Cutter IT Journal

The Journal of Information Technology Management

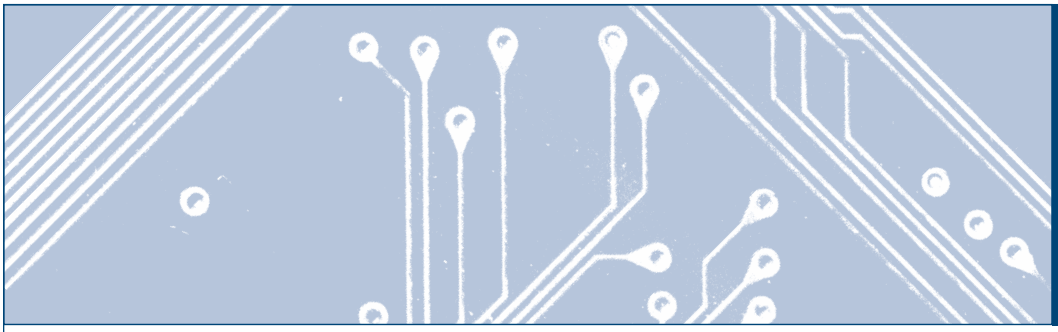
Vol. 29, No. 7, July 2016

"In recent years, a vast range of devices and systems have been designed to support the Internet of Things paradigm, but with little regard to security or privacy — despite the profound impact that breaches of either can have on a user's 'real life.'"

— George Loukas and Charalampos Patrikakis, Guest Editors

Security in the Internet of Everything Era

CUTTER CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster debate and dialogue on the business technology issues challenging enterprises today, helping organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its companion *Cutter IT Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly.

Cutter IT Journal subscribers consider the *Journal* a "consultancy in print" and liken each month's issue to the impassioned debates they participate in at the end of a day at a conference.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and *Cutter IT Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. *Cutter IT Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Cutter Business Technology Council:
Rob Austin, Ron Blitstein, Tom DeMarco, Lynne Ellyn, Vince Kellen, Tim Lister, Lou Mazzucchelli, and Robert D. Scott

Founding Editor: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Chris Generali
Managing Editor: Karen Pasley
Production Editor: Linda Dias
Client Services: service@cutter.com

Cutter IT Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: citjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). Print ISSN: 1522-7383; online/electronic ISSN: 1554-5946.

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.


Opening Statement

by George Loukas and Charalampos Patrikakis, Guest Editors

> On "teleautomation": When wireless is perfectly applied, the whole Earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance … and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.
>
> — Nikola Tesla, 1926

Since Tesla's prediction of "teleautomation," it has taken almost 80 years for the general public to experience what has culminated into the Internet of Things (IoT) and another 10 to truly accept it. The problem is that, in recent years, a vast range of devices and systems have been designed to support this new paradigm, but with little regard to security or privacy — despite the profound impact that breaches of either can have on a user's "real life."

This edition of *Cutter IT Journal* features five articles that discuss existing and future (but not at all fictional) risks in what we currently call the Internet of Things and that in the very near future will evolve into the Internet of Everything (IoE). It presents examples of risks and attacks in the different domains of our personal life, commercial world, and industry in which IoT devices are used, and highlights the corresponding technological and managerial challenges for confronting — even anticipating and warding against — security attacks.

The issue starts with an article from the two of us, in which we provide a quick look into the cyber and physical threats to the Internet of Everything. The article decomposes the IoE into layers representing the cyber and physical aspects that attackers can target and proceeds with a report on threats, attacks, and their impact to each layer. Providing examples from three domains that are currently experiencing dramatic changes thanks to IoT technologies (automobility, domestic environments, and well-being/healthcare), it serves as an introduction to the issues and challenges addressed in more detail by the articles that follow. One of the article's key observations is that looking back in history for inspiration may not be a bad approach when it comes to securing the IoT, as many if not most of the challenges it brings with it are by no means new.

We continue with an article by Cutter Senior Consultant Claude Baudoin, who discusses the challenges of tackling both connectivity and security in the Industrial Internet of Things (IIoT) ecosystem, as these are introduced through the needs of access control, data protection, design, and enforcement of policies and risk management. The article's focus is not only on the technological framework powering the IIoT and the use of technologies for remote access/control and secure data communication between devices. Instead, it provides an example-driven holistic approach in which IIoT security is pursued through the early adoption of policies in IIoT systems design.

In "Social Engineering in the Internet of Everything," Ryan Heartfield and Diane Gan provide specific examples of complex and effective deception-based attacks. Going beyond the reporting of actual attack cases, the authors discuss a series of hypothetical but very convincing social engineering attacks that can be facilitated by smart connected devices in the IoE era. Asking the question "Would your fridge lie to you?" they chart this new and vast landscape of potential deception vectors, which is a security angle that not many people have started thinking about. Yet considering how conventional phishing has evolved, it seems only logical that IoE-based deception attacks constitute the next battleground in cybersecurity.

Our fourth article is by David Tayouri, who discusses the different threats that IoT devices are exposed to, emphasizing personal, household, and everyday use devices and giving examples of attacks or proven vulnerabilities. In addition to identifying the threats, Tayouri provides very clear and well-thought-out suggestions as to what can be done in order to protect the IoT against them and elaborates on the reason the threats have not been effectively addressed up to now. He concludes by proposing action on a number of fronts: legislation, regulation, and, importantly, consumer practices as well.

Finally, in "Security and Privacy in the Internet of Things: How to Increase User Trust," Dimitrios Kogias discusses privacy issues related to the Internet of Things and the impact security attacks on the IoT may have on the protection of personal data. He also presents an overview of privacy-enhancing technologies (PETs) and security solutions and discusses how they can enhance user trust in the IoT.

From this issue, there are several points to take away:

- The wider the (inevitable) adoption of IoT technologies, the greater the range of cyber-physical threats and risks to our professional and personal lives. The physical world's increasing dependence on the IoT is a key factor in the proliferation of cyber-physical attacks (i.e., cybersecurity breaches with adverse physical impact).
- While the range of threats and risks is widening, age-old security design principles and cyberhygiene can go a long way in helping protect the IoT landscape against threats to our security and privacy.
- For targets of higher criticality, such as those in the Industrial Internet, a rigorous threat assessment and appropriate governance and organization are necessary to ensure the effectiveness of defense-in-depth and any technical security solutions put in place.

The Internet of Things — or better, the Internet of Everything — has yet to unfold its full potential to us: a world where humans and machines can communicate and collaborate for improving the quality not only of life, but of everything. Again, Tesla prophesied it with amazing prescience:

> We have soon to have everywhere smoke annihilators, dust absorbers, ozonizers, sterilizers of water, air, food and clothing, and accident preventers on streets, elevated roads and in subways. It will become next to impossible to contract disease germs or get hurt in the city, and country folk will got to town to rest and get well.

It is up to the industry to take security into account from the design phase of IoE devices — and up to the users to demand it. We are confident that the articles in this issue will trigger ideas and provoke thoughts in this direction. We hope you will enjoy them.

George Loukas is Associate Professor in Cybersecurity at the University of Greenwich (UK). Dr. Loukas is principal investigator for several large-scale EU and UK research projects in cybersecurity, ranging from the security of autonomous vehicles, to secure collaboration of communities and law enforcement agencies, to studying the emotional impact of security breaches in smart home environments. He is the author of Cyber-Physical Attacks: A Growing Invisible Threat*, one of the first textbooks dealing with cybersecurity breaches with adverse physical impact. He can be reached at G.Loukas@greenwich.ac.uk.*

Charalampos Patrikakis is an Associate Professor in the Department of Electronics Engineering of Piraeus University of Applied Sciences (Greece). Dr. Patrikakis has participated in more than 30 research programs and is currently scientific/technical coordinator of two European projects in the area of security. He has more than 100 publications and two contributions in national legislation. Dr. Patrikakis is a senior member of IEEE. He can be reached at bpatr@teipir.gr.

UPCOMING TOPICS IN CUTTER IT JOURNAL

AUGUST

Whynde Kuehn

Business/Customer-Driven Digital Transformation

SEPTEMBER

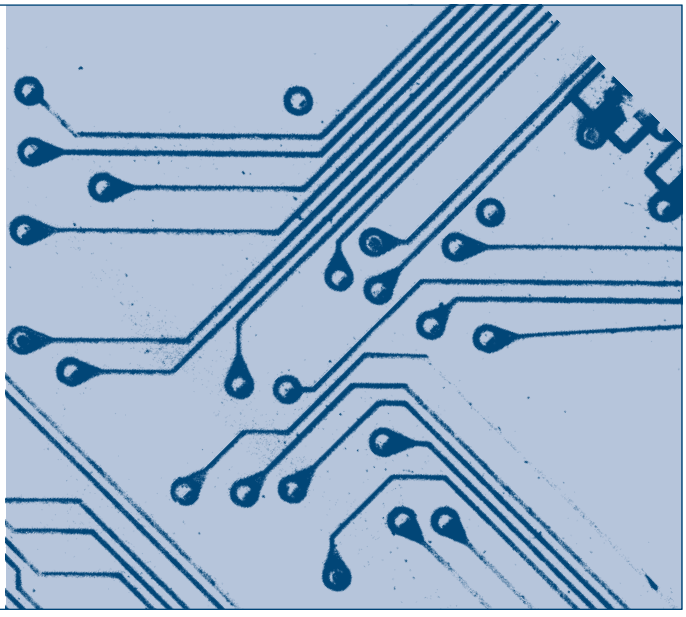
Philip O'Reilly

FinTech

OCTOBER

Paul Harmon

Cognitive Computing



Cyber and Physical Threats to the Internet of Everything

by George Loukas and Charalampos Patrikakis

> Prepare for the unknown by studying how others in the past have coped with the unforeseeable and the unpredictable.
>
> — George S. Patton

What does a quote by General Patton have to do with cyber and physical threats and the Internet of Things (IoT)?

After over 40 years of the Internet faithfully serving the needs of the Earth's human population for information, communication, and entertainment, we have now entered the era of the IoT. Of course, when we refer to the Internet, we also mean the Web and therefore the Web of Things (WoT), where distributed applications benefitting from networking through the Internet are no longer a privilege of humans. *Things* can also take full advantage of the capabilities, simplicity, and potential of Web technologies and protocols. Following current developments in this field, it is not difficult to see the inevitability of the convergence of the two worlds, of humans and of things, each using the Internet as a primary means of communication. Possibly the most appropriate term to describe this evolution has been proposed by Cisco: the Internet of Everything (IoE), which "brings together people, process, data, and things to make networked connections more relevant and valuable than ever before."[1] In the IoE era, machines are equal to humans as Internet users.

In an ecosystem in which everything is connected, and where physical and cyber converge and collaborate, the threats of the two worlds not only coexist, but also converge, creating a still largely unknown environment, in which an attack in cyberspace can propagate and have an adverse effect in physical space and vice versa. So how can we be prepared for and confront this new unknown? How can we study and learn from the ways this has been dealt with in the past? First, it is important to simplify the problem by attempting to identify the components of IoE and the threats and effects an attack can have in each one.

Composing the Internet of Everything and Decomposing It to Its Threats

Let us pick up the thread of IoE evolution and follow it back to its origin, identifying its composing elements and corresponding threats in terms of attack impact and means to achieve it. We will not use the standard computer network practice of visualizing a layered hierarchical structure, as the one found in OSI or TCP/IP layers, but will structure the components based on their physical or virtual representation, with the cyberworld built on top of the physical (see Figure 1). In this representation, we can identify four different layers of components for the IoE:

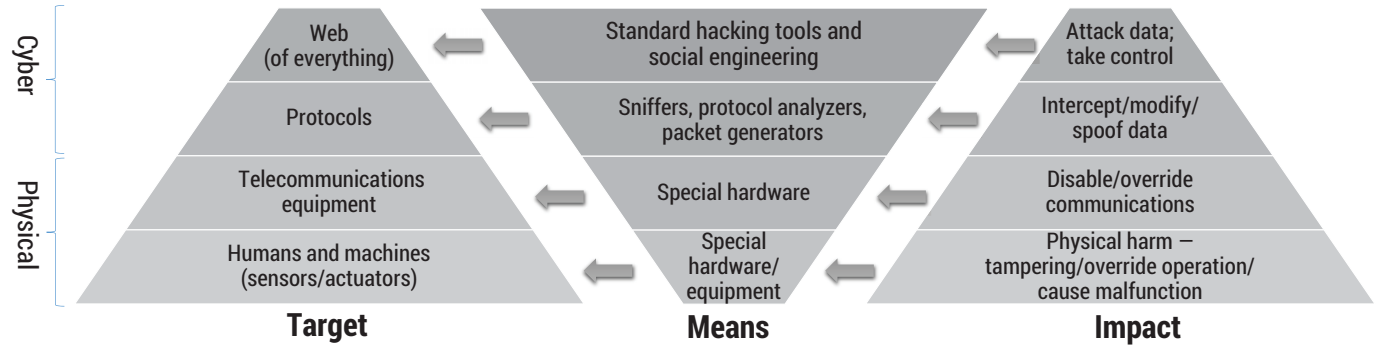


Figure 1 — Attacking the Internet of Everything.

1. The lowest physical layer corresponds to the "everything" of the IoE, including humans and things (i.e., sensors, actuators, and embedded systems that combine them). This is the basis of the physical part of our representation, including all communicating members in the IoE ecosystem. The impact of a possible attack here can directly affect humans or things by causing an adverse physical effect to humans or operation of devices that does not comply with their specification or their users' intentions. This may require special hardware and equipment that can affect the operation of machines and, through them, the physical privacy, convenience, or — in extreme cases — health and safety of human beings (e.g., as a result of a physical explosion in the context of the Industrial Internet or a malfunctioning life support medical device).

In a connected world, we tend to take the telecommunications infrastructure for granted, focusing only on protocols and applications.

2. The physical world representation is completed by the telecommunications equipment. In a connected world, we tend to take the telecommunications infrastructure for granted, focusing only on protocols and applications. Even though an attack at this level would require considerable access to resources, the results could be catastrophic, as the clear impact of such an attack would be to render all of the communication infrastructure incapable of operation in its intended way (or even to completely disable it). Such attacks are achieved through special hardware, which is able either to operate in a non-standard way (thereby overriding communications) or damage communication equipment (e.g., signal jammers, frequency transmitters).
3. From the physical part of the IoE pyramid, we now move up to the cyber part, the lower layer of which consists of the communication protocols. This part is probably the most familiar to communication engineers, as attacks here target the transport of data in order to intercept it, modify it, and/or prevent it from reaching its intended destination, or simply to generate illegitimate traffic. As this is the most widely studied layer, there are several means and tools for achieving any kind of mischief in this space, such as protocol sniffers and analyzers, packet generators, and so on.
4. The top layer is the most recently introduced, but also the one that is evolving the most quickly: the Web of Things. Here, the attacks no longer target the communication between IoE entities, but the actual purpose for the communication, focusing on the information/data and control. Depending on the target, standard hacking tools or social engineering can be used.

Based on these four layers, we refer to those attacks that target the sensing and telecommunications infrastructures as physical security breaches, while we refer to attacks that target the IoE at the level of the protocols and the WoT as cybersecurity breaches. The following is a brief overview of security threats that correspond to each of the four layers.

Physical Security Breaches

Sensing

Depending on the type of sensing technology a system uses, a capable adversary with physical access may attempt to deceive the sensor.[2] For instance, some infrared sensors are known to have difficulty detecting objects hidden behind window glass. Wearing a costume made of foam or other material that absorbs sound waves can theoretically defeat ultrasonic motion sensors. Full-body scanners based on backscatter X-ray imaging technology might fail to detect a pancake-shaped plastic device with beveled edges taped to the abdomen, a firearm affixed to the outside of the leg and scanned against a dark background, and so on. These techniques for deceiving sensors used by physical security systems have been proven experimentally and documented publicly by researchers.[3]

One particularly impressive example of such experimental attacks aimed to defeat lidar (Light Detection and Ranging) by producing an overwhelming number of spoofed echoes or objects.[4] This could be loosely characterized as a sensory channel denial of service attack. A simpler but no less effective attack on cameras has been demonstrated by the same authors.[5] By emitting light into a camera (e.g., with a laser pointer), they showed that it is possible to blind the camera by rendering it unable to tune auto exposure or camera gain, effectively hiding objects from its view.

Another interesting example is the use of sound-based attacks that aim to impede the ability of drones to maintain themselves in an upright position. This approach, described by researchers at the Korea Advanced Institute of Science and Technology,[6] works by generating a sound at a frequency close to the resonant frequency

of a drone's micro-electro-mechanical-system gyroscope. If the gyroscope's resonant frequency is within the audible range, as is the case for several types used in commercial drones, the sound causes resonance. This increases severely the standard deviation of the gyroscope's output and consequently incapacitates the drone. The civilian drone used in their experiments crashed shortly after the attack every time.

