AUTOMATION 2020

VOLUME 6

OT/ICS Cybersecurity

- 10 Things Not to Tell Your Board about Cybersecurity
- Open Secure SCADA
- How Process Safety Best Practices Improve OT Security
- A Zero-trust Approach to OT/ICS/SCADA Security
- New Threat: DNS Protocol Misuse

AUTOMATION.COM

A subsidiary of the International Society of Automation

Introduction

OT/ICS Cybersecurity

With attacks on industrial control systems (ICSs) escalating and attackers seeming to change their approaches by the minute, it is important for operational technology and SCADA professionals to be continually learning. For those managing complex OT systems and plants, vital skills include the ability to manage expectations, understand and communicate complex and sensitive situations, and to stay on top of emerging threats and possible mitigations.

In this edition of **AUTOMATION 2020**, you'll discover an emerging cyberthreat—misuse of DNS protocols—as well as learn how a zero-trust approach to OT/ICS/SCADA cybersecurity works. You'll also learn about open and secure SCADA systems, as well as how safety best practices can improve OT cybersecurity. Communicating this knowledge to various stakeholders, including corporate board members, is essential.

The **AUTOMATION 2020** Ebook series from Automation.com delivers sponsored and curated articles featuring best practices and cutting-edge insight from a variety of subject-matter experts. Subscribe online to not miss a single issue.

Table of Contents

AUTOMATION 2020 VOL 6
OT/ICS CYBERSECURITY

10 Things Not to Tell Your Board about Your OT Cybersecurity Program

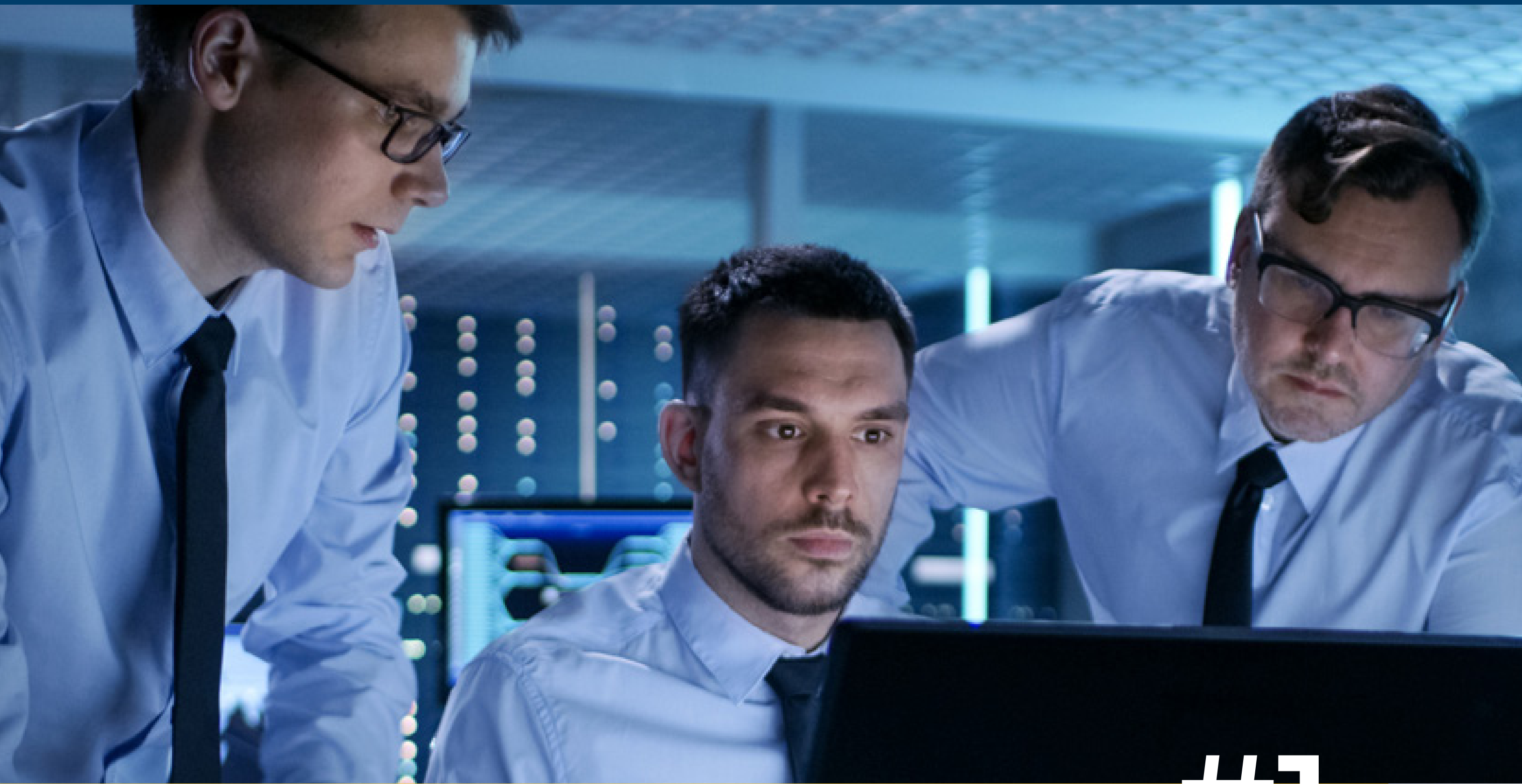
When managing complex operational technology systems and plants, a vital skill is the ability to manage leadership expectations while communicating sensitive issues related to cybersecurity

By Marty Israels,
Honeywell Connected
Enterprise

Within a corporate Board environment, cybersecurity can be vastly misunderstood, and yet it remains a critical priority for oversight. As recently as two years ago, Gartner estimated that 100 percent of large enterprises would be asked to report to their Boards on cybersecurity and technology risk by 2020. Operational security experts may be called upon by Boards for data, status, or perspectives. As Boards increasingly add technology committees and even cybersecurity committees to their structures, the need for a balanced dialogue and expertise will only increase.

For those managing complex operational technology (OT) systems and plants, a vital skill is the ability to manage leadership expectations while communicating sensitive situations in a factual and informative manner. By far the most dangerous situation for a security practitioner advising a business group is to misrepresent the level of risk facing an organization. This can open the company to costly lawsuits and unwelcome publicity, not to mention the direct risk concerns of human safety and environmental damage. Similarly, overreacting on risk can deplete company resources and unnecessarily divert focus.

Managing your operations information flow and approach with leadership can create a positive and mutually beneficial relationship if a few considerations are kept in mind. This article notes the top ten comments that are best avoided when handling cybersecurity situations with your Board or leadership teams.



#1

#1 "You have nothing to worry about."

While confidence can be a reassuring leadership trait in certain roles, when it comes to cybersecurity, pretending that risk does not exist is irresponsible. There is always risk, and leadership needs to understand precisely what that risk is in order to make policy and organizational decisions. Communicating that the Board has nothing to worry about completely misses the granular and rich discussion necessary about risk and how to handle it. It is for them to weigh in on what can or should be worried about at the corporate level; masking particular risks can be misleading.

For example, if leaders are unaware of remote connectivity's impact in an operational setting, they may drive ahead on initiatives that create dozens of uncontrolled connections, and they may miss investing in countermeasures and controls that can limit the risk while embracing the opportunity. Rather than stating "you have nothing to worry about," communicate what measures will be needed as part of the initiative, such as "if we need to allow remote connectivity to our mine in Chile, we need to implement monitoring software to record and log those remote sessions and to change our access privileges."

There is always something to worry about in security, and helping leadership understand that makes for a more realistic and balanced risk management discussion. It also allows security to become part of all conversations, rather than an isolated domain disconnected from the organization's key initiatives.

#2

#2 "None of our systems are vulnerable."

With attackers changing approaches on a minute-by-minute basis, it is impossible to share the status that all systems are protected against every vulnerability. Even if you have patched all systems recently, there are still zero-day attacks yet unpublicized, as well as other mechanisms that are always available to attackers. For example, addressing vulnerabilities in an operating system may not address chip vulnerabilities.

Leadership teams need to recognize that there are always outstanding vulnerabilities. Whether it is worth the cost, resources, and hit to production to address these vulnerabilities is part of leadership's oversight responsibilities. As the operational leader, it can be best to describe what categories or areas of vulnerabilities have been addressed in that moment, while making it clear that there can be other unknown risks or a set of liabilities that are intentionally not addressed.

In addition, when it comes to vulnerabilities, Boards are interested in which technology systems contribute to which levels of risk. They may find it helpful to know that 60 percent of the infrastructure is running on systems with the most vulnerable OS type. They can then decide if it is critical to upgrade those systems, or to accept the risk those systems bring relative to the value they provide to the business. Implying that no systems are vulnerable makes it difficult to plan upgrades or otherwise make trade-off decisions regarding operational infrastructure.

#3 "The person who knows the most about the cybersecurity of our systems left the company."

Talent and people with expertise in cybersecurity may be in short supply, and this is well known at Board levels. Rather than finding yourself in a situation where key expertise is missing, proactively review resources to clearly articulate to leadership both your high potential and critical talent resources.

