the u-blox technology magazine

No. 9
May 2020

IoT Security

ublox

Imprint

u - the u-blox technology magazine
Published by: Thomas Seiler
Chief Editor: Sven Etzold
Senior Editor: Natacha Seitz
Writer: Jan Overney
Graphic Design: Klaus Erlinghagen, Marina Sancho Vila
Circulation: 20'000, bi-annual
Contact: info@u-blox.com

Contributors: Michael Ammann, Kent Baker, Rudolf Baumeister (holoride), Stefan Berggren, Sabrina Bochen, Ludger Boeggering, Juan Cruz Moroni Funes (GSMA), Agnès Derderian, Alex Diekmann, Patty Felts, Paul Gough, Diego Grassi, Patrick Hauert (Kudelski), Eric Heiser, André Kudelski (Kudelski), Davide Lenzarini, Thomas Nigg, Daniel Profendiner (holoride), Alberto Sampino, Natalie Sandmann (holoride), Christopher Schouten (Kudelski), Thomas Seiler, David Shriqui (Davidshriqui.ch), Giovanni Solito, Pelle Svensson, Hari Vigneswaran, Ousmane Yatera (GSMA), Matej Zachar

Dear Readers,

The global spread of the COVID-19 pandemic has forced many individuals, businesses, and entire countries to leave their comfort zones and explore new ways of working. As a result, reliable and secure connectivity has become more essential than ever, to keep workers online, safeguard corporate IP, and protect national sovereignty.

That's why it's fitting that this ninth edition of "u" focuses on IoT security and the measures it requires. These include developing devices that are secure by design, enabling robust end-to-end security, and consistently applying good cyber-hygiene practices. In the following pages, you will find out how hackers are constantly finding new ways to weaponize the IoT and monetize their activities, and learn what you can do to implement security that meets the IoT's unique needs.

But what is IoT security? And why should companies invest in it? Our expert interview with Patrick Hauert, VP and Head of IoT at Kudelski Group, explores what companies can do to protect their customers and their businesses from cyberattacks. Few companies possess the broad-ranging and deep skills required to secure IoT applications from scratch, making working with the right partners essential to stand out from the crowd, strengthen brand reputation, and accrue an increasingly vital asset: trust.

The future is uncertain. But amid the uncertainty, there is no doubt that as connected technologies penetrate deeper and deeper into every aspect of our lives, the importance of IoT security will not cease to grow.

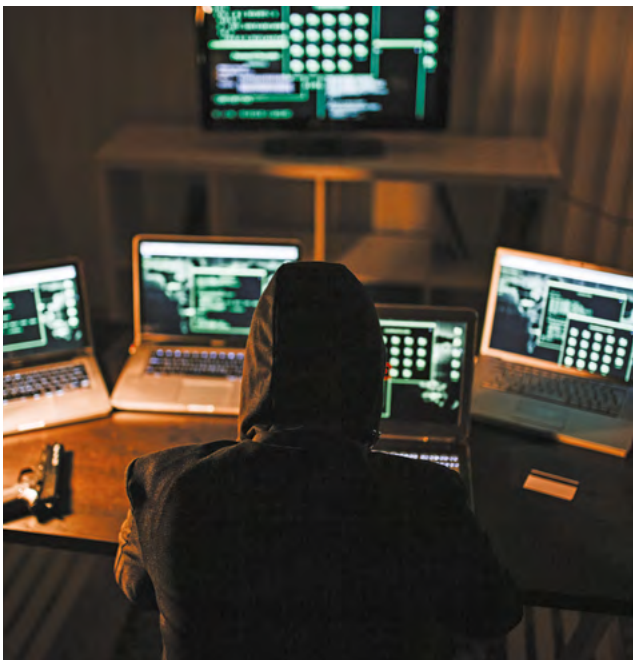
We wish you an insightful and enjoyable read.

Yours sincerely,

Thomas Seiler, CEO

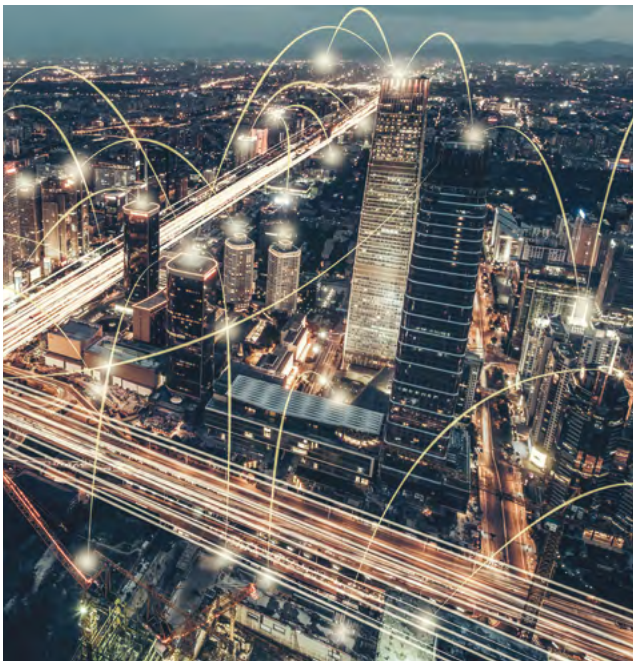
Content

7 It's time to get serious about IoT security



18 Minimal resources - maximum security

22 In the IoT, there is no safety without security



36 Innovation on all fronts

42 Discussing IoT security with…

It's time to get serious about IoT security

The future will be digital. Building out security on the Internet of Things will be vital to making our connected future a positive, fair, and sustainable one.

In the twelve seconds it takes you to read this sentence, around 1000 new devices will have connected to the internet, opening the doors to countless new applications that promise to make our lives, our cities, and our businesses better.[1] But it isn't all good news. In the 40 seconds you'll need to read this paragraph, Russian antivirus vendor Kaspersky's honeypots will have detected an estimated 270 attacks on IoT devices.[2] And in the roughly twelve minutes you'll spend on this article, skilled hackers recruiting a freshly connected IoT device into their botnet could do so not once, but twice.[3] Because the IoT bridges the virtual and physical worlds, their nefarious activities could well extend into your business, your home, or your body.

By connecting devices equipped with sensors or actuators to the cloud and leveraging powerful Big Data analytics algorithms, the IoT is already transforming every aspect of our lives, our society, and our economy. Adding cloud connectivity to previously disconnected devices – watches, phones, televisions, refrigerators, and coffee machines – is delivering services that dramatically increase our comfort and convenience.

Continuously monitoring ourselves and our environments and analyzing the gathered data for anomalies is offering new ways to improve our health and our physical safety. Automatically monitoring supply chains, production processes, and product quality is transforming the productivity of our businesses. And the new communication channel between businesses and their fielded devices is creating new, lucrative business models. By 2024, the global IoT is expected to represent a US$ 6.5 trillion market.[4]

---

[1] Estimated from https://iot-analytics.com/iot-2019-in-review/ and https://iot-analytics.com/iot-2018-in-review/
[2] https://www.infosecurity-magazine.com/news/over-100-million-iot-attacks/
[3] https://www.theregister.co.uk/2016/10/17/iot_device_exploitation/
[4] https://www.energiasmarketresearch.com/global-internet-of-things-iot-market-size/

But the vast space generated by the IoT is also a lucrative playground for hackers of all stripes. Incentivized by new (and less new) monetization models, from industrial espionage and extortion to the more recent disciplines of ransomware, smart meter tampering, and cybercrime-as-a-service, novice script kids, advanced hacktivists, professional cybercriminals, organized crime rings, and nation states can hone their skills, amass wealth (typically in cryptocurrencies), and even exert their influence on global geopolitics.

Cyberattacks targeting the IoT cost the US economy alone an estimated US$ 8.8 billion per year.[5] And that number is poised to grow. As the IoT is penetrating deeper into sensitive and critical applications including medical devices and the power grid, the damage malicious actors can inflict is also increasing. This has not gone unnoticed by business leaders, many of whom strongly feel that security concerns have discouraged them from pursuing an IoT strategy.[6]

Recognizing the importance that IoT security plays in protecting their customers' data, in positioning themselves on the market, and in keeping themselves in business, tech vendors are taking action, fueling the growth of an IoT security market that is now slated to reach US$ 35.2 billion by 2023.[7] With more and more at stake by the day, they aren't a minute too soon.

Where's the S in IoT?

There's an old joke that says that the S in IoT stands for security. While it may be a harsh oversimplification, there is some truth to it. In the two decades since the term IoT was first coined, security has not received the attention it warranted, often brushed aside to meet size, price, and power requirements that are critical to IoT applications. These tight resource constraints have made it seem impossible to adopt many of the hard-won advances that have transformed IT security, such as robust but computationally expensive cryptographic algorithms.

Furthermore, driven by fierce competition to be the first to bring new connected "things" – smart meters, health sensors, industrial machines, and the like – to market, hardware developers, device makers, and solution designers have not all done enough to guarantee a minimum base level of security in their devices. And seduced by the immediate benefits they promise, end-users have been all too eager to adopt them, often overlooking even the most basic "cyber-hygiene," such as thinking through the security implications of connecting to the internet or resetting default passwords.

Somewhat predictably, the sheer quantity of connected devices and the technological complexity of the ecosystem they operate in has led to an explosion in the number of attack surfaces hackers can zoom in on in their quest for exploitable vulnerabilities. And whereas traditional computers tend to be carefully accounted for, maintained, and eventually disposed of, IoT devices can be deployed for years on end in hard-to-reach settings where they are easily overlooked, left unpatched and, once their service is no longer needed, forgotten altogether – at least by their original users.

Learning lessons – the hard way

In the early days of the IoT, companies developing devices targeting the consumer market were largely forced to write the rules as they matured. Inevitably, a wealth of poorly secured devices have made it to market. Toy manufacturers venturing into the IoT space brought us connected teddy bears and other fluffy friends that leave user data exposed.[8] Manufacturers of smart domestic appliances have sold us products, from connected ovens to intelligent vacuum

"Poorly managed digitalization initiatives have increased the threats companies are exposed to."

[5] https://www.ibtimes.com/internet-things-counting-cost-cyberattacks-2804695
[6] Securing IoT, The Economist Intelligence Unit, ARM
[7] https://www.prnewswire.com/news-releases/iot-security-market-worth-35-2-billion-by-2023--exclusive-report-by-marketsandmarkets-300832722.html
[8] https://threatpost.com/cloudpets-may-be-out-of-business-but-security-concerns-remain/132609/
[9] https://www.zdnet.com/article/security-flaw-in-lg-iot-software-left-home-appliances-vulnerable/
[10] https://futurism.com/the-byte/parents-giving-kids-gps-trackers-hacked

cleaners, with exploitable vulnerabilities.[9] And GPS trackers for children, pets, and elderly people with easy-to-guess default passwords let hackers hijack the devices and track their users.[10]

But it isn't just new entrants to the IoT market that have struggled to implement robust security. Even companies well aware of the consequences of neglecting IoT security have seen their devices fall prey to cyberattacks. As companies compete to be the first to hit the market with competitive prices, poorly secured Wi-Fi routers, connected surveillance cameras, and smart TV boxes have become widespread in homes the world over.

In industrial settings, legacy technology adds to the challenge, as pre-internet-era machines lacking the beefed-up defenses required in today's world go online. Once they become accessible to plant operators, they often also become easy targets for cybercriminals. More generally, poorly managed digitalization initiatives have increased the threats companies are exposed to as the calculus behind implementing security changes when a previously closed solution is connected to the wider internet.

Fortunately, for all the difficulties involved in securing IoT devices – protecting data authenticity and integrity as well as user confidentiality – and ensuring that they stay that way, they can be solved. First and foremost, awareness is key to effectively securing small, cheap, and low-power connected devices, as is access to relevant expertise and the right hardware and software IP.

Best in class security

But let's be clear: perfect security does not, and will likely never, exist. As Kudelski's Patrick Hauert pointed out poignantly in our expert interview, "Anyone pretending that they have the perfectly secure solution is either naive, incompetent, or a crook." Fortunately, however, it is possible to achieve a sufficient level of security for most applications. By judiciously striking the optimal balance between the value of the assets that are to be protected and the investment needed to protect them, devices and the platforms they connect to can be effectively safeguarded from most malicious actors that are active online. Most, but not all, as keeping out state-sponsored actors and organized crime rings, with their formidable financial and human resources, would require measures that are out of reach of all but the largest corporations.

Achieving this level of security requires a persistent effort across all levels of the product development, production, and post-market

phases. It begins with carrying out a meticulous threat modeling focused on understanding the threats to which products and services will be exposed. It further involves translating the findings from a risk assessment into a resilient security architecture tailored to the needs of the IoT solution under consideration, taking into account everything from hardware and software design to supply chains to inputs from third parties. The next step involves qualifying a device's security robustness using accepted references and methodologies. Finally, the solution has to be deployed, scaled, and sustained in the field, not only at the time of sale, but throughout its entire lifetime.[11]

The periphery of IoT networks – the distributed industrial sensors, the surveillance cameras, the wearable medical devices, the cloud-connected data loggers – is where implementing robust IoT security is most difficult. Here, the aforementioned tug of war between opposing constraints – size, power consumption, price, computing power, bandwidth, and security – is strongest. Highly efficient cryptographic key management systems, cryptographic hardware accelerators, and technologies to create a unique and immutable device identity are just a few of the ingredients required to meet these demands.

From the edge to the cloud

Ultimately, however, solutions need to be secured from end to end, which is why security solutions tailored to the needs of low power wide area (LPWA) devices are but one element required to secure the IoT. At the other end of the chain, cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) have a clear financial incentive to prioritize and facilitate the development of secure solutions, as customers expect a certain level of security in return for their monthly fees.

Moving forward, there is little doubt that emerging technologies such as artificial intelligence (AI) and machine learning (ML) will play a growing role in securing connected devices. By monitoring in- and outgoing communications and detecting anomalous behavior at the edge of the network (i.e. on the device itself), users can be flagged when the algorithms detect potentially illicit behavior. With the constant appearance of new security threats, maintaining an encrypted channel of communication to fielded devices is essential to let hardware suppliers remotely apply security patches when needed. This, again, requires a high level of security to prevent hackers from using the same pathway to introduce faulty firmware onto the devices. And while data communication is a vital – and vulnerable – facet of IoT solutions, it is by no means the only one. Smart meters, industrial sensors, and environmental monitors are just a few examples of IoT devices that sense and often trigger actions based on data. This gives hackers another attack surface to exploit, for instance, by directly manipulating the measured physical quantities near the sensors. In the case of satellite-based positioning receivers, they can feed the antenna fraudulent signals or simply drown out legitimate ones in a sea of RF noise. In areas such as highly assisted driving, ensuring that such failures do not endanger human lives – designated as functional safety – have become a market requirement.

