Securing Complex Cyber-Physical Medical Device Landscapes
# Table of Contents

## Developing and Connecting Cybersecurity Leaders Globally

### Feature

14. **Securing Complex Cyber-Physical Medical Device Landscapes**  
   *By Ulrich Lang*  
   The author presents innovative approaches to cybersecurity that should be considered to securely integrate medical device landscapes (and many other IoT environments) in the coming years as IoT rapidly matures.

### Articles

20. **The Dangers in Perpetuating a Culture of Risk Acceptance**  
   *By Matt Wilgus – ISSA member, Raleigh Chapter*  
   This article details the prevalence of risk acceptance within organizations, why IT security departments may be putting too much confidence in their controls, and how excessive risk acceptance is often cultural.

26. **Using PKI to Build a Secure Industrial Internet of Things**  
   *By Mike Nelson*  
   This article provides an overview of how device manufacturers can address security concerns for IIoT devices by using public key infrastructure.

32. **The Two Faces of Innovation: From Safe and Dumb to Vulnerable Smart Products and Infrastructure**  
   *By Steven W. Teppler*  
   This article discusses the ongoing proliferation of “crime-as-a-service” and its facilitation by insecure and/or defectively coded Internet of Things (IoT) or “smart” devices.

36. **Cyber-Physical Intelligence**  
   *By Tyson Brooks – ISSA member, Central Maryland Chapter*  
   In this article, a novel model for cyber-attack defense modeling for intelligence collected from a cyber-physical system network and its devices themselves to evaluate the security of these systems in the presence of cyber attacks is proposed.

### Also in this Issue

3. **From the President**  
   Securing the Internet of Things

5. **Sabett’s Brief**  
   It Will Be Massive in 2018

6. **Herding Cats**  
   EYE OH TEE

7. **Perspective: Women in Security SIG**  
   Using IoT to Build a Stronger Cybersecurity Community Fabric

8. **Gray Hat**  
   Get it Right: Offense Versus Defense

9. **Security Awareness**  
   Getting Permission to Use “Have I Been Pwned?” from Your Legal Dept

10. **Open Forum**  
    The End of Security

11. **Crypto Corner**  
    Now That’s Computing Power

12. **Security in the News**

13. **Association News**

30. **Book Review**  
   InSecurity

41. **Career Center**

©2018 Information Systems Security Association, Inc. (ISSA)  
The ISSA Journal (1949-0550) is published monthly by Information Systems Security Association  
1964 Gallows Road, Suite 310, Vienna, VA 22182  
+1 (703) 382-8205 (local/international)
Hello, ISSA Members and Friends

Keyaan Williams, International President

Securing the Internet of Things

The April Journal focuses on security and the Internet of Things (IoT). The articles in this edition discuss the risks, impacts, concerns, and solutions used to secure the IoT in modern enterprises. The role that the security professionals play in IoT security is an important part of the conversation. Developing the right knowledge and awareness is key to managing the unique concerns inherent in the IoT. It is also important to distinguish between the industrial Internet of Things (IIoT) found in industrial environments and commercial IoT developed for traditional enterprises and consumers.

Many security professionals are unfamiliar with the distinction between IoT and IIoT. They are also unfamiliar with the nuances and requirements in IoT that differ from what people normally encounter in a traditional corporate enterprise, data center, or the cloud. As security professionals, we must understand and engage with operations security standards to ensure the risks of industrial and commercial IoT are managed properly in our respective organizations, for example, understanding how Internet-based protocols like Message Queuing Telemetry Transport (MQTT) operate to influence the design of controls and security architectures for IoT.

Numerous studies and analyses show that the cybersecurity skills gap is a growing problem. Most of these assessments focus on traditional enterprise security and overlook the need for skilled operations and industrial control systems (ICS) security professionals. The need is no longer restricted to manufacturing and critical infrastructure verticals. As the IoT continues to permeate modern businesses, the shortage of people who understand and are equipped to manage its security poses a serious risk to safety and operational resilience of organizations across all industries with few exceptions. Failing to understand the foundations of operations security can lead even experienced enterprise security professionals to jeopardize the infrastructure upon which we all depend.

Security professionals can develop a deeper understanding of IoT security by learning the standards for industrial automation and control systems security. For example, “ISA99 outlines standards, recommended practices, technical reports, and related information that define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance.” Security practices defined by ISA99/62443 and functional reference models like the Purdue Enterprise Reference Architecture, which establishes logical operating zones based on the functional capabilities of ICS equipment, provide the knowledge required to make the right decisions about managing the risks posed by industrial and commercial IoT.

Security professionals also have many opportunities to engage in person at operations security events and conferences. It is imperative that professionals responsible for managing IoT security attend events that help outline the scope of the ICS security problem and provide meaningful practices and solutions that attendees can apply in their environments. Some of the most mature and successful industrial cybersecurity events include Digital Bond’s S4 events, the Cyber Security for Critical Assets Summit (CS4CA), the SANS ICS Security Summit, and the Industrial Control Systems Joint Working Group (ICS-JWG) meetings.

ISSA Has a New Executive Director

Effective April 2, 2018, Marc Thompson will serve the ISSA as our new executive director. Marc brings nearly 20 years of executive management experience to the ISSA. He is best known for managing (ISC)² during its rapid growth years (2001-2011), leading all the CISSP education efforts, founding (ISC)² event programs and member publications, and building out the international infrastructure. Marc was also instrumental in the early years of ISSA development, including founding one of the largest chapters (Northern Virginia) and working with ISSA chapters around the world to help build CISSP training programs. Marc will help ISSA complete the transition to self-management and will help the association grow substantially over the next few years by increasing membership value through education and improved chapter initiatives.

Thank you,

Keyaan Williams

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author’s experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see www.issa.org.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.
We’ll start this month’s column off with a quiz. The title to this month’s column paraphrases “what famous entity is describing the Internet of Things?” Is it (a) Forbes magazine, (b) Pee Wee Herman, or (c) President Trump? It wasn’t Pee Wee Herman, though I did bring him up in my June 2015 and August 2016 columns on IoT. It wasn’t President Trump, who hasn’t really weighed in (or tweeted) yet on IoT. It actually was IBM, in an article that appeared in Forbes magazine in January.

In the article, Forbes attributes Gartner for the statement that the IoT will top 11 billion devices in 2018 (excluding computers and phones). With that many devices being connected to the Internet, many of them with little if any security, is it any wonder that there haven’t been more denial of service attacks crippling the Internet like the one caused by the Mirai botnet?

More interestingly, the legal eagles working in this area wonder when the lawsuits will begin and, to a much lesser extent, when legislation will pass. While the Internet moves at, well, Internet speed, legislation continues to move at a glacial pace. Many commentators point out that this is particularly true with today’s lawmakers. For an indication of this, one need only look at the IoT-related bills that have been introduced in Congress.

For example, the Internet of Things Cybersecurity Improvement Act of 2017, introduced on August 1, 2017, was referred to the Committee on Homeland Security and Governmental Affairs and no further action has been taken. As currently drafted, the bill would:

- Require vendors who provide Internet-connected devices to the federal government to ensure that their devices can be patched, rely on protocols that are based on industry standards, do not use default passwords that have been hard-coded, and do not contain any known security vulnerabilities.
- Direct the Office of Management and Budget (OMB) to develop and promote security requirements specifically designed for IoT devices that contain limited data processing and software functionality.
- Direct the National Protection and Programs Directorate (NPPD) within DHS to issue guidelines regarding vulnerability disclosure policies required of contractors providing connected devices to the US government.
- Provide an exemption from liability under the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA) to cybersecurity researchers engaging in research (in good-faith) when engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines.
- Require each executive agency, in an action reminiscent of the Trusted Internet Connection (TIC), to inventory all Internet-connected devices in use by the agency.

While all of these sound great, the provisions (a) only apply to interactions with the US government and (b) are contained in a bill that is stuck in committee. As many of you know, I am not someone who prefers legislation if market forces will take care of whatever particular problem may exist. In this case, I’m not sure that legislation such as the bill described above (even if it were extended to private parties) would necessarily improve security. The concern that I have, however, is that market forces do not seem to be solving the problem. Devices and sensors continue to flood the market with little (if any) security integrated.

Congress may not be moving as quickly as everyone would like on IoT, but recently a hearing was announced by the Consumer Product Safety Commission (CPSC) regarding the intersection between IoT and consumer product hazards. While consumer safety and product liability have often been dismissed in the context of cybersecurity, this hearing gives an example of where they will have an audience. The hearing will examine topics such as the prevention of hazardous conditions designed into products and hazards created from intended product features. The results could potentially change how all stakeholders look at IoT devices.

We often talk about privacy by design and security by design. I believe those same philosophies can be applied to IoT. If engineers were to build in security to their IoT devices from the start, we might be able to address the security problems that continually get pointed out. Until that time comes, we are just counting down until the next major IoT-based incident…or should I say “massive”? Talk to you all next month.

About the Author

Randy V. Sabett, J.D., CISSP, is Special Counsel at Cooley LLP (www.cooley.com) and a member of the Boards of Directors of ISSA NOVA and the George-town Cybersecurity Law Institute. He was a member of the Commission on Cybersecurity for the 44th Presidency, was named the ISSA Professional of the Year for 2013, and can be reached at rsabett@cooley.com.
What will the business plan need to be in order to ensure the long-term security of an IoT device? We have a few things to consider. The major difference is more devices and a concerted focus on the ability to update devices in the field.

My refrigerator doesn’t have an IP address, but I can’t say I’d be thrilled walking up to my refrigerator acting all weird and telling me that an update failed.

IoT devices that make it to market don’t have a couple of features that our mobile phones do: good user interfaces and a robust system for updates. Both of these features may materially impact the manufacturing costs of the IoT device. Adding an LED display or buttons costs money and introduces failure points, and complex crypto tasks may require a processing chip more powerful than required to measure the amount of steps you take in a given day.

So when we examine the main problem of modifying software running on an IoT device, we have a few things that have to be decided in order to ensure the business plan adjusts accordingly.

AAA (authentication, authorization, access): In order for a device to receive updates or changes to its code, there needs to be some level of trust that allows updates to be made securely: things like code signing, non-static passwords for authentication, and what actions remote processes and users will be able to do to the device. There are plenty of examples of devices that fail due to accepting an update without checking to make sure it was authentic. There are even more examples of fiddling with devices to cause harm, such as insulin pumps or ATM machines, all made possible by not validating the action to the device against a simple AAA process.

Updates: Patches to security vulnerabilities come in two major forms: code changes or configuration changes. Over my career, configuration changes are used to disable vulnerable protocols or as a temporary fix to turn off vulnerable code, while code changes are used to patch vulnerable code or modify a protocol in a way that removes the vulnerability. Both are extremely effective, and both may be required depending on the nature of the vulnerability. This also must align with the support model. Should a manufacturer of an IoT device declare on the packaging that the device will brick itself after a number of years? Support costs must be built into the business model.

Support model: What will the business be expected to do for supporting IoT devices long term? In many cases, we’re looking at another version of SCADA systems, or IP-based remote access added to an industrial system. The two machines have vastly different expected lifespans, just like the difference in how long a smartphone will last versus how long a refrigerator will last. We tend to look at appliances as a decade-long purchase while a phone may last only a few years. How long will support be provided for devices in the field? More importantly, what happens if you end up with a bricked device because of an update gone wrong?

RSA Conference is back in April this month, and no doubt you will see many vendors proposing solutions to this problem. They will likely be focused on discovering, containing, and controlling them in your environment. All of these things are great to ensure you have accurately measured and accounted for the risk associated with these devices, but it does not fix the fundamental issues with IoT described above.

Awareness of and understanding the risk is critical to including these devices in our work places and at home. The goal should be to allow these devices to co-exist (in some form or fashion) to provide the value they can with the smart circuits included in their builds. Companies that properly build lifespans and secure connectivity into their devices could be better partners than those who do not.

For the other practitioners, what is your position on IoT? Friend or foe? Do you have the same posture at home that you do at work? Let’s keep the conversation going! Find me at RSA Conference this year or tweet me your ideas (@Branden Williams).

About the Author

Branden R. Williams, DBA, CISSP, CISM, is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at http://www.brandenwilliams.com/.
Using IoT to Build a Stronger Cybersecurity Community Fabric

By Rhonda Farrell – ISSA Distinguished Fellow, Central Maryland, National Capital (Washington, DC), and Northern Virginia Chapters

For those new to the Internet of Things (IoT) arena, a quick definition is “[a] network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. IoT technologies are ubiquitous, now pothily being called the Internet of Everything (IoE). The spectrum of industry sectors covered includes automotive, consumer products, life sciences and health care, manufacturing, media and entertainment, oil and gas, power and utilities, retail, security and defense, smart cities, technology, travel, and others. According to recent research, the biggest value drivers currently being focused on from an IoT/IoE technology perspective are four-fold (table 1).

To capitalize on this opportunity space, accompanying “fabric” technologies are currently being developed at a fast clip to increase functionality, allowing IoT/IoE devices to better interconnect, analyze, and/or take automated actions across multiple levels of the technology stacks, including at the data, network, services, and cybersecurity layers. From an ISSA International community perspective, this wave of maturation activities is a veritable cybersecurity gold mine requiring ongoing risk, threat and attack analysis, standardization, and continuous technological innovations.

In April 2017, the Interagency International Cybersecurity Standardization Working Group (IICS WG), which was established by the National Security Council’s Cyber Interagency Policy Committee (NSC Cyber IPC), stood up an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. The task force focuses on all three typical aspects of security and privacy, including confidentiality and integrity, but focuses most heavily on availability as the priority for cybersecurity.

The National Institute of Standards and Technology (NIST) then released the NIST Interagency Report (NIST IR) 8200, “The Status of International Cybersecurity Standardization for IoT. NIST IR 8200 compiles a table of potentially relevant existing standards separated into eleven core cybersecurity areas. These areas range from cryptographic techniques and cyber-incident management, through IAM and network security, to supply chain risk management to system security engineering. It becomes the raw material for a gap analysis between existing and necessary standards [5].

If you are an information security thought leader or practitioner who would like to offer expertise, NIST is seeking feedback on NIST IR-8200 and requests information about the state of cybersecurity standardization for IoT by replying to NISTIR-8200@nist.gov by April 18, 2018. Help us build a stronger ISSA community fabric by offering your expertise now!

For those wishing to know more about the above topic, contribute to a more in-depth analysis on the subject, want more information on working with the ISSA International Global SIGs, or to suggest your own topics for future columns, we welcome your feedback and questions at wissig@issa.org or SIGs@issa.org.

### About the Author

Dr. Rhonda Farrell, D.Sc., J.D., CISSP, CSSLP, CCMP, CMQ/OE, CSQE, is a Cybersecurity Change Management Specialist at Booz Allen Hamilton (BAH), a member of the Board of Directors at ISSA International, and an ISSA Distinguished Fellow. She can be reached at rhonda.farrell@issa.org.

---

**Table 1 – IoT/IoE value drivers**

<table>
<thead>
<tr>
<th>VALUE DRIVERS</th>
<th>OPPORTUNITY SPACE</th>
<th>SERVICE OFFERINGS</th>
</tr>
</thead>
</table>
| Supply Networks     | Transform traditional, linear supply chains into connected, intelligent, scalable, and customizable digital supply networks | • Factory and operations  
                      |                                                                                   |   • Planning and inventory  
                      |                                                                                   |   • Supply network and logistics  |
| Customers           | Create seamless customer experiences and enhance customer support and services | • Channel connectivity  
                      |                                                                                   |   • Customer experience  
                      |                                                                                   |   • Post-sales support  |
| Products            | Create opportunities for innovation and efficiency throughout product life cycle | • New business models  
                      |                                                                                   |   • New products and extensions  
                      |                                                                                   |   • Product development  |
| Security and Privacy| Safeguard connected networks and mitigate risks                               | • Infrastructure monitoring and security  
                      |                                                                                   |   • Smart safety and management  |

---

April 2018 | ISSA Journal – 7
Get it Right: Offense Versus Defense

By Mark Anderson – ISSA member, Australia Chapter

The news has been replete with claims of North Korea being behind a range of hacking activities, high-impact theft of IP by other countries, and more recently reporting of possible contemplation by the UK to undertake a cyberstrike on Russia as a response to the Skripal poisonings. In this particular case the ex-director of the UK’s GCHQ, which houses much of the military-grade cyber espionage, security, and warfare capability for the UK, has been reported as suggesting actions other than the use of a direct cyberstrike.