Since you will regularly communicate regarding risk, it is important to decipher for leadership which talent relates to which levels of risk. If your organization has stated headcount limitations or other resourcing constraints, it is your responsibility to find other means, such as outsourced relationships or contracted expertise, to address unacceptable levels of risk. This may also be required for compliance, which is a high-priority topic for Boards.

When considering your responsibilities for cybersecurity, it can be helpful to broaden beyond technology to ensure people, processes, and systems are actively managed relative to the risks the company faces. For example, if you only have limited personnel with specific cybersecurity knowledge, consider how to transfer knowledge to others and how to offset the risk that a single individual's departure could impact your cybersecurity program. If you face staffing shortages, plan ahead for augmented expertise or new service contracts with OT cybersecurity partners.

#4 "We don't need to spend any more on our cybersecurity programs."

Some surveys have concluded that in the industrial sector in particular, investment in security countermeasures is not on par with levels of risk. For example, there are still organizations that are not even performing any manner of risk assessments (a basic cybersecurity step). In addition, it has been well documented that the nature of OT-targeted attacks is dynamic, and involves ongoing pressure from nation states, activists, competitors, and financially motivated hackers.

Considering these pressing "hazardous" conditions, there is always cybersecurity work to be done. With your cybersecurity program, you have your key objectives identified and an ongoing practice that can always apply more resources to offset risk. For example, if your objective is to centralize security operations, there are multiple automation and management software solutions that could be added to expedite remote team data sharing in a secure manner, or solutions to control and monitor access.

Layering in security across people, processes, and systems is an ongoing practice. Investment should be commensurate with reaching your objectives. Many companies keep an ongoing list of key cybersecurity work as budgets evolve, based on their risk assessment findings or a review of program objectives and status. For example, changing out routers to allow for newer levels of encrypted communication may not be on the first priority order ahead of patching high-value servers, but it can be a useful investment should funding become available.

#5 "We don't think we're a target."

The volume, speed, and dynamic nature of today's threat landscape has led some security experts to suggest that ICS is a target, and recent alerts pinpoint specific risks for industrial control system operators. From local hospitals, to major brands, to water processing facilities to fertilizer makers, every connected organization is at risk of compromise. Trends change, and the nature of threats constantly evolves, from the past denial-of-service waves to today's

ransomware campaigns. Rather than diminish the level of risk, clearly identify the company's high-value assets, then assume someone will want to target them. Advising that your company is not a target reduces vigilance and starves security resources, leading to greater levels of risk.

To balance the conversation, it is worth discussing what level of effort will be required to protect your organization as a target. For example, if you make farming equipment with remotely controlled tractors, a potential target could be taking over control of those tractors, causing crop damage or putting operators in danger. Discuss if the organization could tolerate such an incident, and if not (as is likely), direct the conversation toward what obstacles could be layered in to slow down attackers. Through such discussions, Board members often recognize that always assuming they are a target can actually expedite protection. Focusing on not being a target increases risk through omission and can also hold back the organization from modernizing systems and practices.

As the operations leader advising on cybersecurity, it is in your best interest to keep the organization vigilant and on top of security resources at all times. This builds in the assumption that the organization is a target.

#6 "Unless we have the latest technology, we don't stand a chance."

Technical solutions are indeed an essential part of a cybersecurity program, considering the intricate technicalities that hackers leverage to perform malicious acts. At the same time, engaging people controls and process controls is equally essential for your security posture. Layering in defenses across all of those dimensions can help manage risk. As you communicate with leaders, continually broaden their horizons to consider these three areas (people, process, technology). This approach can support the Board to better balance investments relative to the organization's risk appetite and ability to mitigate threats.

For example, if you overinvest in technology but do not train your personnel how to avoid phishing attacks, you have left open a major avenue of attack. While you may have better automated and streamlined technical controls, you have done little to reduce risk from social engineering, a common and problematic source of compromise. Similarly, having the best technology does not eliminate the need for ongoing risk assessments, which commonly uncover concerning risks, such as uncontrolled remote access points or visible passwords posted alongside servers.

All that said, it should be noted that in certain areas, the latest technology updates are a critical part of the cybersecurity practice. For example, when addressing USB-borne threats or exploits of OS vulnerabilities, having an evergreen system of known attacks and mitigations is essential. This does not necessarily require procuring new technology but ensuring a rigorous process for updating existing systems. The main point is to balance the emphasis on technology with the equally important dimensions of people and process investments.

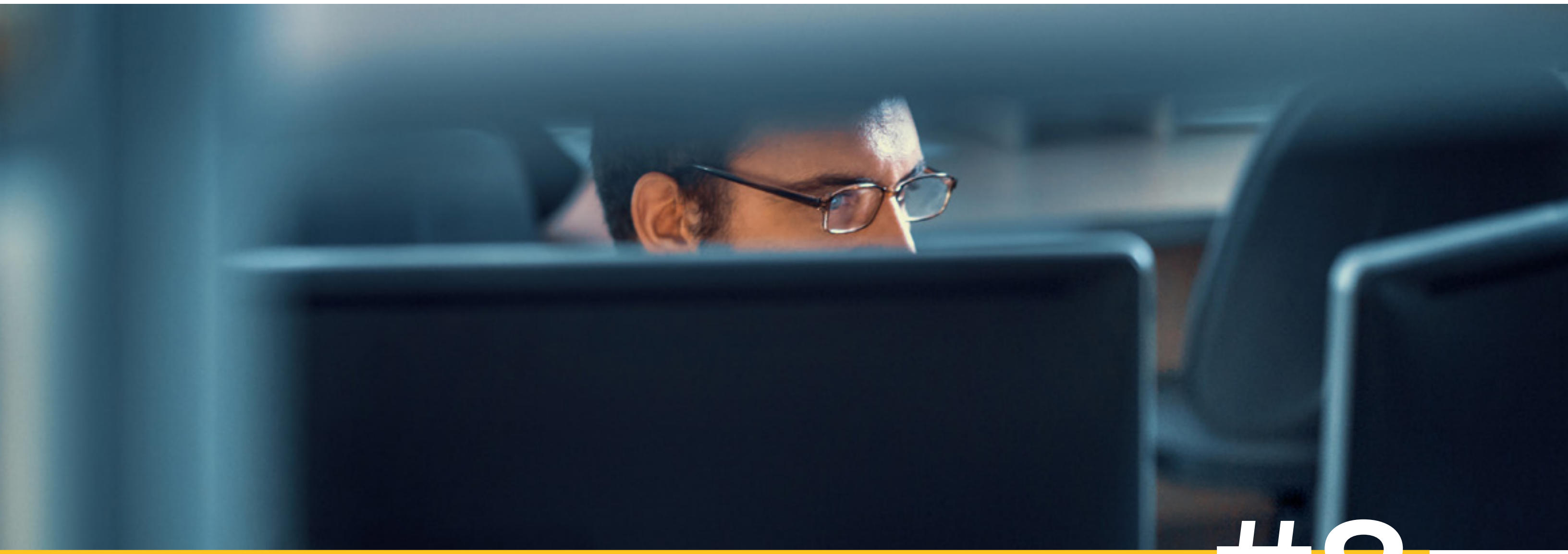
#7

#7 “The difference between IT and OT security is too small to treat them separately.”

At the Board level, cybersecurity may be viewed as an umbrella term, much like medicine or law, with little understanding of the vast differences among practitioners and related solutions. As you discuss risk and mitigations, it can be helpful to clarify why particular IT methodologies cannot work in industrial OT settings. This can range from ensuring basic requirements are well known, such as the ability to operate under extremely hot or cold temperatures, all the way to educating about newer risks, such as hardening any off-the-shelf Windows servers or adjusting patching schedules to avoid interference with production.

Aligning to IT procedures without protecting against the greatest OT risks will only open the organization to more liabilities and internal conflict. The voice of OT is essential in guiding security oversight at the Board level, to help match vigilance and investment with the specific type of environments, systems, and working conditions of operations.

Similarly, considering people and process concerns specific to OT can help mitigate risk. For example, personnel with ICS security expertise or people approved and trained to work at an offshore platform may be important requirements for OT talent recruitment but not for IT. Rather than simply grouping IT and OT together, advocate for specialized OT compliance or training needs to ensure the company and its customers are adequately protected.



#8

#8 "Our IT and OT cybersecurity teams don't need to work together."

Similar to voicing the unique requirements of OT, it is in your company's best interest to have dialogue between IT and OT. Especially as the volume of assets in an industrial organization increases, there will be greater scrutiny on security across these devices, as well as inevitable security concerns amidst ongoing digitization. Moving laterally or between networks is an increasingly common hacker technique, further requiring varied security teams to address threats holistically.

While it can be pragmatic to group categories such as "devices" into a single Board conversation, it is still essential to convey that IT and OT will need to manage such devices differently considering their usage and role within each area. It is also beneficial to work together to secure resources and funding in more cost-effective ways that still honor the differences in requirements.