"Maintaining an encrypted channel of communication to fielded devices is essential to let hardware suppliers remotely apply security patches when needed."

New laws, regulations, and guidelines

Common Criteria certifications, a requirement for a growing number of mass market connected devices, are another example of how the public sphere is raising expectations in terms of IoT security. Around the world, regulations and laws are being drafted to put the IoT on a path from a weakly regulated green field to a new space

[11] Four steps to IoT security, White paper, u-blox

that serves the public good. The US Food and Drug Administration (FDA) was among the first organizations to actively regulate medical devices to ensure their safety and effectiveness. In 2012, their purview was expanded to cover cybersecurity risks posed by medical devices as well. As a result, the FDA has repeatedly approached major players such as GE Healthcare and others, urging them to tighten their cybersecurity.

In addition to the FDA, the EU's Agency for Cybersecurity (ENISA), and the German Federal Office for Information Security (BSI), have released binding standards and have the authority to enforce them in their respective jurisdictions. Organizations such as the US National Institute of Standards and Technology (NIST) and the Global System for Mobile Communications Association (GMSA) have released guidelines on implementing IoT security, while the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have defined standards at least partly covering IoT security. Meanwhile, standardization bodies such as the Third Generation Partnership Project (3GPP) are defining the standards for the next generation of mobile communication technology with IoT security in mind.

"Brand trust is becoming a critical decision factor in technological investments."

Over the past years, we have seen regional and national governments launch initiatives and laws demanding IoT devices to be better secured against cybercriminals, both directly and indirectly. By making companies responsible for protecting the privacy of consumer data, the EU's General Data Protection Regulation (GDPR) has companies scrambling to put protective measures in place.

And at the national level, Finland took the lead, adopting an approach based on a labeling system that scores IoT products in terms of their digital safety, much like the already well-established labeling systems used to quantify power efficiency in domestic appliances.[12] The initiative, designed to raise public awareness of cybersecurity threats and promote IoT products that are secure by design, both protects customers and contributes to increasing the sustainability of the IoT in general.

In parallel initiatives, the UK and the US State of California unveiled legislation demanding manufacturers of connected devices to meet a minimum set of security requirements. In the UK, smart products need to allow users to define their own usernames and passwords, as well as provide users with more information on how long vendors promise to offer security updates for devices.[13] In California, the law calls for manufacturers to ensure that smart devices are equipped with what they refer to as reasonable security features, outlined in the law.[14]

It all boils down to trust

With IoT security and data privacy on the hearts and minds of businesses and end-consumers, brand trust is becoming a critical decision factor in technological investments. Hard earned, easily lost, yet vital to the success of public facing corporations, companies are having to learn how to accrue trust while constantly being threatened by cyberattacks. Given that no security solution can fully eliminate the risk of being hacked, being able to show that IoT security risks were sufficiently considered in developing products is a surefire way to grow trust among customers. Having robust contingency plans in place when disaster strikes and managing the situation gracefully can be equally, if not more, important.

To learn more on how to contribute to a sustainable connected future, visit our website at u-blox.com. ■

[12] https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

[13] https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

[14] https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-advisory-outlining-new-data-privacy-rights

The secret life of your smart security camera (and other connected devices)

Once compromised, your surveillance camera, or any other connected device, might end up enlisted by the internet's dark forces into one of countless competing botnets that wreak havoc online.

It starts the second you plug in your smart home surveillance camera and connect it to your home network. If poorly configured, your Wi-Fi router might make your device visible to the broader internet, in which case its manufacturer, model type, IP address, and other information provided on the service banner will show up as search results on Shodan.io, censys.io, or zoomeye.org, best described as Google search engines for connected devices. Now, let's say you forgot to reset the default password, or your device has a known and exploitable vulnerability listed on metasploit.com or exploit-db.com. In a matter of minutes, it might find itself the target of competing strains of malware, each fighting to silently infect it.

To be fair, we are postulating a long series of ifs, making it quite unlikely that precisely this chain of events will play out in your home. But because of the myriad connected devices that connect to the internet via routers in millions of households, commercial buildings, and companies the world over, the number of accessible, infectable end devices adds up, with consequences that range from invisible, to creepy for individual end users, to devastating for global companies.

That's because once your connected video camera, your smart TV, or your smart lighting sockets are infected, you are no longer their sole master, though there's hardly anything that would give this away. Your device has effectively been pwned (pronounced pawned), recruited into a botnet, as one device among hundreds, thousands, or more, awaiting orders from the network's command and control center. Next thing you know, your devices might be flooding a corporate website with data traffic in a distributed denial of service (DDoS) attack,

liking YouTube clips to artificially drive up advertisement value, or mining Monero or Bitcoin on someone else's behalf.

"The number of accessible, infectable end devices adds up with consequences that can be devestating for global companies."

As parts of a larger cybercrime-as-a-service solution, they could be rented out to the highest bidder interested in perpetrating crimes online without having to bother with building up a zombie army of connected devices themself. And individual devices could become VPN endpoints, rerouting traffic to give users access to websites that are blocked by their governments, or, in the case of strategically located webcams, rented out to hungry eyes.

An arsenal long in the making

Malware targeting IoT devices (which may not have gone under that name at the time) was pushed into the limelight back in 2010, when the Stuxnet worm attacked programmable logic controllers (PLCs) used by Iran's nuclear program. A natural extension of decades' worth of malware development targeting IT systems, cybercrime exploiting IoT devices has given denizens of the dark web a niche to settle into and exploit. But because the devices targeted operate under a different set of conditions, they require a different set of strategies to be successful.

Mirai is arguably the most well-known malware designed specifically to recruit IoT devices into botnets and subsequently launch DDoS attacks to shut down websites. After its source code was released, countless successors to Mirai were developed, featuring new exploits to conquer additional classes of IoT devices, or competing aggressively with older strains of the malware.

In 2017, IT systems were targeted by ransomware attacks such as WannaCry, which used a cyberattack exploit – essentially a piece of code written to take advantage of a vulnerability – called EternalBlue, which had been developed by and leaked from the US National Security

US$ 1.5 trillion

Revenues 2018 from illegal online markets[1]

Agency (NSA). WannyCry went on to spread to computers running Microsoft Windows in over 150 countries. Once the malware had infected a system, it would encrypt data and demand ransom payments from users seeking to decrypt it. Later that year, NotPetya, another ransomware attack that used the same EternalBlue exploit, followed a similar approach, only it offered no way to decrypt the data upon receiving the ransom payment.

Now, IoT systems are also likely to come under threat by bad actors using ransomware, albeit with a twist. Ransomware targeting computers worked by encrypting data stored on the local hard drive – a strategy that fails on IoT devices that host little to no data. But ransomware threats to IoT devices can be successful by targeting critical applications, perhaps even at strategically chosen times. Threatening to dramatically raise a smart thermostat while homeowners are absent, taking over control of a traffic management system during rush hour, or disrupting production in a connected factory unless a defined sum is paid are a few obvious examples.

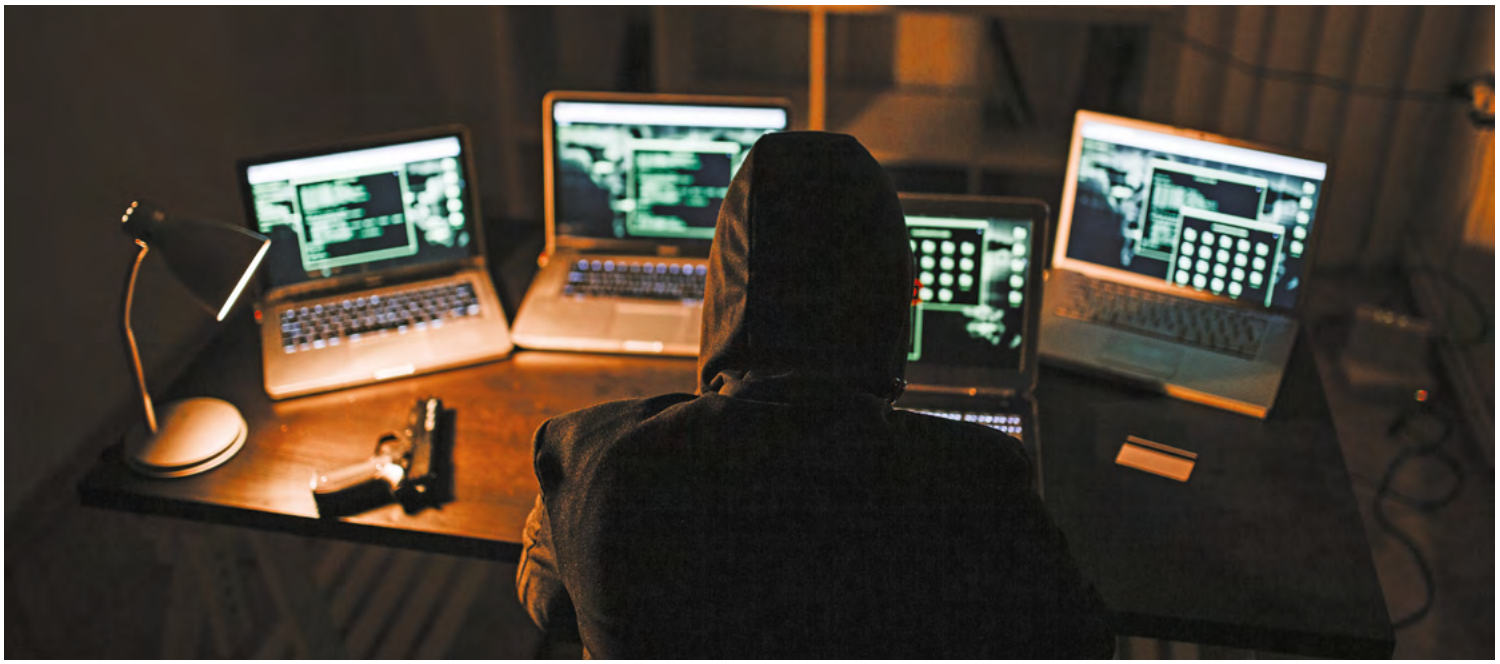
A market to be reckoned with

In 2018, hardware virtualization firm Bromium issued a report dissecting cybercrime's complex economy. Tallying up revenues from a range of illicit activities, from illegal online markets and IP theft to ransomware and crimeware-as-a service, the industry's total revenues amounted to around US$ 1.5 trillion, comfortably ranking it in the top 15 countries by GDP. Organized much like a legitimate economy, with a few large operations with revenues measured in billions of US dollars and many smaller ones generating incomes in the tens of thousands, the cybercrime market is a force to be reckoned with, selling and leasing a range of listed services and products.[1] Individual exploits can be purchased for tens to hundreds of thousands of dollars, depending on the software they target.

According to a report by Trend Micro Research[2], monetization schemes for IoT device hacks are

[1] https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/

[2] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground



still in their infancy. In fact, they argue, the lack of a viable business model may be what has kept us safe from oft-discussed IoT doomsday scenarios. But, by immersing themselves in the forums and communication platforms of the cybercrime underground, the researchers were able to get a unique perspective on the day's hot topics, citing routers, webcams, printers, and industrial PLCs as objects of widespread interest. And, unsurprisingly, innovation in monetization schemes is high on the agendas of some underground communities.

Russian underground organizations, in particular, have taken the monetization of IoT device hacking the furthest, possibly pointing at what should be expected from the rest of the world in years to come. From peddling exploits targeting routers and webcams, to selling hacked smart electricity meters that let users cut their utilities bills, to repurposing infected devices as VPN exit notes for a fee, business model innovation is alive and well in the Russian underground. In an attempt to stop cybercriminals from using Shodan.io, mentioned in the opening paragraph, for cybercrime, the platform has restricted its free service offering and requires users to justify the more advanced queries that hackers depend on. With limited effect, as Russian hackers have found a way to sell premium – and incognito – access to the search engine's results for a US$ 59 monthly fee.

"The cybercrime market is a force to be reckoned with, selling and leasing a range of listed services and products."

No end in sight

In the ever-escalating arms race between cybercriminals and cybersecurity experts, there are no signs of a truce, and no shortage of exploitable opportunities in the pipeline. Largely, these are the result of technological progress. Take the ongoing rollout of 5G technology. All

the discussions on which countries to source components from fail to address one of the main sources of vulnerabilities: the standards, protocols, and software that 5G technology relies on, argues renowned security expert Bruce Schneier on his blog.[3] Overly complex standards, backward compatibility, and an emphasis on other factors over security all contribute to leaving in vulnerabilities, some of which have already been documented by researchers.

Furthermore, every time product developers update their devices to the latest technology, they risk introducing new exploitable bugs into their devices. The result is another cycle of hackers detecting and exploiting vulnerabilities, after which device manufacturers release patches, which may again contain vulnerabilities, and so on. And because exploitable vulnerabilities are worth most as zero-day exploits when they are only known to their discoverers, there is little incentive for hackers to use them. This makes it difficult to know exactly how many IoT devices are vulnerable at any given time.

