software.org
BSA Foundation

FEBRUARY 2018

Encryption's Vital Role in Industrial Control Systems

Introduction

In today's media, the term "Internet of Things" (IoT) has been getting considerable attention. The reasons for this are varied, from fascination with new and innovative technologies to the discussion of new risks that come hand-in-hand with them. Whether it is high-tech thermostats, appliances, lights, or any of the other thousands of devices entering our daily lives, the realization and promise of an increasingly connected life is everywhere, and consumers are paying attention.

> Partnerships between government and industry are essential to create an environment where encryption research can flourish and promotion of strong encryption can be a universal goal for protecting ICS.

Although IoT may be a useful catchall term, it fails to capture some important differences among the types of devices that are in use today and predicted to grow in ubiquity and importance. One such category of devices is known as Industrial Control Systems (ICS). As the name suggests, ICS encompass a wide range of devices that are most commonly found in commercial, manufacturing, and critical infrastructure environments. For example, ICS are used to control the generation and transmission of electricity, to control mixing reactive substances at chemical plants, and to direct automated assembly lines at manufacturing facilities. The foundational principles behind ICS have been integral to manufacturing and other industries largely since the dawn of automation, and long before the Internet became an essential tool. As technology advanced, ICS advanced as well, bringing with them incremental improvements in efficiency, safety, connectedness, and overall productivity. And there is little reason to doubt that this evolution and expansion will do anything but increase its breadth and pace. Although ICS advancements are clearly providing significant benefit, risk has also increased, particularly as connected ICS find their way into critical infrastructure. In those sectors, ICS are especially

attractive to individuals or organizations seeking to do harm to an adversary. This is one of the most dangerous threats we face, and we must take steps to secure our infrastructure from cyberattacks.

Key elements in securing ICS, and in turn the critical infrastructure that they support or control, are the development and implementation of strong encryption tools to ensure the security of communications between ICS and command and control systems and the authentication protocols that dictate access to sensitive devices. Partnerships between government and industry are essential to create an environment where encryption research can flourish and promotion of strong encryption can be a universal goal for protecting ICS.

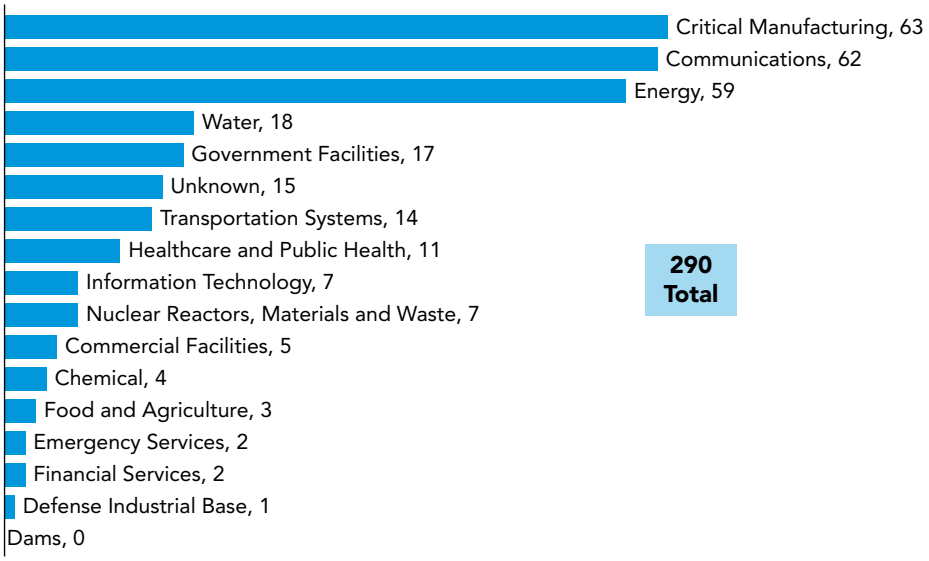
A cyberattack disrupting major critical infrastructure is no longer a hypothetical scenario. In December 2015, after months of planning, attackers took down significant portions of the Ukrainian power grid using a combination of methods.

Risk

A cyberattack disrupting major critical infrastructure is no longer a hypothetical scenario. In December 2015, after months of planning, attackers took down significant portions of the Ukrainian power grid using a combination of methods. A key part of their plan involved uploading malicious firmware to several devices used to transmit operator commands to and from the substation control systems. Once those devices were under their control, any damage the attackers could do at the substations would be impossible for operators to correct remotely.[1]

Although the incident in Ukraine stands out, it is far from the only one that has occurred in recent years, including incidents in the United States. Figure 1 shows the breakdown of incidents that the Department of Homeland Security's (DHS) ICS Cyber Emergency Response Team (ICS-CERT) responded to in 2016 by sector.