Telecommunications

As telecom operators are rapidly embracing the cloud in order to improve their efficiency in operations, services rollout, and content storage and distribution, the need for cloud security is becoming critical, yet security strategies seem to be in place for only 50% of telecom companies.[7] In addition, the emerging trend of "shadow IT" (i.e., the use of IT systems within an organization without the involvement of corporate IT) intensifies security and privacy risks, adding personal data protection requirements to the traditional challenge of uninterruptable service provision.

Cybersecurity Breaches

Protocols

In order to enable communication between things in the IoE, different protocols governing communication at all layers of the communication stack need to be deployed, each presenting different challenges in terms of security. Though the risks and impacts are well known (i.e., interception of communications, alteration of transmitted data, spoofing of information), the tools and means that attackers can use to achieve these impacts differ. As new protocols appear, new threats (in the form of old ones appearing in new clothes) arise, and countermeasures have to be reinvented. Unfortunately, there is no recipe for success here, as past experience is only to the advantage of the attackers. After all, you have to know the threat before you can confront it.

Web of Things

As in the case of the World Wide Web, attacks here may have little to do with the communication or even the computing infrastructure. The virtualization offered by the Web, where traditional services have been substituted by their "e-quivalents," has opened a new world of cyber rather than physical threats. Instead of someone capturing something tangible and asking ransom for it, ransomware can block access to an electronic asset or service and ask for ransom in an automated manner. In the case of devices and things being part of the WoT, the situation can get even worse: seizing access to critical infrastructure could lead to serious hazards affecting public health or other key public sector services. With electronic devices controlling practically every critical infrastructure, from power grids to telecommunications and even elections, protecting the connected things over the Web from cyberattacks is critical.

The need for cloud security is becoming critical, yet security strategies seem to be in place for only 50% of telecom companies.

An Overarching Threat: Deception

Traditionally, the attack avenue that has overcome most technical security measures is deception. In computer security, the term used is "semantic attack," which is "the manipulation of user-computer interfacing with the purpose to breach a computer system's information security through user deception."[8] Although not as precise, an umbrella term that is commonly used for both technical and nontechnical deception attacks of this sort is "social engineering." Social engineering attacks can range from email phishing and infected website adverts to fraudulent Wi-Fi hotspots and USB devices with misleading labels, all of which aim to lure human users into disclosing private data, such as their password, or performing some compromising action such as downloading malware. The great strength of deception-based attacks is that technology security measures can be rendered irrelevant. For instance, it does not matter whether users have installed strong firewalls and antivirus systems in their home network if they themselves are fooled into downloading malware on the smartphone that they have linked to all their smart home devices.

To an extent, the concept of deception can be extended to physical threats. Examples would include most sensory channel attacks described in the previous section, as their aim is likewise to deceive (in this case a sensor rather than a user). Sensor-based systems are designed and operate with the assumption that they can trust their sensors to provide an honest — even if inaccurate — representation of their physical environment. Sensory channel attacks ensure that this is not the case.

Use Cases

To illustrate the extent and breadth of cyber and physical threats to the IoE, we have chosen to focus on the aspects that directly and comprehensively affect a citizen's actual safety and perception of safety. In this section, we discuss the brief history, current state, and future of physical and cyber threats to automobility, the domestic environment, and well-being. For each one, we investigate whether General Patton's approach of turning to (safety and security) history for solutions would help.

It is seen as so obvious that citizens' private cars will become targets of cyberattacks that researchers have already started studying the impact that future cybersecurity warnings will have on drivers.

Automobility

Over the past seven years, attacks on modern connected cars have become a highlight in pretty much every high-profile security conference. It would not be an exaggeration to observe that there is such a thing as automotive cyber fatigue, with reports of different models of cars hacked making the news every week. In fact, it is seen as so obvious that citizens' private cars will become targets of cyberattacks that researchers have already started studying the impact that future cybersecurity warnings will have on drivers.[9] Will drivers interpret the warnings correctly? Will they be affected psychologically, and would that by itself compromise their safety? This is a concern in the IoE in general. It is accentuated in the automotive sector because of the imminent danger to drivers and passengers posed by a mere distraction from a security warning, let alone an extensive security breach affecting the engine or brakes.

But surely this is not the first time the automotive industry has had to deal with driver distraction from warnings. The European Union (EU), US, and several countries have developed rigorous guidelines for the provision of information to drivers in a manner that reduces driver distraction by taking into account single glance duration, amount and priority of information, and so forth. In 2015 the International Organization of Motor Vehicle Manufacturers issued a recommended worldwide distraction guideline policy,[10] which can be adopted by engineers developing mechanisms and content for in-car cybersecurity warnings as well. It is also not the first time the automotive security sector has dealt with command injection attacks that render critical systems unavailable. For example, large-scale EU-funded projects, such as FP7 EVITA,[11] have provided practical solutions for securing the communication and embedded computation of modern cars since the previous decade, long before concerns about the cybersecurity of cars reached the mainstream media. The increased vulnerability of modern cars to cyber-physical threats due to recently introduced technologies can be addressed with existing security mechanisms, as long as the buyer is willing to pay for them. So, it is more a matter of price elasticity than of availability of cyberprotection solutions for cars.

Currently, sensory channel attacks can be considered too exotic to be a significant concern. This is expected to gradually change as automation and reliance on sensing increases, especially in the automotive sector. A prime example is the driverless car, which is expected to become a commercial reality in the next decade. As driverless cars depend heavily on lidar, a low-cost device that generated volumes of misleading fake objects would render them completely unable to operate. This would be a very intelligent type of attack without doubt, but from the perspective of automotive safety, the end result is an unreliable or unavailable sensor. If one ignores for a moment the malicious intent, this is just one more case of a sensor reliability problem, which mathematicians, computer scientists, physicists, and engineers have addressed in great detail over several decades. After all, given the adverse environment in which a car's sensor operates, it is much more likely to fail naturally than as a result of a sensory channel attack. Therefore, redundancy (i.e., using more than one sensor for the same data collection, often supported by an algorithm for estimating a sensor's predicted measurements) and diversity (i.e., using more than one type of sensor for the same problem and cross-correlating their data) are natural solutions for cyber-physical resilience, too.

The Domestic Environment

Most smart home devices are small and inexpensive. They frequently have to offload their processing and storage to a cloud environment and rely on the home router for security, unable to provide any sophisticated onboard protection mechanism. On a real-world commercial level, security is usually limited to a simple authentication mechanism, typically a password, which is often left to its factory default, in addition to HTTPS encryption of network traffic. Guessing or stealing the

password via commonplace social engineering semantic attacks or compromising any of the control interfaces of the smart home, such as the owner's smartphone or a corresponding cloud-based interface, is sufficient to take full control of its devices. In practice, it has been argued that a typical smart home's only real protection is the fact that network address translation (NAT) prevents individual devices from being directly visible on the Internet and that the number of devices globally is still not large enough to economically justify the focus of organized cybercriminals. This is rapidly changing. The total number of connected devices (including smart homes, wearables, and other smart devices) is projected to grow to between 19 and 40 billion globally by 2019.[12]

Yet the reality is that almost all actual cybersecurity breaches publicly reported in this context have involved no extraordinary effort or advanced hacking techniques and would have been prevented if common sense and age-old security design principles, such as those proposed by Jerome Saltzer and Michael Schroeder in the 1970s, had been followed (see sidebar).[13] Take, for instance, the principle of the *least common mechanism*. Companies that develop cameras for home automation systems tend to reuse their code for multiple versions and multiple models, but assumptions originally made about their use may no longer be valid as more features are added, leading to libraries with excess features and security holes. Similarly, such principles as *economy of mechanism* and *minimization of attack surface* are commonly violated by smart lock developers. For example, in a home with multiple door entrances (e.g., a main one with a smart lock and a conventional one from the garage), a user may accidentally unlock more doors than the one they used when returning home. That is because of the (possibly excessive) auto-unlock feature, which unlocks a door when the user is returning home and is within 10 meters (for Bluetooth low energy) of the door. However, just because a user is near a door does not necessarily mean that they intend to unlock it.

Similar examples of violations of the basic security design principles can be found behind most security failures in domestic environments. The problem is that embedded system developers simply do not know them. In fact, these principles (as well as other relevant subjects, such as wireless networks and cloud computing) are often omitted from the curricula of software engineering bachelor's degree programs. Making sure that basic security design principles are included in software developers' education and expected by standardization bodies would be sufficient to prevent the vast majority of security breaches without needing to develop new security technologies.

Saltzer and Schroeder's Security Design Principles

1. **Economy of mechanism.** Keep the design as simple and small as possible.
2. **Fail-safe defaults.** Base access decisions on permission rather than exclusion.
3. **Complete mediation.** Every access to every object must be checked for authority.
4. **Open design.** The design should not be secret.
5. **Separation of privilege.** Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
6. **Least privilege.** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
7. **Least common mechanism.** Minimize the amount of mechanism common to more than one user and depended on by all users.
8. **Psychological acceptability.** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Well-Being and Healthcare

The episode of the TV drama *Homeland* in which terrorists assassinate a senator by tampering with his pacemaker (accelerating his heartbeat) was seen by many as far-fetched, but it was a scenario that former US Vice President Dick Cheney considered sufficiently realistic in 2007 to ask his doctors to disable his pacemaker's wireless functionality.[14] This was long before "connected healthcare" and today's numerous options of available wearable devices. In fact, the term "wearable" already falls too short in describing the variety of devices capable of monitoring and wirelessly reporting on well-being and personal health status. If we were to correctly identify all options, then we should also add implantable, adhesive, patched, and even ingestible devices. Regarding the latter, the US Food and Drug Administration (FDA) recently declined to approve the first mass-market drug incorporating an ingestible sensor (a collaboration between Proteus and Otsuka Pharmaceuticals), instead requesting more tests and "data regarding the performance of the product under the conditions in which it is likely to be used, and further human factors investigations."[15]

Despite this temporary regulatory roadblock, it is inevitable that personalized, daily monitoring of our health conditions and well-being will be carried out through the use of one or more devices, while it is also

only a matter of time and acclimation before we widely accept a more active role for these devices: insulin pumps, drug infusion pumps, and pacemakers with integrated defibrillators. The FDA has already acknowledged the criticality of the situation, issuing recommendations on how manufacturers should safeguard medical devices against cyberbreaches, making security by design a top priority.

The Internet of Everything may be much larger than the Internet we have become used to, but it is still the Internet.

In terms of safety criticality, there appears to be a distinction between devices that are related to health issues (e.g., a blood pressure monitor device and or app) and those that relate to well-being (e.g., calorie calculators, apps to help you cut smoking), but even this is debatable. Imagine your bedside device, programmed to lull you to sleep through the gentle sound of waves and wake you up at the right time (based on your sleep cycle) with the sweet sound of a nightingale. It does not take more than compromising your IFTTT account to change the settings so that at 3 am you're woken up to a loud AC/DC power riff. Or consider a compromised training app that pushed you to speed up for the last mile on your jogging run, instead of stopping you based on your (increased beyond normal) heart rate readings. If you are in good health, these breaches would simply be nuisances, but for a person with a heart condition, they could be life-threatening incidents.

So where in security practice do we turn for inspiration when it comes to protecting our well-being and health from cyberattacks? Suitably, it is probably more about hygiene (i.e., cyberhygiene) than anything else. Medical devices in hospitals are notorious for relying on very old operating systems (e.g., Windows XP in network-connected MRI machines) that have long been discontinued in every other industry and are no longer supported officially. It is not that demanding to expect medical software developers to provide updates in the same way as the rest of the IT industry, but will hospitals install them? Introduction of cyberhygiene training would be the minimum requirement for the needed culture shift. It would also help if medical personnel refrained from leaving Post-it Notes with their shared account passwords on hospital computers.

Then, there is privacy in wearables. This is commonly based on proprietary/secret cryptography methods, so as to tick the "encryption" box, but closed cryptography is never as robust as open cryptography because it has not been subjected to the same level of scrutiny. It is a key principle in cryptography, set by Dutch cryptographer Auguste Kerckhoffs in the 1880s, that a cryptographic system "must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience." Once again, following cyberhygiene and age-old security principles should be sufficient to thwart most realistic cyber-physical threats.

Parting Thoughts

Security is about protecting from realistic threats that require realistic effort. Protecting against extraordinary threats that require extraordinary effort has never been a goal in this sector, because it would simply never be practical. The advent of the IoT, and soon the IoE, has undoubtedly expanded the attack surface and the range of our daily life activities that are affected. By supporting devices rather than being supported *by* devices, the Internet of Everything may be much larger than the Internet we have become used to, but it is still the Internet. If we have been able to produce trustworthy communication over basic communication infrastructure and network protocols designed in the 1970s, there is little fundamentally new in terms of emerging threats in the IoE. It is still about protecting systems and networks by following security principles that have withstood the test of time, whether these are the original principles by Saltzer and Schroeder, modern cybersecurity hygiene practices, or mere common sense, preferably cultivated through security education for software developers and awareness programs for users.

Endnotes

[1]"Internet of Everything FAQ." Cisco (http://ioeassessment.cisco.com/learn/ioe-faq).

[2]Loukas, George. *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann (Elsevier), 2015.

[3]Mowery, Keaton, et al. "Security Analysis of a Full-Body Scanner." *Proceedings of the 23rd USENIX Security Symposium*. USENIX Association, 2014 (www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-mowery.pdf).

[4]Petit, Jonathan, et al. "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR." Paper presented to *Blackhat Europe*, Amsterdam, Netherlands, November 2015 (https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf).

[5]Petit, Jonathan, and Steven E. Shladover. "Potential Cyberattacks on Automated Vehicles." *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, No. 2, April 2015 (http://goo.gl/N2Z8eL).

[6]Son, Yunmok, et al. "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors." *Proceedings of the 24rd USENIX Security Symposium*. USENIX Association, 2015 (www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son-updated.pdf).

[7]Ben-Shimol, Snir. "Today's Cyber Security Threats in the Telecom Industry." Radware, 23 March 2016 (https://blog.radware.com/security/2016/03/cyber-security-threats-in-telecom/).

[8]Heartfield, Ryan, and George Loukas. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks." *ACM Computing Surveys*, Vol. 48, No. 3, February 2016 (http://dl.acm.org/citation.cfm?id=2835375).

[9]Altschaffel, Robert, et al. "Simulation of Automotive Security Threat Warnings to Analyze Driver Interpretations and Emotional Transitions." Chapter 5 in *Computer Safety, Reliability, and Security*, edited by Floor Koornneef and Coen van Gulijk. Springer, 2015.

[10]"Recommended OICA Worldwide Distraction Guideline Policy Position." International Organization of Motor Vehicle Manufacturers (OICA), March 2015 (www.oica.net/wp-content/uploads//OICA-Position-Paper-Driver-Distraction-Final-2015-03-03.pdf).

[11]Henniger, Olaf, et al. "Securing Vehicular On-Board IT Systems: The Evita Project." Paper presented to the *25th Joint VDI/VW Automotive Security Conference*, Ingolstadt, Germany, October 2009 (www.evita-project.org/Publications/HRSW09.pdf).

[12]Thierer, Adam, and Andrea Castillo. "Projecting the Growth and Economic Impact of the Internet of Things." Mercatus Center, George Mason University, 2015 (http://mercatus.org/sites/default/files/IoT-EP-v3.pdf).

[13]Saltzer, Jerome H., and Michael D. Schroeder. "The Protection of Information in Computer Systems." *Proceedings of the IEEE*, Vol. 63, No. 9, September 1975 (http://web.mit.edu/Saltzer/www/publications/protection/index.html).

[14]Clery, Daniel. "Could a Wireless Pacemaker Let Hackers Take Control of Your Heart?" *Science*, 9 February 2015 (www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart).

[15]Comstock, Jonah. "FDA Declines to Approve Proteus-Otsuka Sensor-Equipped Pill, Asks for More Tests." *MobileHealthNews*, 27 April 2016 (http://mobihealthnews.com/content/fda-declines-approve-proteus-otsuka-sensor-equipped-pill-asks-more-tests).