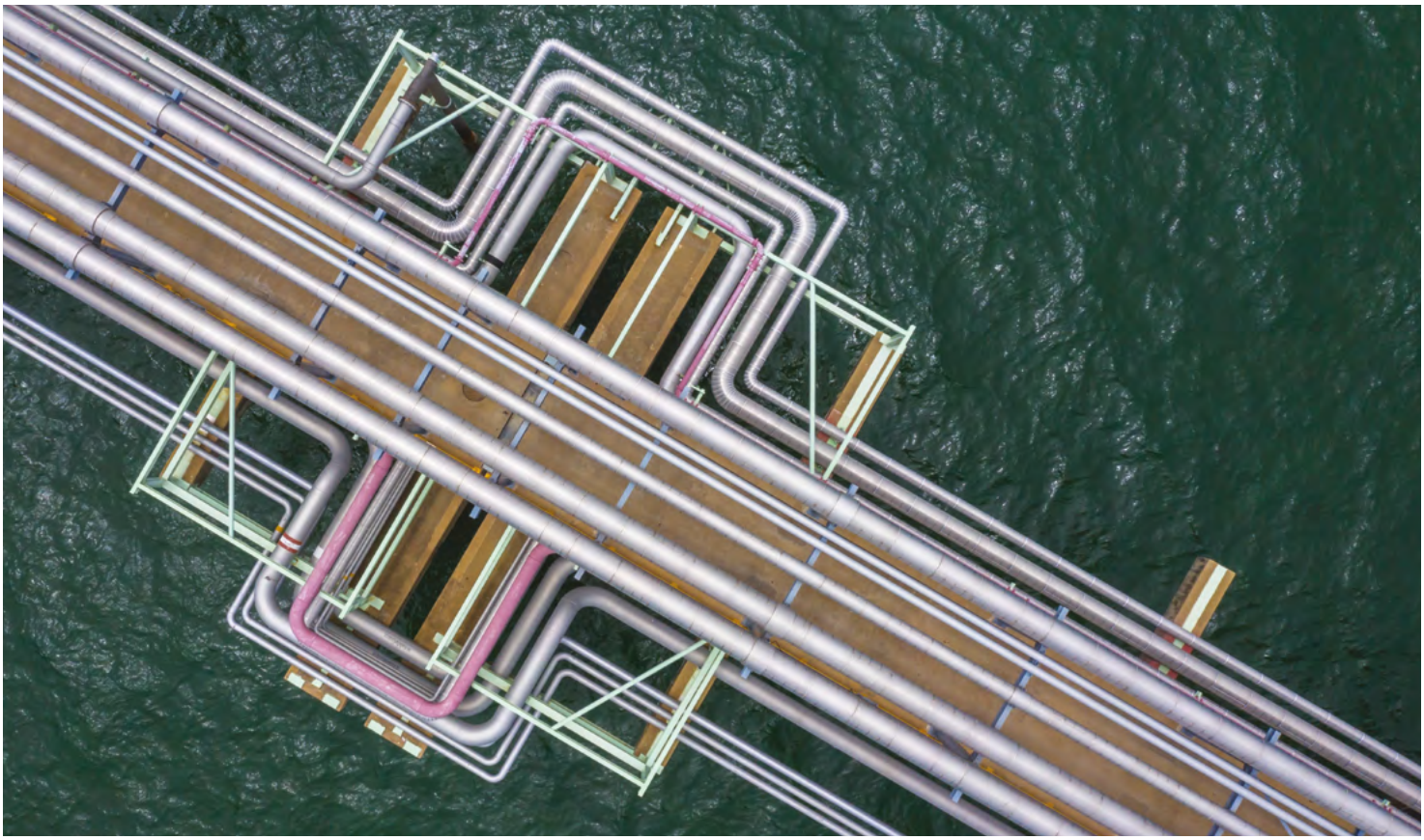
Wash your hands and reset your passwords

Whenever we venture into the world, we are confronted with threats, in the form of accidents, diseases, criminals, or natural disasters. Ignorance can be the biggest danger, the global spread of the covid-19 being a case in point. A clear-eyed understanding of the risks these threats present offers a vital head start in dealing with them. It begins with recognizing that, like anything that is connected to large-scale computer networks, IoT devices are constantly being reconnoitered and attacked, as is every other element of the network.

The only defense is to carefully evaluate and address security threats at every step of a product's development process, from the design and production phases, to its deployment and operation, all the way through to its decommissioning. It takes an "all-hands-on-deck" effort, placing stringent demands on the product manufacturers at all levels. The advice to end-users is the technological equivalent to the ubiquitous calls to wash your hands: reset your passwords and, whatever you do, take security hygiene seriously. ■

"A clear-eyed understanding of the risks these threats present offers a vital head start in dealing with them."

[3] https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html



IoT Security

Minimal resources – maximum security

IoT networks are only as secure as the end devices that connect to them. Here's what it takes to enable robust IoT security - even in the most resource-constrained environments.

It's one thing to implement IoT security in friendly environments – with unlimited power, plenty of computing capacity, ample bandwidth, and a team of security experts present and prepared to catch and patch up any security flaws. But these conditions are rare in real-world IoT deployments, where droves of battery-powered devices scattered far and wide run on stripped down operating systems, with minimal computing power, and tightly rationed data plans, often beyond the physical reach of tech support.

The task is made more challenging still by the fragmented mix of technologies, protocols, and vendors that are thrust together into dedicated solutions. A domestic air quality monitor, for instance, might combine multiple particulate matter sensors, a host processor, and a wireless modem, each from a different supplier. After sensing and processing, the data may be sent to a smart home hub, then to a router, and finally up to the cloud, passing at each hop through products made by different suppliers from all over the world.

In this specific case, confidentiality might not be a high-stakes concern. But given the psychological cost of raising false alarms, data integrity might be. And because nobody wants their smart home devices to be recruited into a botnet and pulled into a nefarious online conspiracy, so might access control. Pet trackers, domestic surveillance cameras, smart TV boxes, connected thermostats, and coffee machines – the list of exposed devices is long and getting longer by the day.

The stakes are far greater in the industrial IoT, where compromised smart sensors, smart meters, or smart devices might expose confidential data of thousands to millions of devices. Public and private utilities rely on hundreds of thousands of such devices that are expected to work in the field for a decade or more. And it goes beyond protecting confidentiality. Compromised devices can be a conduit for hackers to bring operations to a halt, leading to downtime that can cost companies millions of dollars.

Respect for data privacy is absolutely critical to build public trust in connected health applications. Because of the sensitive nature of the data involved, patients count on eHealth service providers to treat their data with as much or more care than their doctors. And because smart health devices such as cardiac pacemakers and connected insulin pumps interface directly with the body, the consequences of being hijacked by hackers can be dramatic, both for the patient and the producers of the device.

Municipal authorities are also developing and deploying applications that aim to positively impact their residents' lives. To be successful, they need to be able to count on the authenticity, integrity, and confidentiality of the data they sense.

In each of these settings, the ability to patch and update firmware to address inevitable vulnerabilities is vital for a connected business to stand the test of time.

A foundation of core protection

Ultimately, the end-goal is always the same. Devices must be secured so that users can trust and control their devices. The privacy of the data should be protected both on devices themselves and as it transits from the devices to the cloud to ensure authenticity, integrity, and confidentiality. Access to the devices, their data, and their features needs to be restricted to authorized users. And measures should be put in place to detect and respond to intrusions, mitigate their effects, and correct the vulnerabilities at their source.

Because their businesses depend on it, major cloud service providers such as AWS, Microsoft Azure, and Google Cloud Platform are constantly building out their services to offer a solid security baseline. But for entire solutions to be secure, the end devices at the periphery of the network also need to pull their weight. To hackers, vulnerabilities at the network's edge can be an open door into the protected portions of the network. They can exploit them unnoticed to sniff or manipulate data as it transmits to the cloud. Or they can modify a device's firmware to make it serve their own needs.

Building a foundation of core protection – services capable of withstanding attacks from all but the most sophisticated actors such as nation

states – requires establishing a chain of trust, from the device end all the way up to the cloud, even as data travels through poorly secured, or even hostile, environments. This requires taking security seriously from the design phase through manufacturing, all the way to operations. While there is no one-size-fits-all security solution, there is a general script that helps ensure that the important boxes are checked and that best practices are followed.

In their draft recommendations for IoT device manufacturers, the US National Institute for Standards and Technology (NIST) lays out six voluntary but recommended activities to tighten cybersecurity of commercial IoT devices.[1] The GSMA, which represents the interests of mobile network operators, has laid out its security guidelines in a series of reference documents.[2] And we have outlined a four-step path to developing and deploying IoT ecosystems that are resilient to evolving cyberthreats in a white paper.[3]

An IoT security cookbook

Such a secure solution needs a rock-solid foundation to build on. In this case, this foundation is provided by an immutable chip ID and a robust root of trust, which is best explained as a source that enables a trusted set of advanced security functionality. These can include the ability to securely execute user applications, protect against and detect tampering, and securely store and handle encryption keys and other security assets.

A secure boot sequence and secure updates ensure that only authenticated firmware runs on the device. A secure client library generates keys and crypto functions needed to securely connect devices to the cloud, and encryption keys derived from the root of trust protect the confidentiality and integrity of all data, whether at rest or in motion.

If all that sounds extremely resource intensive, well, it can be. But, with the right expertise, we and Kudelski, a Swiss-based digital security provider, are proving that it is possible to fit best-in-class security onto a 16 by 26 mm module designed to transmit data for years on end under a tight power budget. It combines Kudelski's unique security architecture and sophisticated lightweight algorithms to offer a highly scalable key management system aligned with the needs of the IoT.

Root-of-trust-based encryption means that customers no longer always need to incorporate a dedicated, separate Secure Element – also referred to as a crypto-chip. End-to-end encryption from the device to the backend or cloud applications means that all the gateways, routers, and other intermediaries on the journey remain blind to the data being sent. And a unique LPWA-optimized key management solution can reduce data overhead eight-fold over standard public key infrastructure (PKI) certificate-based solutions.

Pre-Shared Key Management: Security + Efficiency

What makes the solution unique is the way in which the root key of each device is known to Kudelski's hardened secure servers in the cloud. Both the device and the cloud also contain the proprietary, battle-tested algorithms that generate ephemeral, one-time use keys to provide critical IoT functions like the encryption of data, the authentication of commands, and the validation of new firmware updates. This provides the highest possible level of data confidentiality, device security, and finite access control while limiting bandwidth and power usage.

Most devices designed for secure communications are assigned multiple, usually two or three, root keys during production. If one key is compromised, they can cycle through the remaining ones until they are all used up. Thanks to the pre-shared keys connecting our secure modules to the cloud, users can effortlessly create any number of encryption keys. As a result, every single communication to and from each individual device can be uniquely secured.

This can be invaluable in common IoT use cases. Take, for instance, a device that uses machine-learning-generated algorithms to identify suspicious data traffic suggesting the device is

[1] https://csrc.nist.gov/publications/detail/nistir/8259/draft
[2] Available here https://www.gsma.com/iot/iot-security/iot-security-guidelines/
[3] https://www.u-blox.com/en/publication/white-paper/four-steps-iot-security

being exploited by unauthorized users. Because the devices themselves have limited computational power, the algorithms are typically trained on the cloud using oodles of data before being transferred to the devices.

The resulting algorithms, often the more valuable intellectual property, can then be sent over the air to the deployed devices using an encryption key that is unique to the device and to the session. This is but one example of how tying each device's physical root of trust to the cloud raises the level of security users can leverage to protect their business and their data.

And in the event that these keys are disclosed, the same scheme can be used to transparently renew all of the security of the system without impacting the backend or cloud applications, ensuring that active security is available throughout the lifetime of the IoT devices. Another one dovetails with the growing popularity of OSCORE, a lightweight security protocol designed specifically for highly resource constrained IoT end devices. OSCORE decreases security overhead and bandwidth usage by encrypting only the sensitive portion of messages being transferred, so that the gateways, routers, and servers the data travels through do not need to decrypt the data to reroute as it travels towards its destination.

Furthermore, OSCORE uses pre-shared keys rather than a resource intensive key negotiation process. The protocol, however, leaves open how the keys are shared between the IoT end device and the destination server. Again, the Kudelski key management scheme from the end device's root of trust to backend applications offers an ideal solution.

An IoT SAFE investment

By aligning the solution with the IoT SAFE standards and working group, overseen by the GSMA, we are ensuring that our solution runs seamlessly on all GSMA networks. In addition to leveraging existing security hardware resources to securely store and manage keys and enabling remote management of deployed security applets, abiding to IoT SAFE makes it easy for device manufacturers to develop solutions using an immutable identity pre-provisioned in the SIM.

As the IoT continues to expand deeper and deeper into our lives and our businesses, securing devices and encrypting communications are becoming ever more critical. With the right technology, security architecture, and expertise, enabling a foundation of core protection for the IoT with minimal resources in terms of battery power, CPU power, and bandwidth is becoming possible. ■

IoT Security

In the IoT, there is no safety without security

Reaping the IoT's goodness without its pitfalls will require coming to grips its inherent security challenges.

Be it by protecting our homes, assisting us as we drive, helping us preserve our health, watching over our loved ones, or by summoning emergency rescue services in the event of an accident, the Internet of Things has tremendous potential to transform our lives for the better, increasing our physical safety and wellbeing as we go about our day-to-day lives.

At the workplace, the IoT can help companies protect their workforces by tracking them as they enter high risk environments such as mines, engage in dangerous activities such as power line maintenance, or drive long distances. Collision avoidance between heavy machinery on construction sites, automated maintenance checks on equipment, and real-time heat-stress monitoring are just a few other measures that contribute to reducing the 2.78 million deaths that occur globally as a result of occupational accidents and work-related diseases every year.[1]

The impact of the IoT extends to society as well. The 2018 Winter Olympics in PyeongChang, South Korea, saw IoT helmets featuring cameras, radio functionality, and GPS receivers worn by police forces, and a 24-hour surveillance center that pulled in data from varied sources, such as intelligent CCTVs, unmanned aircraft, and location control systems.[2] By collecting data to feed early warning systems against natural disasters, and ensuring the robustness and resilience of critical infrastructure such as utility and transportation networks, the IoT could well

[1] https://www.levitt-safety.com/blog/what-does-iot-mean-for-workplace-safety/
[2] http://v.media.daum.net/v/20180225130110981?f=o

usher in a shining new era of reduced societal risk and increased wellbeing.

And as they say in business: if you can't measure it, you can't manage it. From remote tracking of resource extraction to monitoring waste and inefficiencies across supply and production chains, insights gleaned from real-time data gathered by distributed wireless sensor networks will help us improve strategies to manage or adapt to environmental threats such as natural resource depletion and climate change.

But there is a caveat. For all their potential to change the world for the better, Internet of Things applications exist within an extremely hostile environment where they are constantly under attack from bots unleased by hackers and other bad actors that are active in the online world. For the IoT to unleash its full potential, security will have to be treated as a top priority.