I was asked quite some years ago during a theoretical red-teaming exercise on defense of critical infrastructure to speculate on how the Western Alliance would fare in a cyberwar after my managers had listened to the preening of various officials and “courtiers” as to various latent capabilities. Ever the heretic with a “suicidal” tendency of speaking truth to power, I indicated that we would probably “lose.” The obvious riposte came virulently and at lightning speed with indications that the speculated adversaries had little or no cyber-defensive capability and their offensive capability considered weaker. It was also noted that “the best defense is a good offense,” and this had worked with MAD to avoid nuclear war. Gritting my teeth as the populace and most business activities have listened to the preening of various officials and “courtiers” as to various latent capabilities. Ever the heretic with a “suicidal” tendency of speaking truth to power, I indicated that we would probably “lose.” The obvious riposte came virulently and at lightning speed with indications that the speculated adversaries had little or no cyber-defensive capability and their offensive capability considered weaker. It was also noted that “the best defense is a good offense,” and this had worked with MAD to avoid nuclear war. Gritting my teeth as the only person in the room with an actual qualification in IT let alone cybersecurity, I then indicated that you could have a massive offensive capability, but if defensive capability was low then unless the adversary was matched with a closely symmetric potential level of loss, the implied assumption of the MAD doctrine was not valid. In the case of cyber, you had better be absolutely sure your adversary has as much identically, if not more, to lose as you, and that they actually, in a rational manner, understand that. This is one reason why a cyberstrike against North Korea, as a speculative example, may not yield hoped for results; there simply is not that much to affect along with a per capita less impact. If you have the most to lose in a cyberwar, your defensive capability had better be very, very good with comprehensive coverage and coupled with a concomitant investment ratio when considering offensive versus defensive. Some reporting speculates that in the case of the intelligence agencies that have an iron grip on the control of national cyber capability is that it could possibly be 80 percent for espionage/offensive purposes, and 20 percent defensive. If this is true, or even half true, then something is very wrong.

I don’t know if the ex-GCHQ director is counseling against a cyberstrike on Russia due to knowledge that the UK capability available may not be as precise, reliable, and repeatable as one would like, or whether he has deduced from his reported previous public statements that securing the broader, non-national security cyber infrastructure, which truly powers the UK economy, is severely lacking. But I tend to agree with his reported attempt to shift the conversation to one of economic impacts via what is probably seen as more traditional means.

Whatever is decided or pre-empted by circumstance, the UK and its allies had better be able to put on a reliable, repeatable defense across the entire cyber sphere that includes more than just core government networks and the absolute largest of our critical infrastructure, which make our bureaucrats feel comfortable while leaving the majority of the populace and most business activity “out in the cold.” As indicated above, GCHQ has been reported as stating that it cannot protect the broader cyber infrastructure despite the incredibly large investment it and its counterparts in other Western nations have received in developing cyber capabilities and has pretty much said the masses—that pay for the GCHQ cyber capability based on the original, or at the very least heavily implied promises, it would deliver broad-scale protection with high-end capability—are on their own.

Unfortunately, unlike issues involving nuclear weapons, we have not yet fully come to grips with just how much real and societal damage can be wrought with a truly genuine serious attempt at national-scale-level cyber disruption. Maybe the strategists have decided that the matter will go kinetic before that level is reached and thus “all bets are off.” But I prefer not to have to find out since the West in this regard may possibly still have more to lose per capita compared to the usual suspects; although as they continue to develop their cyber infrastructure to parity or beyond, then their vulnerability to similar negative impact also increases and maybe MAD, as long as the actors are rational, becomes a valid doctrine for strategic consideration by our policymakers. Otherwise some really big investment in defensive capability compared to offensive and where the defensive capability is easily obtainable by law abiding netizens needs to take place.

About the Author

Gray Hat is an ACM Distinguished Engineer and principal inventor for several patented devices and major systems that have entered operational service with the US Armed Forces, as well as other national governments, for high-grade information security purposes. He can be contacted at msanderson@ieee.org.
When people use their work email addresses to register for external websites, it causes a security risk because so many people reuse the same password for all their accounts. When an external account is breached and the password is disclosed, it means that our internal systems could be at risk as well as other external services the user has registered for. “Credential stuffing” is when attackers re-use username and password combinations in bulk on popular online resources to exploit password reuse.

Ideally, websites would always tell us if our password had been compromised, but this isn’t always the case. Keeping up with which of our online services has been compromised and which passwords need to be changed can be a challenge given the sheer number of security breaches. Fortunately for us, Troy Hunt has created an online service called “Have I Been Pwned?” that can advise if anyone on your organization’s email domain has been associated with a security breach. It will show you which breach it is associated with so that you can take action to change passwords if needed. “Have I Been Pwned?” is a fantastic security awareness tool to help people understand the risks of password reuse. It’s also worth encouraging users to register their personal email addresses. Best of all, it’s free!

Unfortunately, in my experience legal teams can be neophobic and object to registering organizational domains with this service, especially for organizations subject to EU privacy law. Here are some common legal objections and some suggestions on how you can deal with them:

- **This is stolen content and it’s wrong for us to subscribe to a service that indexes stolen data.** It’s useful to make a physical comparison here. Imagine that someone illegally leaked stolen data from a supplier that showed that the fire protections in your organization’s head office were ineffective. Would you really say that you couldn’t act on it and the right thing to do was to remain at risk? Once you know that someone is at risk, regardless of the source, you have to act. It would be unethical to do anything else.

- **We need people’s permission to process their personal data.** This stems from a work email address being considered personal data. While it’s ideal to get people’s permission for any kind of monitoring at work, it’s not strictly required. By all means let people know that you’re using the service, but don’t wait for permission. Principle seven of the Data Protection Principles requires us to use “appropriate” security controls to protect people’s personal data. Given that password re-use is endemic, we can’t ignore the relevance of external breaches to our own authentication systems. This is a case where the processing of personal data is clearly in the interests of the data subjects since there’s a good chance they use the same password (or variations) for their personal accounts at home.

- **How do we justify doing this?** How can we justify not doing it? See above about the data subject’s best interests.

- **How can we trust “Troy Hunt”?** How can we trust anyone? On the Internet we can’t tell the difference between a dog and organized crime. Troy has made every effort to be transparent about the service he runs, but the real point is about the impact of false positives and false negatives. In the case of a false negative you’re no worse than where you started. For false positives, changing a password when you didn’t need to is a minimal overhead. The prize here is the chance to take action to change passwords and protect accounts before criminals can exploit them.

- **What if it shows that users have been using their work emails for registering with embarrassing services such as AshleyMadison.com?** Nobody in legal wants to be the one who approved a process that could result in huge embarrassment, potentially for senior executives. However, the breach has already happened. Not taking action invites further harm and also increases the chance of blackmail.

“Have I Been Pwned?” is rapidly passing a cultural tipping point in security best practice. Breached sites are turning to “Have I Been Pwned?” to help notify their users, and even government departments are registering their email domains to better protect their users. If you haven’t already registered your company’s email domain, then you need to book a meeting with your legal team.

**About the Author**

Geordie Stewart, MSc, CISSP, is the Principle Security Consultant at Risk Intelligence and is a regular speaker and writer on the topic of security awareness. His blog is available at [www.risk-intelligence.co.uk/blog](http://www.risk-intelligence.co.uk/blog), and he may be reached at geordie@risk-intelligence.co.uk.
The End of Security

By Mike McCormick – ISSA member, Minnesota Chapter

“The battle is over. We lost.”

This gloomy proclamation was made by a world-famous security expert at a professional association chapter meeting. (You know who are, Bruce.) It was before Equifax, DNC, Sony, Yahoo, Target, and other recent mega-breaches. Yet even then, attackers were making rapid gains, while defenders seemed to fall further behind.

The trend became known as “Shamir’s Law” in 2007, when renowned cryptographer Adi Shamir suggested it at a security conference. Modeled on Moore’s Law, which posits that computing power doubles every 18 months, Shamir’s Law states: “Every 18 months, computer security gets 50 percent worse.”

Especially after Equifax, it’s starting to look like Shamir was right, in which case winning the battle might seem hopeless.

Decades of data support Moore’s Law. Integrated circuit transistor density has more or less doubled to double every 18 months as Moore predicted in 1965.

Data for Shamir’s Law is harder to come by in a world where companies and governments can downplay or hide security breaches from the general public. This is compounded by disagreement about how to measure security. Many metrics have been proposed, few are widely adopted, even fewer publicly quantified.

Cyber-breach cost is a rare metric for which verifiable historical data is available. The Ponemon Institute has measured this for years. Their most recent study showed breach cost increased steadily for at least the past five years (27 percent in 2017).

While they may be correlated, rising breach cost isn’t the same thing as worsening security. The cost of breaches can rise even in an improving security environment, due to other factors such as insurance rate hikes or regulator penalties. The Ponemon data varies by country and industry, a strong indicator other factors besides security influence breach costs. The nature of the attacks themselves even influences their cost. For example, a recent uptick in ransomware put an added financial burden on victims.

Another metric is to simply count publicly disclosed incidents, without considering cost. A recent Online Trust Alliance report tells us 2017 continued a long trend of being “worst year ever” with 159,700 total cyber incidents. The number of records compromised increased fourfold over 2016, a surge driven by trends in ransomware and IoT, plus the colossal Equifax breach.

Rising incidents aren’t quite the same thing as worsening security either, due to factors such as victims’ willingness to disclose incidents. US companies have new disclosure incentives due to a new SEC ruling and a renewed push in Congress for national breach disclosure laws. So while more incidents are shared with the public, the total number of security incidents remains hard to extrapolate.

Although available data doesn’t prove Shamir’s Law, it is at least consistent with it, and supports the view that security has continuously worsened significantly year over year for a long time. Better agreement on how to measure security—and more data—are certainly needed.

Shamir’s Law has an ominous corollary. If security does weaken 50 percent every 18 months, then it could reach a point of no return. A singularity. The end of security.

Suppose Shamir was right back in February 2007. Then by August 2008, 18 months later, security was only 50 percent as good. By February 2010, it was 25 percent. Then 13 percent in August 2011, six percent in February 2013, three percent in August 2014, two percent in February 2016. Next August we can expect it to fall below one percent. Beyond 2018, diminishing returns, a future dystopia where any effective security costs more than no security at all.

Shamir’s Singularity is like Zeno’s arrow; we may never quite reach it. But once security falls below one percent of where it was a decade ago, it seems unlikely we could reverse the trend.

Defenses may actually be improving. Shamir’s Law implies attacks improve faster than controls, the gap doubling every 18 months. We can bend the slope of either line to postpone the singularity.

With a steady stream of bad news, it’s natural to feel discouraged. But if defenders grow disheartened enough to give up the fight, Shamir’s Singularity becomes self-fulfilling prophesy. Let’s not fall into that trap. For every Equifax disaster, there are a thousand unsung victories. Let’s focus on those.

Maybe we “lost the battle,” but the war isn’t over yet. Now is not the time to give up. It’s time to bend the curve, just a little, and then a little more. We do this the same way we always have, by improving defenses, educating business and users, studying attackers, and keeping faith in our mission.

About the Author

Michael McCormick is an information security consultant, researcher, and founder of Taproot Security (www.taprootsecurity.com). He can be reached at mike@taprootsecurity.com.
Now That’s Computing Power

By Luther Martin – ISSA member, Silicon Valley Chapter

It was recently discovered that more than one business were surreptitiously using computing power of visitors to their web sites to mine bitcoins. Maybe they did this as an alternative way of paying for their costs instead of using advertising. Maybe they did this for other reasons. But this should not be too surprising. The cost of electric power is the single biggest cost in solving hard cryptographic problems these days, and that is true whether you are trying to crack a key or just to mine bitcoins. And that means that there is a strong incentive to get someone else to pay for that power. But exactly how much power does it take to do cryptographic calculations?

Back in 2012, at DARPA’s “The Impending End of RSA” workshop, Dan Bernstein gave a talk in which he described how much electric power it would take to crack various RSA keys. He assumed that an attacker would spend a fairly modest amount on hardware, say just a few million dollars or so, and would then use that hardware to crack a key, with the goal being to crack a key within one year.

Dan claimed (but I have never checked his calculations) that for a 1,024-bit RSA key, it would take about one year of computing power of a couple of young programmers at Silicon Valley start-ups. Or it is roughly enough energy to crack two RSA-1,024 keys. Or it is about 16 megatons of energy, or more energy than several Cold War era strategic nuclear weapons.

Those are unwieldy numbers to deal with. Fortunately, there is a handy yardstick to use for measuring energies that are roughly that big, and that is the megaton (MT).

The very first nuclear explosion, the Trinity test, had a yield of about 20 kilotons (KT), or 0.02 MT. The W87 warhead, which the American Peacekeeper missile carried 10 of, had a yield of about 300 KT, or 0.3 MT. The American B83, another typical Cold War strategic nuclear weapon, had a yield of about 1.2 megatons. The biggest nuclear bomb ever, the USSR’s Tsar Bomba device, had a yield of about 50 MT.

By comparison, the crack of RSA-1,024 that Dan proposed would use about 7.5 megatons of energy, or more energy than several Cold War era strategic nuclear weapons.

That is a lot of energy. Is the amount of energy needed to mine bitcoins more than that or less than that? It looks like bitcoin miners currently spend about 18 terawatt-hours of energy, or about 65 petajoules, per year mining bitcoins. That is roughly the energy from two power plants. Or it is roughly enough energy to crack two RSA-1,024 keys. Or it is about 16 megatons of energy. Or it is about the energy released by the nuclear weapons from five Peacekeeper missiles. Or it is about the energy of a couple of young programmers at Silicon Valley start-ups.

No matter how you measure it, that is still a lot of energy.

By comparison, the crack of RSA-1,024 that Dan proposed would use about 7.5 megatons of energy, or more energy than several Cold War era strategic nuclear weapons.

By comparison, the crack of RSA-1,024 that Dan proposed would use about 7.5 megatons of energy, or more energy than several Cold War era strategic nuclear weapons.

The very first nuclear explosion, the Trinity test, had a yield of about 20 kilotons (KT), or 0.02 MT. The W87 warhead, which the American Peacekeeper missile carried 10 of, had a yield of about 300 KT, or 0.3 MT. The American B83, another typical Cold War strategic nuclear weapon, had a yield of about 1.2 megatons. The biggest nuclear bomb ever, the USSR’s Tsar Bomba device, had a yield of about 50 MT.

By comparison, the crack of RSA-1,024 that Dan proposed would use about 7.5 megatons of energy, or more energy than several Cold War era strategic nuclear weapons.

That is a lot of energy. Is the amount of energy needed to mine bitcoins more than that or less than that? It looks like bitcoin miners currently spend about 18 terawatt-hours of energy, or about 65 petajoules, per year mining bitcoins. That is roughly the energy from two power plants. Or it is roughly enough energy to crack two RSA-1,024 keys. Or it is about 16 megatons of energy. Or it is about the energy released by the nuclear weapons from five Peacekeeper missiles. Or it is about the energy of a couple of young programmers at Silicon Valley start-ups.

No matter how you measure it, that is still a lot of energy.

About the author

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com. If you are a fan of classic interactive fiction games, you can also reach him at xyzzy@microfocus.com.
What Would a Regulated-IoT World Look Like?

Security often takes a back seat in the rush to get new Internet of Things devices into the hands of consumers as quickly as possible. Although regulators try to keep pace, they tend to be reactive rather than proactive. It’s time to shift our thinking. Instead of waiting for a scandal or crisis to take place before implementing change, wouldn’t it be nice if security was part of the IoT product development process?

What You Need to Know about the New NIST Report on IoT

There is a growing recognition that we need universal standards in place to improve IoT cybersecurity and to increase data privacy protection. As a result, in February the US National Institute of Standards and Technology (NIST) released a report that covers guidelines for what has to happen next in the development of the Internet of Things.

Gartner Expects 2018 IoT Security Spending to Reach $1.5 Billion

As the IoT enterprise attack surface continues to increase, it is not surprising that organizations are earmarking more of their resources for IoT security. Analysts are predicting a 28 percent increase in spending this year to help combat the rising number of threats.

“Utterly Horrifying”: Ex-Facebook Insider Says Covert Data Harvesting Was Routine

At the moment, it’s not easy being Facebook. Former platforms operations manager Sandy Parakilas has gone public with numerous concerns he had during his time with organization. He said he warned senior executives at the company that its lax approach to data protection risked a major breach. Furthermore, he said that the company did not use its enforcement mechanisms, including audits of external developers, to ensure data was not being misused.

How Facebook Made It Impossible to Delete Facebook

Thanks to the recent disclosures involving data breaches and privacy issues, many are tempted to call it quits with the social media giant. However, when it comes to actually disconnecting, quite a few people are finding that it’s not that easy to leave a network that has spent more than a decade integrating and embedding itself into our day-to-day experiences.

Good Luck Saying “Sorry I’m Late, I Had to Update My Car’s Firmware”

Consider this: If IoT devices, by design, will not function without updating, this raises collateral questions of connectivity interruption. Will IoT devices ultimately yield an entirely new service sector providing updates? Will these be offloaded/outsourced (oh, I mean “centralized”) to a provider? Won’t that provider then be a low-hanging security target that will need to offer robust security and authentication management? And who will resource the provision of tech support for update issues? This is why the Internet Engineering Task Force (IETF) wants to make IoT firmware updates fast and easy.

Top Robotics Expert on Uber Crash Questions Whether Sensors Worked

In addition to cybersecurity, we must be confident that connected cars are actually ready to perform the tasks they are required to do. Experts suggest that a technological failure was responsible for the fatal self-driving car incident in Arizona. Once again, are we moving too quickly in order to bring a product to market?

The Success of Your IoT Initiative Will Depend on Your Data Proficiency

Industry 4.0, otherwise known as the fourth industrial revolution, is a new way to think about data across processes. As you move through the stages of digital transformation, it is important to remember that in the connected world, IoT solutions are ultimately all about data.