For example, procuring an outside organization to perform risk assessments can package different, specialized types of OT and IT assessments under one purchase order, aligning to common Board requests for quarterly reviews. As IT and OT work together to review assessment findings, areas of investment that can support both teams' missions may appear, such as securing patch updates through a secure mechanism from software providers, or personnel training about threats. Rather than duplicating training programs and overloading employees, a combined training can cover both the business network concerns and operational network concerns. This cross-training can also help educate each group about the other while complying with training needs.

#9

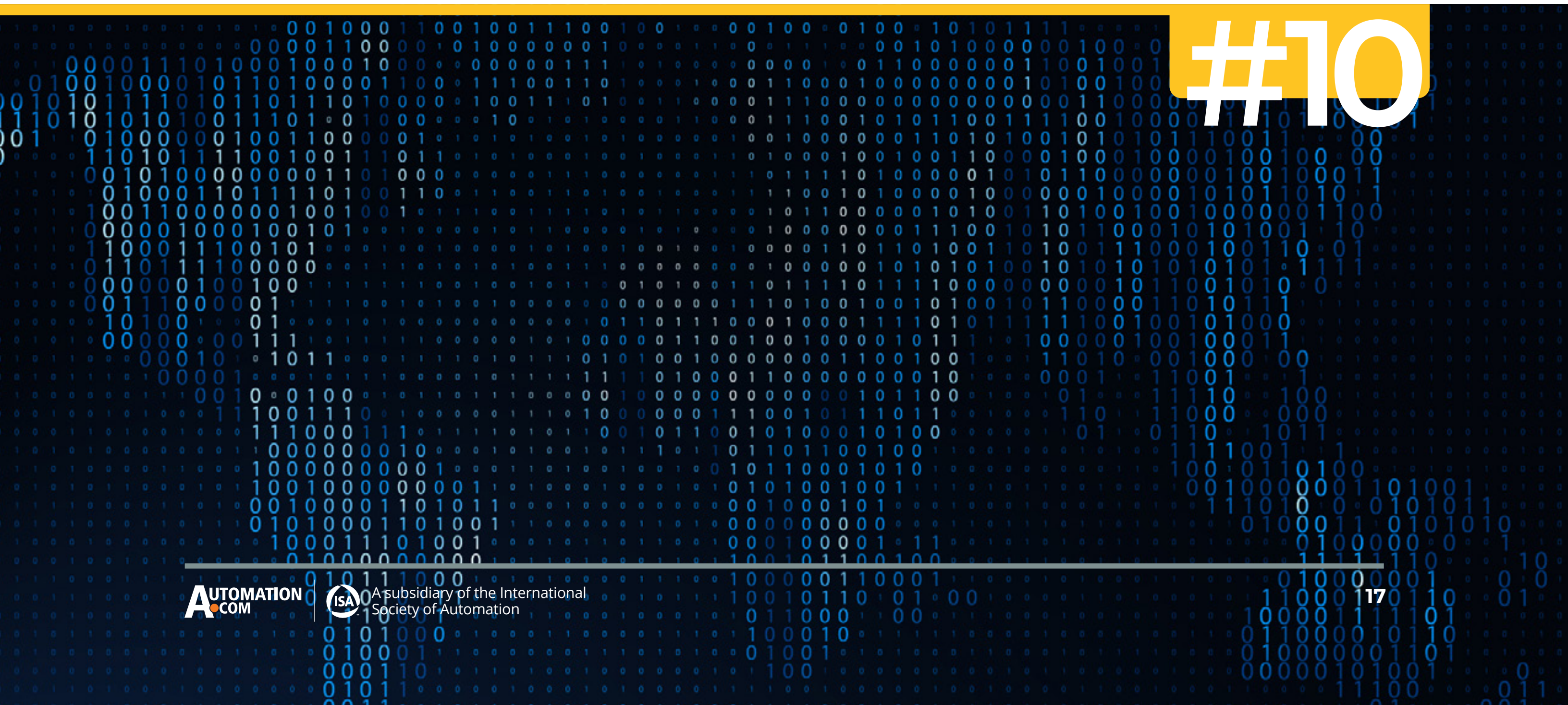
#9 "Our systems change so slowly over time; we can afford to focus efforts away from cybersecurity."

Legacy systems are not immune from attack. Recent cases have shown nation states targeting critical infrastructure providers, showing little regard for what systems are in place for how long. In addition, as recent high-profile breaches have highlighted, a consistent patching regime for any system is an essential part of ongoing cybersecurity. A further trend affecting legacy systems is the global drive toward manufacturing connectivity, seeking to leverage data from devices and systems to optimize performance or gain insights. Often this requires upgrading those systems or adapting them to allow for monitoring or data extraction. These trends increase the risk that older infrastructure will be exploited or disrupted and will thus require ongoing cybersecurity vigilance.

Beyond the direct technical concerns of legacy systems, the organization can never lose sight of the fact that processes and people introduce risk. This has little to do with how slowly systems do or do not change. For example, many processes have been in place for years, and have not been updated to reflect current conditions. An offshore oil rig may have a process that requires opening up a remote connection, inadvertently allowing workers to relax while watching a movie after long shifts.

Today, that connection can serve as a penetration point to reach other systems on the rig and represents a security risk that requires associated controls. Just as systems are slow to modernize, processes and training programs can be obsolete and introduce risks that must be mitigated to protect the organization.

#10 “We’re always one step ahead of any attackers.”



While it is prudent to deploy preventative measures as part of your cybersecurity program, response and mitigation investments are equally important. Leadership appreciates models and frameworks such as the NIST Cybersecurity Framework to recognize where and how risk will be addressed. Implying that all efforts in the preventative category will always work every time to stay ahead of attackers is simply naïve. Attackers are often highly motivated, agile, and well resourced, sometimes far more resourced than corporate security teams! Characterizing attackers as less advanced than commercial enterprises can be misleading and can result in poor investment choices and an inaccurate assessment of company risk.

Boards can instead be briefed on any active campaigns, particularly those applicable to their region or industry, and on overall threat trend changes and related mitigations. Ongoing risk assessment findings can be shared at a high level, as well as attacks averted.

These views into the threat landscape are a more realistic way to represent the dynamic nature of cybersecurity and to further reinforce its function as an ongoing practice, not a static field. The operations leader can always bear in mind that Boards want to see and manage risk as responsible stewards. They are not seeking sales pitches or rosy pictures that ignore potential risks.

Views into the threat landscape are a more realistic way to represent the dynamic nature of cybersecurity and to further reinforce its function as an ongoing practice, not a static field.

OT experts lead the way

Corporate Boards are accountable for the viability and longevity of an organization. Understanding cybersecurity risks is an increasingly common need for Boards globally. Through a balanced conversation across people, process, and technology needs, together with established standards and frameworks, operational experts can engage with Boards as informed and valuable leaders. Avoiding common mistakes such as mispresenting risk, avoiding risk mentions, or not protecting OT-specialized requirements can support a positive ongoing relationship to steer an organization through today's complex digital environments.

ABOUT THE AUTHOR

Marty Israels is the director of product marketing at Honeywell Connected Enterprise (HCE). He has global responsibility for leading, managing, and directing all product marketing–related activities for HCE's cybersecurity business focused on operational technology (OT). He has more than 25 years of business acumen, sales, marketing, and operations experience supporting software and technology growth in both startup and corporate environments. Israels holds an MBA from the University of Windsor in Canada and an economics degree from Western University in London, Canada.

ISA GLOBAL CYBERSECURITY ALLIANCE™

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

Honeywell

Johnson Controls

Rockwell Automation

Life Is On Schneider Electric

NOZOMI NETWORKS

PAS

CLAROTY Clarity for OT Networks

WALLIX CYBERSECURITY SIMPLIFIED

xage SECURITY

MOCANA

BAYSHORE

radiflow Secure your Assets

senhasegura by MT4 TECHNOLOGY GROUP

INL Idaho National Laboratory

威努特 WINICSSEC

exida

munio security

tenable

DRAGOS

TiSafe

aeSolutions™

tripwire

DIGITALIMMUNITY™ STAY PRODUCTIVE, STAY SECURE

WisePlant® Smart, Safe & Secure

MSi Mission Secure, Inc.

1898 & Co.

ACET SOLUTIONS

CYBEROWL

Nova Systems

Open **Secure** SCADA

How OPC UA and MQTT work with built-in cybersecurity to reduce costs and improve safety across your infrastructure

By Craig Allen, Bedrock Automation

Industrial control systems (ICSs) are typically systems of systems. Traditionally they are organized in a hierarchy. Level 0 is the process with its analog and digital sensors and actuators. Level 1 is defined by digital control devices such as programmable logic controllers (PLCs) and others that perform real-time control functions. Above this are Levels 2 and 3, frequently referred to as SCADA (supervisory control and data acquisition), that include human-machine interfaces (HMI) for operators and other applications that monitor the process in real time, manage alarms, enable adjustments, and automate other key functions to ensure safe and efficient control of the process. In recent years these complex digital ICSs used in oil and gas, water, power, and other critical infrastructure are prime targets for cyberattack.