George Loukas is Associate Professor in Cybersecurity at the University of Greenwich (UK). Dr. Loukas is principal investigator for several large-scale EU and UK research projects in cybersecurity, ranging from the security of autonomous vehicles, to secure collaboration of communities and law enforcement agencies, to studying the emotional impact of security breaches in smart home environments. He is the author of Cyber-Physical Attacks: A Growing Invisible Threat*, one of the first textbooks dealing with cybersecurity breaches with adverse physical impact. He can be reached at G.Loukas@greenwich.ac.uk.*

Charalampos Patrikakis is an Associate Professor in the Department of Electronics Engineering of Piraeus University of Applied Sciences (Greece). Dr. Patrikakis has participated in more than 30 research programs and is currently scientific/technical coordinator of two European projects in the area of security. He has more than 100 publications and two contributions in national legislation. Dr. Patrikakis is a senior member of IEEE. He can be reached at bpatr@teipir.gr.

Security Challenges and Approaches in the Industrial Internet

by Claude R. Baudoin

While the explosion of the Internet of Things (IoT) will present security risks in consumer-oriented applications such as smart houses or health monitoring, the consequences pale in comparison to the damage that can be inflicted, whether accidentally or intentionally, on critical infrastructures such as the electric grid, oilfields and refineries, smart cities, transportation systems, or nuclear plants. The ability to interconnect systems and the desire to make data available remotely for operational and analytical purposes have outpaced the implementation of appropriate security measures.

In this article I provide examples of the risks and a discussion of the methods available for mutual identification, authorization, and access control between IoT devices and control systems, as well as protection of data and commands as they cross the network. I will also discuss how policies and risk management, not just the technology, need to be components of the overall approach.

IIoT vs. IoT

When we talk about the Industrial Internet of Things (IIoT, or Industrial Internet for short), we imply that the devices, and what we do with them and the information they supply, serve the purpose of an industrial actor, rather than that of a consumer. So we're not signaling to a person, based on sensing their jogging pattern, that it is time to stop and drink water, or adjusting a household thermostat based on detecting that the owner is 10 minutes away from home after their day at work. Instead, we're automating or recording something about a factory or other industrial environment and making decisions that improve how this environment performs. The Industrial Internet Consortium (IIC), the most active nonprofit membership-based organization in this domain, defines the IIoT as "the convergence of machines and intelligent data," or "an Internet of things, machines, computers, and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes."[1]

Note, in passing, that the last part of the sentence ("enabling…") distinguishes the Industrial Internet from its predecessor, Supervisory Control and Data Acquisition (SCADA). SCADA systems are usually working in closed circuit, reacting in real time without any longer-term analysis of the data they capture, which they often do not even store.

The boundary between the consumer-oriented IoT and the Industrial Internet is not sharp. Certain applications overlap or form a continuum of solutions that can be viewed from the perspective of an individual user or from that of an industrial stakeholder. For example, a smart home can function in a closed loop for the benefit of its residents, but if the data from the home devices is sent to the electric company, it can help it optimize the delivery of electricity and decrease the cost of peak generation. There are similar examples of overlap in areas such as remote patient monitoring, smart cities, water management, smart cars, and more.

The distinction between the consumer and industrial use of the IoT approach is not so much in the types of devices used, or the nature of the analytics performed on the data, as it is in the objectives of the system. The consumer IoT is generally aimed at providing better personal services, such as a more comfortable home with lower energy bills, a faster route to one's destination, or an alert that your prescription refill is ready when you are driving near your pharmacy. The main objectives of the Industrial Internet are things such as:

- Preventing outages and failures
- Decreasing energy usage in a factory
- Scheduling equipment maintenance based on actual usage, not on a fixed cycle time
- Optimizing the routing of shipments based on traffic conditions

- Tracking expensive assets to optimize their allocation
- Surveilling unmanned locations
- Detecting leaks and other hazards
- Improving safety through personnel monitoring

For example, Marathon Oil, in collaboration with Accenture, has equipped a refinery with gas detectors that help create a real-time map of hazards in the control room. Operators wear connected devices that track their location and movement, alert them when they approach a dangerous zone (based on gas level sensors), and send an alert if they stop moving. Incidents are automatically logged. This deployment has resulted not only in safety improvements, but also in greater regulatory compliance and better observance of safety rules by personnel, who know that their movements are being recorded and that this is to their benefit.

Security Challenges in the IIoT

It is hardly necessary to explain or justify that security is a concern when we think of applying IoT technology to industrial applications, but it is useful to consider *how it differs* in this context from the consumer domain. In the consumer-oriented IoT, some of the main threats might be:

- Stealing personal information, such as credit card numbers
- Finding out when a house is unoccupied (e.g., by remotely observing the thermostat settings or the energy consumption) in order to plan a robbery
- Tracking delivery trucks in order to steal shipments left at the doors of unoccupied homes
- Tracking the movements of people (e.g., if they drive in a connected car) for kidnapping purposes — a problem endemic to certain developing countries
- Nuisance actions, such as setting all the thermostats in a neighborhood to the wrong temperature as a misguided joke or as a "badge of honor" for hackers
- Capturing a surveillance camera feed for intimidation, blackmail, or the like

Done on a small scale, these actions are petty crimes. Done on a large scale by an organized agent, in an area where there are many connected homes and cars, they could serve to create panic — a form of psychological attack for economic or ideological purposes.

In the industrial world, the risks are generally different and present immediate danger on a larger scale. Figure 1 is an oversimplified view of the components that an Industrial Internet system connects. (Note that the "actuator" part of a device is not always present. Many devices in an IIoT network — and sometimes all of them — are passive sensors.[2])

Figure 2, by contrast, adds to this diagram the various ways in which attacks can be performed on such a system. This diagram shows three forms of attack, against which most current systems are woefully unprotected:

1. **Eavesdropping.** This is the least disruptive form of attack, because intercepting traffic between a device and a control system or an analytics application does not directly impact its function. Unfortunately, this also means that it is the type of intrusion that is the least likely to be detected. The goal of the listener will often be industrial spying, or it can be government-sponsored monitoring of

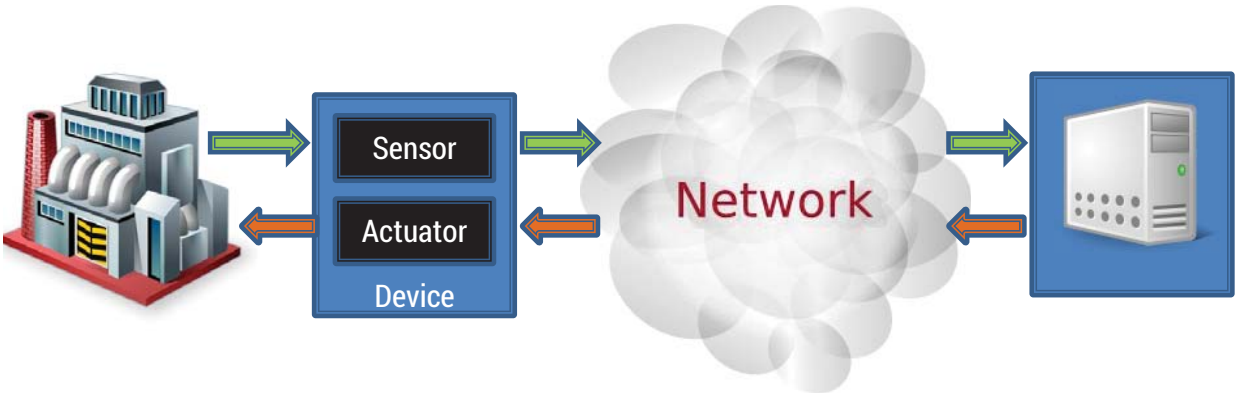


Figure 1 — An IIoT system, simplified.

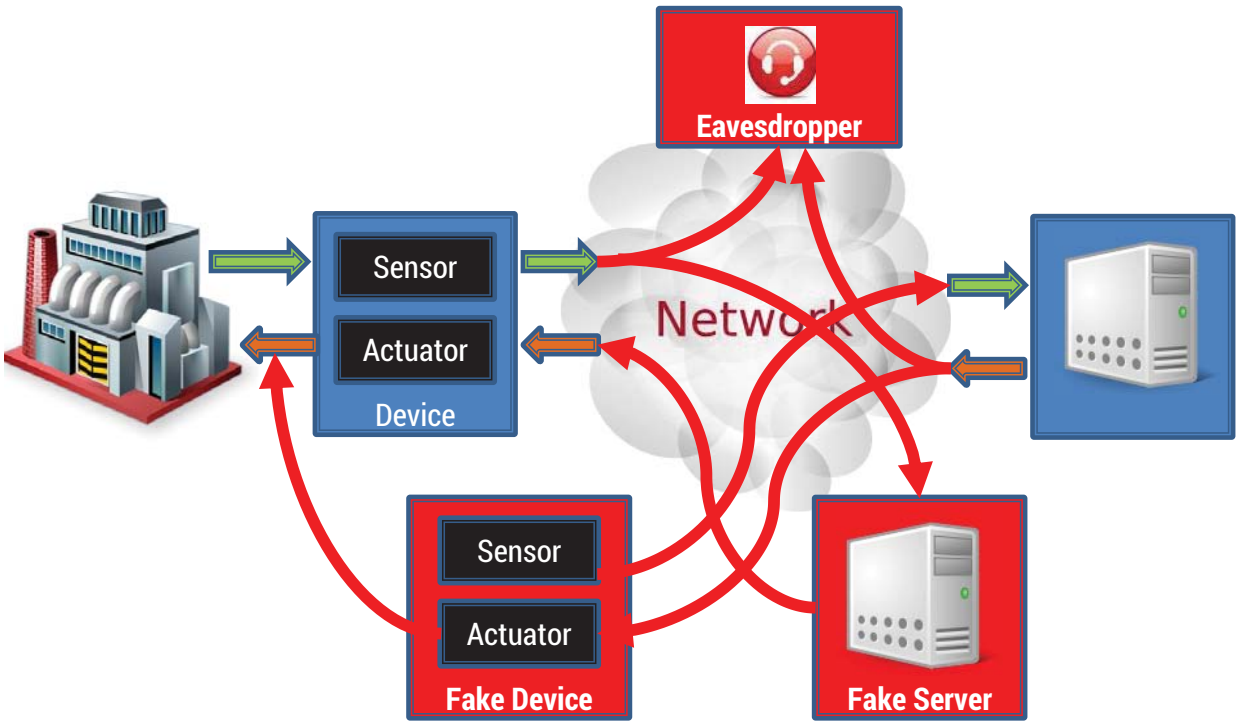


Figure 2 — Possible intrusions into an IIoT system.

economic activity. The goal may also be monetary. By monitoring the information that traverses the IIoT network, a third party may be able to predict certain fluctuations in commodity or stock prices and make money from knowing about impending events ahead of the market. Or it can monetize the information by selling it to an unscrupulous competitor. There is also the increasing occurrence of "ransomware": the intruder accesses enough information to prove to the owner of the system that it contains serious vulnerabilities and then demands a large sum of money to cease the attack or provide remediation information.

2. **Device masquerading.** Inserting a fake device into the network is actually fairly easy in most cases, because enrolling a device in the system is usually a very primitive process. Simply by virtue of physically connecting the device to the network, it can start receiving and sending data. Since sensing devices may be manufactured by the tens or hundreds of thousands, they are fairly easy to procure from legitimate manufacturers. This form of intrusion can result in several distinct (and non-exclusive) consequences:
   - The fake sensor can inject false data into the network to cause erroneous reactions or interpretations. These may include false alarms (i.e., sending data that appears to indicate a malfunction when there is none, which may trigger a disruptive shutdown), or data that skews the analysis of what is going on in the physical world (e.g., reporting higher or lower values of a key measurement) so that the control system sends commands that affect production or create dangerous conditions.
   - A fake device that includes an active component can receive information and intentionally perform actions that are not what is necessary under the circumstances, such as increasing the speed of a motor instead of decreasing it, turning a monitoring light green when it was supposed to be red, and so on.
   - A "denial of service" attack can be performed by a fake device to overwhelm the network with messages, preventing normal operations. At that point, if the industrial system's design is fail-safe, it may shut down safely, but if not, the consequence can be an accident.
3. **Server masquerading.** Especially when the IIoT network uses the cloud rather than a private network to connect devices to servers, it is possible to insert a fake server into the network. As long as that machine is able to discover the addresses of the devices on the network and "speaks" the same communication

protocol as the devices, it could send them requests or commands. IIoT networks are not well protected against this form of attack because the devices rarely have the logic (or the hardware and software capability) to authenticate the servers that are talking to them. Most devices will simply respond to well-formed requests or commands without verifying that the originating machine is legitimate (IP addresses can be spoofed). With this form of attack, it is even easier to cause sensors to send their data to an unauthorized recipient or cause active devices to shut down a machine or a valve — or reopen it in a destructive manner after a legitimate command has closed it.

At this point, readers may wonder why companies that deploy such capabilities do not simply isolate them from the Internet to make sure that attacks cannot be performed remotely. There are a few reasons why the remedy is not that simple:

- We live in an increasingly connected and global world. Remote operations monitoring often leads to a control room being thousands of miles away from the location of the equipment it monitors. Engineering an international private network would be costly. In theory, one can implement a secure, encrypted virtual private network that piggybacks on the public Internet, but organizations may not have the awareness or the expertise to put in place the right solutions. Furthermore, there are inherent vulnerabilities in the Internet Protocol, which was not designed with the current level of threat in mind.
- Solutions that were initially designed to be accessed from within the firewall have often been extended to provide outside access. A manufacturing manager may want to see a dashboard of their factory's operations on their smartphone after dinner or when they get up. As soon as legitimate access is provided to one device from the outside, a potential port of illegitimate entry has been opened.
- Even if the industrial network is isolated from the outside, malware can be brought in through other methods. The Stuxnet attack, described in the next section, is a good example.

When we consider the opportunities for cyberattacks in the industrial world, and the potential severity of their consequences, we are reminded of the famous dialogue between reporter Mitch Ohnstad and serial bank robber Willie Sutton: "Why did you rob the bank, Willie?" "Because that's where the money is!"

Sample IIoT Cyberattacks

In this section, we'll look at three examples of Industrial Internet cyberattacks as a way to show the methods of attack, the types of vulnerabilities they exploited, and the potential consequences. These incidents also serve to show that IIoT vulnerabilities are nothing new.

Most devices will simply respond to well-formed requests or commands without verifying that the originating machine is legitimate (IP addresses can be spoofed).

The BTC Pipeline (2008)

A concrete example of how security vulnerabilities can escalate into physical disasters is provided by the explosion of the Baku-Tbilisi-Ceyhan (BTC) pipeline in 2008, a story fairly well known within the oil industry but not outside of it. According to the Wikipedia article on this accident:

> On 5 August 2008, a major explosion and fire in Refahiye (eastern Turkey Erzincan Province) closed the pipeline. The Kurdistan Workers Party (PKK) claimed responsibility. The pipeline was restarted on 25 August 2008. There is circumstantial evidence that it was a sophisticated cyberattack on line control and safety systems that led to increased pressure and explosion. The attack might have been related to [the] Russo-Georgian War that started two days later.[3]

At the time of the accident, the BTC pipeline capacity was 1 million barrels per day (it has since been increased), and the price of oil was at almost US $125 per barrel. With 20 days of lost deliveries, the potential economic damage if the pipeline had been running at full capacity could have reached $2.5 billion.

It seems that this was a two-pronged attack, electronic as well as physical. The attackers penetrated the monitoring and control system for the pipeline through the network of security cameras placed along the pipeline — cameras that in effect were nodes in an IP network but were installed without changing their default factory passwords. Having penetrated the network, the attackers disabled alarm systems. Finally, they either manipulated valves and compressors to increase the pressure until the pipeline blew up, or (in a more credible version) an explosives truck was detonated next to the pipeline.

This happened in 2008; that is, way before we started seriously talking about the Internet of Things, let alone the Industrial Internet. In fact, the BTC pipeline did not really include an analytics component, but the attack leveraged the presence of connected devices and took into account the presence of a remote control room.

Stuxnet (2010)

In 2010, the Stuxnet bot was introduced into Iranian nuclear research facilities and disabled a number of that country's controversial uranium enrichment centrifuges. It was reportedly developed jointly by US and Israeli intelligence agencies for this specific purpose.[4] Let's look at some of the key aspects of this attack — how it happened and its impact.

There was a widespread belief, until Stuxnet was let loose, that programmable logic controllers (PLCs) used to control most industrial equipment were immune to viruses because these PLCs do not run a real operating system. But those PLCs, by definition, are *programmable*. And in an installation like the ones in Iran, the industrial control system connected to multiple PLCs runs Microsoft Windows and the Siemens Step 7 industrial control software. Therefore, infecting the host system was possible using the same techniques used to infect any Windows machine. Then, the Step 7 software could be subverted to reprogram the PLCs, causing them to execute incorrect instructions that would damage the equipment.