Exhibit 1: Connected health
Nowhere is the link between digital security and physical safety as salient as in connected health devices. Battery-powered implantable cardiac pacemakers came into use in the 1960s. Designed to stimulate the heart to alter or stabilize its rate, artificial cardiac pacemakers have saved and extended countless lives. Over the past years, manufacturers of these devices have embraced wireless connectivity, using it to collect health metrics with which healthcare professionals can assess the progression of the condition.

Insulin pumps are yet another class of devices that have recently been connected via patients' smartphones to the cloud. Enabling new features such as alerts to family members when glucose levels drop below a predefined threshold, they too have saved their share of lives, in addition to simplifying the management of diabetes for patients who have to live with the disease.

But as many new applications, these newly connected life-saving devices have already experienced their share of growing pains. Numerous vulnerabilities have been found in connected artificial cardiac pacemakers and insulin pumps that could put not only the privacy but also the lives of their users at risk.

"Wireless sensor networks will help us improve strategies to manage or adapt to environmental threats such as natural resource depletion and climate change."

As a result, connected health devices manufacturers are under increasing scrutiny from hospitals and other healthcare providers, as well as regulatory agencies such as the US Food and Drug Administration (FDA), to ensure that their products are able to fend off cyberattacks.

Exhibit 2: Smart homes and cities
Smart home devices have also increased the physical safety and wellbeing of their users. Today, elderly individuals can rely on IoT devices to support them in their daily tasks, create a real-time communication channel with their healthcare providers and their loved ones, and trigger alerts in the event of accidents. But because they are more likely to be overwhelmed by the technological complexity of the solutions they depend on, they are also more vulnerable to different forms of cybercrime, harassment, and extortion.

And it isn't only the elderly who are exposed. Poorly secured smart home devices serving

broader demographics can be also hijacked to cause harm by threatening the physical safety of their owners. Connected door locks can be compromised, either opening doors to intruders or locking residents into their own rooms. Sensors on smoke detectors or fire alarms can be disabled, leaving residents unprotected. And connected devices such as thermostats, ovens, and other kitchen appliances that include a heating element could be exploited to consume excessive power or start a fire.[3]

"Combining navigation assistance with connected video surveillance cameras will let people spend less time circling the neighborhood to find a parking space."

These aren't just hypothetical risks. According to a 2019 report by Plum Consulting and the Internet Society,[4] several of these threats have been demonstrated, including at security events. Furthermore, security cameras produced by Amazon-owned Ring have been hacked, leaving users feeling "violated," "scared" and "concerned about their privacy and safety," according to an article by the New York Times.[5] Though no one was hurt, these types of experiences can be traumatic to their users.

Exhibit 3: Mobility

One of the IoT's strongest suites is in orchestrating the behavior of complex systems. Traffic management is no exception. The IoT is uniquely able to sense the environment from every imaginable vantage point and display messages on digital signposts and smart devices. Add to that all the currently available flavors of wireless communication technology, from short range Bluetooth and Wi-Fi to cellular 4G LTE and, increasingly, 5G. And top it off with the computation power and artificial intelligence resident in the cloud. The result is V2X (vehicle-to-everything) communication, which links cars to the road-side infrastructure, nearby vehicles, and potentially even pedestrians.

V2X promises to make roads safer by helping drivers see beyond their line of sight, effectively looking around corners and raising alerts in the event of slower traffic or accidents. Cars equipped with the technology will be able to carry out otherwise dangerous maneuvers such as overtaking, merging, and negotiating priority at complex junctions more safely. And combining navigation assistance with connected video surveillance cameras and smart parking sensors will let people spend less time circling the neighborhood to find a parking space.

Achieving this will, however, require an unprecedented level of trust, both in the data as well as in the system that processes it. Data accuracy is essential, but no longer sufficient. Now the integrity of the data that is processed also has to be ensured. Unlike the navigation system you may have in your car today, advanced driver assistance systems (ADAS) intervene directly in the actions of your vehicle. As a result, they require a higher level of security. One component, referred to as functional safety, ensures that malfunctioning sensors in no way threaten the safety of the car's passengers.

No safety without security

In their report on the Physical Security Business, Memoori, a smart building research firm, makes the point that the future for smart connected buildings is bright, but that customers will only invest in the technologies when they are convinced that the benefits outweigh the risks. They further note the irony of physical security

[3] https://www.internetsociety.org/wp-content/uploads/2019/04/The_Economics_of_Consumer_IoT_Security.pdf
[4] ibid
[5] https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html

protection being perceived as “having the highest level of risk of all types of building elements.”

It’s a realization that transfers to other areas as well: The physical safety of people is typically valued higher than the material safety of assets and goods. This value also puts it at a higher risk of being attacked. Be it in healthcare, at the workplace, on the road, or in factories, because they make attractive targets to hackers, IoT solutions designed to protect physical safety will, themselves, have to meet some of the most stringent IoT security requirements.

The good news is that the IoT is at a turning point. Driven by increased customer awareness of the risks of cyberattacks – due at least in part to the abundance of news stories covering hacked devices – more device manufacturers are beginning to appreciate the importance of taking IoT security seriously. Even in the long-neglected area of consumer goods, new national and regional policies in the US, UK, and Finland are raising the bar on IoT security. Others are likely to follow. And component suppliers are pulling their weight as well. With new security solutions tailored to the diverse and demanding needs of the IoT, securing solutions has never been as attainable. ■

[5] The Physical Security Business 2019 to 2024, Access Control, Intruder Alarm / Perimeter Protection & Video Surveillance, Published: Q4 2019

IoT Security

Building trust in the Internet of Things

The short history of our digital era is already rife with lessons highlighting the importance robust security and well thought-out contingency plans have in growing and maintaining trust.

If there's one thing CEOs agree on, it's that the IoT and the fourth industrial revolution will transform their businesses. Not only are digitization and seamless connectivity, which underlie the IoT, streamlining operations, increasing efficiencies, and improving services by leveraging data sensing and analytics, they are also enabling altogether new business models. This broad footprint will have a massive financial impact: According to a report by Particle, the IoT is expected to have a total potential economic impact of US$ 11.1 trillion by 2025.[1]

But, as we've seen throughout this edition of our magazine, with ubiquitous connectivity come new risks. The very decentralization of data gathering, analytics, and control that make it such a game changer exposes companies to a variety of new threats that need to be carefully understood and managed. The Economist Intelligence Unit found that 13% of executives they surveyed were discouraged from pursuing an IoT strategy by security and privacy concerns.[2]

It's hardly a surprise. The short history of our digital era is already rife with lessons highlighting the importance of security that should serve as cautionary tales to companies designing connected solutions. And despite its youth, it also already features a fair number of tales of transformation, in which some of cybercriminality's worst victims have bounced back, not necessarily unscathed, but better equipped to deal with future threats.

If the past decade of IoT security breaches has taught us anything, it's that no organization, regardless of its size, is immune to them. According to a survey carried out in 2017, just under 50 percent of organizations and businesses that leverage the IoT have already seen their systems breached.[3]

Given that the number of attacks on IoT devices tripled in the first half of 2019,[4] that percentage is likely to be much higher today. Banks, factories, public utilities, hospitals, smart cities, and even casinos have seen their systems attacked, either by IoT devices or through them. It's likely that many more breaches go unnoticed and unreported, as companies attempt to protect themselves to the reputational damage and the stigma associated with falling victim to cybercrime.

Cyberattacks have fostered a scarcity of trust

Clearly, companies caught taking IoT security lightly undermine trust in their brand. Still, they all too often cut corners in securing connected products in the race to develop and sell them quickly and cheaply. By giving rise to yet another IoT security-related scare story, they end up further undermining trust in the connected future they themselves are building.

Sometimes it begins in the playroom. CloudPets, a brand owned by SpiralToys, sold hundreds of thousands of connected Teddy bears that let children and their parents (or other friends and family) talk to each other. Once the users involved registered via an app, the CloudPets Teddy bear became an avatar for the parents. The company stored the registration data and all of the audio transcripts on an unprotected online database. Though it was encrypted, the strength of the encryption depended on the quality of the password used. In many cases, it could easily be broken, revealing private conversations mediated by the Teddy bear.

"The history of IoT security breaches has taught us that no organization is immune to them."

[1] The 2019 State of IoT Report, Particle
[2] The Economist Intelligence Unit, The IoT Business Index 2020, Securing IoT
[3] http://www.altvil.com/wp-content/uploads/2017/06/AVCo.-IoT-Security-White-Paper-June-2017.pdf
[4] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Implantable connected health devices dramatically raise the stakes further, both for end-users and manufacturers. Over the past years, the US Food and Drug Administration (FDA) has released a number of cybersecurity safety communications to inform healthcare providers and patients of cybersecurity vulnerabilities found in connected medical devices, such as implantable cardiac pacemakers and insulin pumps. Although there have been no reports of patient deaths or injuries, these communications highlight the importance of closely scrutinizing connected health products.

In 2016, Verizon Security Services reported on an IT security breach that gave hackers access to a programmable logic controller (PLC) controlling a water treatment plant.[5,6] As revealed in a white paper by Vericlave and Blueridge Networks, the plant's poor security architecture and outdated software systems made it an obvious target for hackers. These went on to access the plant's financial system and open and close the valves controlling the chemicals used to treat the water.

Reports of industrial PLCs being hacked are rare, though cybersecurity researchers and "friendly" white hat hackers have discovered numerous vulnerabilities in industrial computers (PLCs) and the SCADA systems used to interface with the industrial machines. An article in the Wall Street Journal lays out how hackers able to penetrate into one Siemens Simatic S7-1500 would be able to access all other similar PLCs in the same company.[7] The potential harm that hackers could inflict on a manufacturing site, both in terms of manipulating industrial processes and stealing sensitive data, is considerable.

Even mobile network operators that are intimately aware of cyberrisks can fall victim to hackers. In 2017, over 800'000 Deutsche Telekom customers lost internet access when their Wi-Fi routers were attacked by Mirai malware. As is often the case, Deutsche Telekom was simply collateral damage in a greater scheme to inflict harm on a different target. A 29 year old British hacker, who was eventually captured and pleaded guilty to his crimes, had been amassing a large Botnet that he could rent out to mount a DDoS attack on a Liberian mobile network operator. His reward: US$ 10,000. The cost of the Mirai-related attacks for Deutsche Telekom: roughly US$ 2,000,000.

Building trust by bouncing back gracefully

If this whistle-stop tour through the history of IoT security breaches shows us anything, it is that given enough time, every company under the sun will at some point see its defenses breached. And, as we saw, it can happen entirely unintended.

A brief excursion into IT security shows how one company was able to bounce back from one of the biggest cyberattacks of all time: the NotPetya ransomware attack. In June 27, 2017, Maersk, the Danish global maritime shipping megalith, saw a malicious malware allegedly designed to target the Ukrainian economy infect one of its computers, and from there spread across the company's entire network until basically all devices were infected.[8]

"Every company under the sun will at some point see its defenses breached."

The company's operations were shut down entirely by the malware, which encrypted the data and demanded ransom to decrypt it. When ransom payments failed to recover the data, the company, which transports about a fifth of the world's maritime cargo, went into overdrive to keep operations going while it sought to recover

[5] https://www.vericlave.com/wp-content/uploads/2018/10/Vericlave_WhitePaper_KemuriWater_1018_F.pdf
[6] https://www.theregister.co.uk/2016/03/24/water_utility_hacked/
[7] https://www.wsj.com/articles/researchers-hack-into-industrial-equipment-thought-to-be-secure-11565688602
[8] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

“Those with a strong commitment to designing secure systems will be able to reap the rewards of their efforts.”

its systems. Two weeks later, Maersk’s computer systems were back online.

Remarkably, after suffering a financial blow estimated in the hundreds of millions of euros, Maersk emerged strengthened, its trust largely intact. How? By gracefully managing the aftermath of the crisis. By opting for an attitude of openness and transparency rather than attempting to play down or hide the incident, and going the extra mile to keep customers satisfied, Maersk succeeded in convincing its customers that their needs were their central priority. It’s a case study in managing the aftermath of a massive cyberattack that can be transposed to the IoT.

As companies compete for customers, consumer trust and brand reputation are growing in importance as key differentiators. But, because it takes a sustained effort across all levels of a business, banking consumer trust and brand reputation is a challenge not all companies are accustomed to. In the end, however, those with a strong commitment to designing secure systems – from the drawing board to deployment and operation – and to drafting robust contingency plans for when things go awry will be able to reap the rewards of their efforts. ■

The A-Z of IoT security

IoT security is full of jargon from botnets and pwned devices to logic bombs and worms. Here's a short, non-comprehensive glossary for the curious and the confused.

a

Attack surface: All different vectors attackers can exploit in efforts to penetrate devices.

b

Botnet: A network of connected devices that have been infected by malware, allowing them to be used, i.e., to launch large-scale attacks.

