve smart-compliance, that is, using compliance spending to drive practical security risk mitigation. Specific examples and considerations for energy, manufacturing, smart cities, and transportation are discussed.

History of Incidents

While Stuxnet’s discovery in 2010 represented the dawn of widespread awareness of the physical impact from threats against industrial networks, significant security incidents across an array of market segments, including energy and manufacturing, indicate the reality of the threat, the magnitude of the impact and the extent that these sectors are being targeted. In risk-management vernacular, considering the likelihood of attacks, the persistence of threats and the significance of the potential impact points to critical risks. External attacks employing sophisticated tactics have increased security awareness across industries. For examples of security incidents both before and after Stuxnet see Figure 1, “IoT Security Timeline.”
IoT Threat Landscape

What do these incidents reveal about the patterns of impacts and threats in IoT? While there are fewer IoT security incidents reported due to the lack of public reporting, likely undiscovered incidents, secrecy, and the early deployment cycle compared to enterprise IT security (with a much longer history of reporting significant security incidents), we can see patterns in these incidents in terms of the potential impacts. In fact, in [9] a SANS 2014 survey, “Breaches on the Rise in Control Systems,” indicates that IoT intrusions are increasing. This year almost 27 percent of the respondents indicated a breach or infection in their control system environments, up from 20 percent the previous year. Another 13 percent had suspected breaches.

Impacts

Physical and economic impact is a reality in IoT networks. This has significant implications for IoT operators, particularly in energy, manufacturing, smart-cities, and transportation, because an exploited network can result in human injury and supply-chain disruptions.

Public Safety

Because IoT systems inherently control physical systems, public safety is a natural concern. In the public sector, this applies to transportation systems, electric distribution, and water treatment, as well as distribution and storage. According to experts cited in DHS analysis, “The inherent level of automation and controllability of PTC [positive train control] systems makes vulnerabilities particularly dangerous if a malicious actor can exploit them. After obtaining system-level access, an actor could execute a variety of commands, many of which could cause a chain of automated reactions with little or no human oversight” [10]. In manufacturing it can apply to both employees as well as customers, for example, in the recent case of cars vulnerable to remote exploits while being driven.

System Downtime

Availability, along with safety, is the most critical attribute of IoT environments, as compared to traditional IT environments (which favor confidentiality and availability rather than the availability and integrity requirements prevalent in IoT deployments). IoT systems combined with their high-availability requirements means that these systems are more at risk of unintended, non-malicious downtime. For example, when a natural gas facility had a security consultant scan its network as part of a penetration test, the tester moved laterally from the corporate
network to a SCADA system, which went down such that the utility was not able to send gas through its pipelines for 4 hours, during which its customers lost service [11].

**Community Impact:** Federal, State, and Local Municipalities

Any disruption in public services can have significant economic impact at the local, state, and federal level. The 60 gigawatt power outage in 2003 in the Northeastern United States and Canada and the March 2015 multihour power outage in Turkey in which 44 of 81 provinces were left without power clearly have economic impacts that can be measured in billions of dollars. However, even more localized incidents can be significant. When a bug in San Francisco’s BART system caused three rail lines to shut down for more than 7 hours, the economic cost of the shutdown was estimated at $1 billion because 35,000 commuters were stranded. According to DHS, hackers could manipulate the function of intersections, onramps, toll plazas, interchanges, and other critical components across a city, affecting a city’s transportation grid for extended periods of time. [10]

**Brand Damage**

The Dow Chemical Company is still suffering brand damage 30 years after the Bhopal tragedy in which thousands of people died and many more were injured as half a million people were exposed to toxic gas and chemicals due to a runaway chemical reaction at the pesticide plant in Bhopal, India. For example, The London Assembly, criticized the International Olympic Committee for its Dow Chemical sponsorship based on their links to the tragedy, saying it “caused damage to the reputation of the London 2012 Olympic[s]” While various causes likely factored into the incident, including deferred maintenance, operating errors, design flaws and even sabotage, out of order pressure, temperature and level sensors prevented the early detection of the runaway reaction at the Union Carbide Corporation (UCC) facility which Dow acquired in 2001 [13].

**Loss of Trust**

According to DHS analysis, “any system error resulting in a train collision, particularly involving fatalities, could increase public fear of rail travel.” [10] There have been various attacks against the nuclear industry, for example, including several confirmed incidents at the NRC, by foreign and unknown attackers last year [14]: for example, a 2008 incident in which a Georgia nuclear plant was forced into an emergency shutdown for 48 hours after a software upgrade caused safety systems to misinterpret missing data as drops in water reservoirs that cool the radioactive fuel rods [15], as well as the 2003 Davis-Besse nuclear power incident [16].

These nuclear examples highlight the impact of a security incident on an industry that already delicately balances the need for energy and the public’s perception of safety.