Figure 1. Cybersecurity Incidents in 2016 (by Sector)



[1] Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, Wired.com, available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

It is notable that critical manufacturing was the largest single sector targeted. DHS defines critical manufacturing as any manufacturing where disruption would have a significant negative effect at the national level and across multiple critical infrastructure sectors. Examples include metals, machinery, electronics, and transportation equipment.[2] In conjunction with communications and energy, these three sectors account for more than half of all incidents reported in 2016.

Although the frequency of incidents is concerning, it isn't the entire story. ICS continue to have pervasive vulnerabilities across hardware and software components and malicious actors are paying attention.

Between July and August 2017 alone, ICS-CERT issued nearly 50 alerts highlighting both software and hardware vulnerabilities in various ICS across multiple sectors.

In 2017, Symantec released a report detailing evidence of a sophisticated hacker group infiltrating the ICS of US electric companies.[3] It remains unclear whether these hackers would be able to create the sort of trouble seen in Ukraine, but the fact that they are able to gain any access to these critical systems is reason enough for concern.

Indeed, you don't have to go any further than the US ICS-CERT website to see that risks are prevalent. Between July and August 2017 alone, ICS-CERT issued nearly 50 alerts highlighting both software and hardware vulnerabilities in various ICS across multiple sectors.

DHS has been collecting and releasing these alerts for years and the pace has only increased. Beyond the growing focus and sophistication of malicious cyber actors, the increase in pace can be attributed to at least two factors. First, ICS, unlike computers and smartphones, are complex and expensive systems manufactured for use over decades, rather than years. As a result, many ICS built long before the emergence of current cybersecurity threats and defenses remain deployed throughout industry. Second, more and more devices are being developed and implemented without fundamental security features built in or turned on by default.

Because of these two factors, basic features we expect from our technology, like not requiring remote access passwords to be changed or enabling encryption, remain weak or missing entirely from many ICS.

Cryptography: Encryption

Generally considered to be a foundational element of good security across all sectors, encryption, over the last several decades, has moved from being limited largely to government systems and communications to being featured in most technology devices in use today, such as mobile phones, laptop computers, servers, and others. Additionally, encryption serves as

[2] *Critical Manufacturing Sector*, DHS, available at https://www.dhs.gov/critical-manufacturing-sector.

[3] *Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group*, Symantec Blog (October 20, 2017), available at https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group.

the backbone for secure communications across the Internet, ensuring that consumer, business, and government data can be kept secure anywhere in the world. Indeed, much of modern commerce and national security depends on this being the case.

Despite its well-deserved success, encryption is not without its challenges. For starters, the mathematical and scientific principles that serve as its foundation are complex. As computers have grown more powerful, and therefore better able to "break" encryption, researchers have been under increasing pressure to develop innovative and advanced encryption algorithms. As with most elements of security, it is a constant effort to stay ahead of malicious actors. As computing power has increased, so too has the need for greater encryption key lengths and new algorithms. Fortunately, modern encryption remains secure and viable, but continued investment in research will be necessary for it to remain so, particularly in the face of major increases in computing power, such as those predicted with quantum computing.[4]

Fortunately, modern encryption remains secure and viable, but continued investment in research will be necessary for it to remain so, particularly in the face of major increases in computing power.

Encryption must also be interoperable. It does little good if one company encrypts its data one way, and its business partner another way, resulting in an inability to exchange information. This means that, in practice, encryption methods tend to be ubiquitous; that is, the underlying algorithms are shared by most organizations, thereby facilitating the necessary interoperability. The alternative, where nations and companies create communities of interest around their unique encryption methodologies, simply won't support the modern economy. This need for interoperability extends beyond the algorithms and in to implementation. Well known cryptographer Bruce Schneier said as far back as 2009 that "…encrypting the data is the easiest part; key management is the hard part."[5] For key management to work, all parties to a communication, such as between ICS devices and their command and control structure, must be able to understand and process the keys on which the encryption and decryption of the data rely. If implemented improperly or weakened in any way, attackers can take advantage and gain control of the ICS they are targeting.

Encryption is important to ICS in deploying cryptographically signed updates and patches. The need for software updates and patches are as old as software itself. As a society, we have grown accustomed to regular software updates adding new functionality to our software and patching frequently discovered bugs. We get them on our computers, mobile phones, even our gaming systems. And while developers strive to reduce the number of vulnerabilities, code bases are growing larger and more complex, meaning that the challenge of producing bug-free software is only getting harder.