c

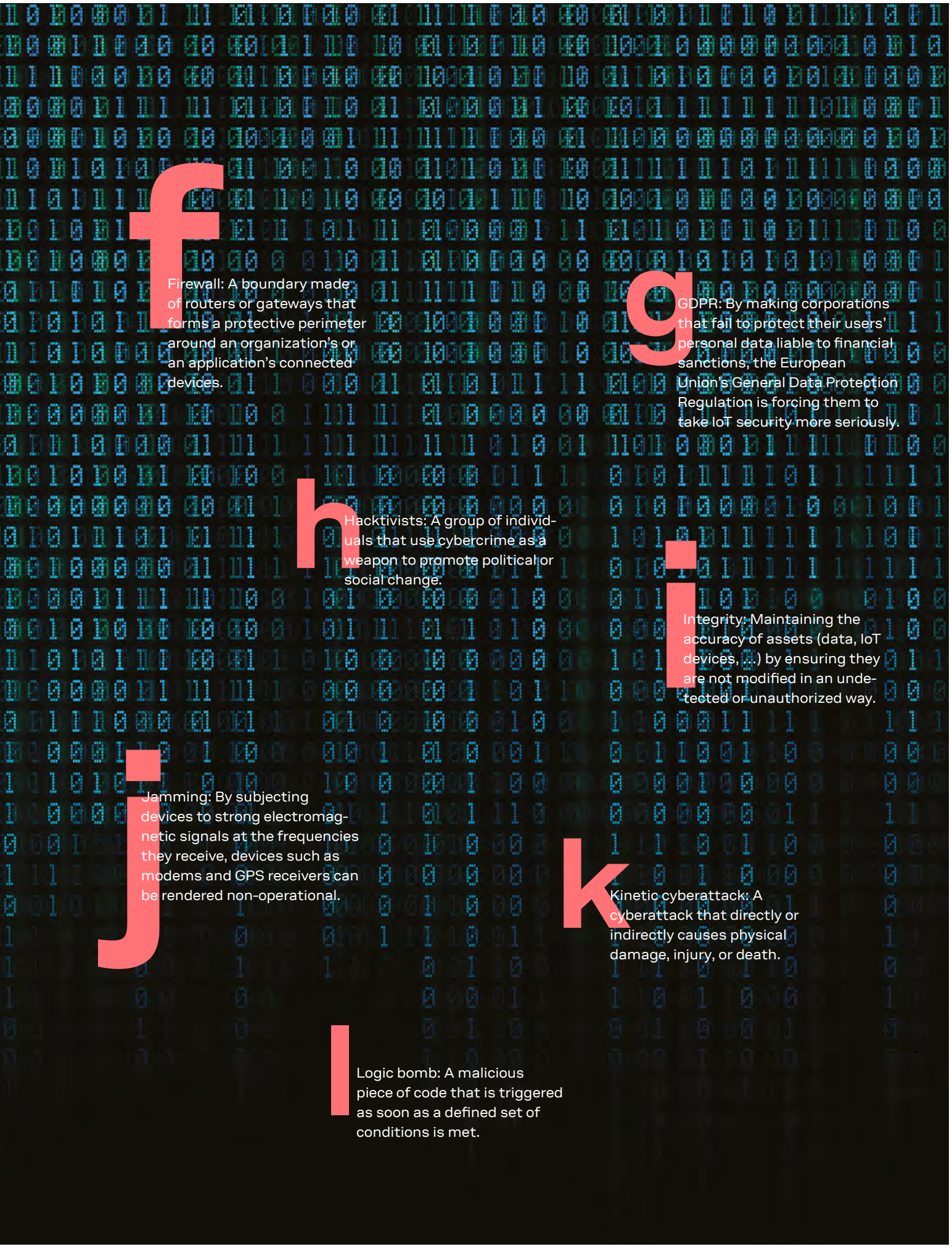
Chain of trust: A chain of trust is a linked path of verification and validation from the root of trust, typically through all the components that make up the fully functional system.

d

DDoS attacks: Distributed denial-of-service attacks, often launched via a botnet, are designed to bring down web servers by flooding them with traffic.

e

End-to-end encryption: A form of encryption that secures data from the end device at its source all the way to the end devices at the other end of the communication chain.



f

Firewall: A boundary made of routers or gateways that forms a protective perimeter around an organization's or an application's connected devices.

g

GDPR: By making corporations that fail to protect their users' personal data liable to financial sanctions, the European Union's General Data Protection Regulation is forcing them to take IoT security more seriously.

h

Hacktivists: A group of individuals that use cybercrime as a weapon to promote political or social change.

i

Integrity: Maintaining the accuracy of assets (data, IoT devices, ...) by ensuring they are not modified in an undetected or unauthorized way.

j

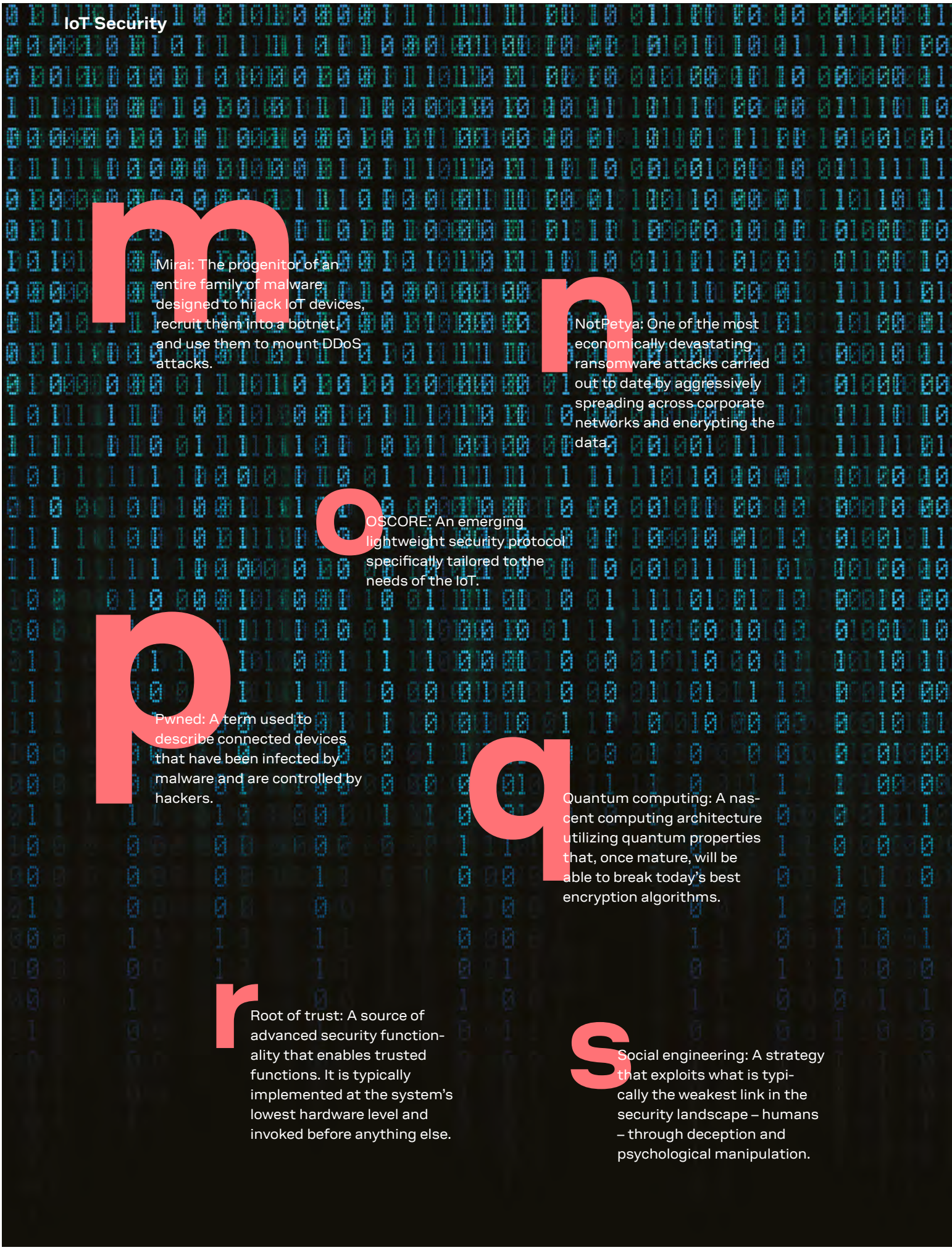
Jamming: By subjecting devices to strong electromagnetic signals at the frequencies they receive, devices such as modems and GPS receivers can be rendered non-operational.

k

Kinetic cyberattack: A cyberattack that directly or indirectly causes physical damage, injury, or death.

l

Logic bomb: A malicious piece of code that is triggered as soon as a defined set of conditions is met.



m Mirai: The progenitor of an entire family of malware designed to hijack IoT devices, recruit them into a botnet, and use them to mount DDoS attacks.

n NotPetya: One of the most economically devastating ransomware attacks carried out to date by aggressively spreading across corporate networks and encrypting the data.

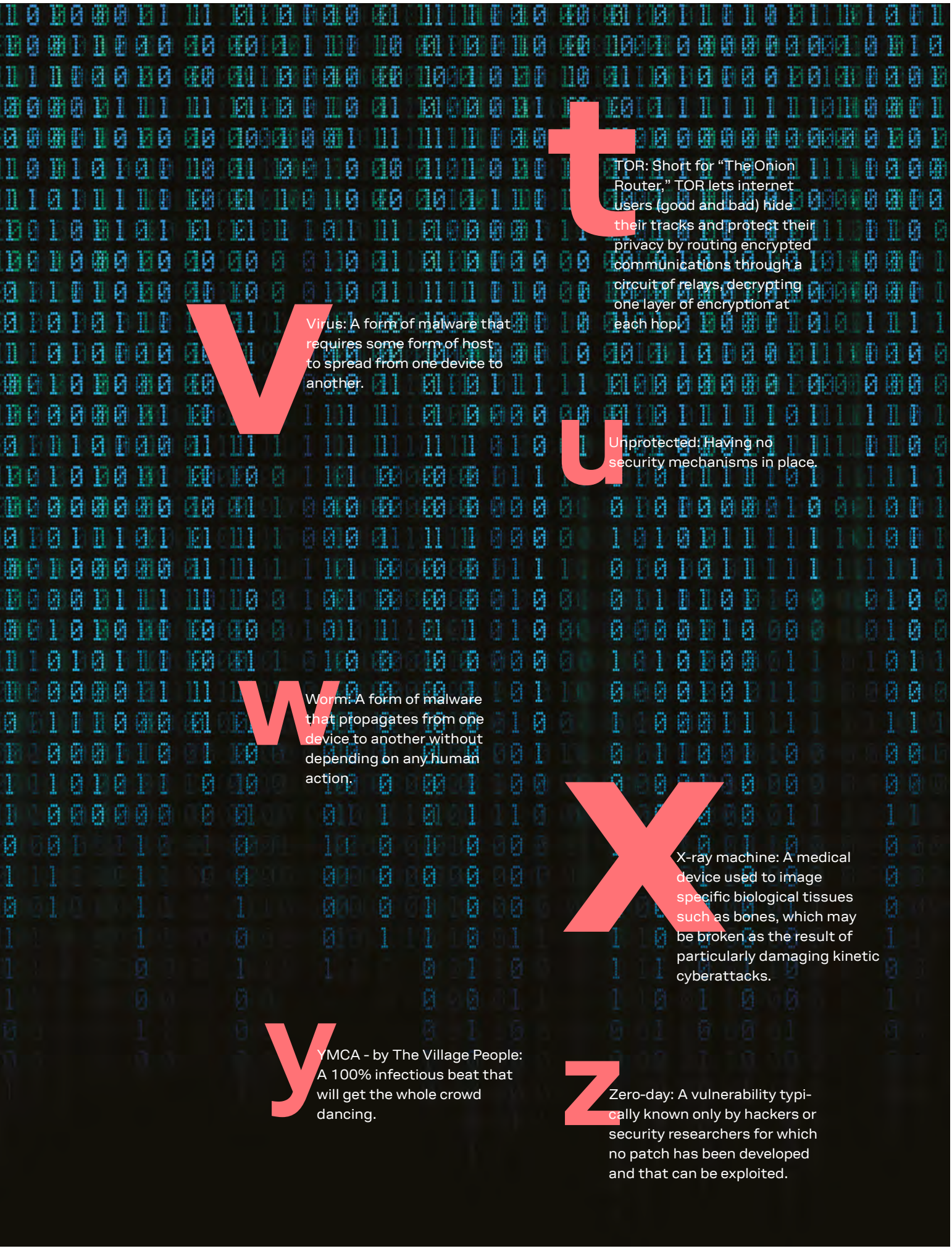
o OSCORE: An emerging lightweight security protocol specifically tailored to the needs of the IoT.

p Pwned: A term used to describe connected devices that have been infected by malware and are controlled by hackers.

q Quantum computing: A nascent computing architecture utilizing quantum properties that, once mature, will be able to break today's best encryption algorithms.

r Root of trust: A source of advanced security functionality that enables trusted functions. It is typically implemented at the system's lowest hardware level and invoked before anything else.

s Social engineering: A strategy that exploits what is typically the weakest link in the security landscape – humans – through deception and psychological manipulation.



t

TOR: Short for “The Onion Router,” TOR lets internet users (good and bad) hide their tracks and protect their privacy by routing encrypted communications through a circuit of relays, decrypting one layer of encryption at each hop.

V

Virus: A form of malware that requires some form of host to spread from one device to another.

u

Unprotected: Having no security mechanisms in place.

w

Worm: A form of malware that propagates from one device to another without depending on any human action.

X

X-ray machine: A medical device used to image specific biological tissues such as bones, which may be broken as the result of particularly damaging kinetic cyberattacks.

y

YMCA - by The Village People: A 100% infectious beat that will get the whole crowd dancing.

z

Zero-day: A vulnerability typically known only by hackers or security researchers for which no patch has been developed and that can be exploited.

Enabling technologies

Innovation on all fronts

Emerging technologies promise to bolster IoT security at every level.

The IoT is a complex organism. On one end of the spectrum, it comprises billions of data-gathering, functionality-enabling IoT end devices deployed the world over in homes, cities, vehicles, factories, and just about anywhere else. On the other end is the cloud, a network of data centers distributed across multiple continents, where data are stored and processed, often using artificial intelligence (AI) algorithms to reveal otherwise hard-to-gain insights.

This simplistic breakdown overlooks the many technological layers required to make the IoT what it is. End devices host a large number of hardware components and sensors, potentially leveraging signals emitted by distant satellites or nearby radio beacons. Typically, they transfer data – often encrypted – to the internet over wireless short range (e.g. Wi-Fi and Bluetooth) or cellular (e.g. 4G LTE, 5G) communication technologies using one of many data transfer protocols.

To gain meaningful insights from the devices or to save resources, these data can be processed

“On the other end is the cloud, a network of data centers distributed across multiple continents that uses artificial intelligence to reveal hidden insights.”

on the device (the edge), in the cloud, or somewhere in between (the fog). Ultimately, the data are integrated into some kind of cloud-based platform or other backend solution, where they can be accessed, leveraged, and shared with other users.

Every step in this process lends itself to varied approaches geared at increasing the security of the overall system. In this article, we’ll explore a selection of emerging technologies that promise to bolster the security of IoT applications, from the incoming radio signals they harness to the encryption solutions they use all the way to the distributed ledgers where the data might ultimately be stored.

Safer signals
A growing number of IoT devices – asset trackers, smart watches, drones, to name a few – rely on location information, typically determined using satellite-based positioning technology. But GNSS (global navigation satellite system) signal jamming and receiver spoofing have become the technology's Achilles heel, slowing down its adoption while data gathered using these devices could play an increasingly vital role in often mission-critical applications. Highly autonomous vehicles are a case in point.

