Cyber and physical threats to the Internet of Everything

George Loukas, Charalampos Patrikakis

Introduction

"*Prepare for the unknown by studying how others in the past have coped with the unforeseeable and the unpredictable.*" What does a General George Patton quote have to do with cyber and physical threats or the Internet of Everything?

After over 40 years of the Internet faithfully serving the needs of the Earth's human population for information, communication and entertainment, we are now in the era of the Internet of Things. And of course, when we refer to the Internet, we also mean the Web and therefore the Web of Things, 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) *"brings together people, process, data, and things to make networked connections more relevant and valuable than ever before"*. In the IoE era, machines are equal as Internet users.

In an ecosystem where 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, where an attack in cyber space can propagate and have an adverse effect in physical space and vice versa. So how can we be prepared 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.

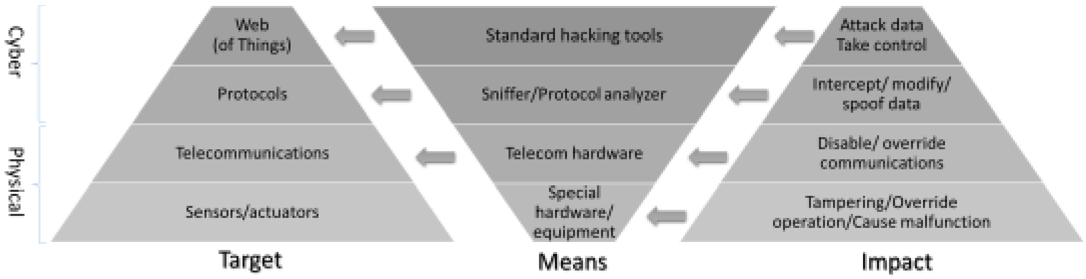
Composing the Internet of Everything and decomposing it to its threats

Let us take 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 for 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 cyber world built on top of the physical. According to this, we can identify four different layers of components for IoE:

1. The lower layer corresponds to the "everything" of the IoE, including humans and things (namely sensors, actuators and embedded systems

which 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 can affect the physical privacy, the convenience or, in extreme cases, the health 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).

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 issues of 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 (disabling or overriding communications) is to render all the communication infrastructure incapable of operation in its intended way (or even completely disable it). The way to achieve it is through special hardware, which is able to either operate in a non-standard way (i.e. for overriding communications), or damage communication equipment (i.e. 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 them, modify them or prevent them from reaching their intended destination, or simply to generate illegitimate traffic. As this is the most widely studied layer, there are several means and tools to achieve any kind of mischief in this space, for example with protocol sniffers and analyzers, packet generators etc.
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 communication, focusing on the information/data and control. Depending on the target, standard hacking tools and social engineering can be used.


Cyber
Physical
Web (of Things)
Protocols
Telecommunications
Sensors/actuators
Target
Standard hacking tools
Sniffer/Protocol analyzer
Telecom hardware
Special hardware/ equipment
Means
Attack data Take control
Intercept/ modify/ spoof data
Disable/ override communications
Tampering/Override operation/Cause malfunction
Impact

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

Cyber: Web of Things

As in the case of the world wide web, the attacks here may have little to do with the communication, or even computing infrastructure. The virtualization offered by the web, where traditional services have been substituted by their "*e-quivalent*", has opened a new world of cyber rather than physical threats. Instead of someone capturing something tangible and asking ransom for it, a 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 web of things, 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 grid to telecommunications, and even elections, protecting the connected things over the web from cyber attacks is critical.

Cyber: Protocols

In order to enable the communication between Things in 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 impact are well known (interception of communications, alteration of transmitted data, spoofing of information), the tools and means that attackers can achieve them differ. As new protocols appear, new threats (in the form of old ones appearing under a new suit) arise, and countermeasures have to be re-invented. Unfortunately, there is no recipe for success here, as the experience from the past is only to the advantage of the attackers. After all, you have to know the threat before you can confront it.

Physical: Telecommunications

As Telecom operators are rapidly "*embracing the cloud*" in order to improve their efficiency in operations, services rollout and content storage and distribution, a new challenge is emerging: the need for Cloud security, for which security strategies seem to be in place for only 50% of telecom companies [Radware2016]. To add to this, the emerging trend for "Shadow IT" (use of IT systems within an organization without the involvement of corporate IT) intensifies security and privacy risks, adding to the traditional challenge of uninterruptable service provision, that of personal data protection.