"Unlike business enterprise networks, which manage information, ICS manage physical operational processes. Therefore, cyberattacks could result in significant physical consequences, including loss of life, property damage, and disruption of the essential services and critical functions upon which society relies. The use of cyberattacks to cause physical consequences makes ICS attractive targets for malicious actors seeking to cause the United States harm," write the authors of *Securing Industrial Control Systems: A Unified Initiative Fy 2019 – 2023* from the U.S. Cybersecurity and Infrastructure Security Agency.

Open *and* secure

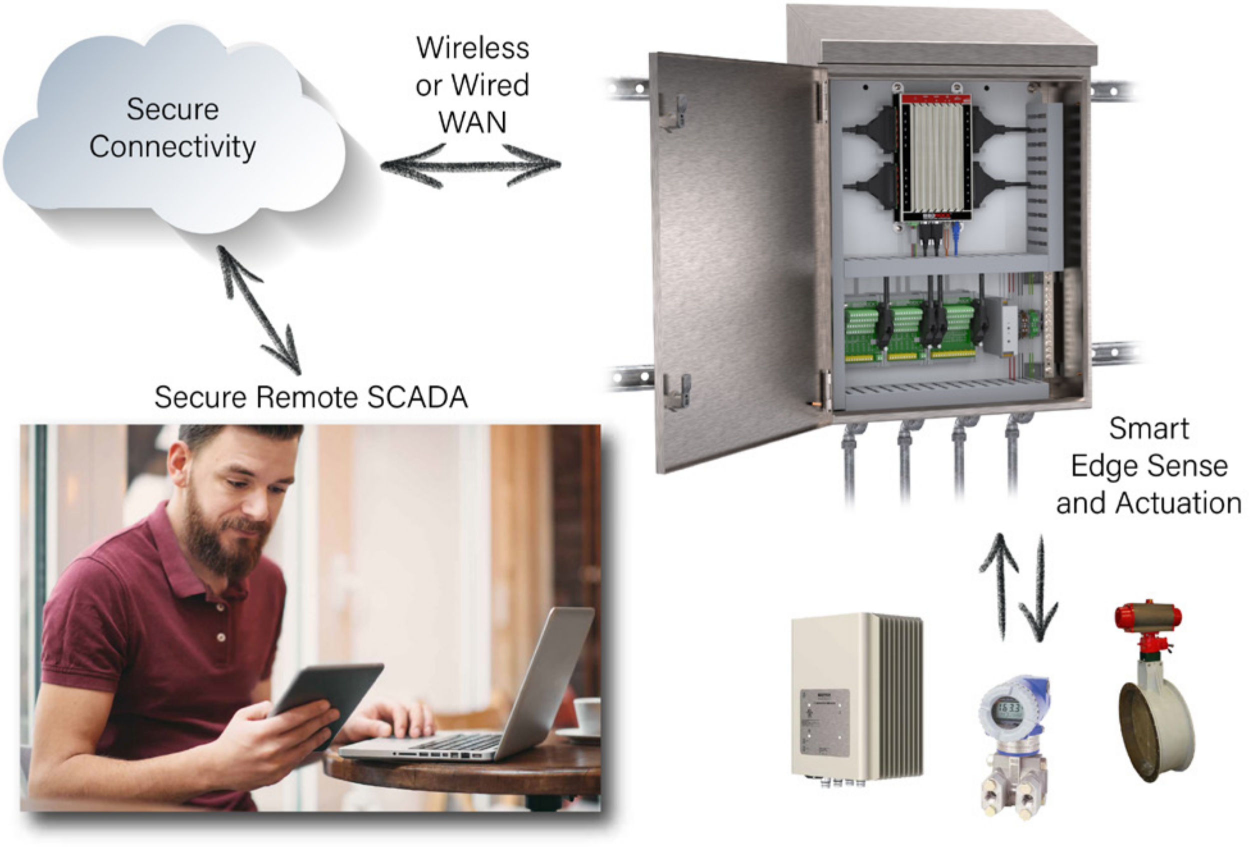
There is an inherent conflict between being open and being secure. In today's world, there is an enormous emphasis on making data flow in real or near real time to wherever it has the potential to be useful. IIoT sensor devices may send data directly to the cloud for analysis with results that come back to a controller as optimized set points. Outside vendors may have remote connections directly into the control network to monitor and maintain equipment. All this openness brings opportunities for saving cost and improving efficiency. It also creates opportunities for cyberattacks.

The bad news is that until very recently designers of control systems had no reason to worry about cybersecurity. In consequence, the vulnerability of most existing systems is very high. The basic defense is to hide behind firewalls and isolated networks to minimize access. This bolt-on security is both costly to install and difficult to maintain.

The good news is that there are proven ways to move data securely. The magic is cryptography called Public Key Infrastructure (PKI). The details are beyond the scope of this article, but the most important point is that the technology is defined by open international standards. It relies on public credentials called certificates that authenticate identity and possession of corresponding secret key values. The same basic mechanisms that secure an ecommerce transaction on Amazon can secure control devices and communications. Secure and open control systems begin with open and secure communications.

The OPC UA connection

One significant step in securing open communications is the advancement of OPC UA (Open Platform Communications Unified Architecture). It provides a standard for managing open communications across multivendor applications and devices. Its latest rendition includes protocols by which users can authenticate



An intrinsically secure controller manages remote connections between the edge and the cloud from anywhere to anywhere with Role Based Access Control (RBAC).
Source: *https://bedrockautomation.com/video/bedrock-power-lunch-september-2020*

and encrypt communications, so that each device or workstation participating in the network has maximum certainty that communications are protected and authentic.

OPC UA has become a relevant standard for SCADA communications because it is simple and scalable, as well as more secure than other communications protocols. When used with a secure control system, the controller has an embedded OPC UA server. SCADA client OPC UA software can easily discover any controller on the network that is running an OPC UA server, know what data is available, and connect to any data the requestor has rights to access.

Once the OPC UA programs find a device running an OPC UA server, it scales easily to allow multiple clients to connect and exchange data securely among servers and clients. That data can then be used in applications that run on PLCs or other controllers, drawing on industry-standard application software and engineering tools, which can be used to construct powerful, complex programs using reusable programming objects.

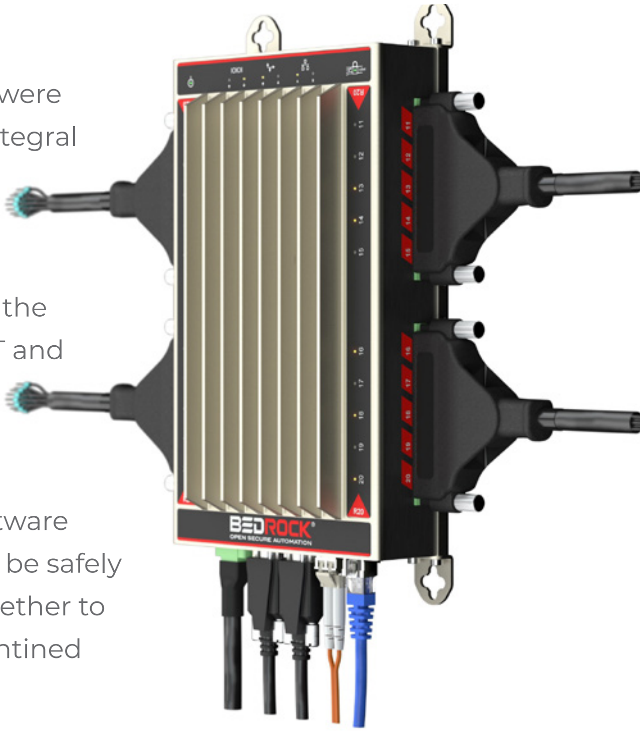
The MQTT low-bandwidth connection

Another emerging open communications protocol is Message Queuing Telemetry Transport (MQTT) using Sparkplug B, a publish/subscribe protocol with built-in report-by-exception capabilities. It optimizes connections from remote locations with only minimal code. Devices publish data to and subscribe to data from a central broker that manages all the connections and routes the data. MQTT supports real-time data. For example, a field device simply publishes its data to the broker once, on change. The broker immediately forwards the data to all subscribers. This approach simplifies the design of the SCADA network and makes providing data for other applications easier than ever. And, like OPC UA, MQTT has the capability to be secure.

MQTT offers SCADA communications many of the same benefits it gets from OPC UA, including ease of use and scalability. However, the server no longer needs to run on the ICS, but instead connects all client nodes securely to a remote broker, enabling each node to both publish and subscribe data. By eliminating the server overhead, efficiently packaging data, and reporting by exception, MQTT reduces bandwidth requirements otherwise needed to connect ICS and SCADA. This reduction in bandwidth makes MQTT well suited for remote IIoT applications implementing a high level of security with a low communication footprint.

Securing OPC UA and MQTT communications

In the past when most of the ICS and SCADA in current use were designed, nothing connected to a control network except integral trusted parts of the control system. This kind of strict air-gapped isolation is no longer viable. To maximize value, the data must flow where it is needed. In today's pandemic-constrained world, this could include a laptop on the employee's kitchen table connected over the Internet. MQTT and OPC UA specifications include PKI-based provision for security. These cryptographic mechanisms allow both verification of identity and encryption of transferred data. The open specification allows integration of devices and software applications from multiple vendors. Authenticated data can be safely sent over untrusted networks. This includes the Internet, whether to exploit cloud-based analytic computing power or the quarantined employee's laptop.