A number of innovations are increasing the reliability of GNSS positioning solutions. For one, Galileo, the European GNSS constellation, has implemented a long-awaited signal authentication service (Open Signal Navigation Message Authentication, OS-NMA), which it has announced should become available in 2021.[1] By emitting signed messages, GNSS receivers and the applications they enable can be sure that they are working with valid signals, making it much more difficult to spoof GNSS receivers unnoticed.

Moreover, today's modern GNSS constellations emit signals in multiple frequency bands that the latest generations of receivers are designed to track. In addition to dramatically improving the accuracy of GNSS position estimates from several meters to the order of one meter (or much lower using GNSS correction services), the redundancy these signals offer further increases the difficulty of spoofing GNSS receivers without being detected.

Better protocols
IoT devices are designed to operate under extremely tight constraints in terms of size, price, battery power, and bandwidth. Squaring these with demands for high security has been challenging, as conventional encryption methods tend to considerably increase the size of the

[1] https://insidegnss.com/brussels-view-galileo-to-transmit-open-service-authentication/

data payload that the devices have to transfer. Because data transfer is the most power-hungry process in most IoT devices, encryption thus comes at the cost of reduced power autonomy.

Recently, a new lightweight security protocol specifically tailored to the needs of such power-constrained use cases has been gaining

“GNSS receiver spoofing has become the technology's Achille's heel. ”

traction. Defined by IETF (the Internet Engineering Task Force), OSCORE, which is short for Object Security for Constrained RESTful Environments, offers a number of improvements in securing messages sent using CoAP (constrained application protocol), one of the preferred communication protocols used in LPWA (low power wide area) use cases.

First, it only encrypts the sensitive part of the data payload, which is the data, reducing message size, cutting bandwidth requirements, and saving power. And because metadata, such as the destination, is not encrypted, the encrypted message can be relayed all the way to its destination without ever revealing itself. Second, OSCORE uses pre-shared keys rather than the conventional, and significantly more resource expensive, key negotiation process, offering message sizes down to a dozen bytes - ideal for typical LPWA use cases. It looks good on paper. But the jury is still out on its success, both in terms of adoption and the actual security it offers in the field.

AI AI AI

Just as artificial intelligence and machine learning are offering new ways to gain important

“Digital twins offer a virtual platform to monitor and optimize the performance of real-world systems.”

insights from highly complex data, the technologies are offering new tools to improve IoT security. By training a machine learning algorithm with data on the bandwidth a device uses during normal operation, it can learn to recognize – and flag – abnormal behavior that would otherwise be overlooked. To save computational resources and battery power, these algorithms can be trained on the cloud and disseminated to hundreds or thousands of deployed IoT devices using a firmware-over-the-air update.

AI can also play a new role in securing connected systems at much grander scales. Across industries, smart cities, and other use cases that leverage the IoT, digital twins are gaining in importance. As virtual representations of the physical system the devices are deployed in, digital twins offer a virtual platform to monitor and optimize the performance of real-world systems. But it doesn’t have to stop there.

Rather than leaving the fine-tuning up to human security architects, the security engineers could let two artificial intelligences play cat and mouse: As one AI continuously improves the security of the overall system, the other one comes up with more and more devious attacks to thwart its defenses. In the same way that Google’s AlphaGo taught itself to play Go at a super-human level, the resulting security architecture could dramatically outperform that of a human-designed system.

Better than the blockchain

Two years after the Bitcoin bubble famously burst, the Blockchain and other distributed ledger technologies (DLTs) have all but disappeared from newspaper headlines. But behind the scenes, startups and industrial associations are hard at work looking for ways to leverage these technologies’ unique benefits. DLTs offer a highly transparent way to keep track of transactions, assets, or steps in an industrial process chain. By running highly autonomously, they can be faster, cheaper, and less prone to failures than more conventional forms of record keeping.

DLTs also offer a number of security-related benefits. Because the data is distributed across countless computers and servers, altering records stored using a DLT is extremely difficult. Data can easily be stored in encrypted form, allowing access to individual records to be tightly restricted. To cite but one example of how the technology could be used: DLTs have been proposed as a secure vault for health data, protecting patient confidentiality, and putting individuals in full control over who receives access to their data and when.[2]

While the Bitcoin was a glutton in terms of its power consumption (the Blockchain was once estimated to use more electricity than Switzerland with its eight million inhabitants[3]), other DLTs offer similar benefits with only a fraction of the power demand. But given the novelty of the technology and a number of challenges, such as ensuring the accuracy of data stored in a DLT, it may still be several years before DLTs begin to live to up the hype they generated in 2018.

Shoring up – and shaking up – security

The technologies driving improvements in IoT security are rapidly advancing on multiple fronts. Artificial intelligence, next generation data encryption and key management approaches, advances in secure hardware, and new solution architectures are increasing the sophistication of IoT security approaches, ultimately making the lives of those seeking to compromise them more difficult. Decades of experience in IT have shown that security progresses similarly to the cat and mouse game described above: It’s a continuous arms race that rapidly improves the security of leading IoT technology, benefiting product managers and end-users alike. ■

[2] Distributed ledger technology use cases, ITU-T, Technical Report

[3] https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

Expert opinion

Discussing IoT security with…

Patrick Hauert, VP, Head of IoT, Kudelski Group , and Thomas Seiler, CEO, u-blox

“When you build on soft ground, securing your business becomes a perpetual catch-22. Secure your solution by design, and from day one you will have a solid foundation upon which to build for the long-term success of your business.”

André Kudelski, Chairman of the Board and CEO of the Kudelski Group

Patrick Hauert
VP, Head of IoT, Kudelski Group

What is unique about IoT security?

Thomas Seiler – When we talk about IoT security, we are talking about very large numbers of devices that are connected to the cloud. Because they are deployed in huge quantities, they are often regarded as relatively unimportant. Take for example a temperature sensor or a device that enables connectivity: they may seem irrelevant but they are actually transporting essential information that should not be compromised.

Patrick Hauert – I agree. It's a large number of devices, with huge attack surfaces. These devices are there for a reason: someone has invested into deploying them to get something in return. Therefore, you want the devices to behave the way you expect, to keep collecting the data you asked them to collect, or to deliver some intended action. Keeping their behavior under control is key to security. Keeping the data that you are collecting and sensing secure, protecting its confidentiality and integrity, is absolutely essential. Because there is no point in collecting data if you cannot use it because you have a trust issue.

The last point of importance is: how do you ensure that you can manage the devices all the time? What people tend to forget is that devices remain deployed for years, sometimes decades or more in the case of large critical infrastructures. Having a very reliable way to manage them is absolutely key to managing the security lifecycle of these devices.

T.S. – Especially because a lot of IoT devices are standing alone. It's not like an IT system, where people are around every day to check it and

manage it. Once deployed, IoT devices are no longer attended to. This makes it very difficult to make any corrections or apply safeguarding measures. Therefore, you must build something that is really solid and cannot be compromised, otherwise the consequences could be dramatic.

P.H. – It's important to embed IoT security from day one. People tend to believe that you can defer it until later, because they want to put the functionality of a device first and get it to market quickly. But failing to include the right security foundations in the first place could lead to disaster. Fixing the problem after the fact, well, in some case it's impossible, and, in the best cases, it is very, very expensive.

Keeping a device operating the way you want it to for months and years rather than having to replace it due to security issues gives you a much better return on your investment, and people need to consider that up front building the business case for their IoT devices.

T.S. – Of course the trouble is also that the learning process takes time. In most cases, our customers don't have much experience when it comes to security and often overlook the important fact that, over a long period of time, problems could actually pop up.

Why should companies – and individuals – invest in IoT security?

P.H. - In my view, the most important reason to invest into IoT security is that you want to be able to benefit from the value of the deployed connected devices. You're deploying them for a reason. It's not because it's cool or all the hype. You expect some return on investment and need to secure that return. Ignoring security when you deploy an IoT device puts into jeopardy the chance to achieve that return.

T.S. – Of course. And often the system or deployment has a wide range, geographically or business-wise. It's not only about making money, but it's also avoiding losing money and running into risks that eventually could compromise, and maybe even bring down, an entire company. And it isn't only about security. You can even potentially get into issues of safety, where physical things and people are endangered. This can have a huge impact on reputation, a damage that is perhaps higher, even lethal to a company.

"Security by design of the technology and the whole related process is fundamental. "

P.H. - The other aspect is that you can enable a business via the IoT. If you do it right, you can enable business models that were unthinkable before because they would have been way too risky. If you do it right, you can suddenly find a way to remotely enable additional features for your customers, which is of great benefit. For instance, Tesla upselling an extended range of its fleet by unlocking the battery via a software update is an interesting business model. But you want to keep that under the protection of a trusted enablement mechanism, otherwise people would defraud it and you would lose the benefit.

T.S. – Absolutely. I think that's the additional benefit of making things secure, because you can upsell and add features that otherwise never seemed to be doable. I'm not saying that this is an immediate return on investment, because it is of course difficult to invest into security when you have not seen all the benefits yet, but here is a clear benefit showing how much more can actually be done thanks to cloud connectivity.

Does perfect security exist? And if not, what can companies or individuals do to protect themselves, their customers, and their businesses?

P.H. – First, there is no perfect security. Whatever perfect means. If by perfect we mean unbreakable, it doesn't exist. Anyone pretending that they have the perfectly secure solution is either naive, incompetent, or a crook. With enough time, the right skills, and proper funding, someone will be able to break it. So what can people do? I think the first thing is to admit that your solution or your technology will be breached one day. As soon as you admit that, you start thinking in a very different way about how to

manage and deploy your devices to keep them secure, because it forces you to ask yourself what is going to happen after the breach. What do I do? I can do a lot of things to prevent that moment from happening, but I have to admit it is going to happen. Then, I can start focusing on what comes after the breach, which is equally important as, or sometimes even more important than, that first phase. So I think that's a very good philosophy. Assume that it will happen and start thinking about how you would manage it.

And then do it from the very beginning. Think about the security in the design of your product, in the process of putting a product into the field, and also in the process of removing it. Decommissioning your product in the field is super important too from a security perspective. People tend to forget about the end of life of a product, the decommissioning, the revoking. If you provide rights to someone and don't revoke them in decommissioning, you might be opening the door to new security breaches. So security by design of the technology and the whole related process is fundamental.

T.S. – Precisely. I think it's also important to do the maximum. When you know a way to make things better, then you must go that way. You cannot make it a little cheaper, because it immediately increases the risk and probably the extra effort you have to do to make the device relatively small. Of course it needs the right knowledge, the right competencies, the right partners that can really deliver. I think that we together, u-blox and Kudelski, have a concept that is unique, that delivers the maximum bidirectional end-to-end security based on a very frequent change of security keys, making it very difficult to allow a security attack.

P.H. – You are right. You mentioned end-to-end, which is also something which is absolutely key about the security from a system perspective. We're always focusing on the device side, because that's the visible part for everybody. But there's always something in the backend that is managing the device, receiving data, or initiating commands. This entire chain must be secure.

T.S. – This is often disregarded. Sometimes people say: "Oh, I am in a cloud solution that I can just source and everything is done," but this is very often not the case. It's just superficial and it's a very different approach to making it end-to-end secure.

"You can even potentially get into issues of safety, where physical things and people are endangered. This can have a huge impact on reputation, a damage that is perhaps higher, even lethal, to a company."

At huge events such as the upcoming Tokyo Olympics, public safety is big on people's minds.[1] In the context of the Olympics, but also in general, what role does IoT security play in ensuring safety?

T.S. – Such high-profile events are of course interesting, because you can quickly gain a lot of attention. Security is also very important for such events considering the high rate of device installations and the amount of infrastructure involved. More and more devices are deployed to make things better and, therefore, when it comes to security, we should make an effort for anything that goes around such an event.

P.H. – I think the exposure is maximum. There's a huge risk of reputational damage for all the stakeholders as everybody will be watching and any incidents will immediately become big news. I think Tokyo is going to deploy a lot of solutions to make the life of the athletes and of the visitors easier, to better manage the flow of people, with autonomous vehicles to drive people throughout the city. There will be hyperconnectivity needed for the events, which also means higher exposure. We already rely a lot on facial ID to manage event admission. And then you have all the personal data, confidentiality issues, and so on. The threats will be fast, the attacks will be bigger than ever, and I think the organizers are very worried about it. They announced last year that the government is going to intentionally hack IoT consumer devices to raise awareness and make sure that the population is taking measures before it's too late. It is quite interesting that the government is passing a law to authorize a company to carry out such a hack in order to prevent attacks and to improve the situation. It's going to be big, for sure, because they cannot afford any glitch in the system. It's very interesting to watch.

T.S. – These events are also platforms to demonstrate new solutions and new technologies, especially in Asian countries this is quite prevalent. But I think that also shows how important it is that security is really at play and how much must be done to ensure it.

[1] Post-script: At the time of writing, the event was scheduled to take place in 2020.

nothing is embedded in a product component, a sub-assembly, or a finished product. It is a question of awareness and training until security becomes as much part of the specification as anything else. Security means completely changing the way we think, and this is not so easy to find these days. I think our cooperation is quite a good model: how we built such a chain together across all the levels of technology so that multiple components play well together and support each other to produce end-to-end security that is robust and cannot be easily compromised, but can be maintained over the whole lifetime of a product.

P.H. – What we are solving together thanks to our partnership is part of the complexity. We come in with something that is already an available, pre-integrated turnkey solution to security, which is easing the adoption for your customers. There's no more excuse about the complexity. The "It's too complex, I don't understand, I don't have the skills!" is going away with the way we are collaborating for our customers, so it's definitely a plus to go in this direction.

"Anyone pretending that they have the perfectly secure solution is either naive, incompetent, or a crook. "

What is keeping us from implementing robust IoT security today? Are the barriers technological? Political? Societal?

P.H. – It's a mix of all of these. There are a lot of biases against connectivity that must be overcome. The first one is awareness. Everybody's talking about security, maybe even too much. The noise level is very high and people in the public and private sectors know that something has to be done, but they seem to be struggling on how to tackle the problem. They tend to assume the problem can be managed by traditional cybersecurity methods. As a result, they're really just pushing the problem down the value chain to the adopters of IoT solutions, and the fears caused by these security risks threaten to slow the adoption of IoT altogether, and that's not good for anyone.

