Innovation Against Cyberattacks

With the challenges of securing cyberspace, there has been a great deal of innovation throughout the past decade, especially in the last couple of years. However, the multitude of attacks and their increasing sophistication is going to require even more innovation for the foreseeable future. The good news is that these innovations are expected to be achievable. The question is, will they be able to keep up with innovations being used in cyberattacks?

A History Lesson

Great challenges foster an environment for creativity and innovation. For instance, on 25 May 1961, then US President John F. Kennedy told the US Congress that the United States would embark on a goal to have the first human set foot on the moon before the end of the decade. On 29 July 1969, Neil Armstrong accomplished that goal.[1]

That goal led to a flurry of scientific and industrial research over those eight years that would have been unthinkable without such a lofty challenge. Oftentimes, the greatest innovation comes in the face of the greatest challenges. Cybersecurity is a great challenge before us.

Use of Artificial Intelligence

I was discussing the security posture of a major cloud vendor, and the engineer I was talking with discussed how their components worked today, as opposed to in the past. One of the things he said had completely changed "the game" was the use of artificial intelligence (AI) to spot patterns and detect where rules and protections needed to change. These changes are being made at a rate that would have been unimaginable a few years ago. For instance, Microsoft recently published a defense report about how cyberattacks are changing. The report cites a staggering 24 trillion daily security signals.[2] Microsoft processes that many signals across their cloud (Azure and Office365), endpoints and intelligent edge.

Traditional data-mining techniques outside of AI/machine learning (ML) simply are not effective for handling this vast amount of data. From this data come the rules and mechanisms needed to protect systems and networks. These are deployed in an automated fashion. While I am citing a Microsoft report, Microsoft is not alone in embracing this technology. Every major vendor has done so. There are simply too many signals to handle by anything less than using AI. The attacks are evolving too quickly and on too great a scale to defend manually. Therefore, AI plus automation is driving defenses.

Internet of Things Security

Smart home technology dates back longer than most would think. The first smart device for the home debuted between 1966 and 1967: the ECHO IV. It never was sold commercially but performed some of the tasks smart devices are known for today, such as controlling the thermostat and turning appliances on and off.[3]

More recently, there has been an explosion of smart devices, and these devices are often connected to the Internet in some way, hence the moniker the Internet of Things (IoT). The issue becomes how to keep these devices secure, especially in the face of new threats, while still allowing them to provide the functionality for which they were intended. This is not an easy task, as widely used libraries, insecure protocol implementations and flat-out bad security practices implemented to deliver solutions to market have led organizations to research how to better secure IoT devices.

Enterprises still lag far behind where they need to be, as was made evident when Mandiant disclosed a vulnerability that was estimated to affect 83 million

K. BRIAN KELLEY | CISA, CDPSE, CSPO, MCSE, SECURITY+

Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions, including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

or more devices.[4] One of the issues is tracking how many devices are vulnerable, and more important, knowing how to update them. Mandiant released frequently asked questions (FAQs) information, which indicated that it could not generate a comprehensive list of affected devices.

From an inventory management perspective, that is not the news one wants to hear. Potentially vulnerable devices could exist on a network, unbeknownst to the enterprise. While Mandiant published the technical details needed to determine what devices were affected, to evaluate devices, information about how and what the devices implement must be available. That is not something consumers expect to have to do with a smart light bulb.

IoT changes the way security must be approached and, along with that, IS auditing of this technology. The US National Institute of Standards and Technology (NIST) has outlined three ways in which IoT is different from traditional technologies:

1. IoT devices interact with the physical world.
2. IoT devices are often black boxes to which agents and other security controls cannot be loaded.
3. IoT devices often lack logging and update support.[5]

"Whether IoT devices are being used in the home or in manufacturing plants, understanding how IoT devices can leave people and systems vulnerable is critical."