On the impact side, many people in the Western world might applaud the motive of the attackers. However, just as it is hard to contain a biological virus, this electronic one got loose and infected a number of systems in other countries. While 59% of the reported infections were in Iran, 18% were in Indonesia, and 1.5% in the US. Siemens had to distribute a detection and removal tool to its clients.

How was Stuxnet introduced into the presumably highly controlled environment of an Iranian nuclear research facility? Through a USB flash drive, handed out at an international conference to an attendee who wanted a copy of an interesting PowerPoint presentation, and whose PC was connected to the facility's intranet.

Ukraine Utility Attack (2015)

We could go on with many more examples. This last one is worth mentioning because it is recent, which proves that little has changed since 2008, except perhaps the scale of the attacks and the sophistication of the perpetrators.

On 23 December 2015, several Ukrainian utility companies were disabled, cutting off power to hundreds of thousands of homes for several hours. There were multiple actions leading to the blackout, indicating long-term planning and a high degree of sophistication:

- A "spear phishing" attack (targeted social engineering) started as early as May 2015 and resulted in installing the KillDisk program in advance on the computers used by utility operators. The malware was left dormant until the time of the attack. KillDisk not only causes a PC to crash, it also prevents it from rebooting.
- The BlackEnergy malware was used to gain access to the utilities' systems.
- At the time of the attack, three things took place simultaneously: the infiltrated control systems were told to "flip the switch" and disconnect power; KillDisk was activated to render the operators' PCs useless; and a "telephone denial of service" attack was launched to flood the utilities' call centers, preventing legitimate customers from reporting outages.

Because the operators could no longer use their PCs and had no real information on the extent of the outage, they had to physically travel to the various substations and manually reconnect the network.

Protecting Critical Infrastructures

As the saying goes, this situation is going to get worse before it gets better. First, the number of systems controlling expensive or potentially dangerous infrastructure (e.g., pipelines, power plants, the electrical grid, airports) is going to grow, and humans will be increasingly taken out of the loop, at least for routine operations, because of the complexity and speed of the decisions required to optimize operations.

Secondly, cyberwarfare skills have become available not only to intelligence agencies, but also to hackers pursuing various motives, who no longer need to be expert malware developers. Hacking groups sell software and services using the "dark Web," often getting paid in Bitcoins. Facing this array of nefarious tools, we are still plagued with human and technical vulnerabilities such as the exchange of USB drives or clicking on an unknown attachment.

Finally, many groups have a stake in disrupting the operations of large industrial systems: actual terrorists, of course, but also intelligence agencies (as in the case of Stuxnet and probably of the Ukrainian attack), various criminal groups (perhaps looking to extract ransom

payments), as well as "hacktivists" pursuing various ideological campaigns or trying to turn public opinion against certain policies and practices (e.g., nuclear energy, genetic engineering, offshore drilling).

Prosecutors look for three things in order to accuse someone of a crime: a motive, a weapon, and an opportunity. We just saw that all three are present: there are groups who want to do harm, they have a veritable catalog of malware at their disposal, and the systems they want to attack are not well protected enough. It is not surprising that attacks occur — it is actually surprising that there aren't more.

Let's now examine some of the approaches needed to get the situation under control.

Extending Identity and Access Management to the Industrial Internet

The identity and access management of IoT devices is not well handled today. When an enterprise adds a new human user (i.e., an employee or contractor), that person needs to be issued a username and password in order to access various systems. They can be asked to perform some of the registration activities, entering certain privileged information on a website in order to be assigned their credentials. A hardware device cannot do that. As noted above, physically connecting a new device to the network is usually all it takes for that device to start receiving and sending data.

Fixing this loophole requires that each device be given an identity that cannot be faked. One solution is to issue a public key infrastructure (PKI) certificate to each device and install that certificate on a tamper-proof electronic module. The device can then authenticate itself by responding to a challenge encoded using its public key. Conversely, the device must respond only to legitimate commands from a verifiable source. This means that the device needs to be able to issue its own challenge to the source of a request. Finally, if the device and the server both have PKI capabilities and certificates, they can encrypt the data they exchange in order to prevent eavesdropping.

Traditional Security Countermeasures

As we saw in the attacks described earlier, human fallibility is an important element of risk. As long as people plug a USB flash drive of unknown origin into their PC, or follow a hyperlink in a convincingly worded message, we can expect malware to penetrate at least regular computers used by people in their daily work.

The challenge, therefore, is to prevent further spreading of malware through defense-in-depth mechanisms. An industrial network should be isolated from the enterprise network to provide a second layer of defense. Intrusion prevention and detection systems should of course be run, and regular penetration tests conducted, although the proliferation of zero-day (previously unknown) exploits makes it hard to provide a 100% guarantee of protection.

The software running on enterprise and industrial systems is still plagued with common vulnerabilities such as buffer overflow, SQL injection, and so forth. Secure coding practices need to be taught and enforced, following in particular the work of MITRE and the Consortium for IT Software Quality (CISQ).[5]

It is not surprising that attacks occur — it is actually surprising that there aren't more.

Strategy and Governance: The IT/OT Divide

The previous paragraphs could lead the reader to focus on technology solutions, but as usual in IT matters, the tools are unlikely to be effective absent good governance, strategy, and organization.

In many organizations, there is a schism between information technology (IT) — which is devoted to enterprise systems, collaboration tools, end-user devices, and user support — and operational technology (OT) — which includes manufacturing systems and the growing realm of the Industrial Internet. While some companies try to "put lipstick on the pig" by claiming that this division of responsibilities is a good thing, it really emerged for three negative reasons:

1. IT developed a reputation, not altogether undeserved, that it doesn't understand the business.
2. IT has usually instituted a project management process that is the opposite of agility and is unable to respond to the changing needs of operations.
3. IT personnel are trained in the development and operations of traditional enterprise systems, using general-purpose operating systems, programming languages, databases, and user interfaces — not in the integration of real-time cyber-physical systems running on resource-constrained, dedicated devices.

Once OT is separated from IT, however, it may not possess the skills necessary for security management in a hostile world. Operations personnel are very good at resolving problems quickly — potentially taking shortcuts that introduce vulnerabilities into their systems.

Organizations in which this schism between IT and OT exists should consider how to cross-pollinate the two sides with the necessary skills and processes so they can work better together to ensure the security of industrial systems. In some cases, the split should be reconsidered. This may require difficult decisions — for example, if the CIO of an industrial organization doesn't know enough (or worse, doesn't care) about the operations side of the company, perhaps they are the wrong person for the job.

Since the Industrial Internet is likely to be a magnet for cyberattacks, organizations need to be prepared to defend themselves with all means at their disposal.

Collaboration

The work of several organizations can be leveraged to help address the issues. I will mention just three of them:

1. The IIC is preparing a "common security framework" to assess and improve the protection of industrial systems.6
2. The US Department of Homeland Security (DHS), recognizing the threat to critical infrastructure elements posed by IIoT vulnerabilities, has launched several initiatives, including an Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[7]
3. The Object Management Group (OMG) is evolving its Data Distribution Service (DDS) protocol to add a security layer as well as the capability to run on eXtremely resource-constrained environments (XRCE).[8]

Adoption Challenges

None of these measures is free or easy to implement. There are multiple challenges to their adoption:

- Technically, the implementation of particular measures, such as device authentication and encrypted communications, requires at least a certain amount of computing power and memory at each device. The installed base of SCADA devices often lacks both features. Either those devices need to be replaced by more capable ones, or intermediary systems — often called "gateways" — will need to be installed to add the security management features to a cluster of dumb devices.
- Cost is an obvious factor, especially if implementing security requires replacing existing control systems and devices with newer ones or adding the gateways just mentioned. Deploying a PKI or similar capability with perhaps thousands of certificates — one per device in addition to one per server — also implies a significant cost.
- Retrofitting security on an existing installation may require interrupting operations.
- If an organizational change is required, or if operations management is ill-prepared to give security the priority it deserves, the difficulty and cost of change management should not be underestimated.

Recommendations and Conclusion

There is no such thing as absolute security. But since the Industrial Internet is likely to be a magnet for cyberattacks, just as banks were for Willie Sutton, organizations need to be prepared to defend themselves with all means at their disposal. If they fail to do so, their ability to conduct their basic business will be in jeopardy. A successful attack against a nuclear power plant or a refinery, followed by the likely discovery that negligence or naiveté played some part in making it possible, can definitely bankrupt the target of the attack or damage an entire industry.

The first step, as in the case of any operational threat, is to conduct a threat assessment. In the case of the BTC pipeline, a rigorous threat assessment of the pipeline system was only conducted after the fact.[9]

The next step is to make IIoT systems more resilient by removing bad security practices that are not specific to these systems but can have more severe consequences in this domain. The errors fall into well-known categories: mistakes in software development, mistakes in system and security management, and vulnerability of users to social engineering practices.

A third step is to make sure that the governance and organization are in place to establish and track the goals, strategies, objectives, and tactics required to populate a plan of action.

Finally, technology can be introduced to strengthen the systems, and this step should leverage collaboration with leading organizations, such as the IIC, and industrial partners, such as the manufacturers of the IIoT equipment used in the network or system integrators with experience in this field.

Endnotes

[1]"What Is the Industrial Internet?" Industrial Internet Consortium (www.iiconsortium.org/about-industrial-internet.htm).

[2]Baudoin, Claude R. "The Internet of Things: Automation Heaven or Security Hell?" Cutter Data Analytics & Digital Technologies *Executive Update*, Vol. 14, No. 3, 2014 (www.cutter.com/article/internet-things-automation-heaven-or-security-hell-402761).

[3]"Baku-Tbilisi-Ceyhan Pipeline." Wikipedia (https://en.wikipedia.org/wiki/Baku%E2%80%93Tbilisi%E2%80%93Ceyhan_pipeline).

[4]"Stuxnet." Wikipedia (https://en.wikipedia.org/wiki/Stuxnet).

[5]"Common Weakness Enumeration." MITRE, updated June 2016 (https://cwe.mitre.org/).

[6]Industrial Internet Consortium: Security Working Group (www.iiconsortium.org/wc-security.htm).

[7]Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (https://ics-cert.us-cert.gov/).

[8]"What's in the DDS Standard?" Object Management Group (http://portals.omg.org/dds/omg-dds-standard/).

[9]Steinhäusler, Friedrich, et al. "Applying Advanced Technology for Threat Assessment: A Case Study of the BTC Pipeline." *Journal of Energy Security*, August 2009 (www.ensec.org/index.php?view=category&id=98%3Aissuecontent0809).

Claude R. Baudoin is a Senior Consultant with Cutter Consortium's Business & Enterprise Architecture and Data Analytics & Digital Technologies practices. He is owner and principal consultant for cébé IT and Knowledge Management, a boutique consulting practice based in Austin, Texas, since 2009. Prior to that, Mr. Baudoin spent 35 years in IT and software management roles in industry, including 26 years at Schlumberger, the global oilfield services company, in France and the US. Since 2015, he serves as energy domain advisor to the Object Management Group and the Industrial Internet Consortium, and sits on the Steering Committee of the Cloud Standards Customer Council.

Mr. Baudoin's undergraduate engineering degree is from École Polytechnique in Paris, and he holds an MS in computer science from Stanford University. He has published two books on software engineering, Méthodes de Programmation *and* Realizing the Object-Oriented Lifecycle*, and numerous papers and conference presentations, including a number of Cutter* Executive Reports, Updates*, and* Advisors*, and* Cutter IT Journal *articles. Mr. Baudoin holds two patents related to IT infrastructure and security. He can be reached at cbaudoin@cutter.com.*

TO ERR IS HUMAN

Social Engineering in the Internet of Everything

by Ryan Heartfield and Diane Gan

It is well known that social engineering attacks are designed to target the user-computer interface, rather than exploiting a system's technical vulnerability, to enable attackers to deceive a user into performing an action that will breach a system's information security. They are a pervasive and existential threat to computer systems, because in any system, the user-computer interface is always vulnerable to abuse by authorized users, with or without their knowledge.

Historically, social engineering exploitations in computer systems were limited to traditional Internet communications such as email and website platforms. However, in the Internet of Things (IoT), the threat landscape includes vehicles, industrial control systems, and even smart home appliances. Add to this mix naive users and default passwords that are extremely weak and easily guessed, and the threat becomes greater. As a result, the effects of a deception-based attack will now no longer be limited to cyberspace (e.g., stealing information, compromising a system, crashing a Web service), but can also result in physical impacts, including:

- Damage to manufacturing plants
- Disruption of train and tram signaling, causing death and injury
- Discharge of sewage from water treatment plants
- Damage to nuclear power plants (e.g., Stuxnet)

In December 2014, a German steel mill furnace sustained damage when hackers used targeted phishing emails to capture user credentials, thereby gaining access to the back office and ultimately the production network, with devastating consequences. Another example occurred when households in Ukraine suffered a blackout on 23 December 2015 caused by an attack that brought down the power grid. Again, the attackers used phishing emails to trick users at the electric company into clicking on an attachment in an email, ostensibly from the prime minister of Ukraine. This is thought to be the first cyberattack that brought down an entire power grid, leaving 225,000 homes without electricity.

The more effective such cyber-physical attacks prove,[1] the more the deception attack surface continues to grow. For example, in the near future, fake tire pressure alerts shown on a car's dashboard or gas leakage warnings on a smart heating system's GUI may be used to achieve deception in a manner not too dissimilar to current scareware pop-up alerts experienced by today's mobile and desktop users. In the extreme, attackers may even begin to target medical devices (e.g., pacemakers or mechanical insulin-delivering syringes) via near field communications or wireless sensor networks, in an approach analogous to ransomware. This has already occurred through the IoT using conventional hacking techniques (i.e., SSH vulnerabilities and unpatched systems with default hardwired passwords) and is commonly known as a MEDIJACK attack. The major problem with these devices is that they remain unpatched throughout their lifetime, and at the moment this is also the situation within the IoT. Figure 1 provides a snapshot of the potential IoT social engineering threat space.

Would Your Fridge Lie to You?

Prior to the advent of the IoT, an email or instant message purporting to originate from your fridge would seem ludicrous. Nowadays, however, the concept does not seem so absurd. In fact, it is exactly this change in our expectations about the way we use technology and the increasing capabilities of system-to-system communication that poses the most risk. Today's users expect greater visibility and control over their environment, leading to a proliferation of distributed interfaces attached to what were traditionally isolated systems, sharing new types of data across a cyber-physical boundary. The result is an ever-richer user experience, but also an augmented attack surface at the disposal of willing cybercriminals. And as cybercriminals tend to go in search of low-hanging fruit in order to exploit a system, the user is now more than ever a soft target.

Since attackers may not always have physical access to IoT devices to exploit them directly, they can instead

Figure 1 — The Internet of Everything: people and smart devices, cars, homes, cities....

target the distributed functionality and associated behavior integrated into new and existing systems. For example, it would not be unreasonable to imagine an attacker crafting a spoofed instant message from a user's refrigerator (see Figure 2), reporting that it is running low on milk and asking whether the user would like to place an order with an Amazon-style "one-click" ordering button — which conveniently leads to a drive-by download. But how did the attacker know the user's milk was low? Well, in the IoT they simply sniffed seemingly unimportant, unencrypted sensor node data sent from the fridge to the home automation controller, which connects to the user over the Internet via their home broadband router. Here, the attacker has exploited platform functionality that interfaces with the IoT device (in this case, a fridge) by manipulating the perceived behavior of the system as opposed to the device itself. In practice, such an attack can lead to a conventional exploitation such as system compromise or theft of banking credentials. It is not a great leap to envision that your fridge could be held to ransom by ransomware. Pay up, or your fridge won't turn on.

Unlike phishing emails claiming to originate from financial institutions and banks (which have existed for nearly 30 years), users are not sensitive to malicious behavior originating from home/city automation systems, smart devices, or social media platforms that provide access to e-health, emergency, or public services. To a large extent, this is because the physical appearance of such systems does not require significant change to become compatible with the Internet of Things; normally it is only the data these platforms generate that is shared. Specifically, the IoT is enhancing data accessibility, which is further augmenting the attack landscape for cybercriminals seeking to develop convincing social engineering attacks.