Smart meters, a technology that already harbors public distrust, is at risk of both public perception sentiment and economic impact. A leaked 2010 FBI report documented that meter tampering of a Puerto Rican utility cost more than $400 million annually in lost revenue and projected that smart meter hacks are likely to spread [17].

**Intellectual Property Theft**

Some estimate that the cyber theft of intellectual property at American companies alone is similar in scale as America’s total exports to Asia, that is, hundreds of billions of dollars annually [18]. The FBI has estimated that this theft has increased 53 percent this year [19]. If those numbers feel abstract given their scale, let’s look at the impact at a single hacked manufacturer. Codan, an Australian company that sells metal detectors and mining technology, had its blueprints for a metal detector stolen, according to Reuters.

This led to widespread counterfeiting in the high-demand African market, which was experiencing a gold rush. As a result Codan had to slash the price on its metal detectors from approximately $3000 to less than $2000, reducing its net profit by 80 percent [20].
Threat Actors
After looking at IoT security incidents, a number of patterns emerge.

Sophisticated Actors
Some threat actors are sophisticated, motivated by economic factors. These actors are commonly associated with nation-state or terrorist threats in energy and the public sector, but also they are motivated by competitive advantage in manufacturing, where a rival may seek details about technology designs and manufacturing processes, pricing and business plans, legal agreements, and contact lists, or supply chain disruption. The level of sophistication is evidenced by what we’ve learned about these attackers and their tools, including a number of malware campaigns and hacking groups (see sidebar, “Sophisticated Malware and Hacking Campaigns.”

Insider Threat
The insider threat in IoT is a multifaceted problem that relates to both malicious and unintentional security incidents involving employees, contractors and vendors. One common form of the unintentional threat from insiders is due to the high-availability requirements of IoT combined with these systems sensitivity to adverse network traffic based on their historical isolation from adverse network traffic and diverse network protocols.

Another vector of the unintentional threat is when third parties are used as an attack vector for self-propagating malware or persistent attackers seeking a foothold in an air-gapped or otherwise isolated network. Many of the incidents documented herein incorporate some form of this attack vector. For example:

- Contractor infecting network with laptop infected with a virus
- USB storage device transmitting virus
- Watering-hole attack in which an employee at a targeted company downloads an IoT software update from a vendor’s site that has been compromised with a Trojaned software update.
- Phishing attack against employees at targeted company

Malicious intent in IoT environments have similar characteristics of traditional insider threats except for the impacts that can feel more tangible, such as the overflow at a wastewater treatment plant [8] or smart-meters that employees configure to underreport electricity usage [18].

Attack Patterns
A number of patterns emerge from looking at IoT security threats.

Targeted Attacks
In IoT, many of the attacks are persistent and targeted, where adversaries use multiple vectors of attack to gain a foothold within the network from which to move laterally. In this environment network managers can’t rely on the security strategy in which they merely get rid of the low hanging fruit of security vulnerabilities hoping that attackers would quickly move on to the next easy target.

Collateral Damage Risk
The growth of IoT specific malware, even when designed for a targeted attack, often employ self-propagating infection techniques. As such, even unintended targets are often compromised. Significant disclosure of new vulnerabilities (and frankly - old but unpatched/unaddressed vulnerabilities), and even zero-day exploits mean that these concerns will only increase. You may not be the target, but you might get compromised.
Social Engineering and Phishing
Just as in traditional IT and operational technology environments, employees are a weak link in the security chain. Many of the targeted attack campaigns use employees to gain an initial foothold on a network. This is also a common initial vector for malware.

Remote Access
The distributed nature of IoT controllers, as well as the common scenario where a vendor is used to manage a system, combined with components that often don’t support modern security controls or protocols, means that remote access is a common vector of attack. Many of the documented incidents use this as a primary attack method.

Vulnerability Landscape
Extensive Vendor Vulnerabilities Exist
ICS-CERT published its own list of advisories for IoT systems, which provide information about security issues, vulnerabilities, and exploits.

Where traditional IT/OT network environments tend to be at risk from the latest threats, the long lifespan of many IoT systems and the challenge of patching mean that new threats tend to be additive, that is, the risk tends to multiply as the vulnerabilities accumulate.