This secure control node from Bedrock Automation combines high-performance edge control with built-in cybersecurity that enables users to tap the full potential of their SCADA systems and the IIoT.

Extending authentication to the control system

Adopting secure communications protocols is only a partial solution. The credentials, keys, and PKI root of trust need to be embedded in the control system devices. This starts with processor silicon that supports secure startup, loads only authenticated software, supports secure storage of secret keys, and can generate the truly random numbers on which the cryptographic mechanisms rely. High levels of security also require physical tamper resistance, secure software updates, and ability to change keys and even new quantum-resistant algorithms when they become available. This is the foundation of intrinsic security and devices that are secure by design. They are also the optimal platform for exploiting the secure variants of open protocols to achieve open secure systems.

"A controller with embedded security provides another layer of protection beyond firewalls and VPNs. As it powers up, it checks to be sure that all hardware and software components are validated. Regular PLCs just can't do that," said Dee Brown, PE, of Brown Engineers, a certified Bedrock Automation integrator.

Toward a safe, open future

In *Securing Industrial Control Systems: A Unified Initiative Fy 2019 – 2023* CISA has a clear vision for how future control systems should be built:

"New OT products, from industrial-scale control systems and networks to Internet of Things (IoT) devices, are secure by design. Cybersecurity becomes a preeminent consideration in the development and design of new OT products, and operators can apply security updates without operational disruption."

Few existing systems approach this goal. Application developers who are interested in taking full advantage of the cost and operational improvement benefits of open SCADA would do well to seek out control technology with embedded cybersecurity. It could reduce operating costs significantly while improving efficiency and safety with minimal cyberrisk.

ABOUT THE AUTHOR

Craig Allen has 11 years of experience in electrical and automation systems. He has been with Bedrock Automation for six years and has been involved with Bedrock from the beginning, managing the field service and technical support teams by leveraging his industrial control experience to ensure customer success. Before joining Bedrock Automation, Allen was a process control engineer, leading efforts to upgrade plants' legacy control systems to the latest systems available across many vendors in the industry. He is experienced in computer and controller programming, system design, fieldbus and IIoT protocols, and network architecture. Allen earned a BSEE from the University of Maine.

How OT Cybersecurity is Improved with Process Safety Best Practices

By Chris Lydon and Eddie Habibi, PAS Global

Information technology (IT) cybersecurity traditionally focuses on the "CIA triad" of confidentiality, integrity, and availability. The practices associated with this model are intended to ensure data is:

- kept private
- not compromised in any way
- available when needed.

OT (Operational Technology) is concerned with the automation systems that facilitate safe production in process and manufacturing industries. OT cybersecurity differs from the IT cybersecurity model because it is not only concerned with data protection, but also with the prevention of cyber espionage and the risk of impact to process safety, reliability, and the environment. OT cyber risk is growing in both frequency and sophistication as malicious actors have recognized the level of dependence modern societies have on OT to manage critical

> Automation and process-safety best practices can also improve control and alarm performance, human interface effectiveness, and automation system resiliency

infrastructure. They are increasingly using automation, machine learning and artificial intelligence to create highly targeted exploits directed at critical infrastructure. These exploits must leverage detailed knowledge of specific automation systems and industrial processes.

The most effective way to counter these exploits is to apply automation and process-safety best practices in addition to IT-focused cybersecurity measures. Beyond protecting OT systems against cyber attacks, these practices also improve control performance, alarm performance, human interface effectiveness, and automation system resiliency. This in turn improves profitability, safety, and reliability.

This article reviews the five operations safety independent protection layers (IPLs) and how applying best practices for each greatly improves OT cybersecurity:

- IPL 1 – Inventory and Configuration Management
- IPL 2 – Automatic Process Controls
- IPL 3 – Human Intervention
- IPL 4 – Safety Instrumented Systems
- IPL 5 – Physical Protection

Safety independent protection layers

Industrial processes and process automation systems are designed with a series of safety independent protection layers (figure 1) that serve as preventive safeguards in the event of an abnormal process event. These layers address the risk of equipment failures but are also highly valuable in the event of a cyber attack. Each layer represents an escalation in the effort to safely mitigate the effects of an abnormal event. When these layers are functioning properly, any operational changes caused by cyber exploits become apparent to plant personnel sooner, so a coordinated OT/IT response can be initiated, and remediation is easier and faster.

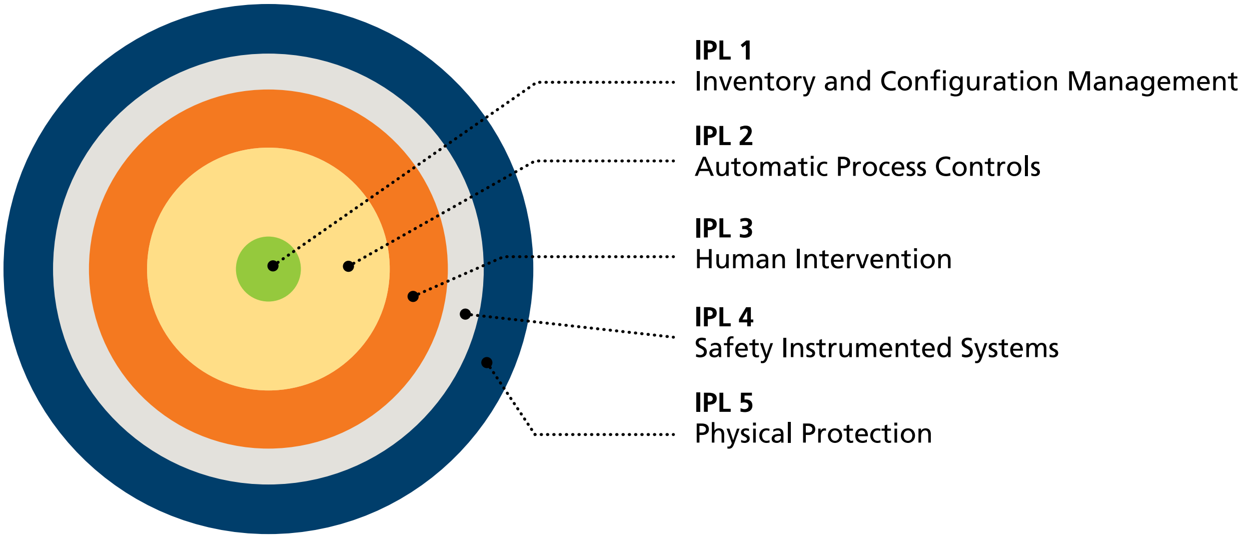

IPL 1
Inventory and Configuration Management
IPL 2
Automatic Process Controls
IPL 3
Human Intervention
IPL 4
Safety Instrumented Systems
IPL 5
Physical Protection

Figure 1. Independent protection layers

Safety IPL 1 – Inventory and Configuration Management

The foundational operational best practice for improving OT cybersecurity is inventory and configuration management of industrial process automation systems. In addition to controlling the process, automation systems are tools for continuous productivity improvement. As a part of daily operation, their configuration is routinely modified by plant personnel in pursuit of this productivity. These modifications may entail controller tuning or alarm limit changes. They may also involve the addition of a new control scheme, or a redesign of an existing one. Ensuring every configuration change is both safe and sanctioned is critical for process operations.

Most companies have implemented some degree of automation Management of Change (MOC) procedures to prevent configuration changes from causing unintended consequences. These procedures usually entail reviews for both operability and safety, and the reviews generally occur before a change is implemented.

There is often no follow-on evaluation after the change has been implemented and accepted by operations, however. In a world where cyber saboteurs seek to do damage by altering automation system configuration, the concept of management of change must expand to include continually monitoring the actual configuration database, and comparing it to a known good and protected record copy.

In the 2010 Stuxnet attack in Iran, the saboteurs used their detailed knowledge of the automation system to deploy a man-in-the-middle attack that portrayed normal operating conditions to the operators, while taking charge of the controls to destroy the process centrifuges. To accomplish this, the attack modified both the control program and the database of the process controller. Inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment facility noticed that its centrifuges were failing at a very high rate. While no one knows for certain, there is evidence that the centrifuge failures may have begun as early as late 2009. However, Stuxnet's role in the centrifuge failures was not recognized until June 2010, months after it first began its sabotage. It is estimated that during this period, Stuxnet damaged or destroyed 984 uranium centrifuges. It is clear from the way Stuxnet functioned, that a robust configuration MOC regimen would have caught the worm long before this level of damage occurred.

> "The **Stuxnet attack** would have been caught much earlier with effective management of change."

Safety IPL 2 – Automatic Process Controls

Although process automation systems perform a variety of tasks, including monitoring, reporting, and historization of production data, they are foremost process control systems. They read critical process measurements and adjust control devices to keep the process at the desired operating state. Process controls are analogous to the autonomic nervous system in the human body; they operate continually and automatically to keep the plant in a stable operating state. Just as with the body's autonomic system, malfunctions can be very disruptive and sometimes dangerous.