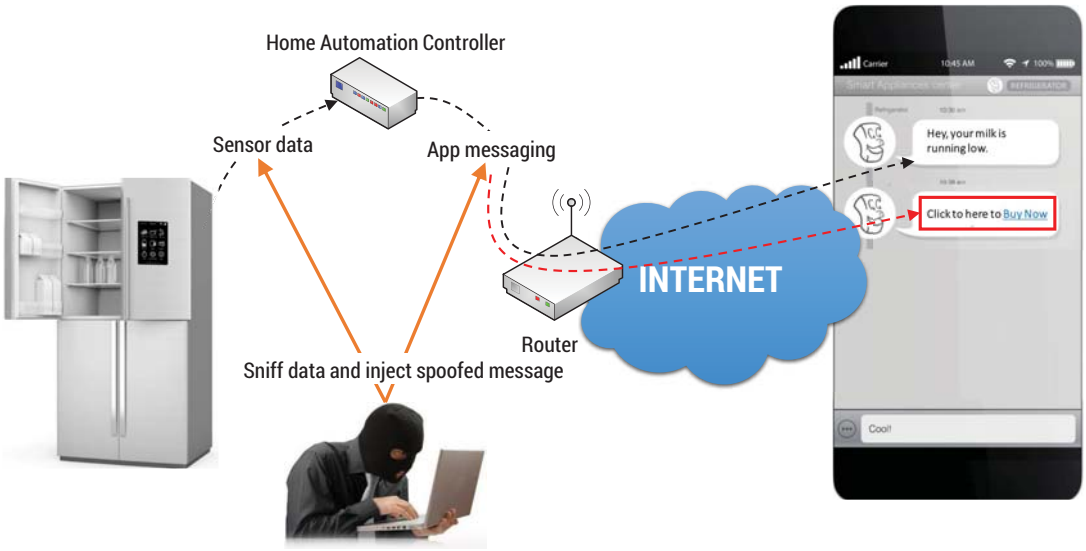


Figure 2 — Attacking a SMART fridge through intercepting and injecting spoofed application messages.

Data Leakage: No Data Is Too Big or Small

Just as the IoT expands the different types of user interfaces that attackers can target, the different types of data (previously hidden from attackers) that can be acquired is also increased. It is well known that attackers are adept at gathering user data and utilizing this information as a mechanism to target a user and better design an attack specific to the user's system or improve the credibility of the deception techniques used. Nowadays, hackers use social networks to obtain personal data about a user, such as their children's names, pet's name, date of birth, where they graduated, and so on. By detecting and exploiting systems that are of high value and using their target's "pattern of life" data, cybercriminals can develop effective deception mechanisms by manipulating information the user has shared and is therefore very familiar with and unlikely to repudiate. Data leakage is exacerbated when geolocation is turned on in IoT devices (see Figure 3). This enables anyone to determine the exact location where a smartphone picture was taken, for example, which can be a problem if this identifies the user's home and they have just tweeted that they are going away on holiday. Burglars use Twitter as well!

Recent research by the C-SAFE team at the University of Greenwich has demonstrated the ease with which an individual can be profiled through their leaked personal data using only social networks (Facebook, Twitter, LinkedIn, Instagram, etc.).[2] Researchers undertook a series of experiments to determine how much information they could extract about three subjects using only social networking sites. By utilizing three freely available tools (Twitonomy, Streamd.in, Cree.py) that harvest information from Twitter, the data revealed where the three subjects lived and worked, the route they took to work each day, where one subject's parents lived, and even where and when another subject went to the gym. It was also possible to follow each of them through cyberspace to other sites such as Facebook, LinkedIn, Foursquare, and Instagram, where information missing from their "profile" was quickly filled in. The experiment demonstrated how easy it is for cybercriminals to gather personal data to construct social engineering attacks that an individual would find credible.

"Smart"er Attacks

Social engineering attacks against IoT devices are by no means hypothetical, and exploitations abusing functionality in smart devices have already been observed in the wild. For example, from December 2013 to January 2014, security provider Proofpoint detected a cyberattack that was originating from the IoT, where three times a day, in bursts of 100,000, malicious emails targeting businesses and individuals were sent out. In total, the global attack consisted of more than 750,000 malicious emails originating from over 100,000 everyday consumer gadgets, 25% of which originated from smart TVs, home

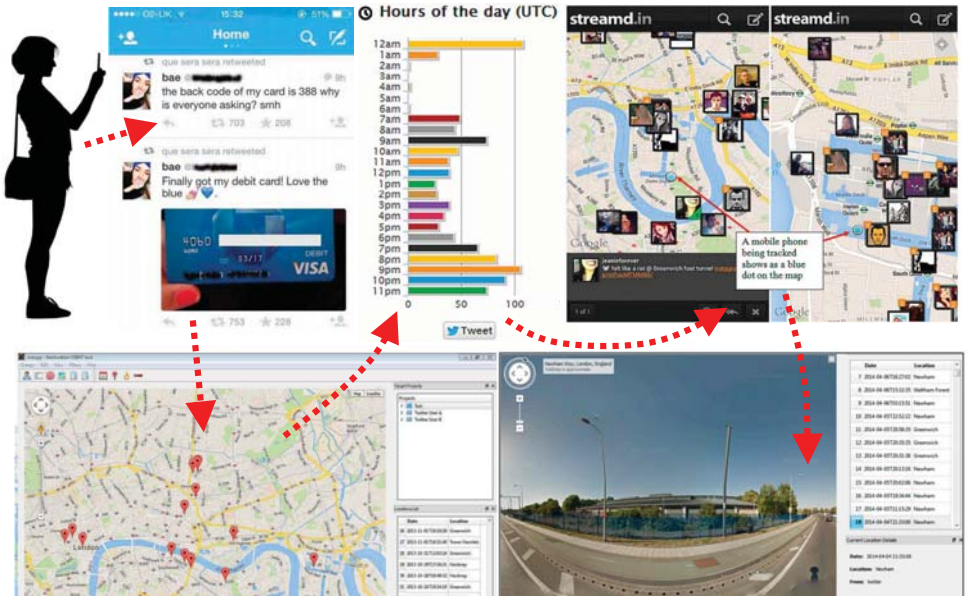


Figure 3 — Example of a cyberstalking experiment monitoring and geolocating Tweets from Twitter user, Twitter feed (top left, middle), Cree.py (bottom left, right), Streamd.in (top right).

routers, and even one fridge.[3] Crucially, the attack demonstrated that botnets are now IoT botnets, capable of recruiting almost any device with a network connection and messaging software.

Attack Case A: IoT Phishing in Smart Homes

Smart homes are becoming more common as people connect up numerous devices and "things" within their home. All these IoT things and devices connect to a network, be it wireless or wired, and eventually connect to a routing device. Individually they may not offer any obvious value to cybercriminals, but they can provide a user interface that an attacker can manipulate to execute a social engineering attack. The following attack considers a threat actor who has gained control of a brand of IoT smart meter cloud-based services platform, bundled with the product to deliver updates or new content. Here, the attack can either monitor (what may be) unencrypted communication between the cloud services and the smart meter and inject information into existing data flows, or potentially send direct messages to the meters if the attackers have gained complete control over the cloud environment. In both examples, the attack triggers the following message to all smart meters when the heating sensor indicates that the users are home (e.g., it has been turned up/down): "Software Upgrade Required. Go to: www.heaterupgrades.com/smartupgrade. Run the patch from a Windows computer on this network." (See Figure 4.) If the user complies, then they have been phished.

Attack Case B: The Internet of Social Things

Social networking and media are at the heart of the IoT, where it is no longer only people that share information with other people, but also things that are able to communicate with users or with other things. Think back to your fridge kindly advising that you are low on milk. Your car might even want to tell your Facebook friends that its carbon footprint is less than four other cars on the road this week (i.e., in-product advertising across social media). The following attack considers a threat actor scanning Twitter and looking for status posts that include metadata from IoT picture frames. IoT picture frames often come bundled with an app that allows their user to automatically download and upload pictures to popular social media platforms. In this example, the attacker finds a tweet containing the metadata; however, it is a retweet from an open Twitter account following a particular user who owns the target picture frame. Next, the attacker sends a direct tweet to the user (whose account privacy settings were locked down) from a spoofed Twitter account purporting to be the picture frame's manufacturer. The tweet contains a shortened URL to a Twitter app that will allow the user to install video functionality on their picture frame for free. In reality, the Twitter app gives the attacker's account rights to download all the pictures from the user's IoT picture frame, which the attacker can then use as ransomware data or to craft future phishing attacks (see Figure 5).

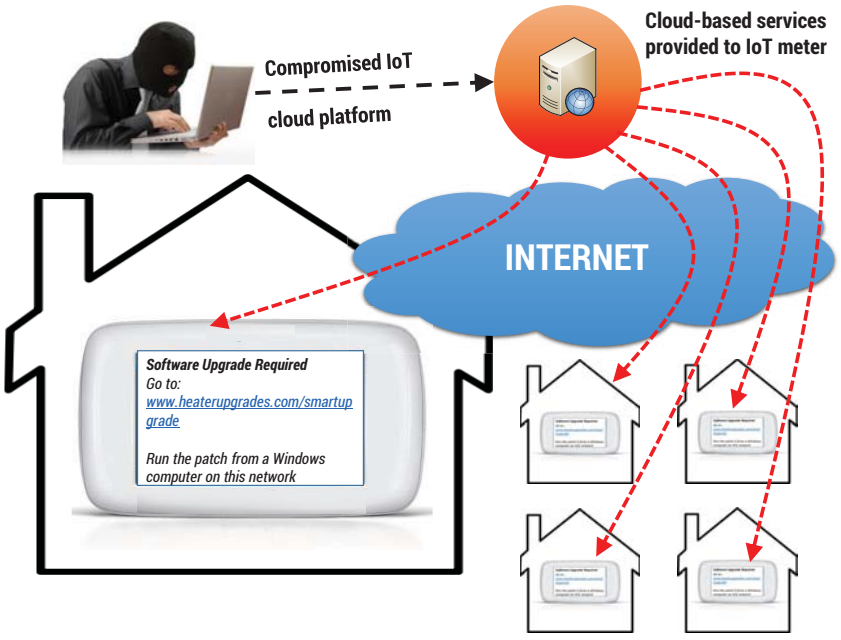


Figure 4 — Example of a smart meter phishing attack via compromised update and content services in the cloud.

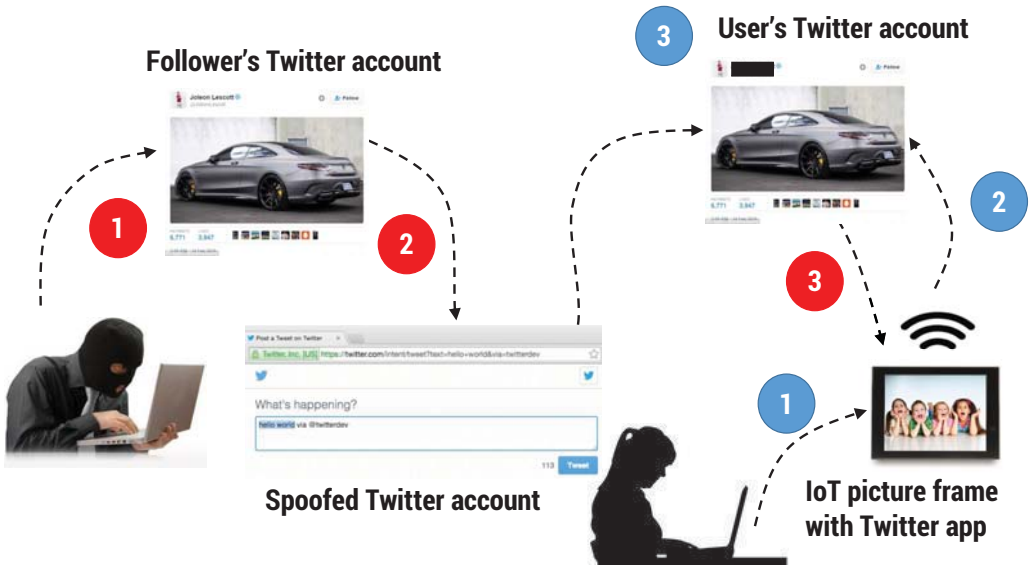


Figure 5 — Example of an attacker exploiting Internet of Social Things contagion to deliver a social engineering attack.

Defense Recommendations

In order to instill confidence in the smart technologies that underpin the IoT, encourage their uptake, and ensure that they will be usable in the long term, it is necessary for the security of these devices to be robust, scalable, and above all practical. Here, we explore four approaches to defending the IoT against social engineering attacks.

Generic Attack Classification

Since deception-based attacks in the IoT can be launched in either cyber or physical space, identifying the source of a deception attempt and the structure of a social engineering attack can be extremely difficult. For developers, the challenge of building an effective defense that addresses a range of deception vectors would appear insurmountable when we consider all the different platforms that may been involved in an attack. It is more practical to employ generic classification criteria to break down attacks into parameterized, component parts. This approach can be used to reveal shared characteristics between attacks, which then aids the design of defenses that address multiple threats sharing similar traits. Using the taxonomy proposed elsewhere by Ryan and Guest Editor George Loukas,[4] and summarized by each root category in Figure 6, the following recommendations can help developers capture the multiple variables involved in the construction, delivery, and execution of a social engineering attacks by applying criteria that are independent of the attack vectors used.

Orchestration

Target Description (TD). How is the target chosen? Determine an attack's targeting parameters to define which user and/or system features a defense system should focus on. A targeted attack is likely to exploit a specific user's attributes leaked by their IoT footprint (e.g., a toll payment spear phishing email based on tweets mapped to the geolocation of their vehicle) as part of the deception. In contrast, promiscuous targeting is opportunistic and random (e.g., an attacker plants a malicious QR code in a shopping center).

Method of Distribution (MD). How does the attack reach the target? Investigate the method in which the attack's deception is distributed and where it is executed to identify the platforms that are involved in the attack. Determine whether it is a remote system (hence involving a network) or a local system that requires monitoring and defending.

Mode of Automation (MA). Is the attack automated? Recognizing whether an attack is automatically or manually executed will help determine the most suitable response mechanism and the type of data that can be meaningful to collect about it. It may be possible to fingerprint a fully automated attack based on patterns of previously observed behavior, while a fully manual attack may need to focus on the attacker's behavior instead.

Figure 6 — A high-level summary of taxonomic classification criteria for social engineering attacks in the Internet of Things.

Exploitation

Deception Vector (DV). Is it looks or behavior that deceives the user? A defense mechanism needs to pinpoint mechanisms by which an attacker can deceive the user into a false expectation by manipulating visual and/or system behavior aspects of a system. Within the IoT, it is not just GUIs that can be abused, but the physical appearance or state of a sensor node in a home/work/city automation system as well (e.g., heating thermometer, heartbeat monitor, vehicle speed, traffic lights).

Interface Manipulator (IM). Is the platform used in the deception only (ab)used or also programmatically modified? Depending on the system involved in an attack, it may be impractical or impossible to patch directly (e.g., pacemaker, legacy actuator). In order to reduce the scope of a defense, developers need to establish whether the deception vector in an attack occurs in code (e.g., embedded within the system or external) or abuses intended user space functionality built into the platform by design.

Execution

Execution Steps (ES). Does the attack complete the deception in one step? Model the effect that a single user action can have on the integrity of a platform, as it may be necessary to build in extra user authentication steps to commit actions, especially in e-health services or industrial control systems. An attack that relies on multiple user response steps may be detected earlier and more easily than a single-step attack, and before it completes, by looking for traces of its initial steps.

Attack Persistence (AP). Does the deception persist? Persistent attempts can be modeled by a learning-based defense system to identify the deception's pattern of behavior in order to block it. At the same time, it may also have a higher chance of success against the target. One-off deception attempts are by definition more difficult to detect and may be missed if a defense is only looking for patterns in system behavior or if the pattern is as yet unknown (i.e., a zero-day vulnerability).

S-SDLC

It is important that IoT platform developers have a detailed understanding of how their system will interface with users, as well as how system functionality may affect the wider ecosystem in which the system may be deployed. The Secure Software Development Life Cycle (S-SDLC) provides developers with a guideline framework for the design and implementation of system software by integrating security considerations systematically into the core requirements and design of the software's architecture. Within the S-SDLC framework (see Figure 7), in each lifecycle stage, the following key concepts can aid the development of IoT platforms and functionality that are resistant to deception-based attacks.