Network Security in the Age of the Internet of Things

Can you see everything on your network? If not, you may have a problem. As the number of IoT devices continue to increase, they create opportunities for cybercriminals who are looking for vulnerabilities to exploit. What is the Golden Rule? Carefully monitor your networks and don’t neglect your IoT devices.

IoT Cybersecurity, “Cascading” Failures, Worry Consumers Most about Connected Home

These days, we find ourselves becoming more and more dependent on devices that make our lives easier. Therefore, you can probably guess what piece of technology most adults in the United States say they can’t live without for more than one day — their Wi-Fi router.
Pre-Professional Virtual Meet-Ups

So, you think you want to work in cybersecurity? Not sure which way to go? Not sure if you’re doing all you need to do to be successful? Check out Pre-Professional Virtual Meet-Ups to help guide you through the maze of cybersecurity.

More than 20+ archived meet-ups!

ISSA.org => Learn => Web Events => CSCL Meet-Ups

ISSA EVENTS
Special ISSA Meeting Webinar
Hosted by ISSA President Keyaan Williams
April 12, 2018 • 12:00 pm EST

To the valued members of the ISSA community, ISSA International President Keyaan Williams has made a commitment to providing more updates to our membership. With that in mind, Mr. Williams will be hosting a special meeting webinar in order to provide an update to ISSA membership on April 12, 2018, at 12:00 pm EST. ISSA members will be able to access this special meeting webinar live via the ISSA BrightTalk channel (sign up to BrightTalk is required), and it will be made available on-demand for those members who will not be able to attend the live event.

We will continue to provide periodic updates throughout the year to keep our members informed of all things ISSA.

2 https://www.brighttalk.com/join?redirect=/

ISSA CISO FORUM
ISSA CISO Executive Forum
San Francisco, CA • April 14 - 15, 2018

Join us to share ideas, learn from informative presentations, and collaborate with your peers. Membership is invitation only, subject to approval.

Topics range from emerging technologies and innovation to redefining security and cyber resilience in today’s Internet of Everything world. These will include break-through projects such as trusted infrastructures, smart algorithms including machine learning and artificial intelligence, data analytics, the Internet of Things, blockchain, smart cities, data-center-on-a-chip, cloud computing, certification frameworks, distributed key management systems (cryptographic), security-as-a-service, and methods for optimizing security and standards in highly regulated markets.

REGISTER: ISSA.org => Learn => CISO Executive Forum

ISSA EDUCATION FOUNDATION
News from the Foundation

The ISSA Education Foundation (ISSAEF) is delighted to announce the receipt of a generous donation from SC Media (formerly SC Magazine), which will support ISSAEF’s Howard Schmidt Scholarship fund. It’s through such donations that ISSAEF is able to provide tuition, books, or other school-related material to assist our future cybersecurity professionals in their education!

The Foundation is pleased to announce that the application period for Foundation scholarships for 2018 will run April 2 through May 31, 2018. Materials will be posted on the website to enable applicants to submit their applications.

JOIN US AT THE SUMMIT. We’ll be at the ISSA Los Angeles 10th Annual Information Security Summit, May 2-4, 2018, at the Universal City Hilton. There will be two full days of top-level, discounted training classes on May 2-3, followed by three forums on May 4th, including Women in Security. Information and registration may be found at https://summit.issala.org/.

Richard Greenberg, LA Chapter president, said “Investing in ISSAEF is investing in our future. We must support and educate the next generation to help protect our country and our companies. Would you please join me in supporting the ISSAEF?” Come network, learn from leaders, and visit us at our booth!

AND HERE’S A PAINLESS WAY to automatically support the Foundation every time you shop on Amazon at absolutely NO COST to you. Simply go to AmazonSmile, select “ISSA Education and Research Foundation, Inc.” as your charity. When you shop, 0.5 percent of all your eligible AmazonSmile purchases will be donated to our scholarship fund! More information can be found on their website. Happy shopping!

SEEKING VOLUNTEERS to participate in fundraising and governance of the Foundation. Those interested in joining a truly dedicated and enthusiastic group, please contact Steve Haydostian at steve.haydostian@nbcuni.com or 818-777-8171.

Visit us at www.issaef.org. Like us on Facebook and LinkedIn.

ISSA International Series
Mobile Security
Live Event: April 24, 2018
9 a.m. US-Pacific / 12 p.m. US-Eastern / 5 p.m. London

INFORMATION & TO REGISTER
ISSA.org => Events => Web Conferences
Securing Complex Cyber-Physical Medical Device Landscapes

By Ulrich Lang

The author presents innovative approaches to cybersecurity that should be considered to securely integrate medical device landscapes (and many other IoT environments) in the coming years as IoT rapidly matures.

Abstract

In this article we will present innovative approaches to cybersecurity that should be considered to securely integrate medical device landscapes (and many other IoT environments) in the coming years as IoT rapidly matures. The article is based on the results of several government-funded R&D projects, in particular a research project to secure a cyber-physical medical environment (for Defense Health Program, DHP), and a research project to automate access control policy testing (for National Institute of Standards and Technology, NIST).

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity that enables these objects to connect and exchange data [1]. The IoT is going to be transformational—significantly impacting most industries and parts of society. Experts estimate that the IoT will rapidly grow to 30 billion objects within just two more years [2] (for comparison, in 2015 there were approximately 4.9 million things connected to the Internet).

Importantly, IoT will also play a major role in achieving “smart health care” to improve patient care/experience, efficiency, and outcomes. Hospitals already use many medical devices today (e.g., numerous monitoring and pump devices, etc.) though mostly not in a very interconnected fashion. Presently, in most cases, there is a human (e.g., nurse) in the loop to ensure safety because the devices in use have not been designed with the security in mind that is required for autonomous operation (e.g., monitoring). According to the latest research, US Department of Health plans to (eventually) save up to USD 300 billion from the national budget due to medical innovations [3].

Such future medical device landscapes pose many cybersecurity and privacy challenges because most of these are “cyber-physical” systems where cybersecurity breaches (and other failures) could directly impact the physical safety of patients.

Today, medical IoT is not fully matured yet, leading to a disconnect: Health IT is increasingly interconnected, while
information security is not keeping up. This limits “smart health care” improvements and health IoT in general. In this emerging environment, hospitals need to prioritize patient safety first, which means medical devices are often not integrated; since humans are usually in the loop, there isn’t much need for automation. This leads to inefficiencies, and patient care/experience is not as good as it could be. Yet, having humans in the loop actually creates its own risks.

In this article we will present innovative approaches to cybersecurity that should be considered to securely integrate medical device landscapes (and many other IoT environments) in the coming years as IoT rapidly matures. The article is based on the results of several government-funded R&D projects, in particular a research project to secure a cyber-physical medical environment (for the Defense Health Program) and a research project to automate access control policy testing (for the National Institute of Standards and Technology).

The presented approach comprises several parts:

1. **Integrated clinical environment**: OpenICE is an initiative to create a community implementation of an integrated clinical environment (ICE). The initiative encompasses not only software implementation but also an architecture for a wider clinical ecosystem to enable new avenues of clinical research. The OpenICE project is run by MD PnP. Our research uses the OpenICE reference implementation and DocBox’s implementation as an ICE layer.

2. **Secure device communications**: The Data-Distribution Service (DDS) provides secure publish-subscribe communications for real-time and embedded systems. DDS introduces a virtual global data space where applications can share information by simply reading and writing data-objects addressed by means of an application-defined name (topic) and a key. DDS features fine and extensive control of QoS parameters. Our research uses RTI DDS Connext, a leading DDS implementation provided by Real-Time Innovations (RTI), Inc. OpenICE uses RTI DDS as a communications layer.

3. **Security policy automation** simplifies the management and technical implementation of security policies. It allows security professionals to manage rich security policies consistently in one place and often automatically technically enforce the managed policies across many devices, layers, and technologies. Our research uses ObjectSecurity OpenPMF, which generates technical policy enforcement for DDS, networks, etc., from generic security policies and imported information about users, systems, applications, networks, etc.

**Cyber-physical systems**

NIST defines cyber-physical systems as co-engineered interacting networks of physical and computational components, which will form the foundation for critical infrastructure and emerging/future smart services. Cyber-physical systems will improve quality of life in many areas, such as “smart” cities, transportation, hospitals, and energy. While cyber-physical systems can be used to improve safety (e.g., public safety), they also pose potential cybersecurity risks especially because cybersecurity could impact every patient’s physical health and safety (in non-cyber-physical systems,

---

2. This SBIR (Phase II) was awarded to ObjectSecurity LLC. RTI Inc was a subcontractor in Phase I. More information about the R&D project: [https://objectsecurity.com/nist](https://objectsecurity.com/nist).
employee credentials to gain unauthorized access. Health IT access control simply isn’t capable of providing the security that will be required: access is overprovisioned, too simplistic (identity-based access control (IBAC) and role-based access control (RBAC)), and unmanageable due to being fragmented and siloed. Add the IoT and ransomware attacks such as Mirai (2016) and WannaCry (2017) into the mix (which both affected medical devices) and it becomes even clearer that locking down access at all levels to the “minimum necessary” is sorely needed.

HIPAA fines are rarely administered but are a risk for health providers (fines have gone up to $4.8M for non-compliance after a breach). Furthermore, with improved access control (and other cybersecurity), hospitals could enable “smart business,” resulting in a forecasted $8.5M in annual savings per US hospital (US$36 billion US total) [7].

Identity and access management (IAM) is an important program/initiative for health providers (and most organizations). However, in our experience, hospital IAM systems are often not fully mature (based on hospital IAM road-map projects the author has completed recently).

- IAM systems are distributed (there is a main IAM and numerous sub-IAMs)
- There are custom batch processes to keep information synchronized
- Onboarding/offboarding is done using manual processes with limited checks
- There is almost no work-flow automation
- There is a flat network with little isolation (including cyber-physical)
- There is almost no fine-grained, automated access control (which is partly IAM)

An example of a maturity score by IAM component for a typical hospital is shown in figure 2, clearly showing plenty of room for improvement around access control.

**Figure 1 – Example OpenICE system setup** [5]

Direct/immediate harm is usually directed towards stealing or changing sensitive, valuable information.

**Smart health care: Integrated medical devices should detect and respond automatically**

Smart health care will comprise at least:

- Networked, smart, and semi-autonomous devices
- Clinical, business, and building systems communication
- Real-time analytics, tracking, etc.
- Automation

Healthcare providers care about smart health care because it has the significant potential to measurably improve patient care, a patient’s experience, and health provider efficiency. In conjunction, healthcare providers (especially hospitals) must implement significantly improved cybersecurity to ensure patient safety, security, and privacy when deploying these automated, autonomous IoT environments.

Figure 1 illustrates an example of an “integrated clinical environment” (ICE) based on OpenICE. The ambitious goal of OpenICE is to provide automated, autonomous communications between medical devices in hospitals. In this example, dongle devices (e.g., secured ARM7 platforms) are put in front of the serial connections of conventional medical devices. This is needed because many legacy medical devices that have no security will be used for the foreseeable future. In the example, medical devices (on the left) are connected to the OpenICE system via OpenICE device adapters; the adapters securely relay traffic between the devices and the ICE supervisor. The supervisor provides a “single pane of glass” view of each patient’s health by collecting, monitoring, and analyzing the data from every device in real-time, alerting the nurse when important changes in the patient’s data arise.

**Health IT needs better access control**

HIPAA breach data underscores that a significant proportion of breaches are due to unauthorized access by hospital employees [6]. On top of that, many hacker attacks focus on stealing...
Close-up on access control

Implementing effective access control across hundreds of devices and layers that form an interconnected IoT device landscape is highly complex. Protections are needed in many places and in many differing, overlapping, technical configurations. For the example clinical ICE environment presented in figure 1, consistent access policies would need to be authored and maintained to dynamically control information flows between the OpenICE device adapters, OpenICE supervisor systems, the enterprise infrastructure, electronic medical record (EMR) systems, identity and access management systems, etc.

Attribute-based access control (ABAC) has been around for a while as part of the solution to implement more granular and fine-grained access policies. According to some industry analysts, ABAC will be used increasingly to protect critical assets in coming years. While ABAC can be quite powerful if implemented correctly, it is also often far too hard to manage/author, implement, integrate, and audit (described more below). Adoption challenges are not only technical, but also psychological. ABAC still collides with the reactive cybersecurity “group think” that revolves around monitoring, coarse-grained blacklisting and RBAC.

The principles behind ABAC are simple: access is expressed as more or less Boolean rules that can draw on various information sources to determine an access decision. Figure 3 illustrates the shift (or rather extension) from RBAC to ABAC (note that the example is for illustrative purposes only, but will not fit to current business processes of most hospitals):

```
RBAC  ABAC

"Nurses can only access medical records of patients + ...whose current treating physician is the same physician who the nurse is currently assigned to assist, and only if the nurse is currently badged into the same physical building as the one the patient is"
```

Figure 3 – From RBAC to RBAC example

While such policies appear intuitive, the “plumbing” under the hood can be highly complex to manage these dynamic information sources for attribute values (i.e., the values need to be fetched at decision-making time by the ABAC system for the blue parts in the example policy in figure 3), which are then compared to the values in the policy by a “policy decision point” to determine an access decision.

Furthermore, it is usually hard to implement “defense in depth” using ABAC—there are too many different technical configurations across too many different devices and different layers. For example, how would you configure your firewalls from an ABAC rule like in the example above. Add to that the fact that IT landscapes (and users) will change over time, it is clear that ABAC could become an administrative nightmare if applied pervasively across many devices and layers. It is therefore often only used to add some granularity to user access (making up a small part of the overall access control challenges faced).

A close-up on security policy automation

Security policy automation is an approach to simplify the management and technical implementation of richer, more dynamic access policies. Depending on the tools used, it allows security professionals to manage rich security policies consistently in one place, using an intuitive, generic policy representation. Security policy automation is a policy management umbrella that helps define, manage, and enforce consistent policy management of rich policies (including access policies) across many devices, layers, and technologies and (often automatically) technically enforce the managed policies.

Some security policy automation tools additionally simplify policy management even in the face of dynamic changes. This is achieved by automatically detecting, importing, and analyzing information about the users, systems, applications, networks, etc. The imported information is used to fill in the concrete details about the generic policy authored by the security professional.

The most comprehensive policy automation round-trip includes all these features, as shown in figure 4 (overlaid on the medical IoT landscape in figure 3):

```
1) Import, Analyze, Visualize
2) Author Intuitive Policies
3) Generate & Enforce
```

Figure 4 – Run-time security policy automation round trip

We have concretely implemented policy automation for an OpenICE medical device landscape as part of a government-funded R&D subcontract. The scenario included infusion pump devices, patient monitoring devices, and ICE managers. Device communications in OpenICE are handled by a real-time, secure data bus built using the Data Distribution Service (OMG DDS): a publish/subscribe middleware platform provided by the prime contractor, Real-Time Innovations. For our demo scenario, we decided to define security based on device attributes (identity, IP/MAC, DDS topics, etc.) rather than on user attributes (e.g., identity) because OpenICE already groups devices by patient, and simulating a full hospital work flow was beyond the scope of the demo test bed.

The policy automation solution included three main steps:

1) Import, Analyze, Visualize
2) Author Intuitive Policies
3) Enforce Policies

To simplify the process for users, the security policy automation system includes a work-flow automation feature and provides prebuilt policy automation work flows, leading the user seamlessly through the different policy automation steps. Users can also specify their own work flows as needed.

1) Import, analyze, visualize

- Imported network traffic logs provide information about the actual traffic flowing across the system.
- Information about DDS participants and publish/subscribe topics is automatically detected and captured by a DDS discovery tool. It provides information about which traffic is important (payload traffic vs. discovery “chatter,” for example), and who is talking to whom.
- The policy automation system automatically configures the “building blocks” for policies based on the importers and exporters available. For example, “the requestor’s IP address” is only available during policy authoring if IP addresses are imported or policies based on IP addresses will be enforced.
- Device types are automatically detected based on various indicators, including matching the device type profile in terms of traffic patterns and other factors. This allows the security policy automation system to automatically create a model of the devices that are on the network and what their interactions are.
- This model is visualized in 2D, 3D, and VR to give users visibility into medical device activities.
- Subsets of the datasets of the functional system model can be selected and analyzed, for example, kinds of traffic that should be whitelisted later.

2) Author intuitive policies

Thanks to the work flow automation feature, default generic policy templates are automatically loaded for the particular use-case scenarios (in our case hospital medical device landscapes). These templates include generic rules that apply to most hospitals. These generic policies use wildcards, mappers between building blocks, inheritance/aliases, etc. (e.g., a “patient monitor is allowed to send dosage data to infusion pumps”). Mappers, inheritance/aliases and wildcards can be used together with datasets in the functional system model to automatically generate detailed, technically enforceable policies from the authored policies.

In our demo test bed, some of the template rules are quite simple, for example, a wildcard rule that whitelists all detected user traffic (as opposed to middleware/network “chatter”). To modify the policy (if needed), several policy editors can be used interchangeably, including a graphical editor and a natural language text editor.

The policy automation system then automatically calculates the “low-level” technical policy model from the authored generic policy, the templates, the datasets, etc. This model is later used to generate concrete technical rules and configurations.