Patterns in IoT Network Vulnerabilities
According to ICS-CERT, based on the security assessments it conducted in FY14, a significant number of vulnerabilities it found (28 percent) on critical infrastructure networks was clustered in six areas (in terms of NIST 800-53 control families):

<table>
<thead>
<tr>
<th>Control Family</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundary protection</td>
<td>Lack of firewall control of IoT networks, including lack of sufficient logical separation from enterprise IT/OT networks or Internet.</td>
</tr>
<tr>
<td>Information flow</td>
<td>Lack of technical access control mechanisms, such as firewalls, routers, proxies, gateways, and tunnels to control the flow of information in an IoT network and ingress/egress between networks in accordance with policy.</td>
</tr>
<tr>
<td>enforcement</td>
<td></td>
</tr>
<tr>
<td>Remote access</td>
<td>Weak security controls for remote access including internet facing systems, vendors and contractors, VPN configurations, the use of personal devices and vulnerable OSs.</td>
</tr>
<tr>
<td>Least privilege</td>
<td>Provisioning users with elevated privileges beyond the minimum required, such as the use of administrator accounts for routing functions, creates a risk for both unintentional and malicious incidents.</td>
</tr>
<tr>
<td>Physical access control</td>
<td>Not securing physical access to IoT equipment.</td>
</tr>
<tr>
<td>Security function isolation</td>
<td>Implementation of flat network topologies without multiple layers of security controls simplify exploitation while making monitoring connectivity between systems of different trust levels more difficult.</td>
</tr>
</tbody>
</table>

Implementing a Risk-Based IoT Security Program
By using a risk-based approach, IoT network owners can cost-effectively manage security risk while achieving near-term compliance. A risk-based approach means using what you know about the threat environment to inform your decisions about deploying security controls. In this way you focus on the most critical risk first. And by mapping these priorities to compliance requirements - and the spirit and intent of those requirements - you can address compliance concurrently, with significant overlap in spending.
While the guidelines documented in ISA-99/IEC-62443, NERC CIP, and NIST SP 800-82 describe a more detailed process for implementing a security program, this description applies the common patterns of impact, threat actors, attacks, and vulnerabilities discussed herein as our threat model. We also make references to selected compliance requirements to illustrate the correlation between compliance objectives and controls deployed using a risk-based approach. To achieve this, we recommend three steps to implementing your security program as shown in Table 2.

Table 1. Three Steps to Implementing Security Programs

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Assess</td>
<td>The objective is to understand and gain visibility into your current network environment by mapping your network and inventorying IoT assets.</td>
</tr>
<tr>
<td>2. Implement</td>
<td>This step is about layering your network, hardening your systems, and implementing security controls based on your own threat model.</td>
</tr>
<tr>
<td>3. Formalize</td>
<td>Document policies and procedures, and train employees.</td>
</tr>
</tbody>
</table>

This lifecycle is iterative, and as security programs evolve, systems should continually be reassessed for new vulnerabilities and changes in the network environment. Because this is an iterative process, this process applies to organizations at various levels of security program maturity, though the emphasis on each step can vary.

Assess

Assessing your environment is about gaining initial visibility into your environment by clearly defining, mapping, and documenting assets that make up your IoT network environment. This activity can be performed at the subnet, facility, or global level. However, at whatever level of granularity this is performed, all network interfaces to other networks should be documented to facilitate evaluation of trust at network boundaries; for example, if analyzing a distinct network, it's critical to understand if its gateway is the enterprise IT/OT network, another IoT network, a DMZ or the Internet. This discussion uses the word network to mean the particular area within the scope for the analysis. Assessing the network can be broken down into these discrete tasks:

Inventory Assets

Create an inventory of all key assets including systems, applications, data, and security controls in the network, including other networks in and directly interfacing the network. PLC, DCS, SCADA, and HMI systems should all be identified. Key network devices should be included, specifically, any routable devices, systems providing remote access, and existing security controls.

Map Network

Map each asset onto a network diagram that clearly identifies logical and physical network segments, such that network interfaces are clearly delineated. This mapping allows each subnet to be evaluated in terms of criticality, access requirements and security levels.

As you evaluate the network map, consider if the assets within network segments share common security requirements. Is access provided to one system by users or systems with trust levels that are not as high as the security requirements of other devices on that segment? Are the connections between segments or zones properly firewalled? Are unneeded ports closed?

Thinking in this way is important because a key activity in terms of both security best practices and compliance is to segment a network to separate systems with different trust levels and to implement a defense-in-depth strategy of layered security.
Document Remote Access

The network map and asset inventory should clearly delineate remote access points. While remote access has also been a traditionally vulnerable point for enterprise IT/OT networks, it’s been the entry point for a disproportionate number of IoT security incidents. These access points should all be identified along with the protocols they allow, the employees, contractors, and vendors that use them, the account permissions, the level of access granted once connected (including the systems accessible that are not necessarily required for the particular user), the type of user account (shared vs individual), etc.

Implement

Apply your threat model to your operational requirements, factor in existing controls and mitigating factors, and then deploy security controls to address residual risk. Here, we use the common patterns we have discussed in terms of threat actors, attacks, and vulnerabilities discussed as our threat model template and use that to suggest some high-value activities that mitigate common areas of risk. We also note some specific compliance requirements to highlight how these risk-based security activities directly correlate to compliance initiatives.

