Security in the Internet of Everything Era - Opening Statement

George Loukas, Charalampos Patrikakis

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

This issue features five articles, discussing existing and future (but not at all fictional) risks in what we currently call the Internet of Things and in the very near future will evolve into the Internet of Everything. It presents examples of risks and attacks in different domains of our personal life, commercial world, and industry, where IoT devices are used, and highlights the corresponding technological and managerial challenges for confronting, even anticipating and preparing against security attacks.

The issue starts with an article from the editors, providing a quick look into the cyber and physical threats to the Internet of Everything. It decomposes the Internet of Everything 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 (automobolity, domotic environments, as well as 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 "Security Challenges and Approaches in the Industrial Internet" by Claude Baudoin, discussing the challenges of tackling both connectivity and security in the Industry IoT 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 IoT and the challenges on the use of technologies for remote access/control and secure data communication between devices. Instead, it provides an example-driven holistic approach in which IoT security should be pursued through the early adoption of policies in IoT systems design.

In "Social Engineering in the Internet of Everything", Ryan Heartfield and Dr. 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. They ask "would your fridge lie to you?". This new and vast landscape of potential deception vectors is a security angle that not many people have started thinking about. Yet, from the sector's experience in how conventional phishing evolved, it looks only logical that IoE-based deception attacks constitute the next battleground in cyber security.

The third article is David Tayouri's "IoT Devices Can Be Exploited to Reveal Personal and Sensitive Information", which discusses the different threats in which IoT devices are exposed to, with emphasis on personal, household and everyday use devices, giving examples of attacks or proven vulnerabilities. In addition to the identification of the threats, the author provides very clear and well thought-out suggestions as to what can be done in order to protect the Internet of Things against them and elaborates on the reason this has not been effective up to now, proposing actions at several levels: Legislation, regulations and, importantly, also consumer practices.

Finally, in his "Security and Privacy in the Internet of Things: How to Increase the User's Trust" article, Dimitris Kogias discusses privacy issues related to the Internet of things, and the impact security attacks on IoT may have to the protection of personal data. He also presents a study of Privacy Enhancing Technologies and the way they can be used to confront threats against privacy.

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

- The wider the (inevitable) adoption of Internet of Things technologies, the greater the range of cyber-physical threats and risks to our professional and personal lives. The physical world's increasing dependence on IoT is a key factor in the proliferation of cyber-physical attacks (cyber security breaches with adverse physical impact).
- While the range of threats and risks is widening, age-old security design principles and cyber hygiene 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 defence-in-depth and any technical security solutions put in place.