A formal verification tool can automatically verify that a generated policy meets specified invariants [8]. In addition, documentation is produced, including natural language text documents of the policy, and a compliance report that details how a policy was exactly generated from the various inputs.

3) Enforce policies (through software agents and native)

Finally, the policy automation system generates the actual technical enforcement. In our solution, enforcement can be via local software agents that intercept information flows, or by exporting “native” security configurations for existing security products and features.

For our OpenICE solution, we did both. First, we automatically generated policy configurations for security policy automation software agents, both for DDS (tied into DDS’ security system via its access control plugin interface), and for the network (using our NetPEP), which interfaces directly with iptables, tcpdump, and syslog on the protected system.

Secondly, we also automatically generated textual configurations of various existing features to underscore the point that effective enforcement on multiple layers and devices is also feasible without the need to install a local software agent on each system. We generated OMG DDS-conformant security permission.xml and governance.xml files to lock down the middleware layer and iptables/arptables (Linux) and advanced firewall (Windows) configuration scripts to lock down the network layer. Those scripts and configurations needed to be pushed to each system manually (using a script).

We also demonstrated these features (for the abovementioned NIST SBIR) on our 20-node Raspberry Pi R&D cluster with individual touchscreens.²

Example in action

The following illustrates an example flow through the described approach from the perspective of the security professional tasked to implement technical security for the interconnected device environment.

First, users can optionally use work flow automation to guide them through the necessary security policy automation steps.

The Experience-Sharing Platform for IT Leaders

Wisegate helps IT leaders achieve more – by thinking together

Benefit from online discussions, live peer calls, peer-tested work product

Get trusted, firsthand insights directly from your peers

Stay connected between conferences and meetings

Request an invitation today
WWW.WISEGATEIT.COM
The Dangers in Perpetuating a Culture of Risk Acceptance

By Matt Wilgus – ISSA member, Raleigh Chapter

This article details the prevalence of risk acceptance within organizations, why IT security departments may be putting too much confidence in their controls, and how excessive risk acceptance is often cultural.

Abstract

Risk management is a basic and fundamental principle in information security. Techniques related to handling risks typically include avoidance, transference, mitigation, or acceptance, with many information security risks being addressed by the latter two. Given the frequency and types of attacks organizations are handling, are security practitioners accepting too much risk to in order to simply meet a compliance requirement or avoid a failing report? This article details the prevalence of risk acceptance within organizations, why IT security departments may be putting too much confidence in their controls, and how excessive risk acceptance is often cultural.

Risk management is a part of many industries. The entire insurance industry is built on risk management; however, there are many relevant examples in other verticals, such as the following:

- **Technology** – What is the possibility a natural disaster results in a shortage of a critical component within a supply chain?
- **Banking** – What is the probability too many lenders default on a mortgage?
- **Automotive** – What is the acceptable testing parameters for safety parts?

In each of the examples, companies have to accept a certain amount of risk. However, by accepting too much risk the company may be in jeopardy of staying in business. In 2011, floods in Thailand affected many technology companies who required a steady supply of hard drives. Many technology manufacturers had multiple suppliers, but many of the primary plants for suppliers were located in one country, Thailand. The result was that primary, secondary, and if they even existed tertiary suppliers all had supply issues. Companies such as Western Digital had a sharp decline in production to end the year, and there was a lot of uncertainty, which could be seen in quarterly filings and comments.1 The shortage affected business operations for many technology companies, but the shortage was not catastrophic to the business. Unfortunately, this isn’t always the case, as can be seen in the second and third examples. In 2009 and 2010, nearly 300 banks failed.2 The cause was generally due to excessive risk taking and non-performing loans during the 2008 financial crisis. Finally, in the automotive example, Takata, until recently one of the world’s largest automotive safety suppliers, filed for bankruptcy after their airbags were found to have caused deaths and injuries. The root cause of the problem was degradation of a key chemical used in their airbag inflators when it was subject to certain environmental conditions and time.3 It was Takata’s responsibility to test their product and ensure it met the required safety standards in a variety

of conditions for an extended time frame, a risk potentially overlooked, or possibly accepted, when the company decided to use certain products as a propellant.

**Information security risk frameworks and tools**

The three examples provided are different than what information security teams address, but the approach to understanding and handling the risk is similar. When addressing a risk within information security, the equivalent question may simply boil down to what is the probability of a breach? Mature organizations may go further and consider what is the likely cost of a breach. However, while vendors and organizations such as the Ponemon Institute publish annual studies on the cost of a breach, very rarely is this cost quantified by an individual organization.

**Frameworks and assigning controls**

Organizations must assess and handle risk on a daily basis. There are many risk frameworks and formulas available to assist companies in quantifying and qualifying risk. Some of the most commonly cited include:

- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation from the Carnegie Melon University (CMU) Software Engineering Institute (SEI)
- COBIT - Control Objectives for Information and Related Technologies from the Information Systems Audit and Control Association (ISACA)

To better understand the various risks a company faces, categories of risk can be used such as financial risk (e.g., loss of revenue) and reputational risk (e.g., brand image in the media). Additionally, there are controls that can be applied to address the risk. Organizations can use high-level categories such as preventative, detective, and corrective controls or get more granular with something like the Center for Internet Security (CIS) Top 20 Controls. Finally, it is commonly said that controls can be implemented with people, processes, and technologies.

**Lack of implementation**

Much of the content in the aforementioned frameworks and approaches has been around for many years. COBIT celebrated a 20-year anniversary in 2016; NIST 800-30 was originally published in 2002; and some practitioners (or CISSP candidates) may recall the Department of Defense (DoD) Rainbow Series dating back to the mid 1980s. The content in these frameworks is still very relevant today, particularly since some of them are continually updated. However, many organizations only pay lip service to the frameworks through reference in policy, while the detailed components and best practices behind them are barely used. This practice alone

---

**NOTE**: choose ePub for Android & iOS; Mobi for Kindles

---

**The ISSA Journal on the Go!**

Have you explored the versions for phones and tablets?

Go to the Journal home page and choose “ePub” or “Mobi.”

**Mobile Device ePubs**

- ePubs are scalable to any size device: iPad/tablet provide an excellent user experience
- You’ll need an ePub reader such as iBooks for iOS devices

**NOTE**: choose ePub for Android & iOS; Mobi for Kindles

Take them with you and read anywhere, anytime…
indicates a lack of a true commitment to risk management within an organization.

The cost of not implementing controls

Organizations have limited resources, in particular time and money, and firms need to use them wisely. While reports from Gartner and others research firms forecast increased yearly security spending, within an organization security enhancements may fall behind other initiatives, especially when the improvement requires time from a development team. For example, a feature request from a large client may take higher priority than a security improvement to a web service used by a subset of clients.

To take the software development example a step further, one only needs to look at the cost of software defect. It is well-known that the cost of a software bug is dramatically less if it is found early in the development life cycle, such as in the requirements gathering or initial design phases, as compared to identifying the issue in production. Security improvements, when possible, should be fixed early in the life cycle as well. The longer they exist, the higher the cost will likely be to fix them later.

There is also a hidden cost of not prioritizing security improvements: if they are not addressed today, they may never get implemented. This may also lead to a long-term tendency to downplay other security enhancements.

Having a culture of risk acceptance

There are organizations that have great defense-in-depth strategies, have the latest security technologies in place, or possess the some of the smartest minds in information security. However, many organizations do not have the resources to have all three and even if they do there are going to be some risks that have to be accepted. Risk acceptance is needed in practice, as organizations can neither afford, nor should, be spending their limited resources on trivial risks. Additionally, many of the most prevalent compliance frameworks take into consideration compensating controls and mitigating factors when assessing risk.

There is a tendency to being comfortable accepting small amounts of risk and then, over time, becoming more comfortable accepting larger amounts of risk, often on the basis that other risk acceptance practices caused no harm. More importantly, meeting minimum compliance requirements often gives organizations a false sense of security that they can accept risks that fall outside those requirements.

What types of risks are accepted?

This is a broad question, but it goes towards what is discussed below related to rationalizations and responses to identified risks. Examples that organizations may deal with include:

- Unpatched systems
- Systems configured with less than ideal security parameters
- Application vulnerabilities
- Lack of end-to-end encryption
- Human/social engineering threats

The following sections address common rationalizations and arguments for accepting risks.

On compensating controls – How attackers bypass single controls

When an information security risk is identified and cannot be easily corrected or mitigated, there is a propensity to want to reduce the risk through compensating controls. There is nothing wrong with this approach, and when a set of controls is properly implemented, there is often a valid reason to do so. However, reducing the risk of a given finding based on the presence of a single control is likely giving too much credence to a particular scenario, as individual controls can be bypassed. Below are ten of the most common controls cited when attempting to reduce risk and a consideration to keep in mind when using them to reduce risk.

1. **Strong or two-factor authentication (2FA)** – Requiring an extra level of authentication beyond username and password is a necessary control to mitigate the potential of weak passwords, brute force attacks, and other attacks against authentication mechanisms. Man-in-the-middle (MitM) attacks can be difficult, but they do occur. NIST issued SP 800-63B, Digital Identity Guidelines, which includes a comprehensive list of threats and security considerations against many commonly used technologies for additional authentication.

2. **Transport layer security (TLS)** – Encryption in transit is a necessary control to protect data in transit, particularly over the Internet, but there are many other attack vectors an attacker would likely try before capturing the traffic in transit.

3. **Not Internet facing** – While assets on the Internet do face more frequent attacks, non-Internet facing assets are frequently less hardened and likely contain the sensitive data an attacker is looking to find. Also, encryption in transit may not be in place at all times, such as database traffic on the internal network.

4. **Segmented network** – Well-designed network segmentation can create an additional layer of defense, but there are always some assets that can get into the segmented network, such as a jump server, assets on a management virtual local area network (VLAN), or a vulnerability scanning box. Additionally, some segmented networks can grow to be quite large and over time essentially be no more secure than standard corporate assets.

---


Rise to the challenge of staying compliant
by Michael Howard, HP Chief Security Advisor

Businesses have a false sense of security behind firewalls. A key and current concern of mine is that businesses are struggling to secure every endpoint due to a lack of awareness and knowledge about certain devices and the risks they carry. They feel safe behind a firewall, despite this being no longer enough to protect against an attack.

Security teams must be aware of every endpoint within their infrastructure and they must ensure that each endpoint has multiple layers of security protection to guard against increasingly sophisticated attacks.

Businesses are failing to implement sufficient levels of defense, especially in the case of printers

I see a lot of businesses ignoring their security and crossing their fingers that there isn’t a breach. Sometimes, they’ll implement security just to pass government regulations after which they’ll disable it because they’re receiving too much data and they don’t have the teams to manage it all. A lot of security solutions we see today end up being shelfware and not deployed to the level they need to be in order to be an effective defense measure.

One of the questions we ask our customers is, “Have you had a security breach through printing?” Largely, the answer we get is, “We don’t know.” The reality is that businesses aren’t monitoring printers. At any one time, a security team may be monitoring 75 percent of their network, leaving 25 percent wide open. That should scare CISOs. They need to have visibility on every device in their network.

Security resource shortage exposes businesses to risk

With the rising number of security incidents occurring in organizations on almost a daily basis, and more endpoints entering the infrastructure, businesses are struggling to hire the resources to monitor and respond to breaches. There’s also a lack of education on how to secure new devices. Printers are a prime example of an essential device that few have expert knowledge of how to implement security, so securing printers gets put on a back burner.

All too often, I see security teams taking care of what they’re comfortable with, rather than pushing themselves to apply even minimum protections to lower priority endpoints. I always recommend to my clients that their security teams be educated on every device, understand built-in security features, and add endpoint security controls into the organization’s security policy.

Brand reputation is a major concern

Everybody knows how hard it is to build your brand. But all you need is one security breach to destroy a brand reputation. Not only do businesses pay the price of costly financial penalties (possibly in the hundreds of millions of dollars), but customers will either never shop there again or use a credit card with the business again. Given that we’re a credit-card driven society, this could result in a severe loss of sales.

On top of that, with every new solution, service, or product we launch at HP, security is the first thing we look at. HP development teams know that they have to answer all the security questions including how the devices or software will work on the network in a secure way. More so than ever before, security should be a first thought, not a bolt-on. It’s been HP’s policy for years—ever since we developed the very first internet-connected printer.

The future is cyber resilience

Cyber resilience is about being prepared for and adapting to changing conditions, including withstanding and recovering rapidly from disruptions. Cyber resilience is key to HP’s design policy for our products and solutions. For example, HP’s enterprise-class printers and MFPs have built-in self-healing technology that can protect, detect, and stop an attack at the device.

The device will then reboot to a known good state by checking and reloading the software down to the BIOS level and get back up and running without IT intervention. In addition, the system sends a report with all the important log information, so security teams can learn from the attack and plan for the future. For us, it’s important to help businesses get back up and running as soon as possible, in the event of a network breach.

Staying secure is more important than ever—so make sure you’re following these guidelines to lock down your IT environment from every entry point.

Learn more at www.hp.com/go/printsecurityissa
5. **Web application firewall (WAF)** – When configured properly, the WAF can greatly reduce input validation type attacks. However, the WAF doesn’t mitigate business logic risks and when not properly tuned, may be relatively easy to bypass.

6. **Inheriting controls from the cloud** – A relatively new control that is often misinterpreted. The cloud provider may handle the basic build of a database, such as Amazon Web Services (AWS) with their Relational Database Service (RDS), but the organization may be still responsible for the authentication, authorization, and data in the database. Similarly, certain cloud services, such as storage (e.g., AWS S3, Azure Storage) can easily be left misconfigured.

7. **Email filtering** – A comprehensive anti-phishing strategy includes technical solutions to identify and block malicious email. Yet, phishing attacks are often successful and the entry point to much larger breaches.

8. **User wasn’t an admin** – When an account is compromised the risk is occasionally downplayed when the account doesn’t have elevated privileges. Much like a phishing attack being the entry point into an organization, the compromise of a single lower-level account is a first step to local or domain administrator access.

9. **Privilege escalation vulnerabilities** – There is an inclination to want to reduce the risk of privilege escalation vulnerabilities since access to a system has to exist before the vulnerability can be exploited. As presented in the aforementioned items, unauthorized access to a system can occur in a myriad of ways and it should not be assumed that local access is impossible, or even difficult to accomplish.

10. **Technology not vulnerable** – Often one may hear “we have a mainframe. By default, it is much more secure than Windows.” While mainframe, midrange, and some other technologies do have a fewer number of reported vulnerabilities when compared to more commonly deployed systems, these systems are by no means less vulnerable to logical access attacks. It is very possible that encryption and other such mechanisms are not always applied, mainly due to the additional cost. Furthermore, should these less prevalent systems exist in an environment, there is a good chance that is where the sensitive data resides.

**On planned activities – Why planned is not implemented**

At the end of a risk or compliance assessment, the organization is given a list of findings where risk exists. The organization then determines how to address the risks posed by the finding. In some compliance assessments, such as FedRAMP, an organization must formally document the steps they are taking to address the risk in a Plans of Action and Milestones (POA&M) document.

Often organizations will ask to lower a risk due a plan being in place; however, simply having a plan does not lower risk. Until the risk is actually addressed and a change implemented, the risk still exists. Some examples of requests include:

- **People (Missing a particular role)** – We have a headcount opened with human resources (HR) to fill a missing position in the coming months.
- **Process (Out of date policy)** – We have an update to the security policy, which is currently being reviewed by legal next week.
- **Technology (Unapplied patch)** – Our DevOps team is currently testing the patch or a vendor will be issuing a patch in the coming days.

Each of the examples has a general time frame (i.e., months, week, days) and an assigned resource (i.e., HR, legal, DevOps), which is good; however, these examples are planned, but not implemented. Tasks that may be high importance for an information security team may not have the same urgency for others in the organization. HR may be focusing more on recruiting for other roles; Legal may be buried in other contracts; and the DevOps team may not accept the patch, or the vendor may miss stated deadlines.

**On severity – Why one can’t go lower than low (or very low)**

To provide a common risk framework that is familiar with many, NIST SP 800-30 is a good place to start. High, moderate (or medium) and low risks based on likelihood and impact is well known. In compliance assessments, all organizations try to move High severity findings that are difficult to fix to Moderate and move Moderates to Low, especially if the number of Moderate buckets gets too big. One of the big reasons...
is a single high-severity finding may result in a failing assessment. Within the standard Risk = Liability x Impact equation, most times companies will attempt to downgrade the likelihood rather than the impact as the impact is easier to define (e.g., remote code execution, privilege escalation, denial of service, undetected attack, etc.)

Low-severity risk items are not exempt from this tactic as well. When downgrading risks, organizations will often try to reduce a low severity finding to a different category, like Informational or Note. Organizations need to realize there is a difference between low risk, which gets little attention but is tracked, and no risk, which is typically dropped off the organization’s radar. As can be seen in table 1, there is no Informational or Note value.

The concept of Informational largely applies to vulnerability scan results, where the tool performs information-gathering activities and reports back things like open ports, version information, setting enumeration, etc. In and of themselves, these findings do not pose a risk and have a risk rating of None. Although, the exported results categorize the risk as Informational, this is what frequently leads organizations to want to downgrade Low severity findings to Informational.