Physical: Sensing

Depending on the type of sensing technology used, a capable adversary with physical access may attempt to deceive the sensor used [Loukas2015]. For instance, some infrared sensors are known to have difficulty in detecting objects hiding 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 fire-arm affixed to the outside of the leg and scanned against a dark background etc. These techniques for deceiving sensors used by physical security systems have been proven experimentally and documented publicly by researchers.

One particularly impressive such experimental attack that has been recently published aims to defeat lidar by producing an overwhelming number of spoofed echoes or objects (Petit2015). This could be loosely characterised as a sensory channel denial of service attack. A simpler but not less effective attack on cameras has been demonstrated by the same authors. By emitting light into a camera (e.g., with a laser pointer), it is possible to blind it by rendering it unable to tune auto exposure or 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. The approach described by Son et al. (Son2015) 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.

An overarching threat: Deception

Traditionally, the attack avenue that has overcome most technical security measures put in place 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" [Heartfield2016]. Although not as precise, an umbrella term that is commonly used for both technical and non-technical such deception attacks is social engineering. It 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 the human users into disclosing private data, such as their password, or performing some compromising action like 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 the user has 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 can be extended to physical threats. Examples would include most sensory channel attacks described in the previous section, as their aim is 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 that their sensors have 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 direction, we discuss the brief history, current state and future of physical and cyber threats to automobility, the domotic environment and well-being. For each one, we investigate whether General Patton's approach to turn to (safety and security) history for solutions would help.

Automobility

Over the past seven years, attacks on 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 articles on different models of cars hacked being on the news every week. In fact, it is seen as so obvious that citizen's private cars will start becoming targets of cyber attacks that researchers have already started studying the impact that future cyber security warnings will have on the drivers [Altschaffel2015]. Will the drivers interpret the warnings correctly? Will they be affected psychologically, and would that by itself compromise their safety? This is a concern in 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 by an extensive security breach affecting the engine or brakes.

But surely, this is not the first time the automotive industry deals with driver distractions from warnings. The EU, USA and several countries have developed rigorous guidelines for the provision of information to drivers in a manner that reduces distraction to the driver by taking into account single glance duration, amount and priority of information, etc. A recommended worldwide distraction guideline policy position has been provided by the International Organization of Motor Vehicle Manufacturers in 2015 and can be adopted by engineers developing mechanisms and content for in-car cyber security warnings too. It is also not the first time the automotive security sector deals with command injection attacks that render critical systems unavailable. For example, large-scale EU-funded projects, such as FP7 EVITA, have provided practical solutions for securing the communication and embedded computation of modern cars since the previous decade, long before cyber security of cars reached mainstream media. The increased vulnerability of modern cars to cyber-physical threats due to the variety of communication, automation and telematics technologies introduced lately can be addressed with existing security mechanisms, as long as the buyer is willing to pay for it. So, it is more a matter of price elasticity than of availability of cyber protection solutions for cars.

Currently, sensory channel attacks can be considered as 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 would generate volumes of misleading fake objects would render them completely unable to operate. 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 one more case of a sensor reliability problem, which has been addressed in great detail by mathematicians, computer scientists, physicists and engineers over several decades. After all, a car's sensor is much more common to fail naturally, given the adverse environment where it operates rather than as a result of a sensory channel attack. So, redundancy (using more than one sensor for the same data collection, often supported by an algorithm for estimating a sensor's predicted measurements) and diversity (using more than one types of sensors for the same problem and cross-correlating their data) are natural solutions for cyber-physical resilience too.

Domotic Environment

Most smart home devices are small and inexpensive. They often have to offload their processing and storage to a cloud environment and rely on the home router for security, unable to feature any sophisticated onboard protection mechanism. At a real-world commercial level, security is usually limited to a simple authentication mechanism, usually a password, which is commonly left to its factory default, and 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 NAS prevents individual devices from being directly visible on the Internet and that the number of devices globally is still not large enough to justify economically the focus of organised cyber criminals. This is rapidly changing. According to Gartner, it is estimated that by 2022, a typical smart home will include around 500 Internet-connected devices [Gartner2014].