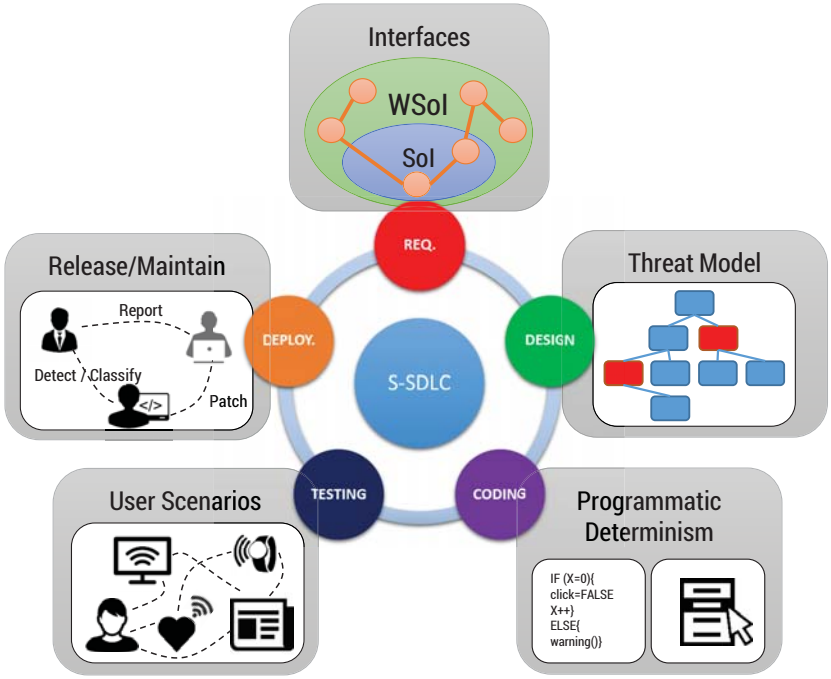


Figure 7 — Key concepts in the S-SDLC framework for developing resistance to deception-based attacks in the IoT.

Requirements

Identify the attack surface for an IoT platform by clearly defining the intended functionality and its expected limitations. Document the system-to-system and system-to-user interfaces forming the overall system of interest (SoI) and determine how these communicate and affect interfaces within the wider SoI (WSoI; e.g., the deployment environment).

Design

Develop threat models that run through different features of the platform's design and WSoI interactions. Pinpoint weak spots in the user interface that can be abused or vulnerabilities in data transfer and network communications that may allow attackers to inject malicious data or code or gather information about the user.

Coding

Employ static code analysis to determine whether the platform's programmatic features are deterministic to ensure spoofed or injected data does not force the platform to exhibit a deceptive behavior toward the user. Similarly, evaluate user interface controls (whether graphical or physical; e.g., a button) to ascertain whether these can be (ab)used through intended functionality.

Testing

Design and implement scenarios where different user behavior is arbitrarily executed (e.g., fuzzing) in order to identify anomalous situations when the user interface or functionality can become part of a deception-based attack. In testing, developers should generate and execute random input parameters, physical and logical, against the IoT platform in an attempt to elicit unhandled or anomalous behavior that may lead to exploitable vulnerabilities.

Release/Maintain

Establish monitoring or reporting functionality within the platform deployment environment to help detect attacks. This will facilitate continuous patching and security hardening of the specific platform and/or external platforms that have lower-security features.

Attack Classification and Defense

By applying each taxonomy criterion against each of the two IoT attack cases, we can use classification to employ S-SDLC principles that help suggest a single approach to defense that would prevent both attacks.

Case A

TD. Promiscuously targets any user who owns the smart meter, by flooding connected devices with messages and commands (e.g., malicious updates) via the cloud.

MD. Distributed to execute the deception via **local software** on the smart meter.

MA. Functions as an **automated message** sent from the cloud-based service.

DV. Deception is both **cosmetic and behaviorally convincing**, as the user would expect communications from the cloud platform.

IM. Injecting malicious messages through the cloud attacks the **programmatic interface** of the smart meter by adjusting the internal code to display a deceptive message.

ES. The user must exercise **multiple steps** in order for the deception to be successful. The first step downloads the supposed patch; the second step then requires the user to install the patch.

AP. The message's particular deception is **one-off**, as it is unlikely the attacker will reissue the same phishing message and thus compromise the attack's integrity.

Case B

TD. Promiscuously targets any user who owns an IoT picture frame with social media app functionality.

MD. Distributed to execute the deception via **remote software** on the Twitter platform.

MA. Functions as a **manual operation** by searching for tweets, then creates a custom Twitter account and tweets once a target is found.

DV. Deception is **behaviorally convincing**, as product suppliers often communicate with customers via social media so as to gain customer data analytics. It is unlikely the Twitter account is visually credible (e.g., there are few or no followers, and as the account is not official, tweets are not authenticated — no blue tick!).

IM. Here the attacks simply (ab)use the **user interface** functionality of the Twitter platform.

ES. The deception completes in **multiple steps**, as the user must click on the URL and then add the malicious Twitter app permissions to their account.

AP. The message's particular deception is **one-off** as it is unlikely the attacker will reissue the same phishing message and thus compromise the attack's integrity.

By applying the taxonomy classification to each attack case, we can establish that a number of similar traits are shared in the orchestration, exploitation, and execution phases of these attacks. First, both attacks target users promiscuously, so it would appear the attacker is seeking to build the deception around a vulnerability in an IoT platform and its use case rather than a specific user's platform profile. Both attacks are behaviorally deceptive, irrespective of whether they are visually convincing or not, and both attacks are one-off in their deception but require multiple user steps to complete the deception and exploitation. By showing that both attacks focus on the IoT product behavior, rather than the users, it becomes clear that the S-SDLC requirements and testing stages would play a pivotal role in helping to mitigate these attacks. Crucially, it is the system-to-system interfaces of each IoT platform and their interaction with the ecosystem's WSoI (Case A: cloud-based services over the Internet, Case B: Twitter application add-ons) that need addressing.

Since both attacks' deceptions are one-off, they may be hard to identify and prevent.

Each of the IoT devices, their interface contracts between other IoT platforms/devices, and the functionality they extend should be clearly defined and then evaluated against different user deployment scenarios. In this way, developers can pinpoint specific functionality supplied by the system that is vulnerable to manipulation. Here, the manipulation of features supplied by the IoT devices in each attack case could easily be highlighted by reviewing each interface contract, then conducting a robust test of its functionality in different user deployment scenarios. Since both attacks' deceptions are one-off, they may be hard to identify and prevent; therefore, it is even more important to rationalize system interface requirements before providing the users with functionality that the developers are not able (or willing) to protect. Where each attack requires multiple user steps to complete, integration of further authentication mechanisms for more significant functionality requests between interfaces should be enforced and reviewed through testing. This approach can help to determine whether extra security procedures should be enforced before a user commits a potentially compromising action (e.g., forcing a user to review a warning or confirm their identity through multi-factor authentication).

User Susceptibility Profiling

In order to provide a robust defense against social engineering attacks, responsibility cannot be laid solely upon the shoulders of system developers or the organizations that provide access to a computer system, whether that is an IoT platform connected to the Internet, a LAN, or a near-field communications medium. The users of the system are just as important, if not relied upon even more to act and use the computer securely to ensure that their actions do not inadvertently result in information security compromise. Remember, there is no silver bullet for protecting against human error.

Identifying a key set of measurable user attributes can help to provide a basis for modeling which type(s) of user profiles are more or less likely to be susceptible to a deception-based attack. Such attributes could be used to define features for predicting and estimating user susceptibility when using a specific platform or range of platforms. Crucially, access to a user susceptibility profile provides the basis for applying a threshold at which the probability of user susceptibility triggers security-enforcing actions aimed at minimizing and/or mitigating exploitation.

Fundamentally, protecting the integrity of the IoT is a two-way street.

Human as a Sensor (HaaS)

The concept of the human as a sensor has been employed extensively and successfully for the detection of threats and adverse conditions in physical space; for example, to report road traffic anomalies, detect unfolding emergencies, and improve the situational awareness of first responders through social media.[5] In a similar manner, human sensing can be applied to detect and report threats in cyberspace as well. In fact, as the IoT crosses the cyber-physical boundary, the ability of users to report suspected attacks, both cyber and physical, may help to detect attacks initiated in one space that result in an effect on the other. In this respect, it then becomes particularly important to be able to tell to what extent users can correctly detect deception-based security threats, leveraging the intelligence provided by users to augment IoT cyber situational awareness.

Within a smart city, users are likely to be exposed to many different IoT interfaces, such as advertising, multimedia, and wireless multicast feeds in the local geographic area (e.g., local car park capacity, what's on at the cinema, popular restaurants). Should any of these interfaces be targeted by an attacker using social engineering, users can play an important role in identifying deception attempts. In this example, the user can open their HaaS tool within their smartphone to report any suspected attacks, which can then be directly fed to the smart city security-monitoring system. Free car parking might even be an incentive for correctly reported attacks!

Conclusion

The IoT promises to synergize technology in new and innovative ways, and in doing so it presents major social, business, and economic benefits for modern society. Equally, for cybercriminals, the IoT promises significant rewards if they can execute a social engineering attack successfully, because hacking the user can provide access to all the "things" that they control. The more successful social engineering attacks against the IoT are, the more user confidence in its security is undermined, ultimately delaying adoption of the IoT and the realization of its potential benefits.

Fundamentally, protecting the integrity of the IoT is a two-way street. System developers should ensure that they employ best practice frameworks for producing secure IoT platforms. Security should be treated as an enabler of system functionality and not be a cost-based bolt-on or ignored completely. For their part, users are a crucial firewall in detecting social engineering threats in the IoT, and it is important that they be empowered to report potential threats, especially as they will be familiar with their own environment and more sensitive to its anomalous behavior. At the same time, it is helpful to be able to measure whether users will likely be deceived by social engineering attacks in an IoT ecosystem; therefore, as part of security awareness, it is crucial that the IoT be factored into training material. Finally, as shown in Figure 8, each of these approaches provides complementary tools that help provide a through-life defense architecture against social engineering attacks in the IoT.

To improve IoT security, system developers must empower user threat detection with a mechanism to report suspected attacks and review/analyze user reports to determine their credibility. If they decide an

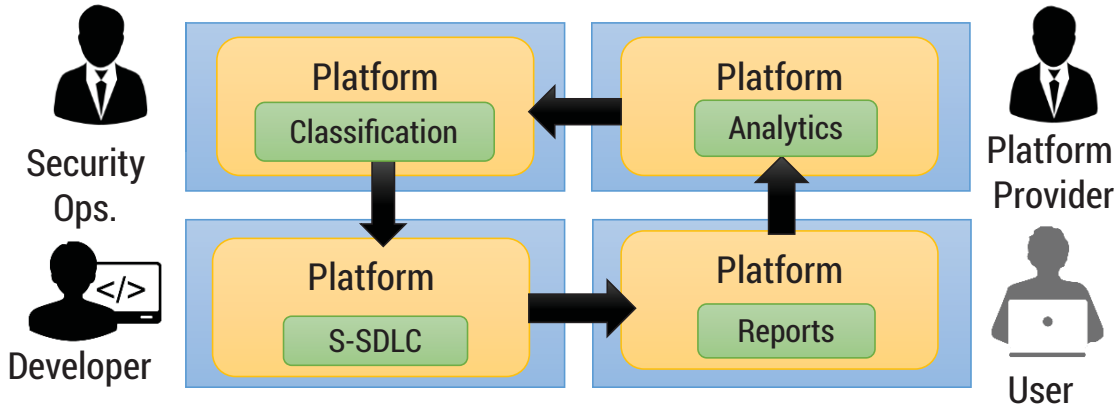


Figure 8 — A four-phase approach to the life management of user interfaces in an Internet-capable platform.

attack report is credible, they can then apply a generic classification to determine the key aspects of the attack and finally integrate these attack vectors as patch parameters within the platform "release/maintain" phase of the S-SDLC.

As cryptographer Bruce Schneier once said, "People don't understand computers. Computers are magical boxes that do things. People believe what computers tell them." Trust lies at the heart of securing the IoT against deception-based attacks, and thus in order to instill trust, it is device integrity that must be protected to prevent user compromise.

Endnotes

[1]Loukas, George. *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann (Elsevier), 2015.

[2]Gan, Diane, and Lily R. Jenkins. "Social Networking Privacy — Who's Stalking You?" *Future Internet*, Vol. 7, No. 1, March 2015 (www.mdpi.com/1999-5903/7/1/67).

[3]"Proofpoint Uncovers Internet of Things (IoT) Cyberattack." Press release, Proofpoint, 16 January 2014 (http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799).

[4]Heartfield, Ryan, and George Loukas. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks." *ACM Computing Surveys*, Vol. 48, No. 3, February 2016 (http://dl.acm.org/citation.cfm?id=2835375).

[5]Dave, Rakesh, et al. "Augmenting Situational Awareness for First Responders Using Social Media as a Sensor." *IFAC Proceedings Volumes*, Vol. 46, No. 15, 2013 (www.sciencedirect.com/science/article/pii/S1474667016330567).

Ryan Heartfield received his BSc degree from the University of Greenwich (UK) in 2011 in computer systems and networking. He currently works as a Network Architect for the UK Government, and since 2014 he has been working toward a PhD in the CSAFE group in the Department of Computing and Information Systems of the University of Greenwich. Mr. Heartfield's research interests include social engineering, computer networks, cloud computing, and network security. He can be reached at R.J.Heartfield@greenwich.ac.uk.

Diane Gan is a Principal Lecturer in the Department of Computing and Information Systems at the University of Greenwich (UK). She has a PhD in the field of computer networks, is a chartered engineer with the Institution of Engineering and Technology (IET), and a Senior Fellow of the Higher Education Academy (HEA). Dr. Gan's current engagements include research and teaching within the areas of cybersecurity and digital forensics. She can be reached at D.Gan@greenwich.ac.uk.

Securing the IoT: It Takes the Global Village

by David Tayouri

The IoT Is Everywhere

The Internet of Things (IoT) today covers many areas of our lives. More and more household appliances are becoming smart, with small computing devices and connection to the Web. Smart TVs and refrigerators are already common in many households. There are also smart thermostats (which collect information about the behavioral patterns of the persons living in the home to ensure efficient heating and cooling), smart door locks (which allow their users to open and close their doors from a remote location), smart security systems (which enable remote control of the security sensors), and so on. In the field of healthcare, there are home diagnostic bedside units, which can quickly give measurements for cholesterol, blood glucose levels, and blood pressure, and systems that can remotely monitor patients' vital signs. Other fields of IoT include autonomous and connected cars, wearable devices, office equipment, and so on.

According to Cisco, there will be about 50 billion networked devices by 2020.[1] The IoT will soon be everywhere.

Vulnerabilities and Risks

Smart Homes and Enterprises

IoT devices have many advantages, but also vulnerabilities and risks. Many smart household appliances are poorly protected (if at all) against cyberattacks. This means that any script kiddie with minimal hacking skills can use them to break into the home network. If, a few years ago, someone had said that TVs and refrigerators could be compromised by hackers to send malicious emails, you would have laughed at them. But such an attack indeed happened on January 2014 — the first known cyberattack to use smart household appliances.[2] This global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multimedia centers, TVs, and at least one refrigerator that had been compromised and used as a platform to launch attacks.

In October 2015, a security researcher demonstrated how to hack into a kettle and steal a home's Wi-Fi password.[3] This vulnerability can be exploited by hackers to break into the Wi-Fi network and from there into the other devices connected to that network. But the risks are even bigger. Researchers have found a way to attack the power grid, by remote manipulation of home and office air conditioners to create a surge.[4] To achieve the hack, attackers target remote shutoff devices installed by utilities on air-conditioning units to preserve power during summer peaks. It seems that these devices are very vulnerable to manipulation by hackers.

To understand how easy it is to hack IoT devices, in March 2016 the MIT Media Lab hosted a hackathon in which it invited 153 hackers to try to find and exploit weaknesses in more than 20 smart home devices.[5] The hackers attempted to control the devices through software vulnerabilities, and they succeeded in taking control of 25% of the devices in less than three hours. Figure 1 depicts the vulnerabilities of the top 10 IoT devices. We can see, for instance, that 8 of 10 such devices use insufficient authentication.

Just as personal computers can be unknowingly compromised to form robot-like "botnets" that can launch large-scale cyberattacks, cybercriminals have begun to commandeer components of the IoT and transform them into "thingbots" to carry out the same type of malicious activity. Cybercriminals intent on stealing individual identities and infiltrating enterprise IT systems have found a target-rich environment in these poorly protected Internet-connected devices, which may be more attractive and easier to infect and control than PCs, laptops, or tablets.