The concept of Note is a bit different and the intended use of this category depends on the framework used. For example, the Open Web Application Security Project (OWASP) defines Note as a vulnerability with low severity and low impact.11 Using Note as category for a vulnerability is acceptable, but it doesn’t mean it shouldn’t be tracked (table 2).

<table>
<thead>
<tr>
<th>QUALITATIVE VALUES</th>
<th>SEMI-QUANTITATIVE VALUES</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>96-100</td>
<td>10</td>
</tr>
<tr>
<td>High</td>
<td>80-95</td>
<td>8</td>
</tr>
<tr>
<td>Moderate</td>
<td>21-79</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>5-20</td>
<td>2</td>
</tr>
<tr>
<td>Very Low</td>
<td>0-4</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1 - NIST 800-53 Table 1-3: Assessment Scale – Level of Risk

- Vulnerabilities in medical devices and industrial equipment that run a common operating system that has routine security updates, such as Windows, but these devices are unable to be patched due to support agreements with a vendor.
- Zero-day vulnerabilities where vendor responses take more time. Spectre and Meltdown are recent cases. While the response by many vendors was adequate, it is difficult to cover every situation. For example, Microsoft is continuing to release updates for their offerings.12
- Separation of duties risks within a small company where employees must perform multiple jobs.

There are also situations where remediation options are available, but may require extensive testing before implementing into production. Kernel and Java updates frequently are found in vulnerability scans month-over-month. If something cannot be remediated, formerly document and track the risk.

**On probability – What are the odds**

An organization may be more or less prone to attack based on the type of data being handled. For example, financial institutions, military and government agencies, hospitals, etc., are more frequently targeted. However, these organizations often have more resources to allocate to defenses. This group could be considered big fish in a relatively small pond. Conversely, there are millions of other entities with smaller datasets that could be viable targets. This group could be considered small fish in a big pond (or ocean). The likelihood any single organization is targeted may be lower, but the likelihood one of them has weak defenses is vastly higher. This is not a new concept, as journalist Brian Krebs wrote about something similar when reporting on the December 2017 Jason’s Deli

---


Continued on page 42
Using PKI to Build a Secure Industrial Internet of Things

By Mike Nelson

This article provides an overview of how device manufacturers can address security concerns for IIoT devices by using public key infrastructure.

Abstract

Security is too often an afterthought when Industrial Internet of Things devices are designed and manufactured. While security awareness is growing, device manufacturers primarily rely on basic username/password protection. This article provides an overview of how device manufacturers can address security concerns for devices by using public key infrastructure.

Industrial plants and factories are expected to be transformed into software-defined facilities by IoT technologies in 2018. Industrial IoT (IIoT) promises to revolutionize industrial prowess by improving efficiency at factories, power plants, refineries, offshore oil platforms, just to name a few. For years, the industrial sector used private networks to control crucial operations, but now manufacturers are reaching into these networks from the IT side. This will keep costs down, but also increases security risks. Consequently, realizing the enormous potential of Industrial IoT requires device manufacturers to adopt a “security by design” approach during the initial design phase.

“Internet of Things” has become the common umbrella term for all connected devices, but there are key differences between consumer devices and IIoT. While consumer IoT devices may make splashy news headlines, it does not diminish the promise that IIoT can transform entire industries. For example, the World Economic Forum estimates $1.3 trillion of value can be captured with IIoT for the electricity sector alone.

The McKinsey Global Institute predicts that IIoT will generate an economic impact of $6.2 trillion by 2025. In its report “Unlocking the Potential of the Internet of Things,” the authors state that “if policy makers and businesses get it right, linking the physical and digital worlds could generate up to $11.1 trillion a year in economic value by 2025.” The report also identifies factories as the top setting “where value may accrue” in areas such as predictive maintenance and operations management.

To date, organizations have only scratched the surface of IIoT’s potential, as most do not analyze and use the bulk of the data they are collecting from their devices. Consider an oil rig equipped with 30,000 sensors measuring everything from depth to flow to pressure to gas detection. Each of these sensors must communicate data back to a server, yet chances are only one percent of the data those sensors generate is analyzed. Typically, the information is used only to monitor for, and control, anomalies—not for optimization and prediction, which provide the greatest long-term value.

As more organizations implement the technologies they need to analyze and use the ever-growing volumes of data their IIoT devices generate, the industry can expect to see IIoT play critical roles in areas such as facilitating predictive maintenance and automating processes. Manufacturing and warehouse facilities will continue to be more technology-driven and predictable as IIoT devices capture data and broadcast to

servers where it can be analyzed in real-time so that operations may be modified according to immediate needs. In fact, the transition from machine-to-machine (M2M) to true IIoT that is fueled by the rapid growth of connected devices and sensors presents new challenges that must be addressed as the IIoT becomes more ingrained in every day operations. While IIoT devices must be designed for the unique environments and applications in which they will be placed, the primary challenge of IIIoT devices is the rise in security risks to data stores and systems.

**Security concerns**

Businesses, government agencies, and consumers are right to be concerned about guarding their privacy. When any organization attaches an IoT device to its network, it creates a new cyber-attack vector that potentially anyone (internal or external) can use to access or steal data, and even gain control of the device itself. Those risks apply to all devices whether they are applied to industrial, government, or consumer applications.

James Clapper, the former US director of national intelligence, warned about the risks of IoT to data privacy, data integrity, or continuity of service in a 2016 presentation5 to the Senate Armed Services Committee. In his written report, Clapper wrote that “devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US government systems.”

By its very nature, any device or thing that can be controlled through a network is vulnerable to threats ranging from botnets, malicious attacks, data breaches, and more. IoT device security is reliant on the security they are built and secured with before hitting the market.

Forrester’s November 2017 “Predictions 2018: IoT Moves from Experimentation to Business Scale” report echoes Clapper’s concerns, and adds that IoT will be at the center of broader and more damaging cyber attacks in 2018. Yet despite that ominous prediction, Forrester has found that “while IoT security awareness is growing, customer experience, cost, and time-to-market requirements continue to take precedence over security requirements.”

That is neither sustainable nor is it acceptable, especially when one considers critical infrastructure. For manufacturers who consider security to be an afterthought, the inevitable result is having to retrofit their devices after a vulnerability or threat is identified—an expensive and time-consuming process. That is why security built into design is the superior approach. When implemented correctly, secure IoT deployments ensure that the basic security requirements for availability, integrity, and confidentiality are properly configured. Manufacturers should also determine whether such devices should be configured to receive automatic updates, or if they should require manual updates to security protocols. This is all part of a “security by design” approach that IIoT device manufacturers must adopt. The incorporation of public key infrastructure (PKI) using digital certificates plays an important role in this approach.

**PKI and alternatives**

A PKI framework supports the distribution and identification of public and private encryption keys, enabling users and machines to both securely exchange data over networks such as the Internet and verify the identity of the other party. In a similar way, PKI can provide assurances for IoT devices and the people who use them.

There are several drawbacks to implementing PKI as it relates to IIoT. It can be complex and therefore requires thoughtfulness and planning to make sure you implement and manage it correctly. Organizations must plan to monitor the implementation, including the management of certificates, the proper storage of keys, and maintenance of encryption algorithms. They may elect to engage a third party to ensure that the environment and its complexities are up-to-date.

Yet, the biggest negative perception and drawback to PKI for IIoT is the storage and processing power that PKI encryption requires. This is mostly a myth built upon the implementation of PKI based on current standards for the Internet. These same standards do not apply to private PKI implementations like sensors. For example, a sensor does not need to validate all the same certificate fields that is needed by a web browser to identify if a site has a certificate or not. Most sensors can have more than enough memory to store keys and crypto algorithms required, especially if one of several nano-crypto libraries is used that has a smaller footprint than its web-PKI cousin.

Next is processing power. PKI has very low computational requirements. In order to run an algorithm without delay, a sensor should have at least a 16-bit processor. Even slower processors will work, but there may be a slight delay in the initial authentication. With deliberate planning, devices can be designed securely with PKI regardless of limited processing power and minimal storage.

Despite common misconceptions and any possible drawbacks, PKI is an ideal technology for the IIoT sector, providing trust and control at scale and in a user-friendly way that traditional authentication methods like tokens and passwords do not. Digital certificates for mutual authentication can be used to authenticate users to devices behind the scenes with nearly no user interaction.

While there are alternatives to PKI, they too have many drawbacks. Symmetric alternatives do not offer bi-directional encryption, although they may be faster in some cases. In addition, a second layer of security is often implemented to

---


Managing a web PKI requires adherence to industry standards, policies that establish trusted roles and ensure compliance, and maintenance of robust architecture to support fast issuance and quick, secure connections.

Setting up a PKI framework involves key ceremonies and key storage policies, providing reliable uptime and best-in-class revocation and renewal capabilities. As IoT communities and devices continue to grow and emerging markets realize the benefits of PKI, these industries can provide greater security for their users by applying the standards-based approach that has been developed over many years for the web PKI.

Whether IoT device security relies on private PKI systems or requires public trust that only comes via a publicly trusted certificate authority with wide ubiquity in online root stores, the principles of web PKI standardization equally apply.

Take, for example, the 30,000 sensors in an oil rig mentioned earlier. Each of the dozens of gas detection sensors needs to communicate securely back to the servers that alert equipment operators of potential dangers. Should a bad actor gain access to these sensors, the results could be catastrophic—from mis-reporting information resulting in a dangerous situation to accessing corporate networks or launching a botnet attack. As a result, each sensor should be properly authenticated to the network, send encrypted data, and receive instructions based on the changes from the operator of the equipment. This process is outlined in figure 1 next page.

On-premise versus hosted

For scalability purposes, many companies will choose a cloud-hosted PKI that provides the flexibility to manage certificates as they come online and avoids the expense of further protect the systems. But this has an unintended consequence by creating more potential vulnerabilities in the system. For example, if biometrics are the authentication system, a password may also be required to further protect the device. This provides bad actors with two doors instead of one into the system and network.

Many IoT devices that use a username/password method may also require TLS certificates to encrypt data as an added layer of protection. In this case, only PKI would be needed, as this adds to the vulnerability points and storage requirements of the device. Many M2M protocols send usernames/passwords as unencrypted data (in clear text). In addition, these methods do not offer the scalability and methodical management that PKI offers. If a password is obtained, bad actors have access to entire systems, not just a device. And these methods do not identify which server the device is communicating with, making it impossible to track down the source of the breach.

As a result, device manufacturers should design devices to support PKI. As more devices come online, scalable PKI also encrypts confidential data, and maintains data and system integrity, including protecting the code used in the system.

Digital certificates enable safe authentication without the friction to the user experience that comes from user-initiated factors such as tokens and password policies. This protects all of your devices and networks from malicious actors, even if a data stream or data source were captured or compromised. Modern-day PKI using up-to-date cryptography should serve as the foundation for security providers’ efforts to scale the authentication of the ever-growing ecosystem of IoT devices.

Managing PKI

PKI has many benefits. However, deploying a trustworthy system that is safe and reliable is not a simple undertaking.

Evolving Security for Digital Transformation

Yesterday’s tried-and-true methods for securing IT are no longer effective in the context of digital transformation and distributed networks. In addition to wide adoption of BYOD policies, the cloud, and the Internet of Things (IoT), data volumes have increased 40x over the last 10 years.\(^1\) When you consider that the Internet has been using the same protocols and infrastructure for decades, an estimated 95% of today’s content no longer fits with its original design.\(^2\) These changes have not gone unnoticed by cybercriminals, who are exploiting the expanded attack surface as well as both existing and new vulnerabilities. They are also leveraging new, more advanced threat vectors to increase the velocity, volume, and variety of their attacks.

Looking back over the past 25 years since the advent of the Internet, the evolution of security has passed through several different generational stages:

- **First Generation:** The first iterations of network security date back to about 25 years ago. Static firewalls were used to control who and what could connect to the network. This eventually was combined with VPN to encrypt traffic. These first-generational firewalls focused on protecting and inspecting data coming through established access points on a defined perimeter.

- **Second Generation:** The next major evolution in network security came with the need to secure richer forms of content and applications. With more data being pushed across the network, we saw the emergence of purpose-built security processors and content and deep packet inspection used to handle the influx of traffic being pushed across the network. This gave rise to unified threat management (UTM) and next-generation firewall (NGFW) devices.

- **Third Generation:** Today, the innovations of mobility, Internet of Things (IoT), and cloud computing require security defenses that reach across broadly extended networks. In addition to expanding the attack surface, these also exponentially grow the amount of data flowing across the network. Without the ability to see and institute policies across the entire network, organizations lack transparent visibility and control and response to threats in real time. Third-generation network security is highly elastic and distributed. It cannot be stand alone, but it must rather dynamically scale and respond to shifting network resources.

An effective third-generation strategy requires network security that extends to the edge and to wherever data exists, across an organization’s growing and changing digital footprint—from endpoints, to on-premise systems, to complex multi-cloud ecosystems.

Fortinet’s Security Fabric architecture broadly covers all parts of the organization as it grows and changes, protecting all aspects of the IT infrastructure and every device, both virtual and physical. It also integrates security components into a unified whole to detect and remediate advanced threats. This also means that it distributes, orchestrates, and enforces unified policies across all domains—from remote workers, to branch offices, to distributed data centers, to private and cloud networks. The Security Fabric is automated and enacts intelligent action as a single, cohesive system, making real-time and coordinated responses to threats through the sharing of threat intelligence.

---

maintaining on-premise servers and other hardware. Some heavily regulated industries want more control and choose an on-premise solution. Still, this requires expertise in managing PKI systems and adhering to industry standards and modern protocols. There are advantages and limitations of each approach, and it’s not a one-size-fits-all proposition.

One key difference is control over the PKI issuance process. An organization that hosts an on-premise implementation directs that process and can make configuration and development changes on its own schedule. Working with a hosted provider gives control to the provider. However, organizations that choose an on-premise solution need to also consider the resulting costs and other complications that such a decision will create.

Acquiring the necessary hardware, training, and resources needed to implement, run and maintain an on-premise PKI solution may introduce substantial costs beyond the initial hardware and software acquisition in order to ensure device integrity throughout the life cycle. Organizations need to decide if they are ready to set up an internal CA and operate it according to industry best practices and established standards, or if they would be better served by a hosted solution from a company exclusively focused on providing hosted services to customers.

A hosted IoT PKI solution offers the flexibility to use both a private PKI and publicly trusted certificates. Beyond the advantages of security and scale, another key consideration is the fact that cryptography is constantly changing. Certificates require a quick turnaround when standards shift or

---

**Book Review**

**InSecurity: Why a Failure to Attract and Retain Women in Cybersecurity Is Making Us All Less Safe**

Jane Frankland

Rethink Press (October 20, 2017)

The shortage of cybersecurity workers is a global issue with millions of jobs unfilled. Worse yet, the percentage of women working in cybersecurity is only about 10 percent, according to a report from (ISC)². Jane Frankland’s new book, *InSecurity*, offers practical tips and advice for women looking to work in cybersecurity, for women already in cybersecurity, and for men and women who want to help fix the gender gap.

*InSecurity* is significant since it is one of the few books on the subject of women in cybersecurity and perhaps the first book to attack the subject head on with such passion from an author showing great dedication to the cause. Part autobiography, part research study, part career guide, there is a lot of material condensed into a single book. It takes a deep dive and shows many disturbing trends, statistics, and issues. It is clear that the gender gap is a serious issue that needs to be addressed in schools, with parents, in the media, and in the industry.

Frankland is spot on that in cybersecurity there are very few women role models depicted in TV and movies, which instead is dominated by men. She did miss one detail when discussing the James Bond movie *GoldenEye*. She mentions the Russian hacker but failed to point out that at the film’s climax his coworker—a woman—manages to thwart the bad guys by changing the access codes to the system. Even after mocking her, the hacker was unable to break her codes to regain system access.

The book does an amazing job pointing out that there are countless heroines in history. Some examples are the women who helped decipher enemy codes during World War II, the women who were crucial in helping NASA’s space program as depicted in the film *Hidden Figures*, the women who helped invent new technology that led to Wi-Fi, and the list goes on. This brings up
InSecurity | Mike Nelson

InSecurity

Mike Nelson, VP of IoT Security at DigiCert, is a leader in digital security. He frequently contributes to media reports, participates in industry standards bodies, and speaks about how technology can be used to improve cybersecurity for critical systems. He may be reached at mike.nelson@digicert.com.

April 2018 | ISSA Journal – 31

Tried and true security measures

Whether or not an IIoT device manufacturer decides to incorporate PKI, the enterprises that implement IIoT devices must still adhere to time-tested security principles. These include encrypting data both at-rest and in-transit, digitally signing code, and device authentication so an organization can identify each single device that connects to its network.

Also, PKI can assure the integrity of the device, including secure boot with proper configuration, secure over-the-air updates and patching, and preventing tampering of code by signing each batch. It is also necessary to regularly train users on the importance of, and how to follow, security best practices such as creating strong passwords for each device.

Still, truly effective IIoT security begins on the device manufacturer’s drawing board. Too often, security is an afterthought, and that needs to change. Otherwise, manufacturers waste time and money (and risk damage to their brand reputations) retrofitting their devices after a vulnerability or threat is discovered. Security built into design is the superior approach, and the incorporation of public key infrastructure using digital certificates and other security best practices play a critical role in ensuring that any IIoT deployment meets basic security requirements for data confidentiality and device control.