Yet, the reality is that almost all actual cyber security breaches publicly reported in this context have involved no extraordinary effort or advanced hacking technique and would have been prevented if common sense and age-old security design principles, such as those proposed by Saltzer and Schroeder in the 1970s, had been followed. The real problem is that embedded system developers simply do not know them. In fact, these principles (as well as other relevant disciplines, such as wireless networks and cloud computing) are often omitted from the curricula of software engineering Bachelor degrees. Take, for instance, the principle of the *least common mechanism*. Companies that develop cameras for home automation systems tend to re-use 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, the principles of the *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 smartlock and a conventional one from the garage), a user may accidentally unlock more doors than the one it 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 m (for Bluetooth low energy) from the door. However, the assumption that just because a user is near a door means that the user intends to unlock it does not hold. Similar examples of violation of the basic security design principles can be found behind most security failures in domotic environments. Making sure that they 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.

Well-being and healthcare

The episode of TV drama Homeland where terrorists assassinated 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 had considered realistic before asking his doctors to disable his pacemaker's wireless functionality as early as in 2007 [Clery2015]. This was long before "connected healthcare" and today's numerous options of available wearable devices. In fact, the term "wearable" falls already too short in describing the variety of devices capable of monitoring and wirelessly reporting on wellbeing and personal health status: If we were to correctly identify all options, then we should also add implantable, adhesive, patched and even ingestible devices. For the latter, the US Food and Drug Administration (FDA) has recently declined to approve the first mass market drug incorporating an ingestible sensor (a collaboration between Proteus and Otsuka Pharmaceuticals) on the basis of request for 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" [MobileHealthNews2016].

It is inevitable that personalized, daily monitoring of our health conditions and wellbeing will be carried out through the use of one or more devices, while it is also a matter of time and culture to widely accept a more active role of these devices: Insulin pumps, drug infusion pumps, pacemakers with integrated defibrillators. FDA has already acknowledged the criticality of the situation, issuing recommendations on how manufacturers should safeguard medical devices against cyber breaches, making security by design a top priority.

In terms of safety-criticality, there is a distinction between devices which are related to health issues (i.e. a blood pressure monitor device and or app) and these which relate to wellbeing (i.e. calories calculators or apps which can help you cut smoking), but 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) at the sweet sound of a nightingale. It does not take more than compromising your IFTTT account to change the settings so that at 3.00 AM you wake up to an AC/DC power riff intro. Or compromising your training app and making it push 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 would simply be a nuisance, 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 cyber attacks? Suitably, it is probably more about hygiene (that is, cyber hygiene) than anything else. Medical devices in hospitals are notorious for relying on very old operating systems (such as 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 expecting medical software developers to provide updates in the same way the rest of the IT industry operates. But would hospitals install updates? Introduction of cyber hygiene training would be the minimum requirement for such a culture shift. It would also help if medical personnel refrained from leaving post-it notes with their shared account's password on hospital computers. Then, there is privacy in wearables, which is commonly based on proprietary/secret cryptography methods, so as to tick that box, but close 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 Auguste Kerkhoff 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 cyber hygiene and age-old security principles should be sufficient to thwart most realistic cyber-physical threats.

Conclusions

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 been 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 cyber security hygiene practices, or mere common sense, preferably cultivated through security education for software developers and awareness programs for users.

References

[Heartfield2016] Ryan Heartfield and George Loukas. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys, 2016.

[Loukas2015] George Loukas. Cyber-physical attacks: a growing invisible threat. Butterworth-Heinemann (Elsevier), 2015.

[Altschaffel2015] Robert Altschaffel, Tobias Hoppe, Sven Kuhlmann, Jana Dittmann. Simulation of Automotive Security Threat Warnings to Analyze Driver Interpretations and Emotional Transitions. In Computer Safety, Reliability, and Security, pp. 47-58, Springer International Publishing. 2015.

[Petit2015] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Blackhat Europe, November 2015.

[Son2015] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In 24th USENIX Security Symposium, pp. 881-896. 2015.

[Gartner2014] Gartner. Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022. September 2014.
http://www.gartner.com/newsroom/id/2839717

[Clery2015] Daniel Clery. Could your pacemaker be hackable? Science, 346(6221): 499. 30 January 2015.

[MobileHealthNews2016] Mobilehealthnews.com "FDA declines to approve Proteus-Otsuka sensor-equipped pill, asks for more tests", April 2016. http://mobihealthnews.com/content/fda-declines-approve-proteus-otsuka-sensor-equipped-pill-asks-more-tests

[Radware2016] RadwareBlog "Today's Cyber Security Threats in the Telecom Industry". March 2016. https://blog.radware.com/security/2016/03/cyber-security-threats-in-telecom/