As the software built into ICS grows more complex in order to support more features, the risk that vulnerabilities and weaknesses exist in that software increases. Moreover, because ICS are intended for long-term use, a system

[4] NIST Technology Laboratory, *Post-Quantum Cryptography*, Computer Security Resource Center, available at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[5] Bruce Schneier, "Cold War Encryption Is Unrealistic in Today's Trenches," *The Japan Times* (December 23, 2009), available at https://www.schneier.com/essays/archives/2009/12/cold_war_encryption.html.

will often integrate significant functional upgrades or entirely new software packages many times over its lifespan. As with other technology, operators and manufacturers of ICS need the ability to correct vulnerabilities and enhance functionality by updating the software and installing it on the ICS remotely. Unfortunately, as seen in the Ukraine example, this same mechanism can be used by malicious actors to upload their own software, gaining control or otherwise compromising the device or devices simultaneously. Ensuring that patches and updates are deployed using encryption techniques to verify their authenticity and integrity means that an attacker will have a much harder time inserting modified software into the ICS.

There is no practical middle ground. Ultimately, what this means is that encryption must remain as strong as possible for as long as possible and work must continue to keep it strong into the future.

Even with the ability to securely update software being built into newer ICS, a challenge remains with legacy devices currently in operation. Because most ICS are designed to be in place for years, sometimes even decades, older devices spread across critical infrastructure are likely to remain potentially vulnerable for some time without major investment in time and resources.

Even when methods exist to update these legacy devices, often they do not have the necessary hardware capabilities to support modern encryption methods, thereby remaining vulnerable until they can be replaced.

And the challenge of inadequate hardware to support encryption isn't limited to just older devices, either. Many types of devices, by the nature of their size and function, may not be able to support encryption. This has led to research into lightweight cryptography, led by the National Institute of Standards and Technology (NIST). NIST's goal is to determine the need for lightweight cryptographic algorithms because "the majority of current cryptographic algorithms were designed for desktop/server environments" and "do not fit into the limited resources of constrained environments," such as the millions of small-scale sensors and devices deployed as part of the IoT.[6]

These challenges demonstrate that without continued investment, the effectiveness of today's encryption will wane over time, and that the risk of compromise increases as it does so. That risk can be understood, measured, and mitigated, but it depends on the encryption being trustworthy from its inception. Poorly designed algorithms that can't be validated by a transparent and open process will only accelerate the potential risk to all sectors, including critical infrastructure. And, because those algorithms will be used across all sectors to support interoperability, weaknesses can't be limited to only one type of device or any given class of user or organization. For example, providing access for certain third parties allows protections against man-in-the-middle attacks to be thwarted, not only for "authorized" parties, but also for malicious actors. There is no practical middle ground. Ultimately, what this means is that encryption must remain as strong as possible for as long as possible and work must continue to keep it strong into the future.

[6] NIST Technology Laboratory, *Lightweight Cryptography*, Computer Security Resource Center, available at https://csrc.nist.gov/Projects/Lightweight-Cryptography.

Cryptography: Authentication

Encryption is just one application of cryptographic technologies; these same technologies are also used to support other critical security functions, including authentication, message integrity, and non-repudiation. Indeed, some of these uses of cryptology can be considered more important in the ICS environment than simply encrypting ICS traffic.

Authentication is known as the means by which a receiver of an electronic transaction or message makes a decision to accept or reject that transaction or message. In simple terms, authentication answers the question "Who are you?" — or in ICS, "What are you?" — when a command or message is received. As ICS components become increasingly connected to each other — and to the Internet at large — the ability of these systems to securely authenticate one another is important, as is the ability of systems to ignore communications from any component that is not properly authenticated.

The implications are significant: as devices and components communicate in real time, any entity holding authentication keys has the ability to send commands to control systems, including commands that can take them over.

The implications are significant: as devices and components communicate in real time, any entity holding authentication keys has the ability to send commands to control systems, including commands that can take them over.

The consequences of poor authentication in connected devices were illustrated by the 2016 Mirai attack,[7] where attackers took advantage of millions of connected devices that had been deployed with default usernames and passwords, leveraging these defaults to take over the devices and launch the largest distributed denial of service (DDoS) attack the world had ever seen.