Vehicles, Fuel

Recently, the US Federal Bureau of Investigation (FBI) released a public service announcement to warn drivers about the threat of over-the-Internet attacks on cars and trucks.[6] The announcement mentions that modern

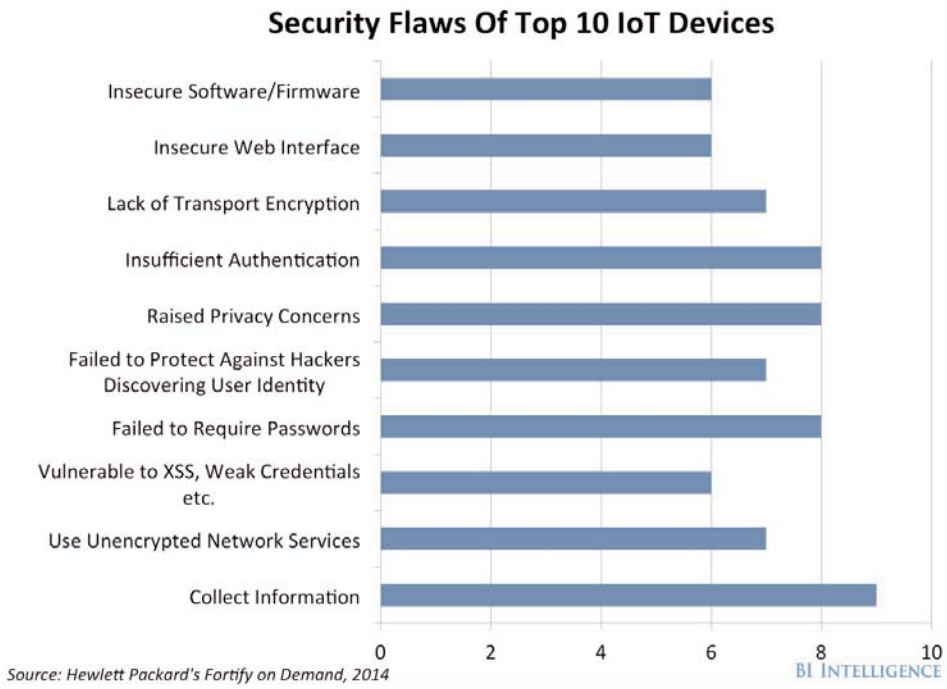


Figure 1 — Security flaws of the top 10 IoT devices.

motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices also offer consumers new features to monitor the status of their vehicles. However, with this increased connectivity, consumers and manufacturers should maintain awareness of potential cybersecurity threats.

Vulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device (e.g., a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi), or within a third-party device connected through a vehicle diagnostic port. In these cases, it may be possible for an attacker to remotely exploit these vulnerabilities and gain access to the vehicle's control network or to data stored on the vehicle. During the "Car Hacking Village" at *DEF CON 2015*, researchers showed how to hack into a Jeep Cherokee and remotely shut off its brakes and engine.[7]

Criminals can also attack business-critical devices connected to the Internet. For example, using the connectivity of monitoring systems on gas pumps, they could cause the pump to register incorrect levels, creating either a false indication of low fuel level or allowing a refueling vehicle to dangerously overfill the tanks, thus creating a fire hazard. Alternatively, they could hack the connection to the point of sale system, allowing fuel to be dispensed without registering a monetary transaction.[8]

Healthcare

From GPS-enabled asthma inhalers to wearable devices that monitor vital functions, consumer-generated health data can hold value not just for the patients, but for a variety of other parties, such as healthcare providers, insurers, public health researchers, and policy makers. Yet the rise of the IoT coupled with the poor state of cybersecurity within healthcare today makes healthcare-related IoT devices a target for both data theft and extortion. A partial electronic health record (EHR) sells on the black market for roughly US $50, and health credentials can sell for $10 each, many more times the value of a credit card number.[9] The reason is that an EHR can be used to file fraudulent insurance claims, obtain prescription medication, and facilitate identity theft.

In addition, one of the latest trends in ransomware attacks is the targeting of hospitals and other healthcare facilities. As a recent *Wired* article notes:

> Hospitals are the perfect mark for this kind of extortion because they provide critical care and rely on up-to-date information from patient records. Without quick access to drug histories, surgery directives, and other information, patient care can get delayed or halted, which makes hospitals more likely to pay a ransom rather than risk delays that could result in death and lawsuits.[10]

In the case of extortion, just imagine what would happen if data for every patient in a hospital were held ransom.

IoT Exploit Strategies

IoT vulnerabilities can be exploited by cybercriminals in various ways. If an attacker succeeds in hacking a smart home device, they can control the device (think what could happen if the device were a pacemaker), hack into the home's/organization's Wi-Fi network, and subsequently hack into the connected computers in order to steal sensitive information, such as bank account passwords, credit card numbers, and private business information. They can also gather information on people's habits (e.g., when they order pizza, which medicines they take, when they take breaks) and more.

The hacker can use the collected information for spear phishing, showing a fake login page to the user and stealing their credentials, sending an email (with relevant content according to the collected information) with an attachment or a link that will install malware on the user's device when opened, and so forth.

A recent FBI alert about the IoT points to several additional risks:[11]

- Exploiting the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices
- Compromising an IoT device to cause physical harm
- Overloading IoT devices to render them inoperable
- Interfering with business transactions

What Should Be Done

The risks are clear, so why don't vendors make an effort to provide more secured devices? The answer is simple: they don't have to. Vendors naturally want to maximize their revenue. So they focus their efforts on improving the devices' price, aesthetics, ease of use, fault resistance, and other characteristics that consumers want. Vendors either are not aware of cybersecurity risks or just ignore them, since it's not cost-effective to handle the risks.

Overcoming this issue will require action from four groups:

1. Consumers
2. Vendors
3. Regulators
4. Researchers

Consumers

We should begin by raising awareness among smart appliances' consumers about the cybersecurity risks. If consumers demand more secured appliances, vendors will have to supply them. In addition, consumers with strong information security awareness may be better protected against social engineering attacks.

Vendors

It is important for vendors to understand that it is only a matter of time until exploiting IoT vulnerabilities will become common, with consequent damage to the vendors' reputation. Publications about cyberattacks on IoT devices raise awareness on cybersecurity among vendors and consumers. Some steps that vendors can take to improve IoT security include:[12]

- **Using open source and open security.** The open source community is totally focused on quality and usability. Thanks to the strength, dedication, and sheer size of the open source community, security flaws are routinely fixed within hours of discovery.
- **Signing the software in embedded devices.** Developers should ensure that the system boots up only if the software to execute is signed by a trusted entity. By anchoring this "root of trust" into the hardware, it becomes extremely difficult to tamper with firmware.
- **Separating critical and noncritical systems.** Manufacturers try to collapse as many functions as possible within one single piece of hardware, but there's no real reason why these separate functional domains should be visible to each other. For example, it shouldn't be possible to access an airplane flight control system via the plane's onboard entertainment platform, or a car's brakes and assisted steering wheel from the car stereo unit.

Regulators

We cannot rely on the efforts of consumers and vendors alone. There should be international standardization and regulation to define the standards of IoT security and enforce those standards among vendors. Most large organizations understand the importance of securing themselves against cyberattacks. Small and medium-sized companies, as well as household consumers, need the regulators to protect them. In some countries, riding

a motorcycle without a helmet is against the law. Bikers know the danger of not using a helmet, but without laws to enforce it, many riders would not wear one. International regulations should enforce "helmets" for IoT devices.

One might question the viability of international regulation, considering that each country has its own interests. Yet if we extend the road rules analogy, we can observe that while every nation has its own driving rules, there are nevertheless many commonalities. There is no need for complete harmony in order for countries to issue and honor international driver's licenses. A similar approach should be considered for IoT cybersecurity. Each nation is free to implement its own rules, but there are certain core defense concepts that will play out (with variations) just about everywhere.

In December 2015, the European Union (EU) agreed on the first EU-wide rules to improve cybersecurity.[13] Under the new rules, companies in critical sectors such as transport, energy, banking, financial services, health, and water supply will have to ensure that the digital infrastructure they use to deliver essential services, such as traffic control or electricity grid management, is robust enough to withstand cyberattacks. This directive marks the beginning of platform regulation. We should expect such international regulations to apply to securing the IoT.

Researchers

From the academic side, researchers are trying to identify different building blocks for security improvement. Many IoT devices use Wi-Fi for communication, and researchers have found a way to detect tampering with this type of communication.[14] Traditional cryptographic operations can be used to authenticate data transmitted from IoT devices. However, tampering with a device cannot be detected using cryptographic methods. Using analysis of transmitted data from devices would allow an additional layer of defense that can detect these tampering events.

The issue of IoT security is also the subject of international conferences. The executive summary of *Cyber³ Conference Okinawa 2015* argues that it is essential to determine an architecture for IoT.[15] The biggest point, from a security standpoint, is to develop resilience in order to prepare for unknown threats, assuming that some threats are unstoppable. Rather than trying to defend against every unknown, we need systems that sustain compromise and keep on functioning with minimal inconvenience. It is vital to establish a shared-goal-driven, multi-stakeholder network to develop regulations and security standards for IoT; we need to find a workable balance between ease of use and security. This can only be achieved through the active cooperation of a body of diverse stakeholders, taking into account privacy, human rights, and legal and moral issues.

Taking Action Now

Until international standardization and regulation are realized, organizations should take the following defensive actions:[16, 17]

- **Identify data assets and access paths.** Organizations should understand the types of data that wearables and IoT devices are collecting and for what purpose, to assess the data's value — both to those who use it and those who may want to hold it ransom. They should identify access paths to vulnerable and sensitive data assets and minimize the impact of phishing attacks by using multifactor authentication.
- **Secure data collection as well as data analysis points.** The IoT data chain starts with the device that collects data, continues through the location where data analysis occurs, and eventually manifests itself in the hands of professionals who can make decisions on the analyzed data. In addition to attacks on the data-collecting device, determined attackers will attempt to compromise the data analysis engine stored in the public or private cloud.
- **Reexamine existing security functions through an IoT lens.** Companies should factor device context into identity and access management. They should look to cloud service providers to assist with incident response, threat management, and security operations in the cloud, where their data repositories are located. Finally, they need to create policies to address data privacy concerns about data ownership, consent, use, ethics, and liability.
- **Isolate IoT devices on their own protected networks.** This will prevent compromising the business network when IoT devices are attacked.
- **Disable UPnP on routers.** UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Hackers can change the configuration and run commands on the devices, potentially enabling the devices to harvest sensitive information, conduct attacks against homes and businesses, or engage in digital eavesdropping. Thus, disabling UPnP on routers is an essential means of stemming a cyberattack.

- **Use current best practices.** Organizations should take extra caution when connecting IoT devices to wireless networks and when connecting remotely to an IoT device.
- **Ensure all default passwords are changed to strong passwords.** Leaving the default passwords in place will enable a cybercriminal to easily exploit the devices to open doors, turn off security systems, record audio and video, gain access to sensitive data, and so on.

Summing Up

IoT is increasingly used for household appliances, business equipment, and critical services; therefore, securing IoT devices against cyberattacks has become a major concern. IoT implies a massive increase in data being collected and transmitted. The growth in the volume of data creates an inherent increase in vulnerabilities.

To reduce the success of cyberattacks on smart devices, consumers should demand secured appliances, vendors should understand the risks, and international regulators should enforce cybersecurity policies. For industrial IoT security, the security of a whole chain must be ensured.

As bikers are required by law to use helmets, international regulation should likewise enforce "helmets" for IoT devices. At the end of the day, each nation or multinational body must establish rules that represent its values and priorities but collaborate to find common solutions and mechanisms that will serve the interests of all.

Endnotes

[1]Taylor, Stuart. "10 Predictions for the Future of the Internet of Things." *Connected Life Exchange* (Cisco blog), 3 June 2015 (http://blogs.cisco.com/cle/10-predictions-for-the-future-of-the-internet-of-things).

[2]"Proofpoint Uncovers Internet of Things (IoT) Cyberattack." Press release, Proofpoint, 16 January 2014 (http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799).

[3]Pauli, Darren. "Connected Kettles Boil Over, Spill Wi-Fi Passwords over London." *The Register*, 19 October 2015 (www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots).

[4]"Hacking the Grid through Air Conditioners." iHLS, 17 February 2016 (http://i-hls.com/2016/02/hacking-grid-air-conditioners).

[5]Meola, Andrew. "Hackers Prove How Easy It Is to Invade Smart Homes." *Business Insider*, 10 March 2016 (www.businessinsider.com/hackathon-for-smart-homes-in-iot-internet-of-things-2016-3).

[6]"Motor Vehicles Increasingly Vulnerable to Remote Exploits." Public service announcement, US Federal Bureau of Investigation (FBI), 17 March 2016 (www.ic3.gov/media/2016/160317.aspx).

[7]Peterson, Andrea. "Here Is How You Learn to Hack a Car." *The Washington Post*, 14 August 2015 (https://www.washingtonpost.com/news/the-switch/wp/2015/08/14/here-is-how-you-learn-to-hack-a-car/).

[8]"Internet of Things Poses Opportunities for Cyber Crime." Public service announcement, US Federal Bureau of Investigation (FBI), 10 September 2015 (www.ic3.gov/media/2015/150910.aspx).

[9]Maruca, William. "Hacked Health Records Prized for their Black Market Value." Fox Rothschild LLP, 16 March 2015 (https://hipaahealthlaw.foxrothschild.com/2015/03/articles/articles/hacked-health-records-prized-for-their-black-market-value/).

[10]Zetter, Kim. "Why Hospitals Are the Perfect Targets for Ransomware." *Wired*, 30 March 2016 (www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/).

[11]FBI (see 8).

[12]Swift, Art. "Improving Security in the Internet of Things." ITProPortal, 20 March 2016 (www.itproportal.com/2016/03/20/the-internet-of-things-improving-its-security/).

[13]"MEPs Close Deal with Council on First Ever EU Rules on Cybersecurity." Press release, European Parliament, 12 December 2015 (http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity).

[14]Bagci, Ibrahim Ethem, et al. "Using Channel State Information for Tamper Detection in the Internet of Things." *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC 2015)*. ACM, 2015 (http://dl.acm.org/citation.cfm?id=2818028).

[15]"Executive Summary." *Cyber³ Conference Okinawa 2015: Crafting Security in a Less Secure World*. Okinawa, Japan, November 2015 (www8.cao.go.jp/okinawa/3/cyber3/summary_en_20160107.pdf).

[16]FBI (see 8).

[17]Zetter (see 10).

David Tayouri, MSc in computer science, has 25 years of experience in software architecture, development, and project management. He has been dealing with different aspects of the Internet since writing his thesis in 1997. Mr. Tayouri is one of the cyberactivity leaders in Israel Aerospace Industries (IAI) and has managed the cyber-intelligence department for the last three years. He can be reached at dtayouri@elta.co.il.

Security and Privacy in the Internet of Things:
How to Increase User Trust

by Dimitrios G. Kogias

Expanding Data, Growing Threats

As the number of interconnected smart things increases from billions to trillions by the end of 2020, and as their special capabilities for cooperation, communication, identification, and exchange of information produce a huge amount of data, the idea of an Internet of Things (IoT) is becoming a reality.[1] In an IoT solution, an interconnection between the physical and virtual world is realized, with humans, devices (or smart things), dissemination of data (or information), and communication as its core characteristics.[2]

From this promising interconnection, the many different sectors of human life where IoT applications and advanced services are employed are proliferating rapidly. Nowadays, IoT systems can be found in: pervasive healthcare applications, building management systems, public surveillance systems, smart city services (e.g., in critical infrastructures such as a smart grid for electricity generation and distribution), and data acquisition and sensing applications covering almost all the aspects of human life, both publicly (e.g., public surveillance) and privately (e.g., healthcare monitoring applications). All these systems consist of sensors, actuators, radio frequency identification (RFID) tags, mobile phones, and/or wearables that generate data and communicate intermittently to share with each other or disseminate the information at specific base stations where it can be further processed and redistributed.

The demanding pervasiveness of this IoT data collection results in an increase in the risks to which everyone is exposed, along with the necessity for better and more efficient security of the systems where this data is produced and transmitted. The massive number of devices that belong to an IoT system, their heterogeneous nature (in terms of memory availability, process capabilities, energy consumption, and protocol application), and their need for ubiquitous Internet communication call for innovative and successful system design in order to provide resilience, robustness, privacy, and security to the users.[3]

Even as our reliance on the digital world increases, so does the variety and importance of the data that is transmitted. Therefore, apart from the classical security threats that a system has to protect against, a new tide of digital hazards and potential threats is rising that must be addressed carefully and effectively, because they can prove extremely harmful for both companies and individuals. In particular, security[4, 5] and privacy[6, 7] issues are of great concern, mainly because of their delicate nature and specifically because of the network's increased size and the wealth of (personal) information that is shared in it.

The notion of security is extremely important for any system and — especially in the IoT environment — is closely related to the crucial notion of privacy, in particular with the identification of sensitive or private data. The relation is such that it is often difficult to distinguish between these two concepts. In an effort to better describe their roles, consider that security covers the whole system, including network security and identity management, while privacy is closely related to the user's trust in the system to protect their data and actions from internal or external intruders.[8, 9] Therefore, any security measures can not only reinforce the system's resilience, but also strengthen privacy, leading to a desired increase in the user's trust in the system and the network (i.e., the Internet).