T.S. – It is still early days. For many products, security is not described in the datasheet, or

T.S. – Unquestionably. I think we need to continue to explain what is involved in making secure solutions. There is sometimes just superficial knowledge, some factors are quickly overlooked where things really should have been corrected. There I think communication is very important. Teaching society about IoT security, and especially our customers and specialists so that they gain a better appreciation of the vocabulary, the principles, and the dominant designs of good security solutions.

P.H. –Also, standardization and regulation are evolving, but it's at a pace that has nothing to do

with technology anymore. Waiting for the regulations to solve the problems is very naive. You'll always be late and insufficient, or you will go for the minimum acceptable common denominator, which is the lowest available security standard.

"I think that we together, u-blox and Kudelski, really have a concept that is unique, that really delivers the maximum bidirectional end-to-end security based on a very frequent change of security keys, making it very difficult to allow a security attack."

T.S. – Ideally, it should be a strong initiative to really build secure solutions and resolve such problems without need for further regulations.

Fast-forward ten years to 2030. Will we have solved the IoT security challenge?

T.S. – Whether it will be solved is indeed the question. We can of course do a lot to solve the IoT security challenge and implement it from a technical point of view. We actually have a solution today. Together, we have a chain of making things secure, as we said before. Now, it's a matter of penetration, how well it is deployed into all the various applications, how successfully we do it, with other partners as well. The question is what is the adoption rate? There is, of course, also some pain. It causes pain in finding customers of our rivals implementing at a different pace.

P.H. – I agree. Adoption is key. I think you will never have a perfect, super clean, best of breed deployment. You will always have some legacy floating around that you'll need to manage within this ecosystem. It can, therefore, be seen as a never-ending game. But the goal is to raise the security level as much as you can every time.

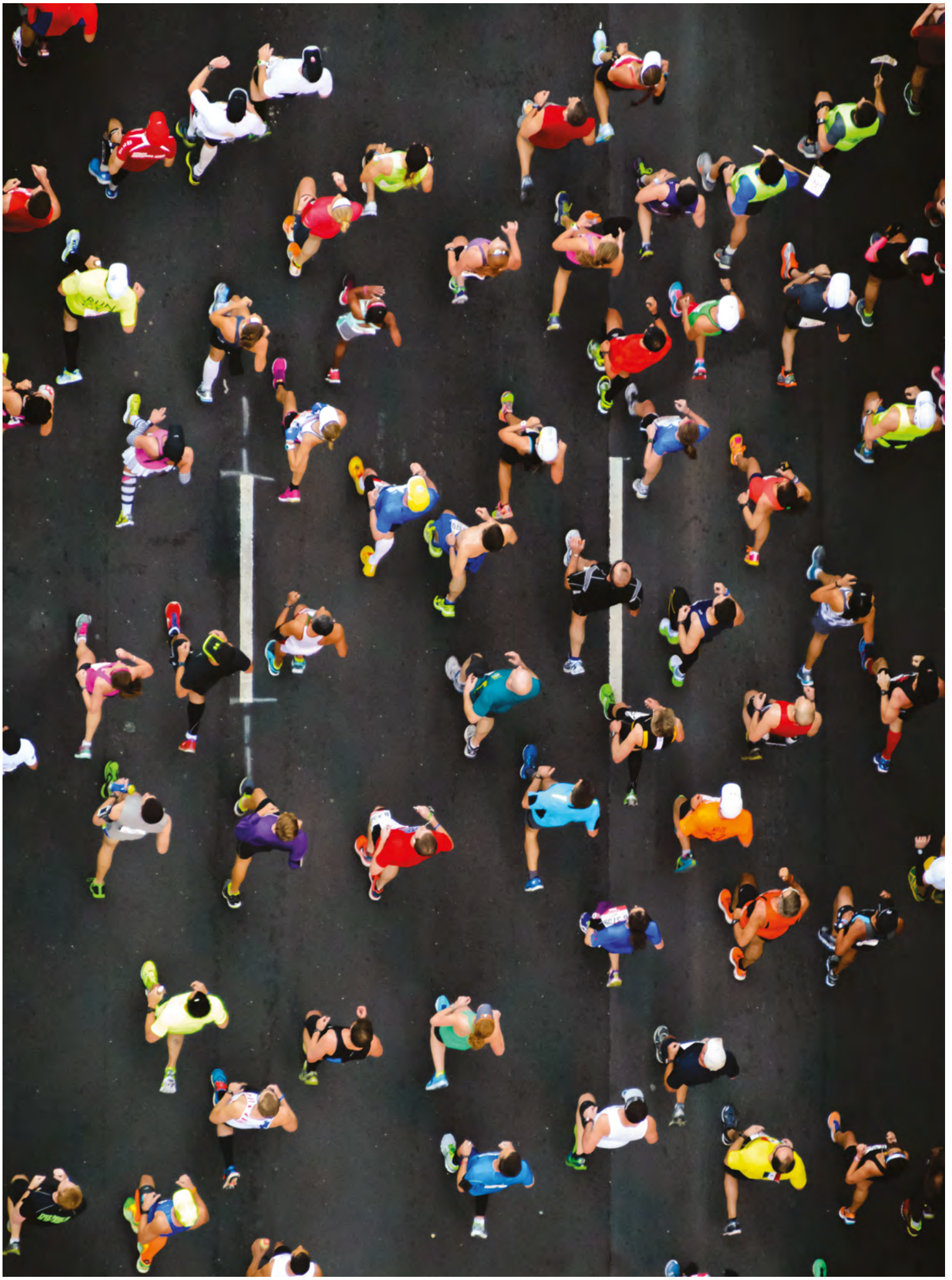
Technically, I think, fast forward ten years, we probably will have solved what we know today as the security challenge, but I can bet that some new ones will emerge in five years and beyond. What was the challenge ten or twenty years ago? Security-wise, has it been solved? We learn from history. Some people are rediscovering the hard way things we learned many years ago.

"Security means completely changing the way we think."

But if I simply look at the way our attack lab is evolving, if you take the example of an attack: ten to fifteen years ago we were using one laser to inject faults into the code execution of the CPU and it was state-of-the-art. We thought it would be impossible to sync more than two different laser sources. Today, we are keeping five to six different sources in sync at the same time. Who knows what we will be able to do in ten years - probably something nobody is dreaming of today. I therefore think it's a very fast evolving situation, but that's not an excuse to stop improving the security. You need to step up your performance every time you have the opportunity when it makes sense business-wise to move towards a bigger, better secured ecosystem.

T.S. – Of course, we are running this technological evolution. But it's also about partners. Trust is very important here: partners that deliver security that can be trusted and never compromise are absolutely essential and central. Here, we also have a personal partnership built to provide such trust to our customers.

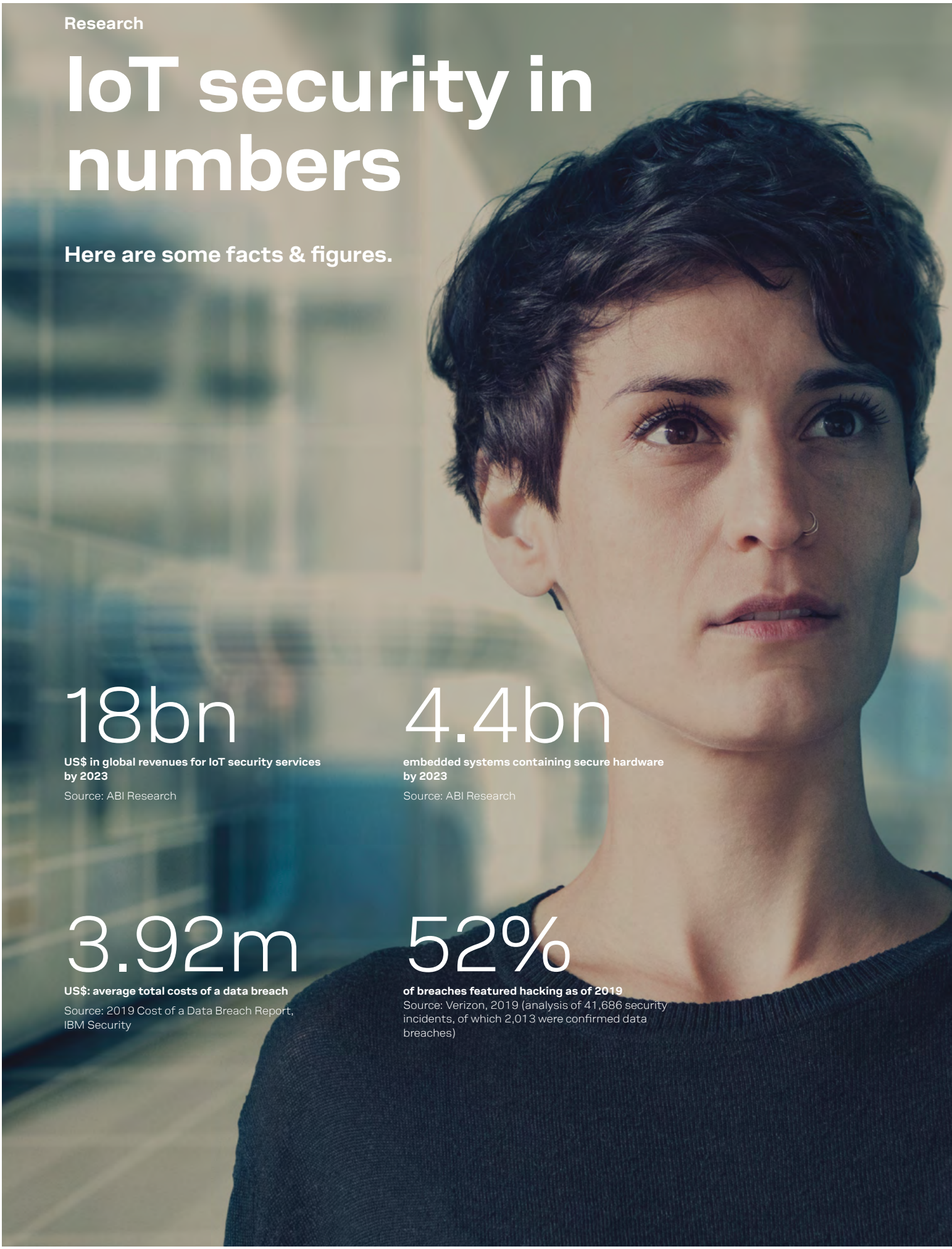
P.H. – For me the real moment of truth is when you deploy something, security issues are happening, and you are able to manage it, solve it, or get over it and you keep the trust of your customer. Those are the moments where trust grows dramatically, not forever, but for a very, very long time and that's key. This brings me back to my initial comment. You have to assume this is going to happen. The key question in the whole problem is knowing how to manage the post-breach situation. ■



Research

IoT security in numbers

Here are some facts & figures.



18bn

US$ in global revenues for IoT security services by 2023

Source: ABI Research

4.4bn

embedded systems containing secure hardware by 2023

Source: ABI Research

3.92m

US$: average total costs of a data breach

Source: 2019 Cost of a Data Breach Report, IBM Security

52%

of breaches featured hacking as of 2019

Source: Verizon, 2019 (analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches)

71%

of breaches were financially motivated as of 2019

Source: Verizon, 2019

94%

of malware is delivered via email

Source: Verizon, 2019

75%

of risk professionals believe that cyberattacks on their organizations are likely to be executed through IoT

Source: The Ponemon Institute and Shared Assessments

5min

The average amount of time that it takes for an IoT device to be attacked once connected to the internet

Source: NETSCOUT

215.7%

Jump of IoT malware attacks to 32.7 million in 2018 (up from 10.3 million in 2017)

Source: SonicWall

Transforming uncertainty into opportunity

The Digital Declaration, a GSMA led initiative, helps companies deliver what matters most to digital citizens, industry, and governments.

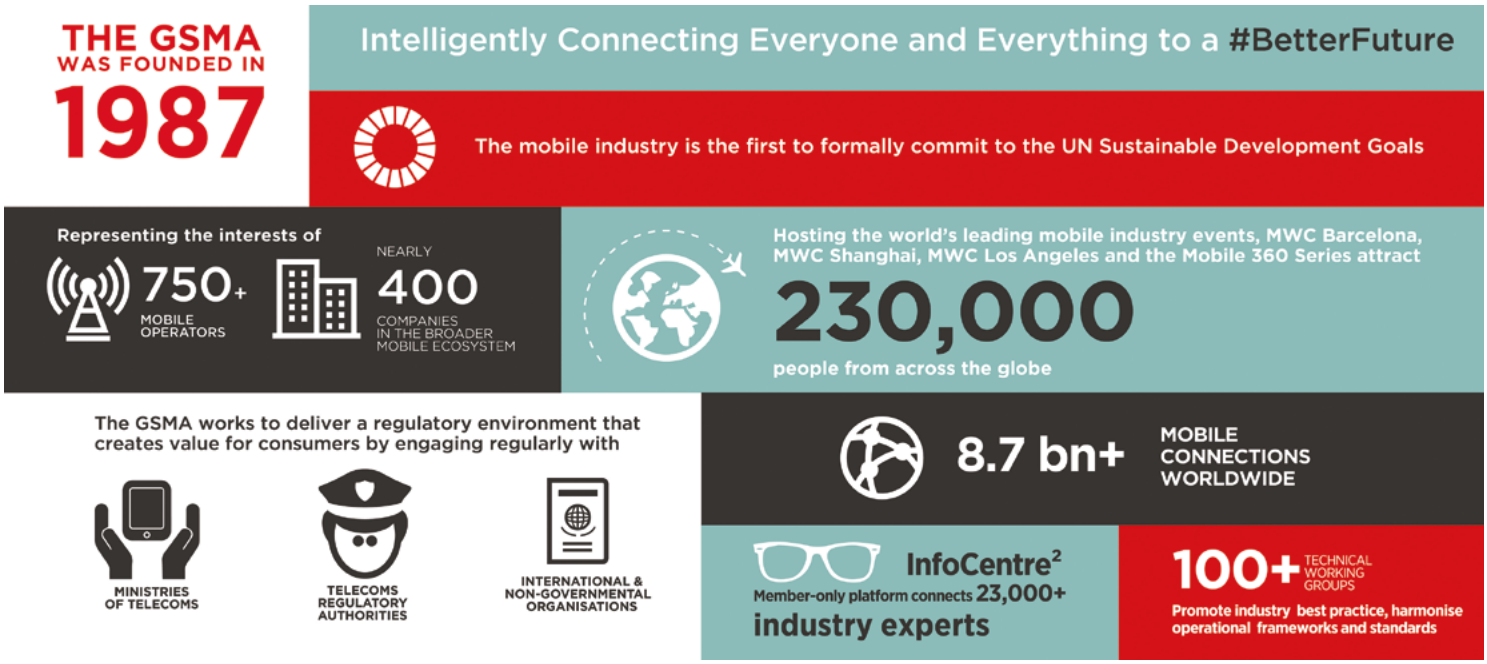
At the dawn of the 5G era, the world faces a perfect storm as technology is driving transformational changes in consumer behavior, politics, and the global economy. Despite their tremendous potential to build a better future, these changes can create uncertainty and confusion for some people. The Digital Declaration is a call to action for the private sector to step up and provide the leadership to change these uncertainties into opportunities, not just for themselves, but for all.