Disruptions to process control stability can occur for a variety of reasons. Commonly, they are caused by poor controller tuning, instrument failures, or control valve problems. A sophisticated cyber attack may modify the tuning parameters of the process controllers to destabilize the process. Tuning parameters control the magnitude and speed of the process controller's response to a change in the process. A control change that is too great or that occurs too quickly can rapidly introduce disruptions to the process. A change that is too small or occurs too slowly will allow the process to drift further from the desired operating point. In either case, the process will become destabilized, which can result in product quality issues, lost production, equipment damage, or worse. The greatest risk in such an attack is that operating personnel may never think of them as cyber attacks, and simply write them off as routine process disturbances. It used to be that hackers did not understand how process controller tuning worked. Now many of them do, thereby, increasing the risk to process stability.

An important best practice in support of OT cybersecurity is deploying a control loop health monitoring application that identifies abnormalities in controllers, sensors, and actuators. It's recommended to implement an application that can report control performance issues and prioritize them according to their impact on safety and efficiency of operations. When combined with risk management visualization and alerting tools, plant personnel can quickly identify abnormal parameters and restore controllers to normal state. In sum, what many have thought of traditionally as an operations tool is equally valuable for cyber defense.

Safety IPL 3 – Human Intervention

Human beings intervene in the handling of an abnormal event using the human interface displays and alarm handling capabilities of the process automation system. The initial design of these critical automation system components is often quite poor, creating an environment where critical operational information may be obscured or lost—exactly when it is needed most. Using tools, services, and methodologies that greatly increase situation awareness for plant operators effectively leverages the operators as another tool in the detection of cyber incursions.

Let's examine how to defeat cyber attacks on the automation system by properly managing process alarms and operations risk management visualization tools.

Process alarms

Process alarms are preconfigured notifications of a measured process variable deviating from its desired value by a significant amount. They are the primary means of alerting operations personnel to process problems. However, cyber attackers may disable alarms to hide their mischief from plant operators.

> "In the **Stuxnet attack**, critical process alarms were disabled, so process operators were unaware of the sabotage."

Consider again the 2010 Stuxnet attack in Iran. It included a rootkit that hid its malicious files and disabled the critical process alarms that would have normally tipped off the process operators to the sabotage.

To prevent attacks such as this, we must ensure the alarm system cannot be disabled or alarms masked. An important part of an alarm management regimen is a process called alarm Documentation and Rationalization (D&R). D&R creates a master alarm database to maintain the alarm trip point settings and other critical alarm information separately from the automation system itself. A comprehensive alarm management solution includes functionality to audit the state of the alarms in the automation system, and if they have been modified, to automatically restore their proper values from the master alarm database. This functionality ensures that alarms disabled as part of a cyber attack strategy will not remain so.

High-performance HMI and risk management visualization tools

Processes are generally operated from a set of computer screens (referred to as Human-Machine Interfaces [HMIs]) that depict the operation of the process by displaying key measurements and process alarms. Because automation systems are so easily customized, project engineers often pack information too densely onto the HMI screen, and use display attributes (such as colors, blinking and reverse video) too generously and inconsistently. This approach produces cluttered HMIs that reduce the ability of process operators to rapidly distinguish abnormal situations as they develop. Figure 2 is an example of a poorly designed HMI display that makes rapid identification of abnormal situations extremely difficult.

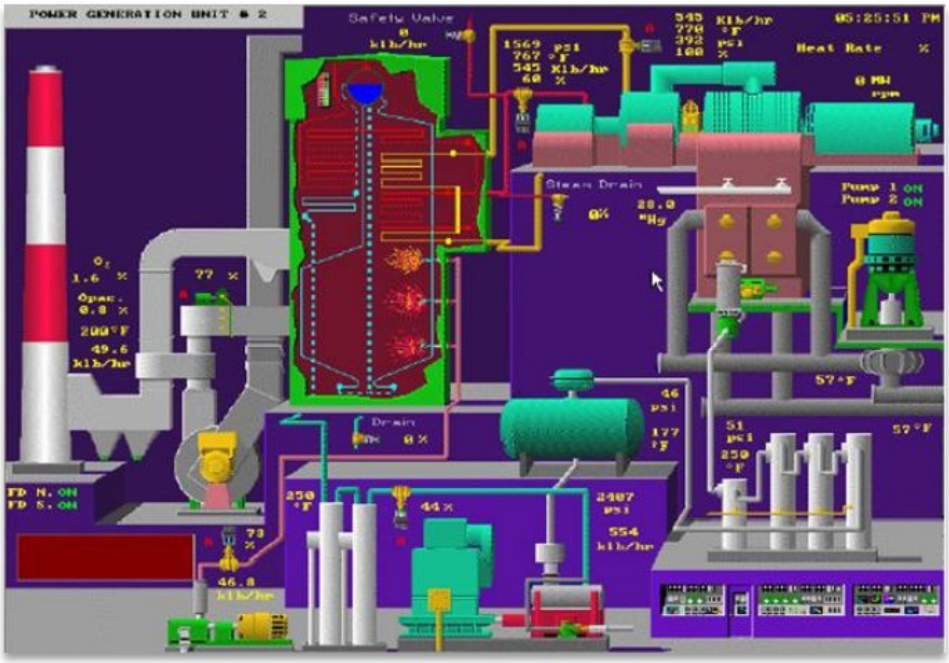
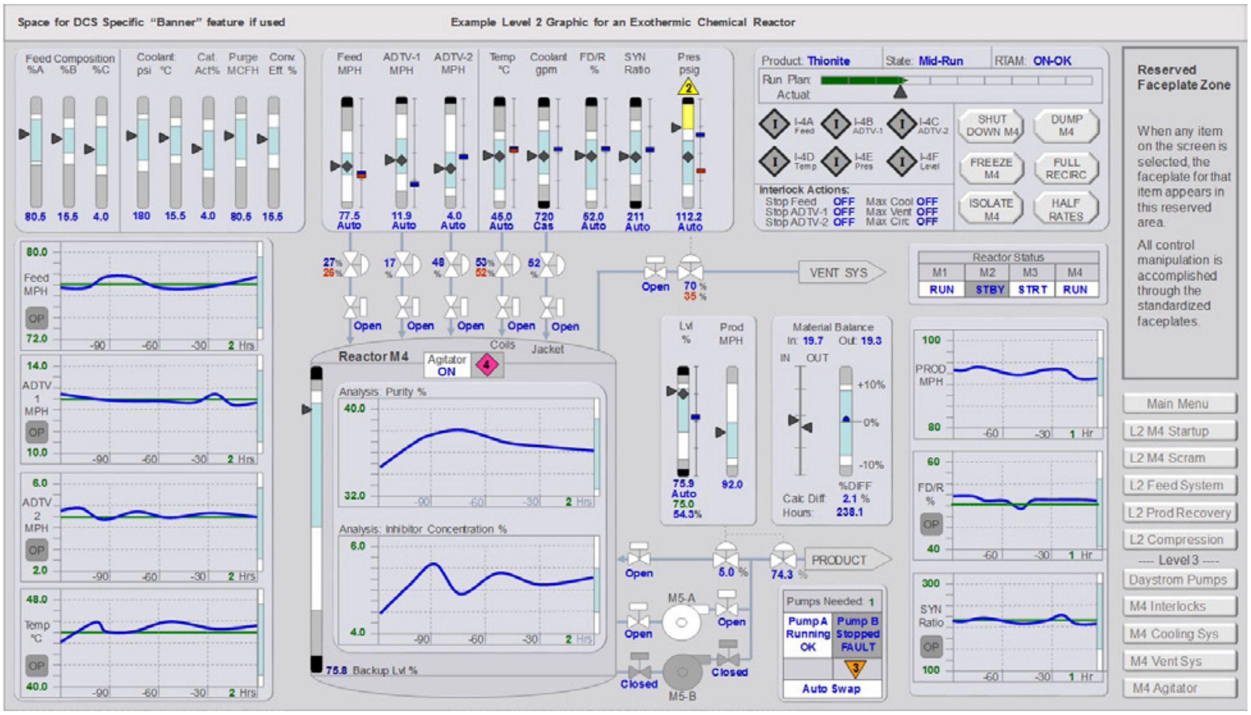


Figure 2. Example of poor HMI design

Source: Maximize Operator Effectiveness: High Performance HMI Principles and Best Practices, Bill Hollifield, PAS Global, LLC, 2015.

For IPL 3 to be maximally effective, plant operators must rapidly identify an abnormal situation and effectively react to it. HMI screens should use a standard set of display objects and be developed using a consistent style guide. Best practices for HMI development call for minimal use of color, and then only to draw attention to a deviation from normal operation. Figure 3 shows a properly designed display. It is easy to see how the display in figure 3 facilitates a faster and more accurate response by operations personnel to both process and cyber events.



Space for DCS Specific "Banner" feature if used

Example Level 2 Graphic for an Exothermic Chemical Reactor

Reserved Faceplate Zone

When any item on the screen is selected, the faceplate for that item appears in this reserved area.

All control manipulation is accomplished through the standardized faceplates.