About the Author

An essential point, that when looking for women role models, instead of looking at our present, we need to dive into the past that is filled with a rich history of amazing women.

The book also mentions the advantages of workplace flexibility. I do agree with Frankland that this is vital, especially for parents. Unfortunately, the book fails to mention the growing list of large companies that have reduced or eliminated this option: Yahoo, IBM, Aetna, Bank of America, and more.

There are many shockers in the book as well. The biggest one for me is how much men can help. One assumes that the best person to speak to girls in schools about careers in cybersecurity would be a woman; not always true. It points out that sometimes a man can reach out in ways that a woman cannot. Further, the book cites many examples where men can and have made a big difference in the lives and careers of many women, including the author.

Unfortunately, one of the biggest obstacles for women working in tech is hardly mentioned in the book, sexual harassment. There are only one and a half pages devoted to the subject, while in the past several months the floodgates have burst in Silicon Valley: Susan Fowler’s blog post about Uber, Ellen Pao’s lawsuit against her venture capital employer, and more. Since sexual harassment is a serious issue today for women, there should be more information to help them should it occur.

Another area that the book neglects to mention are the recent laws enacted by a growing number of states and cities within the United States that ban employers from asking job candidates about their salary history. Advocates have pushed for such laws, citing that salary history has been used as a tool to discriminate against women and pay them less than men. It is hoped that these new laws will help to reduce the gender pay gap.

The ultimate treasure of the book is Jane Frankland’s story. As an autobiographical, it is a powerful narrative of a successful, award-winning female entrepreneur and single mom with kids, struggling to build a business while making a difference in the world. She shares her successes and failures, showing both vulnerability and strength. Many women will read InSecurity and be able to identify with her struggles as many face similar bumps in the road of life. InSecurity is highly recommended not just to women, but to men who want to make a difference.

About the Reviewer

Nathan Chung, ISSA Denver Chapter, may be reached at nathanincal@gmail.com.
Abstract
Starting with an examination of the Mirai botnet, this article discusses the ongoing proliferation of “crime-as-a-service” and its facilitation by insecure and/or defectively coded Internet of Things (IoT) or “smart” devices. Owing to their monoclonal nature and near ubiquity, IoT device life expectancy will likely diverge from the expected viability of embedded device code. The risk of widespread product liability arising from this divergence offers manufacturers three choices: upgrade device code (at substantial recurring cost), let such devices become orphaned, or disable them altogether. Current recommendations for addressing this issue, all of which provide sub-optimal resolution, range from the impractical and expensive (notification of defects and/or vulnerabilities) through and including firmware updates and device/object sunsetting or disabling.

The Mirai botnet starts life as a gaming “booter” service
Probably the most spectacular assault on Internet connectivity in the recent past has been the Mirai\(^1\) IoT botnet.\(^2\) On December 8, 2017, the three defendants, hailing from New Jersey, Pennsylvania, and Louisiana, pleaded guilty to conspiracy to violate the Computer Fraud and Abuse Act in connection with the Mirai botnet.\(^3\) On December 13, the US Department of Justice unsealed documents relating to guilty pleas from these defendants in three related cybercrime cases from the District of Alaska.\(^4\) What was relatively unknown about this series of events, until now, is Mirai’s origin and evolution from a Minecraft\(^5\) “booter service” to one of the most powerful IoT-based DDoS tools developed in recent history.

In or around August 2016, one of the teenage cybercriminals created a scanner that was ultimately incorporated into the Mirai code. The scanner would scan the Internet for devices with an open port, and then attempt to gain unauthorized administrative access to those devices by entering a series of login credentials. If the login attempt succeeded, the IP address of the exploitable device was recorded, and the device infected with Mirai.

Wired magazine reports that FBI Special Agent Elliott Peterson was “part of a multinational investigative team trying to zero in on two teens running a DDoS attack-for-hire service known as a vDoS, an advanced botnet: a network of malware infected, zombie devices”\(^6\) that could be called upon to execute on-demand DDoS attacks. The two teenagers ran the vDoS service as a Minecraft\(^7\)® booter.\(^7\) One of the co-defendant’s recently unsealed plea agreement states that he and his co-conspirators built the botnet in order to:

---

1 “Mirai” is Japanese given name, meaning “the future” – [https://en.wikipedia.org/wiki/Mirai_(given_name)](https://en.wikipedia.org/wiki/Mirai_(given_name)).
3 18 U.S.C. §1030(a)(5)(A) and (c)(4)(A). Id.
5 Minecraft\(^®\) is a game about placing blocks and going on adventures – [https://minecraft.net/en-us/](https://minecraft.net/en-us/).
7 A “booter service” is typically offered by cybercriminals that “provide paying customers with distributed denial of service (DDoS) capabilities on demand.” Booter services (aka “booters”) offer “crime as a service” (quotes mine) DDoS at very low prices. Advertised on a typical website front, clients can target booters to mount DDoS attacks on websites selected by the client. Detection and sourcing of booters is difficult, as the service provider from which the service is provided is in all likelihood not the booter’s real IP address – [https://www.webopedia.com/TERM/B/booter_services.html](https://www.webopedia.com/TERM/B/booter_services.html).
“create a weapon capable of initiating powerful denial of service attacks against business competitors and others against whom [co-defendant White] and his co-conspirators held grudges; (2) provide a source of revenue to [White] and his co-conspirators in the form of a powerful denial of service weapon that could be: (a) rented to third-parties in exchange for payment, and (b) used to extort hosting companies into paying protection money in order to avoid being targeted by denial of service attacks.”

In this case, the Mirai code began life as bootee service used to mount a simple but effective attack on a Minecraft gamer’s adversary during a one-on-one fight: knock the adversary offline and by doing so, defeat him or her. The teens running this criminal conspiracy would charge small amounts (reported to be between $5 and $50,) “to rent small-scale denial-of-service attacks via an easy-to-use web interface, or crime-as-a-service.”

A scalable DDoS weapon for sale

The Mirai programmers continued to develop and tweak their scanner, however, and in so doing created a malware threat different from other scan-and-infect methods (e.g., 2014’s vDoS and QBot IoT attacks) in that it was truly and easily scalable. Research from Google reports that “24 unique Mirai binaries” (a.k.a. iterations) were detected between August and September 2016. As Mirai evolved, it also became cleverer, deleting its executing binary and obfuscating its process ID.

During September 2016, one of the co-conspirators accessed a computer in France to serve as a proxy to conduct Mirai activity. Also during that same month, the French hosting company OVH fell victim to what was one of the first terabit (actually 901 Gbps) DDoS attacks. FBI Agent Peterson is quoted as saying that “Mirai was an insane amount of firepower,” with victims targeted in the US (50.3%), France (6.6%), the UK (6.1%), and a long tail of other countries. Other notable victims include DNS provider DYN, Liberian telecom operator Lonestar Cell, and security blog site Krebs on Security.

Mirai’s success was facilitated by insecure IoT devices

All told, the Mirai IoT botnet successfully infected “hundreds of thousands of Internet-connected computing devices.”

Why was Mirai successful? Google researchers address these questions with what should be obvious to device manufacturers and their programmers.

Google researchers correctly (but somewhat incompletely) set the legal context for putting the Mirai IoT botnet (and what will likely be its successors in interest): “Mirai has brought into focus the technical and regulatory challenges of securing a menagerie of consumer-managed, interfaceless IoT devices.”

Perhaps most notable (and menacing) is their assessment that cybercriminal attacks are the result of “attackers taking advantage of a reversal in the last two decades of security trends especially prevalent in IoT devices.”

More disturbing is their conclusion that “[I]n contrast to desktop and mobile systems, where a small number of security-conscious vendors control the most sensitive parts of the software stack (e.g., Windows, iOS, Android) – IoT devices are much more heterogeneous, and from a security perspective, mostly neglected.”

Not surprisingly, the security recommendations they suggest are (or should be) familiar to almost every security professional in acknowledging the threat of scaled Mirai-like botnets that can infect and compromise hundreds of thousands or even millions of IoT devices:

The first recommendation is security hardening, which includes randomized default passwords as a “first step” and a shift away from default open ports to default-closed. Devices could also incorporate limitations on remote address access to local networks or specific providers through default network configurations, ASLR (address space layout randomization) isolation boundaries, principles of least privilege, and even certification.

A second suggestion is for device automatic updating, which would provide “a timely mechanism to patch bugs and vulnerabilities without burdening consumers with maintenance tasks or requiring a recall.”

A third suggestion, notification, hearkens back to pre-digital days. The Google researchers suggest notifications via out-of-band channels (email, radio, TV, Facebook), but the issue of notifications extends beyond those who initially purchase such devices. For example, how would non-purchasing users (family, re-gifting) be notified?

All of the suggestions offered above pose logistical issues for IoT device manufacturers that must be addressed. First, the costs for hardening may add more to the manufacturing cost than the cost to manufacture the IoT device without security. The cost for updating devices may suffer from the same cost problem, particularly as devices age.

The costs for notification by Internet dissemination would more closely resemble public service announcements or “Amber Alerts,” depending perhaps on the severity of the need for notification and update/upgrade/recall (think of an explod-
ing connected hot-water heater in a home recently sold by the person who installed the IoT device).

The issue of IoT device vulnerability extends far beyond botnets and expands the concept of security to include safety. The chair of the Federal Trade Commission recently acknowledged the expanded effects of IoT devices to include both security and safety in stating that “…the risks that unauthorized access create intensify as we adopt more and more devices linked to our physical safety, such as our cars, medical care, and homes…As an initial matter, some of the developers entering the IoT market, unlike hardware and software companies, have not spent decades thinking about how to secure their products and services from hackers.”

**Differences in digital and device useful life**

Indeed, a one major thorny issue relates to the expected mechanical or useful life of an IoT device as compared with the expected viability of its embedded code. If a connected toaster or oven has an expected useful life of 10 years, does this mean that a manufacturer must:

1. Build in 10 years of anticipated security vulnerability hardening at manufacture,
2. Include 10 years of exploit-preventative updates to subsequent users as well as initial purchasing users,
3. Employ 10 years worth of mass notification to all purchasers and non-purchasing users, or
4. Sunset or orphan (i.e., brick) the device to make it inoperative?

If the device is not bricked after its stated 10 years useful life, what are the legal consequences if the device is used for 12 years and catches fire, destroying property and injuring a houseful of people?

As to the first (and even with the advanced level of security technology), is it reasonable to think that an IoT device can be future-proofed for 10 years—at manufacture? Will there be a warning notice on the box (or on the device itself) with a “Safe to Use Until [Date]” or expiration date imprint? What will happen at that time? Can the device-cum-embedded firmware still function fully, or will it be partially or totally bricked/sunsetted? Even if an IoT device can (or even should) be sunsetted, what if the IoT device regulates your home heating and air conditioning system, and the sunsetting disrupts your heating system when the temperature falls to record lows causing pipes to burst?

As to the second, there will be issues as to both connectivity (as in, whether there is connectivity) and device authentication. Consider the case of a connected oven requiring a critical update for a subsequent owner (house and appliances are sold in foreclosure). The new owner configures his own network, and his firewall blocks any attempt by the device to “phone home.” Will there be an error – “failed to update” – message sent by the manufacturer as a failsafe? How will the manufacturer know that there is a new owner? What if the appliance is sold or given away and removed to a new location? How will authentication and updating take place if the authentication requires information from the prior owner’s network? What if the new user just wants to use the oven and doesn’t care to connect it to his/her network?

As to the third solution discussed by the Google research report, what kind of “mass” notification is necessary, or will suffice? What dissemination methodology should be deployed?

**Current solutions and why they fail to address potential and significant legal liability**

The solutions offered by the Google research discussed above are, in this author’s view, largely Utopian, and largely unattainable on a voluntary basis given the volume, types, manufacturing, and potential updating costs associated with IoT devices propelled daily into the consumer, industrial, government, and healthcare markets. As the FTC chair stated at a recent CES show, “…the small size and limited processing power of many connected devices could inhibit encryption and other robust security measures. Moreover, some devices are low-cost and essentially disposable. If a vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch—or even to get news of a fix to consumers.”

Equally important, and perhaps the most difficult IoT security implementation obstacle to surmount, is consumer awareness, buy-in, and action. Notably, even the FBI has chimed in on this issue, albeit with what this author deems a somewhat naïve approach. Presuming perhaps much more highly advanced technological sophistication by the general public, the following excerpts highlight its recommendations:

- Change default usernames and passwords. Many default passwords are collected and posted on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets.
- If you can’t change the password on the device, make sure your wireless Internet service has a strong password and encryption.
- Invest in a secure router with robust security and authentication. Most routers will allow users to whitelist, or specify, which devices are authorized to connect to a local network.
- Isolate IoT devices on their own protected networks.
- Turn devices off when not in use.
- Research your options when shopping for new IoT devices. When conducting research, use reputable websites that

---


specialize in cybersecurity analysis and provide reviews on consumer products.

- Look for companies that offer firmware and software updates, and identify how and when these updates are provided.
- Identify what data is collected and stored by the devices, including whether you can opt out of this collection, how long the data is stored, whether it is encrypted, and if the data is shared with a third party.
- Ensure all IoT devices are up to date and security patches are incorporated when available.  

Once again, the FBI’s advice purports to assume (and now from the consumer’s perspective) a Utopian viewpoint. For example, and as to the first suggestion, the online magazine The Register somewhat querulously notes that the FBI is advising consumers to become their own system administrators, and asks whether people even know about the existence of an admin user interface.  

### Potential IoT device liabilities

What are the potential liabilities for insecure and unsafe IoT devices? From a legal perspective, a manufacturer may be brought into court for claims alleging breach of merchantability, breach of warranty of fitness for a particular purpose, negligence, fraudulent misrepresentation, or even strict liability. What might be the underlying factual bases for asserting these claims?

- Vulnerable (and thereby defective) by design
- Vulnerable (and thereby defective) by upgrade
- Vulnerable (and thereby defective) by orphaning with no sunset
- Vulnerable (and thereby defective) environment changes to effect defect

Damages for findings of liability may include contract-type damages such as those incidental to or in consequence from the compromise of a device, and in the case of findings of fraud or negligence may include pain and suffering, and even punitive damages. These damages are likely to be increased by orders of magnitude, largely because the monoclonality and ubiquity of IoT devices means that compromise and damage or injury will occur on a widespread basis. In legal terms, widespread compromise and damage or injury means that either a class action or mass tort adjudication will result. A traditional class action litigation mechanism involves hundreds or even tens of thousands of affected consumers who band together in single action against a device manufacturer. A mass tort litigation involves similar numbers of individual lawsuits that are consolidated for pre-trial purposes and then either settled out on a mass basis or sent to trial. Neither of these litigation mechanisms should be attractive to IoT device manufacturers, and taking pro-active steps to avoid such liability seems the more reasonable alternative.

### Conclusion: IoT device manufacturers should lead with security

The Mirai botnet stands as a both a reminder and clarion call to action by the IoT community. We are rapidly advancing to a consuming population that will (or already is) saturated with connected devices exhibiting varying degrees of vulnerability to compromise. While consumers should always take appropriate steps to protect themselves while using these devices, IoT device manufacturers must take the lead in providing better security for devices employing one or more of the above solutions. The answers to these questions posed in this article point out the need for development of some type of uniformity approach to both security and safety of IoT devices, and an acknowledgment that building security into embedded devices also embeds safety.

### About the Author

Steven W. Teppler is a partner at the Abbott Law Group in Jacksonville, Florida, and leads the firm’s complex litigation and electronic discovery practice, which encompasses security, property, and personal injury single event and mass actions arising from emerging technologies. He may be reached at Stepler@abbotlawpa.com.
Cyber-Physical Intelligence

By Tyson Brooks – ISSA member, Central Maryland Chapter

In this article, a novel model for cyber-attack defense modeling for intelligence collected from a cyber-physical system network and its devices themselves to evaluate the security of these systems in the presence of cyber attacks is proposed.

Abstract

Cyber-physical systems (CPS) and Internet of Things (IoT) networks will form a universal computing environment that will motivate modern technological innovation and growth in the near future. CPS arise from the tight integration of physical processes, computational resources, and communication capabilities. Examples of CPS include power networks, mass transport networks, and water distribution systems.

In contrast, the IoT is often an ad-hoc collection of interrelated computing devices with sensors and actuators that have the ability to transfer data over a network without human interaction. Examples of IoT networks include IPv6 over low power wireless personal area networks (6LoWPAN), fog computing platforms, and industrial control systems. The design of both CPS and IoT systems will include seamless integration, security, and usability. However, the dynamic nature of IoT networks presents serious challenges when using formal analysis methods.

In this article, a novel model for cyber-attack defense modeling for intelligence collected from the CPS network and its devices themselves to evaluate the security of these systems in the presence of cyber attacks is proposed.

Recently, great advances have been made towards realizing artificial intelligence (AI) based on access to very large and efficient data and services in cyberspace [7][12]. The precision and real-time nature of AI provides the foundation for fast autonomic decision-making. Cyber-physical systems (CPS) and Internet of Things (IoT) systems based on the integration of human and artificial intelligence functions may greatly raise the decision-making quality. However, information flows within such a system must be secured to assure the integrity of decisions [14]. The word “intelligence” is used to denote two different but related concepts: problem solving capacity [like in “artificial intelligence"] and information gathering and analysis [like in “signal intelligence’].