Announced at the 2019 World Economic Forum in Davos with the backing of 40 CEOs from across the industry, the Digital Declaration sets out aspirational guidelines that put responsible leadership at the heart of decision making, focusing technology on solving problems that are challenging communities. Today the Declaration counts more than 80 CEOs, with u-blox joining in early 2020.

At a time of considerable erosion of trust in businesses, governments, and traditional institutions, the declaration seeks to extend consumer trust for the digital age, deliver inclusive growth and opportunities for all, and foster an environment that nurtures innovation. Putting the concerns of today's customers and citizens front and center, the Digital Declaration aims to support the development of sustainable businesses that prosper and play their part in creating a better future, inspiring a new style of leadership.

IoT security key for a sustainable connected future

"Without security, the Internet of Things as we know it will cease to exist," says Alex Sinclair, Chief Technology Officer of the GSMA. "None of the three pillars of our Digital Declaration can be addressed without tackling IoT security head-on. That's why the GSMA with the mobile industry has assembled a set of IoT security guidelines and an IoT security assessment promoting best practices for secure end-to-end design, development, and deployment of IoT solutions." Leading global mobile operators, their partners,



governments, and industry bodies have since adopted the security guidelines to encourage industry-wide security for a robust and sustainable IoT.

While policymakers and regulators will play an important role in supporting the vision of the Digital Declaration, the principles specifically call on industry leaders to take the lead in setting the values and guiding principles for a sustainable digital future. "We strongly believe we will be able to deliver the promise of a positive digital future only if the private and public sectors work side by side, under a set of shared principles and values," says Mats Granryd, Director General of the GSMA, further highlighting the importance of dialogue across geographies and stakeholders.

Collaboration and cooperation are crucial for the success of the digital transformation of society, and the mobile industry has a demonstrable track record of effective collaboration that has delivered positive change. It's a role the industry aspires to play well into the future, and the Digital Declaration is a fundamental component of this strategy. "Ultimately, the goal of the Digital Declaration is nothing short of ensuring that everyone can benefit from the opportunities presented by the next wave of technological progress," Granryd concludes. ■

Learn more:
www.digitaldeclaration.com/

Saving the world on the way to school

Leveraging the power of advanced virtual reality technology, holoride has carved out a niche at the intersection of mobility and gaming, attracting attention of automakers, film studios, and the public.

Buckle up, put on your headset, and hold on tight! Using advanced virtual reality technology, holoride, operating out of Munich, Germany, is redefining the passenger experience in motorized transport by immersing passengers into interactive adventures in which they become the hero of their own journey. Whether navigating Super Mario-style fantasy worlds, shooting down spaceships, or fending off attacks from a herd of dinosaurs, what they see in their headsets maps one to one with what they feel as the car they are sitting in weaves its way through traffic.

If you get carsick reading in the back seat, you might be surprised to learn that immersing yourself into a computer-generated universe can have the exact opposite effect. By matching up the virtual world seen in a VR-headset and the vehicle's movements through holoride's technology, time lags down to just a few milliseconds. This means your brain won't register the nausea-inducing sensory conflict some people experience when reading while driving up a mountain pass. Especially for children, who are most afflicted by carsickness, holoride's solution might come as a blessing.

"We spend so much time in cars. Why not make it more exciting for the passenger in the back seat?," says Daniel Profendiner, CTO and co-founder of holoride. "Our goal is to revolutionize in-car entertainment and make a passenger's daily commute more enjoyable. Passengers not only need immersive content, but they need content tailored to the duration of their journey – that's where holoride comes in, providing elastic content to all riders. Soon, people won't just expect a car to get them from A to B; they will be seeking an experience in the process."

The company, which spun out of German carmaker Audi, made its public debut at CES 2019, where it immediately caught the attention of visitors and reporters. In its short existence – it was founded in 2018 – holoride has already racked up partnerships with several automakers – Audi, Ford, and Porsche – and film studios –

© holoride

Disney, Universal Pictures, and the Discovery Channel. The results have been spectacular: journalists that have demoed the solution have been anything from impressed to amazed by the experience.

To create such a real-time immersive experience, holoride combines data from several in-vehicle systems, from the accelerometers and gyroscopes that make up a car's inertial measurement unit to its navigation system. Based on this information, it builds a virtual world based on what they refer to as "elastic content", that is, content that responds to the vehicle's actual behavior in real-time. And as the car travels towards its destination, its position is continuously tracked by a u-blox high precision global navigation satellite system (GNSS) receiver.

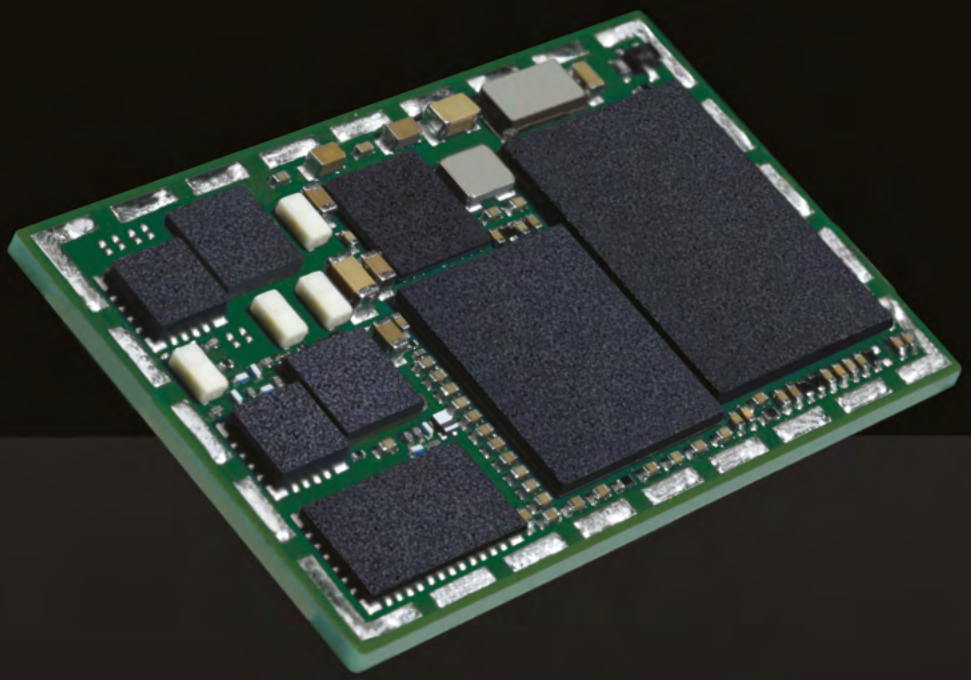
"Getting a precise position of the vehicle is crucial to providing a perfect illusion of a moving vehicle in virtual reality. A solid GNSS positioning signal is one fundamental component of that, as we are mapping all our experiences to real world roads," said Profendiner. "As we build our experiences based on real world road maps, it is crucial for us to be able to pinpoint the vehicle's positioning in the world as best as possible. The better the positioning is, the better the immersion into our virtual world."

It will be a few more years before series production vehicles are technologically fit to feed holoride's virtual reality engine. In the meantime, holoride continues to work with the best content studios, OEMs, and developers to provide unique location-based VR experiences. Location-based VR needs to offer more than putting on a pair of VR goggles at the mall to capture the attention of a broad audience, especially for those who want to be wowed. That's why holoride continues to offer content riders can't get anywhere else. ■

Learn more:
www.holoride.com

Products

In the spotlight



The latest in positioning and wireless communication technologies

Combining industry-leading quality, robustness, sensitivity, and performance with innovative features, u-blox delivers solutions, services and components that meet the needs of even the most demanding designs. We focus on business-critical applications where products need to perform 24/7 with maximum reliability, handling exceptions with minimal disruption to the overall system. Our customers expect improved productivity, quick turnaround, and a head start on their competition.

MQTT data services

Through the acquisition of IoT data service provider Thingstream,we recently expanded the u-blox service offering to include comprehensive, end-to-end solution for global IoT connectivity using the industry standard MQTT protocol.

MQTT, short for message queuing telemetry transport, has become a widely used data transfer protocol in the Internet of Things, along with MQTT-SN, which is tailored to the needs of sensor networks. Designed for constrained environments characterized by low power and bandwidth requirements, MQTT transmits messages from one device to one or many others via a broker.

Learn more:
www.u-blox.com/press-releases/u-blox-acquires-iot-communication-service-provider-thingstream

SARA-R5 series

SARA-R5 LTE-M / NB-IoT modules provide Secure Cloud connectivity with built-in root of trust (RoT), foundation and end-to-end security. The scalable, pre-shared key management system offers best-in-class data encryption and decryption, both on-device as well as from device-to-cloud.

SARA-R510M8S is pre-integrated with the u-blox M8 GNSS receiver and separate GNSS antenna interface, which provides highly reliable, accurate positioning data simultaneously with LTE communication. In addition, the module offers unique hybrid positioning, in which the GNSS position is enhanced with u-blox CellLocate® data, providing location always and everywhere.

SARA-R5 modules are ideal for smart metering, smart lighting, telematics, asset tracking, remote monitoring, alarm panels, and connected health.

Learn more:
www.u-blox.com/en/product/sara-r5-series

NINA-B4

Our NINA-B4-series of Bluetooth® low energy modules is based on Nordic Semiconductor's nRF52833 chip. NINA-B4 is the first standalone wireless module featuring Bluetooth 5.1 with direction finding and operating at 105°C. This, together with its long range Bluetooth capability and cost optimization, makes it ideal for deployment in harsh environments.

Designed to act as both a transmitter and a receiver (using angle of arrival (AoA) and angle of departure (AoD) direction finding), the NINA-B4 series brings the benefits of high precision positioning to indoor applications.

The NINA-B4 series comes either with the u-blox u-connect software, simplifying integration, or with an open CPU architecture, for customized applications.

Learn more:
www.u-blox.com/product/
nina-b40-series-open-cpu

u-blox M9

The next generation of our meter-level precision technology has finally arrived. u-blox M9 is the ultra-robust platform that caters to high performance applications in the automotive, telematics, and UAV arena.

Our NEO-M9N module provides exceptional sensitivity and acquisition times for all L1 GNSS systems. Support for concurrent reception of four global navigation satellite systems maximizes the position accuracy, also in urban canyons.

High update rates of up to 25 Hz as well as jamming and spoofing detection allow for dynamic applications such as unmanned aerial vehicles to receive position information with low latency, flagging any incoming security attacks.

Learn more:
www.u-blox.com/product/neo-m9n-module
www.u-blox.com/product/ubx-m9140-chip

Inside our IPR team's fight for FRAND licenses

By proactively managing standard essential patent licenses, we are going out of our way to protect our customers from the extreme costs and consequences of alleged patent infringement.

Wireless connected devices depend on scores of technically essential patents simply to meet the requirements set out in cellular and Wi-Fi communication standards. Across the industry, there is a broadly recognized commitment agreed to by companies active in setting technology standards. That commitment, required to participate in most standards bodies, mandates that standard members who own a standard essential patent (SEP) enter into licensing negotiations with any company requesting a license. The SEP license negotiation has limitations; the license agreed to must contain fair, reasonable, and non-discriminatory (FRAND) terms and conditions. The patent holder cannot demand a license that merely maximizes its revenues.

In reality, companies do try to maximize their revenues and securing FRAND licenses for all SEPs used in wireless products is impossible. Some companies holding SEPs are not members of any standards group and may not license their patents. Others seek to license patents to end-product manufacturers only in an attempt to receive higher payments than they would receive from a component supplier, even if doing so violates their commitment to a standards group. To achieve even higher revenues, some companies have chosen instead to sell their patents to "patent trolls," whose sole purpose is to sue end-product manufacturers who use them in their devices and receive non-FRAND returns. And lastly, others offer free licenses with restrictions or no licenses at all, but only use the patents defensively to protect themselves if sued for patent infringement.

An obvious consequence of these various practices is that many wireless product manufacturers bring their devices to the market before potential patent use disputes have been resolved and without understanding the substantial risks involved. Not fully understanding SEP practices and managing the patent risks can make wireless device development a financially risky and potentially highly litigious business. SEP litigations can cost tens of millions of dollars in legal fees and internal costs, substantially

disrupt business, or even shut the business down altogether. The u-blox IPR team can help companies understand and manage these risks. Our IPR team has an intimate understanding of wireless standards and SEP licensing practices, and routinely works with our customers to navigate these patent rights minefields.

A unique, proactive approach

"u-blox respects the intellectual property rights of others and has always been and continues to be a willing licensee to standard essential patents," says Thomas Seiler, CEO of u-blox. To protect our customers, the u-blox IPR team has had to file lawsuits to obtain FRAND licenses for SEPs used in our modules, both to give customers the licensing terms to which they are entitled and to protect them from potential litigation in the future. "We believe that our willingness to license, as well as fight for FRAND terms and conditions in the license, positively distinguishes u-blox within the module industry and offers substantial value to our customers."

u-blox's unique and proactive standard essential patent licensing practices for cellular connectivity reduce the risk for our customers from being sued by some SEP holders for infringement, or worse, being banned from importing products into a country based on an alleged SEP infringement. We work strategically to reduce the risk of SEP-related injunctions and lawsuits, thereby reducing the risk of SEP-based business disruptions and unknown costs for our customers. And finally, we provide technical and SEP support where warranted. ■