Figure 3. High-performance HMI design

Source: Screenshot of PAS High Performance HMI™ design

Safety IPL 4 – Safety Instrumented Systems

A Safety Instrumented System (SIS) monitors critical safety-related process measurements in a plant. If the predefined thresholds of these critical measurements are violated, the SIS runs automated procedures to bring the plant back to a safe operating state. Often, the safe operating state entails a complete—but safe—shutdown of the process.

Recently, a tailored exploit called Triton attempted to penetrate the SIS at a large petrochemical plant in the Middle East. The intent of the exploit was apparently to modify the safety instrumented functions in the SIS to prevent it from executing its shutdown function. It is speculated that the exploit may have also intended to penetrate the plant's process control system to manipulate key operating parameters, causing the plant to go out of control. Had this exploit been successful, the result could have been lost production, physical damage to the plant, and possibly harm to plant personnel. Exploits like Triton underscore the importance of SISs to saboteurs and should cause us to place increased cybersecurity emphasis on the SIS.

> “In the **Triton attack**, safety instrumented functions were modified to prevent a safe shutdown.”

SIS monitoring

To ensure that the SIS is available to perform its job if an abnormal event demands it, use an application that monitors and analyzes the performance of Safety Instrumented Functions (SIFs), which are the automated procedures that return a plant to a safe operating state when an abnormal situation occurs.

Tracking the rate of demand on the SIS offers an indication of how often it is called upon to intervene in an abnormal situation. A significant increase in SIS demand may be an early indicator of malevolent cyber activity affecting the process controls, so it is important to monitor this on an operational risk dashboard.

In some normal operational scenarios, such as process transitions, it is necessary to temporarily bypass the safety instrumented functions of the SIS. When this occurs, the safety functions are performed and closely monitored by operations personnel. If, however, the SIFs were bypassed as part of a cyber attack, operations personnel may not be aware of it. This scenario is very similar to the Triton attack mentioned above and would leave a plant dangerously exposed.

Operational boundary management

The nature of some processes requires operations to push production to the limits of equipment physical design constraints. This often requires personnel to monitor a variety of new parameters, which taken together define safe operational boundaries. These parameters include process alarm limits, SIS trip points, environmental excursion limits, and relief valve settings. As long as process operations remain within the boundaries defined collectively by these parameters, they will function safely to onsite and remote personnel.

These safe operational boundary parameters exist in every plant, but they are scattered among a variety of different databases and systems. This distribution of key safety parameters prevents process operators from having a full understanding of their operational boundaries. Therefore, a best practice is to validate and aggregate all of those parameters and visualize them contextually in relation to each other. Look for an application that performs this validation, aggregation, and visualization in real time, and provides automatic notification of boundary excursions.

> "**Cyber attacks** that reconfigure operating boundaries have the potential to do great harm."

Cyber attacks that reconfigure operating boundaries have the potential to do great harm. For example, an attacker may set the value of a reactor high-pressure alarm above the SIS trip point. In this scenario, the reactor pressure could rise to dangerous levels, and the SIS could shut down the process without the operator ever knowing why. Use a tool that validates not only the absolute value of the parameters, but also their dynamic relationship to one another, which would therefore prevent such an attack from being successful. Only by aggregating, monitoring, and validating these diverse parameters, can we prevent such an attack.

Safety IPL 5 – Physical Protection

Industrial plants equipment has built-in physical protections designed into the process itself. These devices include rupture disks and pressure relief valves. Generally, these remedies prevent catastrophic outcomes, but also result in a loss of containment. When an abnormal situation progresses to this point, the focus shifts from proactive protection to reactive mitigation. The intent of a rigorous OT cybersecurity program should be to identify and prevent activities before the physical protections of IPL 5 are engaged.

Safety IPLs essential

Traditional IT cybersecurity practices are a necessary part of a comprehensive OT security program. But OT cybersecurity requires additional tools and best practices based on a detailed understanding of the internal workings of each of the process automation systems implemented in a plant. All five of the safety IPLs described in this article are essential to an effective OT cybersecurity strategy. They quickly identify database changes that may lead to catastrophe and enable plant personnel to serve as additional detectors of potentially malicious cyber intrusions. They facilitate mitigation and remediation in the event of a cyber attack and greatly improve the operational safety and efficiency of the plant, as well as its productivity to the business bottom line. No OT cybersecurity program is complete without them.

ABOUT THE AUTHORS

Chris Lyden, PAS advisor, is an accomplished professional engineer with 44 years of experience in the process automation industry. He has worked throughout the process industries, including in oil refining, petrochemical manufacturing, fine chemicals and pharmaceuticals, and power generation. He has held positions in R&D, project delivery, sales, marketing, strategy, and executive management at Honeywell, Invensys/Schneider Electric, and PAS. Lyden retired in January 2019 and serves in an advisory capacity to PAS.

Eddie Habibi is the founder and CEO of PAS Global, a leading provider of software solutions for the industrial sector. A visionary and thought leader in the fields of industrial control systems and operational technology, Habibi is a renowned industry speaker, author, and business executive. Habibi’s expertise spans industrial cybersecurity, the Industrial Internet of Things, Industrie 4.0, data analytics, and operations management, and his guidance is highly valued by commercial enterprises, government organizations, and industry associations worldwide. In 2017, Habibi was listed by CRN as one of the “30 Internet of Things Executives Whose Names You Should Know.” He is the coauthor of two popular best-practices books on operational risk and safety management: The Alarm Management Handbook and The High Performance HMI Handbook. Habibi holds an engineering degree from the University of Houston and an MBA from the University of St. Thomas.

A Zero-trust Approach to OT/ICS/SCADA Security

Increases in the connectivity of industrial control systems raise important questions about how to secure them—especially heterogeneous systems

By Anton Kreuzer, DriveLock SE

The onward march of smart factory and digitalization initiatives has led to a huge increase in the IT connectivity of industrial manufacturing systems. This raises important questions about how to secure operational technology (OT) and industrial control systems (ICSs)—especially heterogeneous systems. They often run for years, even decades, and many still run on obsolete operating systems—like Windows XP—that are no longer updated or patched. No wonder hackers and cybercriminals increasingly target control systems and other business-critical equipment.

Small and midsized companies in particular are faced with multiple challenges in terms of how to protect their industrial control systems as well as their supervisory control and data acquisition (SCADA) systems against attacks, sabotage, and industrial espionage. The most frequent types of attack include ransomware, infected USB drives, phishing, and social engineering. Downtime and lost data can ruin smaller companies, so security solutions to protect ICS and SCADA systems are essential to their survival.

Never trust, always verify

Conventional security concepts assume that all services, devices, and users in a network are trustworthy. By contrast, the zero-trust model is based on the "never trust, always verify" principle in which there is no distinction between internal and external. But with scarce resources, it can be a challenge for smaller firms to implement a zero-trust approach, especially for application and device control. Updating blacklists and whitelists is extremely labor intensive because the security parameters for each application and device must be entered manually.

> The **security solution** should include self-learning agents that manage the software update process for each ICS by detecting and allowing access by an approved source.

Automatic whitelist and update management

This is where a cloud-based and multilayered security solution comes in, especially if it includes AI and machine-learning features to minimize the human effort needed. The security solution scans and detects which applications and devices are in use when it is first set up, creating the initial whitelist. Using smart application control, it locks and monitors every machine to ensure that no unauthorized applications can be executed on it. This function is complemented by smart device controls that check all connected devices and block unauthorized ones—such as USB thumb drives. This eliminates the risk of insiders illegally copying machine and other critical data.