CPS introduce new dimensions and fundamental new problems in both realms of intelligence [9]. CPS are structured and designed for specific purposes, which facilitate their evaluation of security using techniques such as model-based systems engineering [3]. In contrast, IoT systems tend to be dynamic and frequently change, which make their evaluation more challenging, resource intensive, and less likely to be accomplished. In fact, it is usually assumed that the data from all IoT system “things/objects” (e.g., smart devices, etc.) will be received and processed timely, accurately, and reliably. The data-intensive feature of IoT introduces several specific challenges such as circumstance dynamicity and uncertainties [19]. As the number, type, and processing power contained within IoT devices increase, so will the amount of data generated by these devices [4]. Consequently, the aggregate information flow for network connectivity when integrating CPS and IoT systems should be taken into consideration. The performance of cyber infrastructures has great impacts on the types of operations needed to perform in these environments.

As displayed in figure 1, CPS are systems deployed in large geographical areas and generally consist of a massive number of distributed computing devices tightly coupled with their physical environment [3][9]. The frontier between CPS and IoT has not been clearly identified since both concepts have been driven in parallel from two independent communi-
cies (i.e., sensor networks and radio frequency identification [RFID], respectively), although they have always been closely related [3][9].

CPS components consist of computational computer systems platforms, physical/environmental devices, and the network, which captures the source of information and is the source of all information used in the processing of data throughout the system, as displayed in figure 2. From a defense “intelligence” perspective, the basic task of a CPS is to support the defense for the network through detecting technical loopholes and topographic structures from the various networks and the data/information stored inside the system.

![Figure 2 - Cyber physical system components](10)

By searching, discovering, and determining tactical and technical parameters of wireless equipment and systems, discovering irregularities of electronic tags and their threat levels, and analyzing tag/reader strong and weak access points provides the interoperability for organizing and carrying out defense [3]. The defense in the CPS is to guarantee that the network, devices, and system perform their normal functions. The concrete tasks are mainly, through multiple means and methods, to guarantee the normal operation of a user’s own computing device or network system, guaranteeing the processing of secure data transmissions, and defense against malicious intrusions.

The components in figure 2 are responsible for the processing, transferring, and collecting of information and jointly determine the overall performance of the system. These types of cyber-physical systems can be used for the detection, identification, surveillance, tracking, and location of all acoustic, electrical, magnetic, and mechanical signals in networks. The cyber-physical system is mainly responsible for the security of the data through screening, identification, computation, and encryption of original information [9]. For example, as data is acquired by digital sensors/tags/actuators, information will be fed directly into the network for computation (or storage) and non-digital information is encoded to become digital information before processing.

**A cyber-physical attack model**

Intelligence, when defined as problem solving, is an evolutionary process. As such, intelligence is also a computational process, as coding, variation, testing, and storage of new solutions subsume under a general form of programming, just like heredity as the foundation of natural selection and life is a form of programming. Since the cyber-physical architecture is a network of systems, its basic state can therefore be formulated as a network flow model. Any system architecture, sensing devices, and some computing devices are the sources of information flow; their functions are to generate information and then inject into the communication network. Other computing devices are at the end of the information flow since they are used to receive information and conduct necessarily analysis [18]. The communication network is responsible for transferring information and information exchange devices (e.g., routers and switches) to determine the transmission path of each data packet, or in other words, determine the directions of information flows.

Data automation for the processing of information within communication networks should include the automatic filtering of malicious data. For data processed within a CPS, the CPS should automatically identify and classify the various parameters like the data source, nature, properties, status, and distribution and must discard the malevolent data but retain the valid and necessary information automatically. Data processed in this manner will thus become useful information and after categorizing the collected data, the CPS proceeds with its allocation.

Malicious objects (e.g., viruses, malware, etc.) are injected into computer networks through cyber attacks from insiders (malicious or non-malicious) or hostile outsiders (external entities) through various means (e.g., email, thumb drives, etc.). A cyber attack contains three main elements: 1) Behavior of the attack, 2) object being attacked, and 3) effect of the attack (figure 3).

![Figure 3 - General attack taxonomy](13)

The choice of modeling approaches for a CPS depends on the domain characteristics (i.e., continuous/discontinuous time), range characteristics (i.e., continuous/discrete states), operational logic (i.e., time-driven/event-driven), and modeling complexity [13][15]. CPS depend on proper operation and are susceptible to cyber-physical attacks consisting of cyber and physical components. Since, cyber attacks generally take the form of viruses, malware, or denial-of-service (DoS) attacks with the goal of disabling computers or networks, there are numerous techniques for modeling and defending against cyber attacks [8]. When evaluating which cyber attack to attempt regarding CPS, adversaries consider three high-level aspects of the outcome of executing the attack: 1) the resources required to execute the attack \( RE \), the likelihood of success of the attack \( P(s) \), and the likelihood of being detected \( P(d) \) [2].

Cyber attacks that succeed or those not likely to succeed require resources that often exceed a hacker’s available resources, are easy to detect, and/or do not accomplish the hacker’s goals. Data used to gather this information to support this
model could be derived from laboratory environments consisting of honeypots, honeynets, or network intrusion detection/prevention analysis tools. Therefore, monetary resources expended $RE$ measures the marginal resources required to execute the cyber attack and include funds, time, manpower, equipment, etc., and exclude general development costs—the one-time expenses required to develop the attack [2]. All other things being equal, an attack step that is “cheaper” will be more attractive to a hacker.

The probability of success $P(s)$ measures the likelihood that the attack will succeed and includes the notions of the challenge the attack presents to the attacker’s capabilities and the random nature of circumstances surrounding the attack [2]. The probability of success of an attack corresponds to the likelihood that the hacker will succeed in executing all the attack steps (given that they attempt the attack) in order to accomplish the attack objective [2]. The probability of detection measures the likelihood that a defender (e.g., intrusion detection system (IDS)/intrusion prevention system (IPS), firewall, etc.) will detect an attack. The probability of detection parameter measures the likelihood of any one of the attack steps comprising an attack being detected, but not affecting the probability of success of the attack [2]. An attack step presents a probability of detection.

**Notional attack model**

An attack model involves collecting system-related information and developing a baseline system description that allows the security analysis team to gain an understanding of what the system is and how it works [20]. System information may include hardware, software, system interfaces (e.g., internal and external connectivity), data and information processed/stored, data criticality (e.g., system’s organizational value), system architecture, network topology, users, management/operational/technical security controls, and physical and environmental security controls. When designing security into information systems, security engineers must be aware of the vulnerabilities in the system, the attacks that exploit those vulnerabilities, and the adversaries that can execute the attacks. This will support the risk determination on design alternatives based on the impact on security risks as well as the identification of the highest risk areas in the system and the associated cost of countermeasures to mitigate the risks identified.

Attack identification and analysis can be best accomplished as a collaborative effort between the system security engineers, attack analysts, and risk analysts. Data collection from formal threat models (e.g., attack trees) and computer network attacks (CNA) could be used to provide data for validating the model. Attack trees provide a logical representation of the steps that a hacker could take to complete an attack on the network/system in order to achieve a particular attack objective [20]. Developing attack trees is very productive in determining the cost for various types of cyber attacks and could be used to further decompose the attack steps [20]. Additionally, attack trees can also be used to generate monetary attack portfolios and are represented by various CNAs.

Computer network attacks data against an operational system would be obtained from various sources includes firewall logs, IDS/IPS systems, host-based prevention systems, antivirus logs, honeypots and/or honeynet systems. CNA attacks use networks as the primary vehicle for system attacks, allowing hackers to exploit vulnerabilities in network protocols, operating systems, or system applications to achieve attack objectives [21]. CNA techniques include stealing, corrupting, or destroying information resident on computers and computer networks or disrupting/denying access to the networks and systems themselves [21]. Most CNAs are very inexpensive, requiring only a personal computer and network access. Sophisticated CNAs are also very difficult to trace back to the source, making attribution very difficult and can be lethal weapons against modern information systems.
Most successful cyber attacks have three main attack steps: (1) gain access to the system, (2) escalate privileges, and (3) compromise the system or data confidentiality, integrity, and/or availability as necessary to achieve the attack objective [15][16]. Cyber attacks can then be characterized by an attack tree in terms of \( RE, P(s), \) and \( P(d) \). For example, let us consider a cyber attack against a supervisory control and data acquisition (SCADA) system (which has a data value determined by its senior leadership of $2.5 million on its servers) at an industrial control facility that utilizes a firewall for boundary protection and an IDS to monitor malicious activities. The main attack objective is the alter information in the SCADA system through four defined attack steps. Thus, the \( RE, P(s), \) and \( P(d) \) values for the attack steps for this notional cyber attack may be defined as follows:

\[
RE = RE_i
\]

Where:
\( RE \) = aggregate monetary resources expended of the attack
\( RE_i \) is the total \( RE \) required for each attack step that constitute the attack

The aggregation of probability of success is the product of \( P(s) \) of the individual attack steps divided by a 100% success rate [2]:

\[
P(s) = \prod_{i=1}^{n} P_i
\]

Where:
\( P(s) \) = probability that the attack will succeed
\( P_i \) = probability of success of attack step \( i \)
\( n \) = total number of attack steps in the attack

The aggregation of probability of detection is 1 minus the product of (1 − \( P(d) \)) of the individual attack step [2]:

\[
P(d) = 1 - \prod_{i=1}^{n} (1 - P_i)
\]

Where:
\( P(d) \) = probability that the attack will be detected
\( P_i \) = probability of success of attack step \( i \)

Therefore, the aggregation of the \( RE \) parameter is simply the sum of the \( RE \) of the individual attack steps that constitute an attack [2]:

\[
RE = \sum_{i=1}^{n} RE_i
\]

A hacker utility function represents a hacker’s preference for an attack with respect to a security parameter (e.g., intrusion detection system, antivirus software, etc.); the utility value ranges from 0 “least desirable” to 1 “most desirable” attack from a hacker’s perspective [2][16]. Each cyber attack has an associated utility function for each of the security parameters: \( RE, P(s), \) and \( P(d) \). After aggregating the scores with respect to \( RE, P(s), \) and \( P(d) \) for all attacks, a hacker utility curve should be defined to determine the utility value of the attack to each applicable hacker with respect to each security parameter (e.g., \( RE, P(s), P(d) \) ) [2][16]. For example, given a utility curve for sending an email with malicious code through the SCADA firewall with respect for a probability of success \( P(s) = 0.72 \), the utility of this attack step = .50. Using the utility curve for each of the security parameters, determine the utility of each attack for each applicable type of hacker. That is, for each system attack, determine \( U(RE_a), U[P(s)_a], \) and \( U[P(d)_a] \) for each applicable hacker [2]:

\[
U(RE_a) = \text{the hacker utility for attack } RE_a
\]

\[
U[P(s)_a] = \text{the hacker utility for attack } P(s)_a
\]

\[
U[P(d)_a] = \text{the hacker utility for attack } P(d)_a
\]

Using the notational attack step scores above, the aggregate attack scores for this four-step cyber attack are in table 2.

<table>
<thead>
<tr>
<th>ID</th>
<th>Attack Steps</th>
<th>RE</th>
<th>P(s)</th>
<th>P(d)</th>
<th>( P(s)_a )</th>
<th>( P(d)_a )</th>
<th>Total RE</th>
<th>Avg P(s)</th>
<th>Avg P(d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email malicious code through firewall</td>
<td>$0</td>
<td>72%</td>
<td>83%</td>
<td></td>
<td></td>
<td>$30,000</td>
<td>0.39</td>
<td>0.51</td>
</tr>
<tr>
<td>2</td>
<td>Send malware through firewall via web link</td>
<td>$30,000</td>
<td>44%</td>
<td>67%</td>
<td>0.36</td>
<td>0.30</td>
<td>0.39</td>
<td>0.51</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Gain write access to SCADA system</td>
<td>$500,000</td>
<td>27%</td>
<td>36%</td>
<td></td>
<td></td>
<td>0.72</td>
<td>0.51</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Write deceitful data</td>
<td>$0</td>
<td>12%</td>
<td>20%</td>
<td></td>
<td></td>
<td>0.39</td>
<td>0.51</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Notional example aggregate attack scores for SCADA cyber attack

Using the notational attack step scores above, the aggregate number of attack steps in the attack

\( n \) = total number of attack steps in the attack

A swing weight is used to identify the most important metric for a decision-maker and is assessed by assigning the most important metric an arbitrary value (e.g., 100) to determine the utility of each attack step with respect to each security parameter. That is, for each system attack, determine \( U(RE_a), U[P(s)_a], \) and \( U[P(d)_a] \) for each applicable hacker [2]:

<table>
<thead>
<tr>
<th>Attack Steps</th>
<th>Total RE</th>
<th>P(s)</th>
<th>P(d)</th>
<th>( U(RE_a) )</th>
<th>( U[P(s)_a] )</th>
<th>( U[P(d)_a] )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email malicious code through firewall</td>
<td>$30,000</td>
<td>0.39</td>
<td>0.51</td>
<td>1</td>
<td>0</td>
<td>.50</td>
</tr>
<tr>
<td>Send malware through firewall via web link</td>
<td>$30,000</td>
<td>0.39</td>
<td>0.51</td>
<td>1</td>
<td>0</td>
<td>.50</td>
</tr>
<tr>
<td>Gain write access to SCADA system</td>
<td>$500,000</td>
<td>0.72</td>
<td>0.51</td>
<td>0</td>
<td>0</td>
<td>.50</td>
</tr>
<tr>
<td>Write deceitful data</td>
<td>$0</td>
<td>0.39</td>
<td>0.51</td>
<td>0</td>
<td>0</td>
<td>.50</td>
</tr>
</tbody>
</table>

Table 3 – Notional example utility values for SCADA cyber attack

A swing weight is used to identify the most important metric for a decision-maker and is assessed by assigning the most important metric an arbitrary value (e.g., 100) to determine the utility of each attack step with respect to each security parameter.
a security risk [2][5]. Swing weights reflect the importance of one parameter over another based on the relative importance of the swing in value when going from the worst possible level for that security parameter to the best possible level [2][17]. These values are assigned one attribute for which the change (swing) from worst to best represents the largest impact for the cyber attack in terms of the overall objective—to alter information in the SCADA system. For this notional example, a decision-maker has determined the following swing weights base on an arbitrary value for this type of cyber attack against the SCADA system: $W_{RE} = .35$, $W_{p(s)} = .47$ and $W_{p(d)} = .18$. Therefore, calculate the attack utility ($AU_a$) of each attack to each hacker using the following formula [2]:

$$AU_a = W_{RE} \times U(RE_a) + W_{p(s)} \times U[p(s)_{a}] + W_{p(d)} \times U[p(d)_{a}]$$

Where:

- $AU_a$ = overall utility of attack $a$
- $W_{RE}$ = the hacker weight of $RE$ parameter
- $W_{p(s)}$ = the hacker weight of probability of success parameter
- $W_{p(d)}$ = the hacker weight of probability of detection parameter
- $U(RE_a)$ = the hacker value of attack $a$ with respect to the $RE$ required for the attack
- $U[p(s)_{a}]$ = the hacker value of attack $a$ with respect to the $p(s)$ required for the attack
- $U[p(d)_{a}]$ = the hacker value of attack $a$ with respect to the $p(d)$ required for the attack

Using the above example, the attack utilities are as follows:

<table>
<thead>
<tr>
<th>Attack Steps</th>
<th>$W_{RE}$</th>
<th>$W_{p(s)}$</th>
<th>$W_{p(d)}$</th>
<th>$U(RE_a)$</th>
<th>$U[p(s)_{a}]$</th>
<th>$U[p(d)_{a}]$</th>
<th>$AU_a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email malicious…</td>
<td>.35</td>
<td>.47</td>
<td>.18</td>
<td>1</td>
<td>0</td>
<td>.50</td>
<td>.44</td>
</tr>
<tr>
<td>Send malware…</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gain write access…</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write deceitful…</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The overall $AU$ is a function of the attack characteristics, hacker preferences, and impact. In this notional example, there is a 44 percent chance that a hacker would be successful in executing and performing this attack, investing $530,000 utilizing these attack steps undetected in this hypothetical environment. Given that the data has a value of $2.5$ million on its servers, a hacker may risk the investment of $530,000 given the medium average of detection. The $AU$ would provide system architects, engineers, and designers a metric to identify the most serious concerns to the baseline system with the higher attack utilities representing more preferred attacks. This type of mathematical model will help in finding the probability of a system being under cyber attack (e.g., denial-of-service, etc.), infection by any computer virus/malware, or a group of computer viruses at any time specifically dealing with the speed of breeding of the infection and the hacker injecting the malicious activity into the network [6][11].

However, this assumption may not be accurate depending on the time scale of a virus/malware diffusion process for a CPS system. For instance, in the context of computer viruses, the network of devices in nodes is constantly changing through technological improvements (e.g., wireless, IoT, etc.). Hence, a device-varying network model might be more appropriate, although more challenging, to analyze and devise. There is still a bit of work analyzing these types of device-varying models, which seems to be a promising new branch of research. Extensions to the cyber-attack defense modeling and defense methodologies are required to address cyber-physical attacks [8]. This model can be useful in designing defenses against malicious computer attacks and will help in carrying out analysis and verification by simulation.