Network Segmentation

Network segmentation involves partitioning a network into smaller logical sub-networks to separate security domains based on the level of trust and criticality of the systems and access within those domains. Smaller organizations partition the IoT network from the IT/OT network at the very least and more complex environments have many logical IoT networks in various categories, such as control zones, HMI zones, enterprise zones, and DMZs. Segmentation is a long-standing best practice in enterprise security, but also it’s a basic tenet of IoT security and a key security architecture component of NIST 800-82, Guide to Industrial Control Systems Security (May 2015).

For energy companies following a NERC CIP model, this best practice also applies. While NERC CIP’s model does discuss a monolithic security model of a big network protected at its edges, taken in it’s entirety NERC CIP does implement a defense-in-depth strategy and specifically requires segmentation. For both security and compliance, network segmentation is an important part of securing your infrastructure. This feature makes it harder for intruders to gain access to critical areas of your network, minimizes the threat of malware, and limits the surface area for the accidental or malicious insider threat.

Harden Systems

Individual systems should be hardened including uninstalling or disabling unneeded functionality, patching services, removing unneeded accounts, closing unused ports and services, changing default passwords, etc. NERC CIP, for example, has specific requirements associated with hardening.

Control Remote Access

Controlling remote access points is one of the most important aspects for minimizing security risk. Remote access points should:

- Avoid shared accounts: for example, vendors should not use shared accounts.
- Use least privileges: where possible remote access should allow access only to a minimum set of features needed to fulfill a job requirement. Periodically review access permissions.
- Change default passwords and require change of initial password for new users and accounts.
- Be revocable. Periodically review and remove unneeded accounts.
- Log all access.
● All parties using remote access should agree to conformance with security policy.
● Use strong passwords.
● Disable accounts after repeated remote login attempts to prevent brute force attacks.

Monitor
Implement automated and manual systems to monitor security: intrusion detection system (IDS) and intrusion prevention system (IPS), patch management, system logs, and security information and event management (SIEM) to monitor, analyze, and correlate security events. Ensure malware and antivirus systems are up to date and that periodic auditing of user accounts is performed.

Formalize
A rigorous security program should be formalized, which is both a key compliance requirement across virtually all standards as well as practical security risk management tool.

Document Policies and Procedures
A written security policy clearly defines an organization’s security requirements, creates accountability, and establishes standards for employees, contractors, and vendors. A written policy also is a key element in formalizing a security program. You should also create documentation around specific tasks. For example, document the required steps to hardening systems before deployment and the patch management requirements for different types of systems.

Training
Training in all organizations is key, however, this is especially true in IoT environments. Particularly given the third-party risks, any party, whether an employee, contractor, or vendor, should be required to acknowledge their understanding of the security policy and other procedures around their access to systems.

Lifecycle
Remember, this is an iterative process. The threat environment is as dynamic. The threats and associated controls need to continue to be reevaluated. An effective IoT security program is more about a process that needs to be institutionalized in an organization from top to bottom than it is about technical security controls or a one-time effort.

Conclusion
IoT networks are challenging to secure. Meanwhile given that the nature of the risk emphasizes system availability as a high-priority security attribute means that the threat environment is very polarized: IoT networks need to be worried about both sophisticated targeted attacks from competitors and nation-states, as well as accidental misuse from employees, contractors, and vendors.

However, by using historical attack patterns, vulnerabilities, and lessons learned from previous incidents, IoT network owners can build a threat model that effectively mitigates security risk while also addressing compliance requirements. This risk-based approach is cost effective, practical, and emphasize the most critical areas of risk first. It’s an important foundation to an ongoing information security program that can enable organizations to continue to use the benefits of increased system interconnectedness as dictated by proven ROI, while minimize the very real human and economic risks associated with IoT.
Appendix

References


[3] Zotob Worm hits DaimlerChrysler’s U.S. automobile manufacturing plants
http://www.eweek.com/article2/0,1895,1849914,00.asp

http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807


https://ics-cert.us-cert.gov/


https://ics-cert.us-cert.gov/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk

[11] Penetration testing incident at natural gas utility

[12] Security researchers hack car, leads to recall
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

https://en.wikipedia.org/wiki/Bhopal_disaster
http://www.ibtimes.co.uk/exclusive-30-years-bhopal-gas-tragedy-thousands-victims-still-wait-justice-1475466

[15] Cyber incident blamed for nuclear power plant shutdown
http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

http://www.safetyinengineering.com/FileUploads/Nuclear%20cyber%20security%20incidents_1349551766_2.pdf

http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[18] IP theft, Economist Magazine

[19] IP theft, FBI statistic from Fortune Magazine
http://fortune.com/2015/09/16/obama-warns-china-on-hacking/

[20] IP theft, Codan example, Reuters
http://www.reuters.com/article/2015/06/25/china-cybersecurity-australia-pix-graphi-idUSL3N0ZB15O20150625