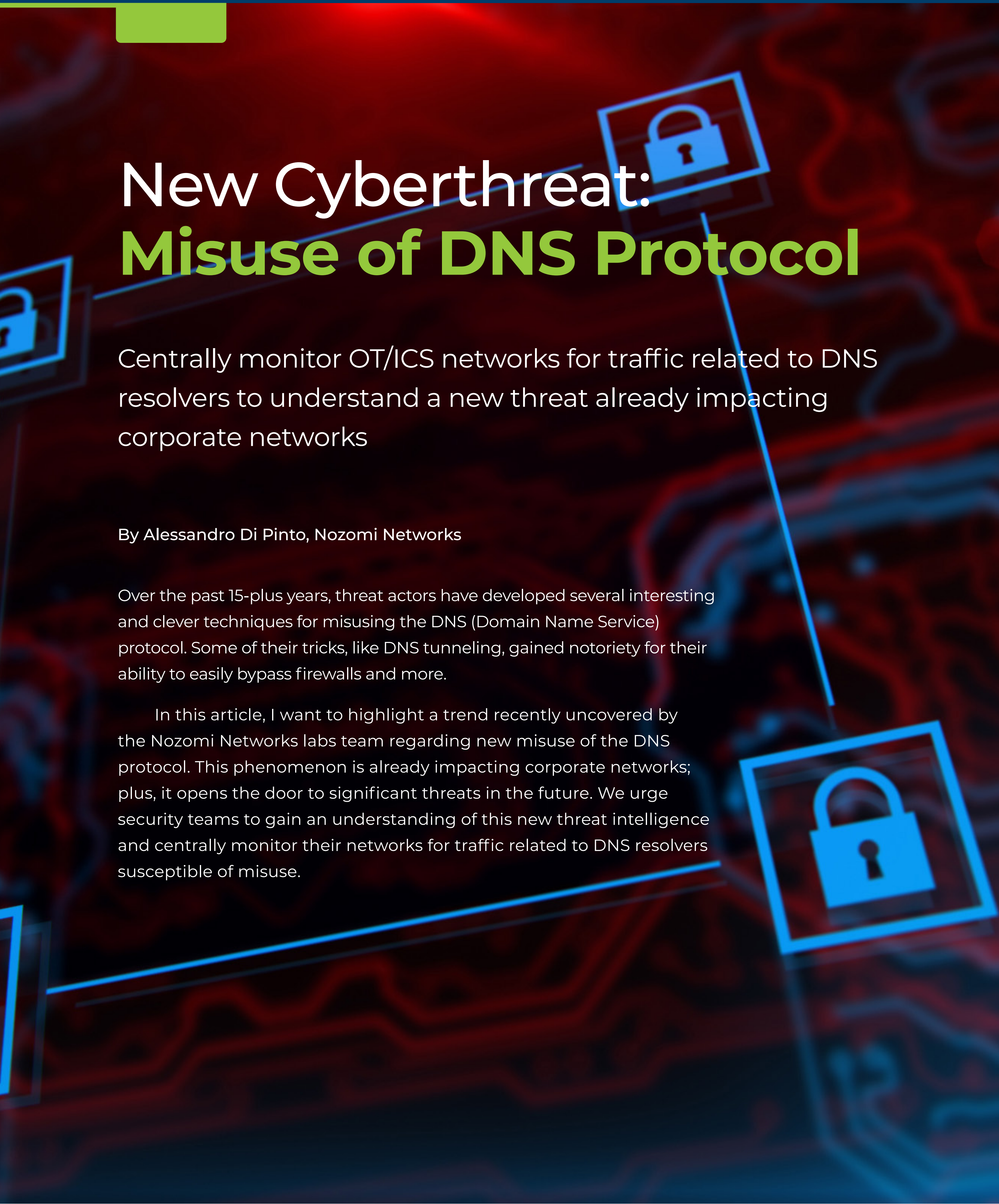
The security solution should also include self-learning agents that manage the software update process for each ICS by detecting and allowing access by an approved source such as the machine's manufacturer. This machine-learning-based management of whitelists and application updates enables companies to keep their ICS and SCADA systems secure with little (human) effort—even old equipment running under obsolete OS like Windows XP.

Smart factories need smart security

The manufacturing industry is undergoing significant transformation, but conventional security solutions are not keeping pace. Manufacturers realize that highly automated and networked machines increase risk as well as productivity. They are an easy target for cybercriminals—and even for employees with a grudge. As a consequence, companies need a comprehensive, affordable security solution based on zero-trust precepts. This ensures that they can leverage all the benefits of integrated production systems while minimizing threats and risk.

ABOUT THE AUTHOR

Anton Kreuzer is the CEO of DriveLock SE, a global IT and security company founded in Munich, Germany in 1999. The DriveLock Zero Trust platform combines data protection, endpoint protection, endpoint detection and response, and identity and access management to protect manufacturing, healthcare and finance systems. Learn more through their website and blog, https://www.drivelock.com/blog



New Cyberthreat: Misuse of DNS Protocol

Centrally monitor OT/ICS networks for traffic related to DNS resolvers to understand a new threat already impacting corporate networks

By Alessandro Di Pinto, Nozomi Networks

Over the past 15-plus years, threat actors have developed several interesting and clever techniques for misusing the DNS (Domain Name Service) protocol. Some of their tricks, like DNS tunneling, gained notoriety for their ability to easily bypass firewalls and more.

In this article, I want to highlight a trend recently uncovered by the Nozomi Networks labs team regarding new misuse of the DNS protocol. This phenomenon is already impacting corporate networks; plus, it opens the door to significant threats in the future. We urge security teams to gain an understanding of this new threat intelligence and centrally monitor their networks for traffic related to DNS resolvers susceptible of misuse.

Blockchain-based domain name resolution

Schemes that leverage blockchain technology to map a domain name to IP addresses have been available for a few years. In these implementations, the blockchain acts as a database that stores the actual mapping.

The main difference between this and a regular ICANN-managed DNS domain lies in the fact that no central authority can prevent the registration of a given domain, nor updates to it. By issuing transactions that are included in the blockchain of reference, a user can independently register any available domain or update its status.

We've seen how malicious operators attempt to abuse DNS to manage their infrastructure through techniques such as fast-flux and domain generation algorithms. We also know that the technique of choice to counteract a botnet using domain generation algorithms is to compile the full list of domains for a given period of time and share the list with the corresponding registry operators. This creates a centralized way to thwart attempts to register malicious domains.

We've seen how **malicious operators attempt to abuse DNS** to manage their infrastructure through techniques such as fast-flux and domain generation algorithms.

Namecoin, a blockchain based on Bitcoin, was the first project to popularize the concept of blockchain-based domain name resolution, as early as 2011. In this scenario, the name to IP resolution is stored in a blockchain rather than a DNS zone. A client who wants to know the address of bitcoin.bit, a specific Namecoin domain, is therefore faced with two choices. The first is to download the whole blockchain and keep it up-to-date. The other option is to connect to a special DNS server that knows that the resolution process of some domains, like .bit, should be performed through a different channel than the one used for typical .com domains.

How the OpenNIC alternative domain name service is misused

OpenNIC is an interesting DNS community project. Its goal is to provide an alternative name resolution scheme to traditional top-level domain registries. Sadly, as is often the case with pieces of Internet infrastructure services that can be misused, there have been instances of malware leveraging OpenNIC to resolve malicious Namecoin domains.

As a result, the part of the infrastructure underpinning OpenNIC ended up in blocklists, with the expected consequences for providers hosting the services. OpenNIC eventually decided to drop support for Namecoin domains in July 2019. Today there's a similar situation with Emercoin, the blockchain behind the .bazar domain.

Emercoin is conceptually like Namecoin to the malicious operator. That is, domain names can be registered with the same level of anonymity as anybody else issuing transactions that become part of the blockchain.

In the last few months, we've seen .bazar domains being used by a piece of malware aptly named Bazar loader / Bazar backdoor. It's typically deployed in an infection chain that ends with the activation of Ryuk, a ransomware known to be targeting healthcare facilities, amongst others.

Malware developers are experimenting with novel techniques to hide their activities, often piggybacking on new technologies that could give them the upper hand in the short term.

The Bazar loader / Bazar backdoor was seen to be relying on OpenNIC to resolve the .bazar domains. Considering how Namecoin was abused, we expect to see some evolution for Emercoin in the near future.

An interesting peculiarity of blockchains is that they're an append-only data structure. For this reason, any IP associated with a particular domain is always available for examination by security researchers interested in tracking down a specific threat.

New threats are using DNS over HTTPS

DNS over HTTPS (DoH) is a recently introduced protocol that resolves domain names over HTTPS, instead of using the typical UDP/TCP port 53-based scheme. Since its introduction, DoH has sparked some controversy. This article isn't intended to explain the rationale behind these positions, but rather to highlight the usage of the protocol by malicious operators.

DoH clearly requires both a compliant client and a server. Some of the major browsers have been implementing the client part of the protocol since its very beginning as a draft. The most popular public resolvers in use today are those provided by Cloudflare and Google. Notably, in February, Firefox started shipping with DoH switched on by default for all users based in the U.S., with Cloudflare set as the default resolver.

The practical effect of DoH is that the payload of a DNS resolution is encapsulated within a TLS session established between a client and a resolver, therefore hiding its content to a passive network observer.

Security researchers at Huntress Labs recently noticed a piece of malware abusing DoH to retrieve the IP of further hosts belonging to malicious infrastructure. The TXT resource record was crafted to mimic a real DKIM record but contained encoded IP addresses instead. In this case, if we isolate the resolution process at the network level, what emerges is a TLS connection between the malware and Google public resolver, although by considering the comprehensive behavior of the threat, several other anomalies will stand out.

Monitor unconventional DNS use

As shown above, malware developers are experimenting with novel techniques to hide their activities, often piggybacking on new technologies that could give them the upper hand in the short term. Given this reality, it's critical for security teams to leverage technologies that centrally inspect DNS traffic. If communications related to resolvers susceptible to misuse (such as Emercoin or DoH) are detected, alerts should be raised and defensive action taken.

Needless to say, a healthy network requires ongoing monitoring using the latest threat intelligence—make sure yours does.

ABOUT THE AUTHOR

Alessandro Di Pinto is an Offensive Security Certified Professional (OSCP) with Nozomi Networks. He has an extensive background in malware analysis, ICS/SCADA security, penetration testing and incident response. He holds GIAC Reverse Engineering Malware (GREM) and GIAC Cyber Threat Intelligence (GCTI) certifications. Di Pinto co-authored the research paper "TRITON: The First ICS Cyber Attack on Safety Instrument Systems" and "Analyzing the GreyEnergy Malware: from Maldoc to Backdoor."