How harmful can it be when IoT data ends up in the wrong hands? Imagine an IoT system in which a home refrigerator can upload data regarding a person's eating habits and store them in the cloud. While this alone might not be important information, when it is combined with data from the house's smart TV and the alarm at the door, the result might be more than someone is eager to share with others. For example, if data on the individual's eating habits is combined with their preferred TV shows, a user profile can be created that advertisers could exploit by directing unwanted targeted advertisements, either digital or physical ones, toward that individual. Exposure of more sensitive information, such as the status of the alarm (or how to control it) or the status of the doors and windows

in the person's house, could bring about more severe, even criminal, scenarios.

In the rest of the article, I will focus on the security and privacy challenges inherent in IoT implementations and propose solutions to help build a feeling of trust between all parties. In doing so, I will try to answer such questions as "How do we assess the security risks in IoT?" and "How can the distinct interests of the sources and the collectors of personal data be expressed in a way that satisfies both parties and increases privacy and access control?"

Security Challenges

For the IoT especially, security needs to be considered at more than one level. From technological issues to more philosophical ones that aim to enhance the privacy of the user's data, paying attention to these concerns will confer a feeling of trust in the system.[10, 11]

The security challenges that an IoT solution might face can be divided into threats of a *physical* nature and threats of a *cyber-physical* origin. The former concern the extremely large number of devices that work in uncontrolled environments, where access might not be easy or frequent, making them vulnerable to physical dangers (e.g., extreme weather conditions) or human attacks (e.g., surveillance cameras, sensors in a smart grid infrastructure). There is also the case in which the device's lifecycle surpasses the embedded technology, demanding a repair or upgrade in order to keep up with what it is expected from it. Considering that such devices may be deployed in a hostile environment or not be programmed to receive an upgrade, this can result in a rather cumbersome task.

Cyber-physical threats must also be taken into account when evaluating the overall system's resilience and security. For example, the large-scale production of several almost identical devices (e.g., RFID tags, temperature sensors) greatly increases the possibility of successful external attacks to the system, since if a malicious party gains remote access to one of these devices by exploiting any protocol's vulnerabilities, other intruders might follow the same process to gain control over the rest of the devices, multiplying the inflicted system damage. The fact that IoT environments often include devices that were not initially designed to provide Internet access (e.g., RFID tags, watches, refrigerators, alarms) creates a rather heterogeneous network with different storage, memory, processing capabilities, and communication protocols. This demands a closer examination for the implementation of security solutions, since the traditional ones will not be applicable without proper modification.

Apart from the above challenges, security breaches in the IoT will very likely be the product of organized cyberattacks,[12] initiated by individuals with significant resources that will apply sophisticated methods to try to gain access to the inside of the IoT network. The targets of these attacks are the network's communications, and the goal is to steal the propagated data. In addition, the attackers have the knowledge and the ability to launch large-scale attacks that will cripple the network and mess with its functionality by controlling a number of software systems and using them for their malicious purposes. "Bots" (i.e., computers that are under the control of the attacker and not their physical owner) are frequently used to send spam emails, launch distributed denial of service (DDoS) attacks, or host false websites in order to attract users, steal their credentials, and thereby gain access to the system "legitimately."

One more popular cyber-physical attack is the insider threat, where outsiders manage to gain access to, mainly, corporate networks by exploiting the mistakes of legitimate users (e.g., their lack of compliance with corporate regulations) or by stealing their credentials through well-orchestrated attacks. The man-in-the-middle attack is another well-known cyber-physical threat, in which a malicious user impersonates a legitimate one during a communication session, gaining access to the network and learning information or eavesdropping undetected on conversations between two legitimate users. Cyber-physical attacks are very difficult to protect against, since they combine the application of highly complex techniques and aim at the most vulnerable elements of the IoT ecosystem.

All the security threats presented here are part of the spectrum of security challenges that should be carefully addressed in order to design a robust and trustworthy IoT environment. Unfortunately, the cost of intrusions cannot be measured in advance; therefore, there is a need to increase security measures and design in order to counter the possible threats and prevent any breaches that might damage the feeling of trust in the IoT environment.

Privacy Challenges

With the involvement of citizens and the characteristic of ubiquitous communication via the Internet, privacy[13] has attracted a lot of attention from IoT researchers and professionals. Since it is crucial to continuously reinforce privacy, the system must be able to protect the identity of the users from being exposed, providing anonymity of the generated data and, ideally, automatic detection of the sensitive content.

In addition, a system has to prevent the continuous tracking of a user's position and actions, which can be easily done through the mobile devices everyone is using. Mobile phones can not only be used to track the location of the user (via triangulation), but also to collect information shared willingly — even in real time — by the user on social networks. This information can later be processed by malicious third parties in order to take advantage of somebody's absence from home to force a criminal action against the victim (e.g., a robbery attempt). Actions that lead to the identification and tracking of the user are regarded as a very important privacy threat that must be carefully addressed with close cooperation between law enforcement agencies and end users. One example of a working project that deals with ways this cooperation can be developed is the EU's TRILLION project.[14]

User profiling, the collection of information on a user's habits (either online or in real life) by companies to enable targeted advertisement during Web browsing, is considered an important privacy threat to everyone. Facebook recently admitted to using "lookalike" techniques to track the habits of not only its registered users, but even people who do not have a Facebook account.[15] This can be accomplished by following a Web user's online "fingertip," which is created based on all the devices that the user owns, certified by an online account. If the user registers with service A, giving personal information, then provides different information to service B, then A can identify the individual with the help of B by comparing and combining the fingertip information that both services have. Profiling is a very popular technique among all major companies that demand a piece of the modern digital pie.[16] Legislation has begun to be enacted against this kind of action both in the US and the European Union.[17]

Perhaps the most serious privacy-related problem in an IoT environment stems from the lack of control over the vast amount of personal data generated. Even if the original data collector is committed to protecting the user's data, there might be a moment where possession of data is passed (legitimately or not) to a third party who doesn't share the same views regarding the processing of the user data. Thus, despite their initial intentions, the original data collector ends up creating a situation that compromises the user's trust and creates a security threat to the system.

PETs and Security Solutions

As we've seen, the security and privacy threats in the IoT environment are many. Privacy-enhancing technologies (PETs) can be used to achieve compliance with existing data legislation to protect the user's privacy and enforce the feeling of trust in the efficiency and performance of the system. For optimal performance, PETs should address the problems concerning all the basic attributes of an IoT environment (e.g., myriad heterogeneous devices, transfer and processing of sensitive data, malicious actors seeking exploitation opportunities). Unfortunately, existing security tools often do not apply well to the special characteristics of an IoT environment because of energy consumption issues or intense processing requirements that are difficult for many smart devices to achieve. Therefore, I will confine the discussion to solutions that closely adapt to the peculiarities of the IoT system.

Cryptography

Cryptography, the most prominent PET technique, aims to hide the identity of the data's owner and secure the transfer of the data in the IoT system, allowing access only to authorized users and protection against profiling techniques. U-Prove[18] is a PET that uses a special token containing attributes that are cryptographically related to the user, and Idemix[19] uses similar encrypted tokens that are based on a "group" signature, allowing an individual to anonymously sign a packet on behalf of a specific group of people. Both technologies have been successfully implemented on smart cards and manage to process authentication requests in less than 1.5 seconds, enhancing the system's resilience and security.

For RFIDs, especially, two PET approaches are to rename the tags and minimize the distance between the tag and the reader. Furthermore, researchers have proposed a "minimalist cryptography"[20] for RFID tags in which the cryptographic computations take place at the end point and are then inserted on the tags. To thwart possible eavesdroppers, the reader can even re-encrypt the tag at a later point using a different key, such that a would-be snoop will receive two different signals at two different times. That way, the prevention of unauthorized access is achieved, and secure communication between the RFID tag and the reader is completed successfully.

Privacy Coaches and Brokers

Another promising PET solution is the use of a third-party mobile app that plays the role of "privacy coach," suggesting the actions to be taken when reading an RFID tag. This mobile application scans the ID of an RFID tag and accesses a back-office database to search for the privacy policy related to the tag. It then compares it with the user's privacy preferences (found in

their profile on the application) and presents the results in an effort to warn the user about the potential dangers of the RFID tags in their vicinity.

Extending this solution, a proxy can be used as a privacy broker, responsible for allowing communication between the information/service providers (e.g., RFID tags) and the users when the credentials of both have been certified by the broker, thus ensuring privacy in the communication. This solution, while promising, could face scalability issues due to the large number of devices that might be interconnected through the proxies, and these issues would need to be carefully addressed before further deploying the solution in an IoT environment. Use of lightweight communication protocols and carefully designed network infrastructures to deal with the traffic are possible solutions to this problem.

Data-Centric Approaches

Data-centric solutions have also been applied to enhance the privacy of an IoT system. These solutions, which utilize privacy-preserving approaches to protect the sensitive data that are the heart of the system,[21] include:

- Data swapping, a technique that suggests the exchange of sensitive data between individual records in a database, thereby increasing the uncertainty and making it harder for malicious users to exploit it
- Data randomization, an approach that can be used in programs written in unsafe languages (e.g., C or C++) to provide probabilistic protection by issuing XOR instructions on data with random masks
- Data suppression, a technique that is used to conceal private information on public documents by withholding information that can easily identify a person or a group
- Synthetic data generation, a technique that uses anonymized data to prevent compromising the identity and confidentiality of particular sets of data (e.g., names or addresses)

Network Approaches

One more popular solution is the use of virtual private networks (VPNs), which can be described as special networks (i.e., extranets) that are created, usually, for business purposes between registered users. Since access to the network is permitted only to a small, registered group of people, VPNs are considered very resilient. Nevertheless, they are not a solution that applies well to a broader information exchange on the scale of an IoT system. Another PET is "onion routing," a technique that encrypts the Internet traffic from multiple sources and mixes it, making it difficult to achieve a match of an IP packet to a particular source. Since it uses multiple encryption layers and the public key from the router, however, the waiting time is greatly increased, hindering the overall performance of the network.

For the described PETs to be successful, the overall security of the IoT ecosystem must be addressed. Solutions that deal with the majority of the physical and cyber-physical threats described earlier include techniques to enforce the confidentiality of the communication between the smart entities, like IPSec and Transport Layer Security (TLS), which have been applied successfully.[22] To increase their efficiency, they are also combined with secure network stacks in order to deal with the resource constraints that are inherent to many IoT smart devices.

Architecture

Furthermore, the network's *availability* must be ensured by the IoT architecture[23] in order to provide the desired link handover to allow for seamless communication in the network, while mechanisms like TLS and TCP can be used to test for data *integrity* (i.e., insurance that the data has not been modified or lost during the communication phase). *Authenticity* of a connection (which also includes the notion of integrity) deals with providing all the necessary mechanisms to confirm the establishment of a connection with an authenticated, legitimate user or device. There are techniques for device *authorization* to communicate when they belong to the same domain (e.g., Kerberos[24]), but solutions are needed that permit the authentication of devices even if they belong to different domains, as this scenario better fits the inherent characteristics of the IoT environment.

Proposed IoT architectures such as IoT-A, BeTaas, OpenIoT, and IoT@Work[25] deal with many of the security- and privacy-related issues presented in this article (achieving varied levels of performance on the many security attributes, as shown in Vasilomanolakis et al.[26]), but they still present several holes in their security. For example, data transmission is partially covered, with the focus concentrated on transmission between the gate and the cloud infrastructure, but not so much on communication between the smart devices or inside the cloud. As noted above, one feature that still must be addressed is inter-domain identity management, which is strongly needed in an IoT environment. Given all this,

the fact is that there is still no universal architecture solution that can be applied to the various IoT scenarios and perform equally well in all of them.

Standards

Finally, the IoT system suffers from the lack of widely available, open, and well-adopted standards. Manufacturers require technical guidelines so as to ensure the seamless performance of the system's functionality between the heterogeneous devices and the provided services it provides. To achieve this, special working groups, both regulatory and technical, should join forces to provide the guidance needed to enable the many different IoT manufacturers to be part of a working and evolving IoT ecosystem. To neglect this task would hinder the IoT system from achieving its great potential.

Endnotes

[1]"The Internet of Things (IoT): An Overview." Internet Society, 15 October 2015 (www.internetsociety.org/doc/iot-overview).

[2]Bertino, Elisa. "Security Threats: Protecting the New Cyberfrontier." *IEEE Computer*, Vol. 49, No. 6, June 2016 (http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7490312).

[3]Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: Threats and Challenges." *Security and Communications Networks*, Vol. 7, No. 12, November 2014 (http://onlinelibrary.wiley.com/doi/10.1002/sec.795/abstract).

[4]European Research Cluster on the Internet of Things. "Internet of Things: IoT Governance, Privacy and Security Issues." European Commission, January 2015 (www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf).

[5]Cirani, Simone, Gianluigi Ferrari, and Luca Veltri. "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview." *Algorithms*, Vol. 6, No. 2. April 2013 (www.mdpi.com/1999-4893/6/2/197).

[6]Vasilomanolakis, Emmanouil, et al. "On the Security and Privacy of Internet of Things Architectures and Systems." Paper presented to the *International Workshop on Secure Internet of Things (SIoT 2015)*, Vienna, Austria, September 2015 (www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/SIoTpaper.pdf).

[7]Porambage, Powani, et al. "The Quest for Privacy in the Internet of Things." *IEEE Cloud Computing*, Vol. 3, No. 2, March-April 2016 (www.computer.org/csdl/mags/cd/2016/02/mcd2016020036.html).

[8]Cirani et al. (see 5).

[9]Vasilomanolakis et al. (see 6).

[10]Porambage et al. (see 7).

[11]Tian, Cuihua, et al. "Analysis and Design of Security in Internet of Things." *Proceedings of the 8th International Conference on BioMedical Engineering and Informatics (BMEI 2015)*. IEEE, 2015 (http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7401589).

[12]Bertino et al. (see 2).

[13]Porambage et al. (see 7).

[14]TRILLION Project (http://trillion-project.eng.it/).

[15]Toor, Amar. "Facebook Begins Tracking Non-Users Around the Internet." The Verge, 27 May 2016 (www.theverge.com/2016/5/27/11795248/facebook-ad-network-non-users-cookies-plug-ins).

[16]Brandom, Russell. "Google and Facebook Still Dominate Tracking on the Web." The Verge, 18 May 2016 (www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising).

[17]"Digital Security." European Commission, updated 30 June 2016 (https://ec.europa.eu/digital-single-market/en/online-privacy).

[18]Paquin, C., and G. Zaverucha. "U-Prove Cryptographic Specification V1.1 (Revision 3)." Microsoft Corporation, December 2013 (www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Cryptographic20Specification20V1.1.pdf); see also http://iiw.idcommons.net/images/8/88/U-Prove_technology_overview-Nov2010.pdf.

[19]Camenisch, Jan, and Els Van Herreweghen. "Design and Implementation of the Idemix Anonymous Credential System." IBM Research, 2002 (http://freehaven.net/anonbib/cache/idemix.pdf).

[20]Juels, Ari. "Minimalist Cryptography for Low-Cost RFID Tags." Paper presented to the *Security in Communication Networks: 4th International Conference (SCN 2004)*, Amalfi, Italy, September 2004 (http://www.arijuels.com/wp-content/uploads/2013/09/J04b.pdf).

[21]Porambage et al. (see 7).

[22]Dierks, Tim, and Eric Rescorla. "The Transport Layer Security (TLS) Protocol, Version 1.2," RFC 5246 (Proposed Standard). IETF, August 2008 (https://tools.ietf.org/html/rfc5246).

[23]Vasilomanolakis et al. (see 6).

[24]Steiner, Jennifer G., Clifford Neuman, and Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems." *Proceedings of the USENIX Winter Conference*. USENIX Association, 1988 (www3.nd.edu/~dthain/courses/cse66771/summer2014/papers/kerberos.pdf).

[25]Vasilomanolakis et al. (see 6).

[26]Vasilomanolakis et al. (see 6).

Dimitrios G. Kogias received his diploma in physics in 2001; in December 2004 he received his MSc in electronics and radioelectrology, and in May 2010 his PhD in designing algorithms for dissemination of information in unstructured networking environments from the National and Kapodistrian University of Athens. Dr. Kogias is an Adjunct Lecturer and a Senior Researcher at the Department of Electronics Engineering of Piraeus University of Applied Science (Greece). He has participated in national and European projects and taken part in international conferences. Dr. Kogias's work has been published in international journals, and he has coauthored two book chapters. He can be reached at dimikog@teipir.gr.

Cutter
IT Journal

About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and Agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Ron Blitstein
- Tom DeMarco
- Lynne Ellyn
- Vince Kellen
- Tim Lister
- Lou Mazzucchelli
- Robert D. Scott