By Lara L. Sowinski

CYBERSECURITY IN — *Chasing the Threat*

Navigate the vast and dynamic technology and information landscape

To fully appreciate how important cybersecurity is to keeping the world's industrial, transportation, communications, and energy systems secure and functioning, consider the vast array of devices and networks that have been hacked.

In a 2017 *Forbes* article, Cesar Cerrudo, a professional hacker and the CTO of IOActive Labs, said that "most technology is vulnerable and can be hacked." His list of examples include: automobiles, a popular U.S. smart home alarm system, implantable medical devices like pacemakers, aircraft systems, critical infrastructure like power grids and dams, mobile banking apps, smart city technology, and a traffic system in Washington, D.C., which he personally hacked.

This presents a sobering landscape for engineers whose job it is to design mission-critical systems and products that support an integrated global economy highly dependent on technology, while simultaneously assuring public safety and security.

TRANSFORMATIONS DRIVING SECURE ACCESS

There are four primary transformations shaping this landscape, notes Jeff Wilson, research director, information & communications technology at IHS Markit. [see Fig. 1]

The first is device proliferation. There are an increasing number of devices that are connecting to networks and the Internet. In turn, "the Internet of Things (IoT) fundamentally changes how you have to think about developing cybersecurity solutions," says Wilson. "As the number of end points and potential end points connected to the Internet has gone from thousands to billions and trillions, the scope of potential attacks has likewise increased exponentially."

He cites the Mirai botnet distributed denial of service (DDoS) attacks of 2016 as an example. Simply put, these types of attacks are designed to overwhelm a resource, such as a network, and make it stop working. "This was not something that we ever needed to worry about in the past," Wilson notes.

Secondly, while new architectures such as cloud technology offer significant benefits in terms of scalability, "the cloud also has major implications for security," he says. For this reason, there are certain regulated industries that will not allow customer data to reside on the cloud. "The way you buy into point security completely changes when it's not a physical resource that you own and control on your site, but is an amorphous resource out in the Internet somewhere."

Companies and organizations that want to take advantage of cloud technology are wrestling with how to deploy security, acknowledges Wilson. "Everybody from engineering teams to product management teams

PRODUCT DESIGN

are architecting new solutions that can deal with IoT scale and work in cloud environments, but it is a huge engineering challenge."

At the same time, the accumulation of multiple security suites, platforms and fabrics over time contributes to cybersecurity challenges, he adds.

"Over the past 20-plus years there has been a buildup of a multi-product, multi-vendor and multi-solution unconnected product environment." In response, companies and organizations are working to reduce the number of cybersecurity vendors and products in their arsenal. Likewise, "engineering and product design teams are looking at how to build platforms that are extensible instead of building single, standalone solutions that solve single, stand-alone problems," because, "security doesn't work that way," says Wilson. "Most of the big attacks that you hear about have multiple vectors that patch different solutions that don't talk to each other."

Banks, retailers, and health care providers are among the variety of commercial enterprises that have been hit by cyberattacks. The cyberattack on Target Corporation in December 2013 ranks as one of the largest data breaches ever reported. According to the Consumer Bankers Association and the Credit Union National Association, the attack cost the retailer $148 million and cost financial institutions $200 million. Target's profits fell 46 percent in the fourth quarter of 2013, while the company's reputation also took a long-lasting hit.

According to Wilson, the cyberattack started with a phishing email to a Target contractor who was involved with the point-of-sale (POS) systems. Once the contractor gave up his credentials, the cyberattackers were able to get a foothold in the Target network and install malicious software on the POS systems.

"This phishing attack was one vector on one company," explains Wilson. The attackers were able to further penetrate Target's systems because the company either did not see, or ignored, alerts that were generated along other points. Three different security solutions in all detected something out of the ordinary, but none of them could talk to each other, Wilson says. This clearly illustrates why companies first need to "slim down the number of platforms they have and make sure the ones they do have are talking to each other," advises Wilson.

EVERYBODY FROM ENGINEERING TEAMS TO PRODUCT MANAGEMENT TEAMS ARE ARCHITECTING NEW SOLUTIONS THAT CAN DEAL WITH IOT SCALE AND WORK IN CLOUD ENVIRONMENTS, BUT IT IS A HUGE ENGINEERING CHALLENGE.