Although avoiding default passwords offers one layer of protecting against these types of attacks, using encryption is essential to protect any system where passwords are used. Per the 2016 ICS-CERT annual report:

> If encryption is not enabled on authentication — meaning password data are transferred as clear text — attackers can simply listen to the traffic and pull the user name and passwords off the wire while in transit. Once compromised, persistent access is granted for the lifetime of the user accounts and passwords.[8]

However, given how much the password itself is attacked — the 2017 Verizon Data Breach Investigations Report (DBIR) reported that 81 percent of hacking-related breaches were executed by exploiting weak or stolen authentication

[7] Steve Ragan, *Here Are the 61 Passwords That Powered the Mirai IoT Botnet*, CSOonline.com (October 3, 2016), available at https://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html.

[8] US Department of Homeland Security NCCIC, *ICS-CERT Annual Assessment Report: Industrial Control Systems Cyber Emergency Response Team FY 2016*, available at https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

credentials[9] — industry is now moving to implement stronger, non-password-based authentication solutions that are built using strong cryptography. These solutions include using both symmetric and asymmetric cryptography.

Importantly, however, ***these stronger authentication solutions rely on the same cryptographic systems and algorithms that also power encryption***. Thus, any weakness or vulnerability in encryption systems creates a path to undermine the strong authentication tools that are used in many cases to protect and control the systems themselves.

Any weakness or vulnerability in encryption systems creates a path to undermine the strong authentication tools that are used in many cases to protect and control the systems themselves.

Specifically, in systems today, a cryptographic key used for encryption may also be used for authentication. There are generally neither distinguishing features among different types of keys, nor do most systems differentiate between how these keys are used; in many cases, a single key might be used to both encrypt and authenticate. In practical terms, that means the same system that allows a party access to read traffic and communications could also allow that party to modify that traffic or those communications. If exploited, this could enable an attacker to leverage compromised keys to wreak havoc in innumerable ways.

If attackers can leverage a weakness to defeat the encryption of a system, they can also leverage that weakness to defeat authentication — and then be in a position to take over the ability to send commands to control systems. For example, most Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) cloud offerings are administered remotely, while the security of the control traffic for these systems is managed through cryptographic keys using standard protocols like Secure Sockets Layer/Transport Layer Security (SSL/TLS). A key escrowed for the purpose of allowing access to data flowing through these systems could also allow the holder of that key to access administrative functions for that system.

Government Role

ICS feature prominently in manufacturing and critical infrastructure, most of which is owned and operated by the private sector in the United States. Nevertheless, due to the economic, safety, and national security risks associated with compromised ICS, the government has an interest in ensuring that ICS are securely deployed and managed.

That interest is expressed in several ways. On the research side, agencies such as NIST and DHS Science and Technology (S&T) Directorate support research and development and the creation of standards and guidelines regarding the safety and security of ICS.

[9] *Verizon's 2017 Data Breach Investigations Report: How Long Since You Took a Hard Look at Your Cybersecurity?*, available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

NIST's *Guide to Industrial Controls Systems Security*, has been downloaded multiple times since its first release in 2005. Updated in 2015, this guide "advises on how to reduce the vulnerability of computer-controlled industrial systems to malicious attacks, equipment failures, errors, inadequate malware protection and other threats."[10]

As noted above, DHS operates ICS-CERT, which works with critical infrastructure organizations across the country to monitor for threats and provide assistance when things go wrong. In addition to their notices regarding vulnerabilities in ICS and their actions to assist the owners and operators of critical infrastructure in responding to incidents, they also have teams of experts that conduct assessment of ICS across the country.

From a legislative perspective, Congress has been struggling to determine exactly how best to regulate ICS in certain sectors for reasons of national security and safety, while ensuring that the innovation essential to a growing economy can continue.

Overall, they conducted 130 assessments in 2016 through which they identified 700 weaknesses, many of which were violations of basic cybersecurity principles such as encrypting sensitive data, insecure authentication methods, and lack of adequate network boundary protection and segmentation.[11]

The US government can also play an important role as a convener and facilitator. The National Telecommunications and Information Agency (NTIA) formed a multi-stakeholder effort in late 2016 that has brought together numerous experts from government and industry to focus on the upgrading and patching issues with IoT devices. The output from this effort will contribute to the ongoing discussion and help to influence device manufacturers and policymakers.

From a legislative perspective, Congress has been struggling to determine exactly how best to regulate ICS in certain sectors for reasons of national security and safety, while ensuring that the innovation essential to a growing economy can continue.