**Conclusion**

The proposed model needs further research, development, testing, and implementation into an actual CPS environment. These forthcoming CPS/IoT architectures will be one of the most powerful platforms for computer networking. A wide range of communication networks, from a single local area network (LAN) to global satellite networks will enable modeling of all IoT network types and technologies and will possess a function of automatic malicious identity recognition. The CPS/IoT system should automatically recognize and verify the identities of “things/objects” that have gained random access to the CPS/IoT system; it should be able to distinguish whether the information that has entered the system is valid from legitimate sources or a potential hacker. The environment surrounding this new environment is extremely harsh and there are many factors posing tremendous threats to the validity of its architecture, which can seriously affect the functions of these forthcoming CPS/IoT systems.

**References**

About the Author
Dr. Tyson Brooks, Security+, CISSP, C|EH, C|NDA, CEA, CAS-ISM, PMP, ITIL v.3, works for the US Department of Defense and as an adjunct professor in the School of Information Studies (iSchool) at Syracuse University. Dr. Brooks has over 20 years of professional experience in the design, development, and production of secure information systems. He may be reached at ttbrooks@syr.edu, dr.tyson.brooks@ieee.org.

The Dangers in Perpetuating a Culture of Risk Acceptance

Continued from page 25

breach.15 Organizations should be very careful when accepting or downgrading the likelihood of an attack based on their sector, size, or other demographics.

Odds like 1 in 100,000,000 may seem a long shot, but given the global nature of many businesses and how connected everything is, there could be millions of potential attacks. In 2017, Facebook report two billion users.14 Even if .001 percent of those users are malicious, that equates to 20,000 potentially hostile actors.

There is also a predisposition to automatically assume that adequate planning simply wasn’t possible. Whenever there is a breach, the press release frequently includes the company mentioning that the breach was due to a "sophisticated attack." To individuals that do not work with information security many attacks may be sophisticated, but for those that do there are very few breaches that are truly sophisticated. An attack may leverage multiple vulnerabilities, for example a successful spear phishing attack that provides initial access to a laptop with a privilege escalation vulnerability, but most exploits occur from publicly disclosed vulnerabilities and zero-day exploits. It also should be noted there is a fair amount of research that shows phishing is still the most common attack vector and that all organizations, regardless of size, are subject to phishing attacks. Two examples of this research include Verizon's data breach investigations report15 and Google's research on how accounts are compromised.16

On size – It takes just one

Size can be a great advantage in business. Economies of scale help with many facets, but with information security it can often be a detriment. An organization with hundreds of thousands of employees on six continents has a much larger attack surface than an organization with ten employees down the street. One employee's mistake can result in huge losses for a large organization. It is very difficult to protect all employees and contractors from unknowingly visiting a vulnerable site that has been compromised with malware allowing for a drive-by attack.

On uncertainty – Consider the unknown unknowns

An organization can’t plan or mitigate every risk. People make mistakes, and given the nature and complexity of information technology, one small mistake can have big consequences. On a given day, a person may inadvertently send a communication to a large group, due to not recognizing a mistake in to whom or how the email is being sent. There have been reported cases of communications being sent to the wrong email list/group and individuals on marketing lists not being blind carbon copied (BCC) to protect their identity. Receiving email that was intended for someone else happens all the time. Sometimes it is inconsequential, but other times it can be a costly mistake.

The US Department of Health and Human Services Office for Civil Rights hosts a Breach Portal, which tracks breaches of unsecured protected health information (PHI) affecting 500 or more individuals.17 Healthcare breaches like that of Anthem are well known due to the number of affected individuals. However, there are many examples of healthcare related companies reporting lost hard drives, stolen computers, and email disclosures in the breach portal. Additionally, health care will continue to a prime target of ransomware, not only because of the sensitivity of the data, but the criticality of many systems.

One other item that is difficult to plan for is attack on a given protocol or standard. In 2017, weaknesses in Wi-Fi Protected Access II (WPA2) and Bluetooth were discovered. The WPA2 vulnerability could be exploited by a key-reinstallation attack (KRACK), while Bluetooth had flaws in the design that enabled potential man-in-the-middle (MitM) attacks.18 19 In 2018, Duo Security identified vulnerabilities in many SAML implementations.20

On compliance – Why it may not matter

Many compliance frameworks focus on what is in place and not so much why. Frameworks like PCI and FedRAMP often deal with in place or not, although areas to describe compensating controls exist. That said, just because an organization accepts a risk internally doesn't mean that is acceptable by a regulatory body, business partner, or government agency.

On the going concern – How perpetuation of risk acceptance occurs

Once a culture of greater risk acceptance is in motion, it will continue to stay in motion, that is until a breach occurs at which point things may change. Rarely does an organization change course unless something adverse happens directly. Occasionally, an event at a rival or industry peer may push

13 Brian Krebs, “4 Years After Target, the Little Guy is the Target,” (December 2017) - https://krebsonsecurity.com/2017/12/4-years-after-target-the-little-guy-is-the-target/.
an organization to look closer at their controls and risk tolerance, but more often than not organizations will find reasons why the same issue couldn’t happen to them.

One other way that a perpetuation of risk acceptance occurs is from hiring employees that come from another organization where excessive risk taking was standard. During an interview process it may be difficult to identify whether a candidate is hard-nosed and by the book, or someone who is more likely to go with the flow.

So, what next?

As shown above, this starts with culture. Any improvements to an organization’s risk posture starts with people who ask tough questions. If the leads within IT and security constantly have the “it won’t happen to us” attitude, there is a good chance it might.

Second, a risk assessment program is like any other piece of the business. Not only should the risks be evaluated yearly, but how those risks are discovered, documented, and evaluated should be assessed yearly as well. An organization can change a lot in one year, and what had been successful in the past may not be suitable for the present or future.

Additionally, organizations should review their practices for risk assessment. Examples of questions that may require modifications to a risk assessment program include:

- Are there new state or federal regulations that need to be addressed?
- Is there a new acquisition that needs to be evaluated?
- Has the competitive landscape changed?
- Have there been any security breaches within the last 12 months?
- What are the requirements for a new key customer?

Lastly, organizations should consider their own independence in risk assessment activities. While the IT security director may be the best technically qualified to assess risk, if he or she has too much influence over the control implementations, the results could be swayed. Not every organization has the luxury of a CISO that sits outside of IT and reports to legal or finance. In such cases, consider bringing a general counsel or CFO into the discussions. Outside advisors may help but are also a mixed bag as they lack ownership. Ultimately, a successful risk management program is driven by culture, and culture is set by its leaders.

About the Author

Matt Wilgus is the Security Practice Director at Schellman where he leads the firm’s threat and vulnerability related offerings. In this role, he continually works with clients to strike a balance between business, security, and compliance objectives. He may be reached at matt.wilgus@schellmanco.com.
More advanced users can define their own work flows. In our implementation, work flows can consist of dialog boxes and actions: first, set up the security policy automation tool for DDS and tcpdump imports (including policy building blocks, data selection templates, policy templates, etc.) and import those data sources; then generate subsets of the imported data for whitelisting; finally, generate and download technical rules and configurations (figure 5).

DDS information is captured on the running system using a DDS discovery dump tool that essentially listens to all DDS discovery traffic and generates an XML file with information about all participants (including IP address), which topics they publish/subscribe, and (where known) on which ports (figure 6).

At the same time, network traffic is captured using tcpdump. In this example, both files are simply uploaded using drag-and-drop file uploaders (automatic detection and importing is an alternative, which would be preferable in more dynamic environments).

In general, the more data sources the security policy automation can tap into, the more detailed the “as is” picture gets—example information sources include network equipment and directory/IAM systems.

The imported information is then analyzed and merged automatically. For example, particular IP:port → IP:port network traffic is tagged information indicating matching DDS topic information flows (Side note: this is not as trivial as it sounds because DDS uses random ports for publishers).

The next step of this example involves calculating/selecting relevant subsets of the imported information. In this simple example, assume we are interested in whitelisting all DDS traffic that actually convey application information (as opposed to discovery and other network “chatter”). The initial setup work flow step already set up numerous useful subsets. The calculated results can be visualized (figure 7).

Now that the data is imported and selected, it can be used in security policies. For example, a simple, generic policy (automatically set up as a default good practice policy) is to only allow all DDS traffic that actually convey application information. This minimizes lateral attacker movement if a system gets compromised. As shown in figure 8, policies include wildcards (“*”), which can be linked to the selected datasets (or the system can infer which dataset is applicable).

It is also possible to reuse (import) already existing policies, for example, from firewalls, IAM systems, XACML deployments, etc.

The next step then calculates the matching “low-level policies” – technical policies in a generic syntactic representation. Exporters take that information and turn it into the specific syntactic output required for actual enforcement, in our example just DDS security and host firewalls (figures 9 and 10).

In our implementation, these files can be simply downloaded from the web interface to be manually installed by the security professional. For a more integrated experience, automated configuration is of course possible using scripts and APIs.
The more exporters are supported by the security policy automation solution, the more pervasive defense in depth can be achieved “at the click of a button” (e.g., network, host OS, middleware, application, databases, etc.).

Some security policy automation solutions often also come with their own decisioning/enforcement agents, for example XACML PDPs automated network configuration software agents and SDKs for developers to call. To prove this point during our research (and somewhat redundant), our example implementation also generates internal configurations for enforcement on the DDS layer and using our security policy automation solution’s own decision/enforcement agent. The implementation also includes an automated network security enforcement agent, which interfaces with network tools (e.g., iptables and tcpdump) to allow push-button traffic capture and enforcement.

This simple example was successfully implemented and tested using a 15-node interconnected DDS application. Note that this only illustrates one security policy automation example (using wildcards based on subsets of imported traffic, and only for host firewalls and DDS). Security policy automation often includes many more features to get from authored generic policies to specific technical implementations in many places. We just focused on a particularly intuitive/simple use case for illustrative purposes.

**Conclusion**

This article explains why medical device landscapes need better security, and why traditional approaches are insufficient. We describe how a security policy automation “umbrella” with workflow automation and prebuilt templates can seamlessly provide the necessary security to enable these interconnected cyber-physical devices to securely operate within hospitals.

Interestingly, while this article focuses mostly on the technical challenges and solutions, we also tackled several non-technical challenges over the course of our research efforts. First, it was difficult to determine policies that should be enforced. While hospitals broadly follow established business processes (especially at the lower echelons), it is not obvious which processes are firm enough to inform security policies. For...
example, is it realistic to restrict access to a patient record to staff that are not badged into the same building as the patient? Nurses may move around between buildings and may need to look up records in another building before attending to a patient. Even without firm access enforcement, rich access policies can still be useful to implement HIPAA “break the glass” procedures where suspicious or unauthorized access is granted, but needs to be documented/justified. Security policy automation should be used for this as well. Second, hospitals do not have large IT departments and IT budgets, so any successful security solution needs to be as seamless and transparent as possible. Also, legacy devices need to be supported (our ICE implementation uses dongles as wrappers).

In summary, a security policy automation “umbrella” solution can be used to improve medical device cybersecurity. It will provide more dynamic, fine-grained, comprehensive, and manageable access control, which minimizes the risk of lateral attacker movement and ensures HIPAA’s “minimum necessary” requirement (access for the right information/devices/people/context only) is met. While this article did not cover user access control due to the specific demo scenario, our security policy automation solution has interfaced with IAM deployments in the past (this is actually one of the better-understood access control layers).

Our approach helps implement powerful technical security policies for users, devices, and applications, while at the same time reducing policy management efforts. The automated process is consistent, testable, documented, robust, and repeatable. The industry needs to move this way. We cannot manually manage technical policies for cyber-physical IoT—it is simply too dangerous.

Acknowledgements

This work is supported by the US Army Medical Research and Materiel Command under contract no. W81XWH-16-C-0175 (RTI, Inc.), and by the National Institute of Standards and Technology (NIST) under grant no. 70NANB16H192 (ObjectSecurity LLC). Also thanks to Paul Pazandak, PhD, Director of Research, Real-Time Innovations, Inc. for comments and edits.

—Data-Distribution Service (http://www.omg.org/dds/)
—ObjectSecurity (https://objectsecurity.com/)
—OpenICE (https://www.openice.info/)

References

8. This OpenPMF Security Policy Auditor tool was developed as part of another SBIR for NIST and is based on NIST Special Publication 800-192: “Verification and Test Methods for Access Control Policies/Models, NIST (June 2017) – https://www.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf.

About the author

Dr. Ulrich Lang (ObjectSecurity CEO, co-founder) received his PhD from the University of Cambridge Computer Laboratory (Security Group) on conceptual aspects of middleware security in 2003, after having completed a Master’s Degree in Information Security (Royal Holloway, University of London) in 1997. Ulrich is a renowned thought leader in cybersecurity, privacy, and data analytics/AI and is on the Board of Directors of the Cloud Security Alliance (Silicon Valley Chapter). He may be reached at ulrich.lang@objectsecurity.com.
ISSA CISO Executive Membership Program

The role of information security executive continues to be defined and redefined as the integration of business and technology as it evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will shape the profession.

The Information Systems Security Association (ISSA) recognizes this need and created the exclusive CISO Executive Membership program to give executives an environment to achieve mutual success. Connecting professionals to a large network of peers, valuable information, and top industry experts the program is a functional resource for members to advance personal and industry understanding of critical issues in information security.

Membership Benefits

- Free registration at four CISO Executive Forums per year, including lodging for one nigh and all meals at each Forum
- Extensive networking opportunities with peers and experts on an on-going basis
- Privileged access to online community
- Direct access to top subject matter experts through educational seminars
- An effective forum for understanding and influencing relevant standards and legislation
- A unified voice to influence industry vendors
- Basic Wisegate membership, including exclusive access to the Wisegate community and ISSA CISO Forum private group

Visit ISSA.org => Learn => CISO Executive Forum for more information or to register for the Forum.

ISSA Chapters around the Globe

**Asia Pacific**
- Bangladesh
- Chennai
- Philippines
- Dehradun
- India

**Canada**
- Alberta
- Vancouver
- Ottawa
- Toronto
- Quebec City

**Europe**
- Brussels
- France
- Germany
- Ireland
- Italy
- Netherlands
- Poland
- Romania
- Spain
- Switzerland
- Turkey
- UK
- Ukraine

**Latin America**
- Argentina

**USA**
- Alamo
- Blue Ridge
- Boise
- Buffalo Niagara
- Capitol of Texas
- Central Alabama
- Central Florida
- Central Indiana
- Central Maryland
- Central New York
- Central Ohio
- Central Pennsylvania
- Central Plains
- Central Texas
- Central Virginia
- Charlotte Metro
- Chattanooga
- Chicago
- Colorado Springs
- Columbus
- Connecticut
- Dayton
- Delaware Valley
- Denver
- Des Moines
- Eastern Idaho
- East Tennessee
- Fort Bragg Fayetteville
- Fort Worth
- Grand Rapids
- Greater Augusta
- Greater Cincinnati
- Greater Spokane
- Hampton Roads
- Hawaii
- Inland Empire
- Kansas City
- Kentuckiana
- Kern County
- Lansing
- Las Vegas
- Los Angeles
- Melbourne, FL
- Memphs
- Metro Atlanta
- Middle Tennessee
- Milwaukee
- Minnesota
- Motor City
- National Capital (DC)
- New England
- New Hampshire
- New Jersey
- New York Metro
- North Alabama
- North Dakota
- North Oakland
- North Texas
- Northeast Florida
- Northeast Indiana
- Northeast Ohio
- Northern Colorado
- Northern New Mexico
- Northern Virginia
- Northwest Arkansas
- Oklahoma
- Oklahoma City
- Orange County
- Phoenix
- Pittsburgh
- Portland Oregon
- Puerto Rico
- Puget Sound
- Quantico
- Rainer
- Raleigh
- Rochester
- Sacramento Valley
- San Diego
- San Francisco Bay Area
- SC Charleston
- SC Upstate SC
- Silicon Valley
- South Bend
- Southeast Arizona
- South Florida
- South Texas
- Southern Tier of NY
- St. Louis
- Tampa Bay
- Texas Coastal Bend
- Texas Gulf Coast
- Triad of NC
- Tucson
- Utah
- Ventura County
- West Texas
- Yorktown
The Information Systems Security Organization’s seventh annual flagship conference is a world-class event bringing together cyber, information, software, and infrastructure security professionals from 92 countries around the world. The two-day conference delivers practical sessions and no-nonsense insights that give cybersecurity professionals the tools to strengthen their security without restricting their business.

**Conference Highlights**

- 800+ attendees spanning all levels of IT and InfoSec
- Six education tracks totaling 40+ sessions
- Expert keynote program on the latest information security trends and technologies
- Intimate roundtables and panel discussions
- Expo floor featuring more than 35 leading technology companies
- Networking lunches, general sessions, and evening receptions and award parties
- Career center

**Topics**

- Emerging technologies (with real-world applications)
- Application security
- Business skills
- Cloud security
- Digital forensics
- APT defense
- Mobile devices and BYOD
- Incident response

Registration opens soon. For more information, visit www.issa.org