— JEFF WILSON, IHS MARKIT

Yet, this also presents a difficult challenge. Vendors that do not necessarily work together are being asked to share information or open up APIs or protocols so that solutions can share information.

"Therefore, getting down to a much more rational set of solutions that can communicate with each other to cover all the holes in between attacks is the third major driver that affects development and employment of commercial cybersecurity solutions," says Wilson. "This is what really sets cybersecurity apart from everything else," he continues. "For instance, when you are building a new Ethernet switch or new networking

product, you're typically fighting against the math, physics or something tangible. But when it comes to cybersecurity, you are developing against human ingenuity. In other words, the attackers are always one step ahead of the people who are looking to stop them."

This leads to the fourth primary transformation driving secure access, which is evolving threats, or stopping the attack that you don't know about yet, and the Mirai botnet attack is a perfect example, says Wilson. Furthermore, it's also why technologies such as machine learning and behavioral analytics are increasingly folded into security solutions as a way to better predict the unknowable future.

TWO PARALLEL PROCESSES FOR DESIGN

Wilson sees two parallel processes coexisting in the engineering community when it comes to designing for the new paradigm—system architecture and threat detection/mitigation—and both camps are required to work together closely.

System architecture essentially covers "what you need to think about and do in order to build things like firewalls, routers or switches," says Wilson. "However, what is unique about security and system architecture is that a lot of what you have to do is very processor-intensive."

He gives the example of a .pdf file embedded with malicious code. While a system may correctly identify it as an attack, the real challenge comes down to how quickly the system can make the identification and execute a subsequent response, which requires a "super high-performance system architecture."

CYBERSECURITY INNOVATIONS AND TECHNOLOGIES MOVE AT A LIGHTNING PACE, AND STAYING ON TOP OF THE LATEST TRENDS AND DEVELOPMENTS IS NOT AN EASY TASK FOR THE ENGINEERING COMMUNITY.

Meanwhile, engineers working on the threat detection and mitigation side of cybersecurity have a number of industry resources where information and intelligence can be gleaned.

The first are threat-sharing information consortiums such as the Cyber Threat Alliance (CTA), which includes founding members Fortinet, Intel Security, Palo Alto Networks, Symantec, Check Point, and Cisco. Member companies share information about threats and the technologies they are developing, such as new signatures, to combat cyberattacks.

In addition, there is an entire "shadow world of threat intelligence that happens on a very loose level between the vendors, governments and others," says Wilson. "People involved in critical infrastructure, like running a water treatment plant or making sure trains run on time," are examples of those who exchange information in this manner.

Next are subgroups, he says. These are commonly industry-oriented groups, e.g., people in the oil refinery sector, for instance, and governments share relative cybersecurity information with these subgroups.

Lastly, there are commercial solutions such as those offered by McAfee and Trend Micro. These and similar companies have their own teams of "white hat" hackers who actively target so-called "black hat" hackers in order to understand the latest threats.

TAPPING INTO A VARIETY OF INFORMATION RESOURCES

Cybersecurity innovations and technologies move at a lightning pace, and staying on top of the latest trends and developments is not an easy task for the engineering community.

Steve Noth, director, standards products and content, IHS Markit, notes that there are a variety of information sources, all of which have their pros and cons.

"Standards can take two to three years to write in a committee structure. The process includes working to gain consensus through balloting and making sure it's an open process," says Noth. It is a time-intensive process that yields standards and codes for basic technologies and processes like network architectures and structural network protections.