While NIST has also identified goals for managing IoT security risk areas, it also states that these goals "can be difficult to achieve with currently available IoT products."[6] IoT is not going away. Whether IoT devices are being used in the home or in manufacturing plants, understanding how IoT devices can leave people and systems vulnerable is critical. Also, this field, much like cloud computing in general, is ever evolving. Auditors need to keep up with the changes. What is true today may not be true in two months.

Passwordless Technologies

I hate passwords. It has reached a point where no one can remember all the passwords created for various logins. That is, if one can even remember their username. Password managers are key to managing this unexpected "sprawl," at least in a relatively secure manner. The reality is that if one has ever accessed a site that has changed its URL for login, especially if the site adopts a new identity provider, a password manager may not match one's login information with the new URL. This is a frustrating experience. Too many passwords that users have to keep changing, combined with tools that cannot always keep pace with the changes to locations where passwords are needed, equals people choosing weaker methods to secure their logins. Given these and other weaknesses, we have reached a point where we need an effective alternative for passwords.

Several key systems have been using passwordless technologies for some time. A different name for them is "frictionless."[7] For instance, with PayPal, a user can initiate a payment from a recognized device without the need to specify a password back to PayPal. Netflix has supported registering a device using a code for years, though that does require users to have initially logged in to Netflix using a browser where a password is required. More recently, Microsoft has announced that passwordless technology is coming for Microsoft accounts.[8] We are entering an era when users will use something other than passwords to verify identities. As long as a system is not put in place where we speak our name and then, "My voice is my password/passport. Verify me," I think we will be fine.[9]

Expect More Research, More Innovation

Given the cyberattacks that have been publicized, especially ones involving supply chain, healthcare, government and energy, we should expect a significant amount of research to be devoted to detecting and stopping these attacks. These attacks will lead to new innovations, which will likely require a change in operations and also in auditing techniques. For instance, looking at how AI is being used to form defenses, it would be impractical to audit every change. Instead, the process, the validity of the rules and the ability to tamper with the overall process are what is being audited. Given the speed at which cyberattacks are evolving, we should expect changes to the way assets and organizations are protected to increase in velocity, too.

LOOKING FOR MORE?

- Read *Emerging Tech: IoT Fundamentals Study Guide.* *www.isaca.org/emerging-tech-iot*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

1 Kennedy, John F.; 1961, "The Decision to Go to the Moon," Joint Session of US Congress, Washington DC, USA, 25 May 1961, *https://history.nasa.gov/moondec.html*

2 Hogan-Burney, A.; "How Cyberattacks Are Changing According to New Microsoft Digital Defense Report," Microsoft, 11 October 2021, *https://www.microsoft.com/security/blog/2021/10/11/how-cyberattacks-are-changing-according-to-new-microsoft-digital-defense-report/*

3 Hendricks, D.; "The History of Smart Homes," IoT Evolution, 22 April 2014, *https://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm*

4 Valletta, J.; E. Barzdukas; D. Franke; "Mandiant Discloses Critical Vulnerability Affecting Millions of IoT Devices," *FireEye*, 17 August 2021, *https://www.fireeye.com/blog/threat-research/2021/08/mandiant-discloses-critical-vulnerability-affecting-iot-devices.html*

5 Cuthill, B.; "Whether You Build Them or Buy Them—IoT Device Security Concerns Us All," National Institute of Standards and Technology (NIST) Manufacturing Innovation Blog, 15 April 2021, *https://www.nist.gov/blogs/manufacturing-innovation-blog/whether-you-build-them-or-buy-them-iot-device-security-concerns*

6 *Ibid.*

7 Malik, Z.; "Apple, PayPal, And Frictionless (Passwordless) Login Experiences," *Medium*, 19 Feb 2020, *https://medium.com/@nyczain/apple-paypal-and-frictionless-passwordless-login-experiences-a58c42009dad*

8 Jakkal, V.; "The Passwordless Future Is Here for Your Microsoft Account," Microsoft, 15 September 2021, *https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/*

9 Robison, Phil Alden; director, Sneakers, 1992, Universal Pictures, Universal City, California, USA