In the absence of legislation regulating ICS and related cybersecurity risks, Congress has advanced legislative proposals to establish pilot programs as well as to devote resources toward research and development of mechanisms to secure critical infrastructure. For example, the Support for Rapid Innovation Act of 2017, sponsored by Congressman John Ratcliffe (R-TX) amends the Homeland Security Act of 2002 to direct the Under Secretary for Science and Technology of DHS to support the research, development, testing, evaluation, and transition of cybersecurity technologies, including assisting the development and support of technologies to reduce vulnerabilities in ICS.[12] Additionally, Congressman Dutch Ruppersberger (D-MD) and John Carter (R-TX) introduced H.R. 3958, a bill to establish a pilot program on securing

[10] *NIST Releases Update of Industrial Control Systems Security Guide* (June 5, 2015), available at https://www.nist.gov/news-events/news/2015/06/nist-releases-update-industrial-control-systems-security-guide.

[11] *ICS-CERT Annual Assessment Report.*

[12] Support for Rapid Innovation Act of 2017, H.R. 239, 115th Cong. (2017), available at https://www.congress.gov/bill/115th-congress/house-bill/239/text?q=%7B%22search%22%3A%5B%22support+for+rapid+innovation+act%22%5D%7D&r=2.

energy infrastructure.[13] One of the bill's purposes is "researching, developing, testing, and implementing technology platforms and standards, in partnership with covered entities to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems…"[14]

Although it remains to be seen how Congress will ultimately address these concerns, these legislative proposals suggest that Congress recognizes a need to explore regulatory solutions with respect to managing threats to ICS while working in conjunction with industry partners.

Making ICS as secure as possible, for as long as possible, is in everyone's best interest: government, law enforcement, manufacturing, critical infrastructure, businesses, and consumers. That means continuing to invest in strong encryption that can be deployed in numerous contexts and that protects everyone equally.

Industry Role

In the United States, the private sector is the primary owner and operator of critical infrastructure and the ICS that support it. Through their own efforts and in coordination with government agencies such as NIST and DHS, critical infrastructure companies have demonstrated a recognition that they have a role to play in securing their systems. However, the challenge doesn't lie solely in their hands. Manufacturers of ICS play an essential role in ensuring that the devices they build have the security capabilities necessary to support a secure infrastructure.

Driving to those secure mechanisms in part means investing in industry-wide standards and in the research and development of new and advanced technologies. Efforts in this area are numerous and difficult to summarize but it is worth noting at least one example, ISA99, a standards development committee focusing on industrial automation and control systems security.[15]

This group's focus is to "…improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems." To that end, significant work is being done across several standards in this family to address specific issues such patch management, security life cycle, produce development requirements, and more.

The ISA99 initiative — now recognized by the International Electrotechnical Commission (IEC) because IEC 62443 is being used globally and has been incorporated in efforts such as the NIST Cybersecurity Framework — gives organizations a simple roadmap to implement cybersecurity. This and other standards work will continue to drive positive change, but it is only part of the solution to having secure ICS.

[13] Securing Energy Infrastructure Act of 2017 H.R. 3958, 115th Cong. (2017), available at https://www.congress.gov/bill/115th-congress/house-bill/3958/text?q=%7B%22search%22%3A%5B%22pilot+program+on+securing+energy+infrastructure%22%5D%7D&r=1.

[14] Ibid.

[15] *ISA99, Industrial Automation and Control Systems Security*, ISA.org, available at https://www.isa.org/isa99/.

The advancement of ICS, and indeed all of IoT, is driving a technology convergence in new and interesting ways. The interdependence of software, hardware, networks, users, sensors, and controllers means that for any given device, multiple organizations have an interest and responsibility for its security and operation. This in turn means that each of these stakeholders needs to participate in understanding other perspectives while sharing their own, particularly in the area of cryptography and its application in encryption and authentication, which is essential to the success of ICS. Whether through standards, policy discussions, or working groups, industry stakeholders need to have a unified voice on these issues; one that addresses the many perspectives inherent in this challenge.

Conclusion

Manufacturing and critical infrastructure sectors of developed nations around the world are at risk. Long designed to be resilient against economic changes, hurricanes, floods, and the occasional backhoe, that infrastructure is, in most cases, ill-suited to defend against human adversaries executing attacks on industrial control systems over the Internet. Government and law enforcement are right to be concerned by these adversaries, whether they be nation states, hacktivists, or criminals, and have the responsibility and authority to identify them and protect this country accordingly.

But making ICS as secure as possible, for as long as possible, is in everyone's best interest: government, law enforcement, manufacturing, critical infrastructure, businesses, and consumers. That means continuing to invest in strong encryption that can be deployed in numerous contexts and that protects everyone equally. It means ensuring that authentication mechanisms are grounded in proven models that are adaptable across technologies. And it means developing the standards necessary to build secure infrastructure that is not only resilient, but resistant to attack both now and into the future.