Another source of information are journal articles and other more timely

THE CYBERSECURITY INFORMATION LANDSCAPE

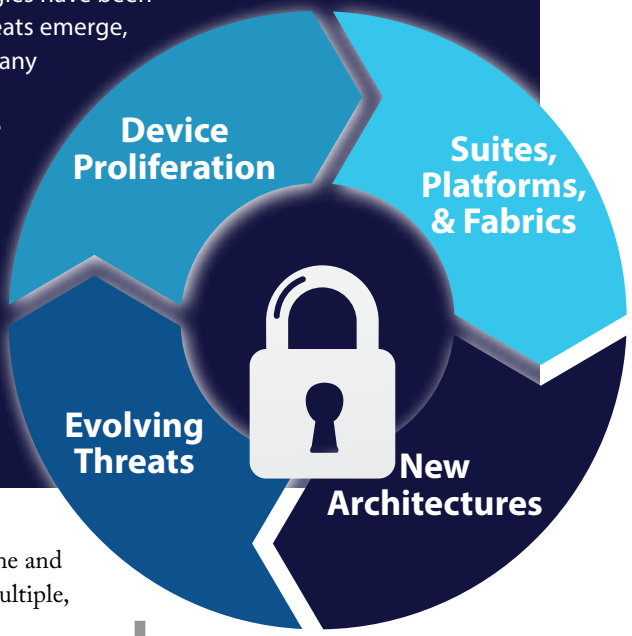
'BLEEDING EDGE'
(Buyer Beware)
current but often unvetted sources such as blogs, online forums, vendor materials, and conference proceedings.

'LEADING EDGE'
(Peer Reviewed)
books, pamphlets, articles, and periodicals, written relatively quickly that encompass developments in the past year or months, but with some level of vetting and peer review.

'TRUSTED BUT LAGGING'
(Consensus Developed)
trusted and fully vetted Standards, Codes, Regulations that might take years to develop and release.

TRANSFORMATIONS DRIVING SECURE ACCESS

- **DEVICE PROLIFERATION.** Smartphones, tablets, M2M, IoT, and IoE drive fundamental changes in how, where, and why security technology is deployed. There are security solutions for every part of the device chain: hardware, software, and network. More devices mean more traffic on the network and more need for network visibility.
- **NEW ARCHITECTURES.** Security technology isn't evolving in a bubble; it's tied to network architectures, and the emergence of virtualization, SDN/NFV, and cloud services. These drive significant changes in IT infrastructure and network architectures, and these changes have a major impact on how security technology is consumed.
- **SUITES, PLATFORMS, AND FABRICS.** Defense tools and strategies have been built over time, layering new technology on top of old as new threats emerge, leaving most companies with a complicated infrastructure with many holes. Everyone from the smallest business to the largest carrier is trying to collapse defense layers and simplify security architecture and protection to make it more effective.
- **EVOLVING THREATS.** Security technology innovation is driven by changes in the threat landscape, which is ever-changing. Security technology solutions have to be engineered to defeat human ingenuity, not physics or math, and as a result there is a cyclical pattern of threat protection technology development. New threats emerge, new technologies are built to combat those threats, those technologies are absorbed into larger platforms, and the process repeats infinitely.



publications and periodicals.

For example, "There are books and pamphlets being written relatively quickly that encompass developments in the past year or months. They provide a more real-time sense of what's going on," says Noth. These types of publications are typically peer reviewed as well.

Meanwhile, the most leading-edge information, albeit least vetted, comes in the form of blogs, online forums, conferences and other industry gatherings. With this information, "you always have to consider your source and how much trust you are willing to put into it," Noth cautions.

This leading-edge information can provide engineers with "hints about where to go and how to approach things. But it requires engineers to perform their own validation," he says. "It definitely falls under the 'buyer beware' category."

Organizing and centralizing these various sources and kinds of information into "knowledge bases" is equally important for the engineering community, which continually looks for solutions that can streamline and optimize their search across multiple, disparate sources.

The Engineering Workbench solution from IHS Markit (ihs.com/ewb) is an example of a cloud-based/SaaS tool that can be customized to access subscription libraries, such as those for standards or technical reference content, along with internal content and/or disparate sources from the Internet.

According to Noth, Engineering Workbench has the potential to index information, particularly the leading-edge information, for engineers to access quickly. In the future, he envisions expanded capabilities that would allow a subscriber to create of custom index of sources.

"Imagine a company that identifies various clearing houses of information, or a couple of really valuable and trustworthy forums. They believe these sources are well managed with good information," says Noth. "A custom index could support the creation of these powerful types of knowledge bases."