R. Roman, J. Lopez, and S. Gritzalis, “Evolution and Trends in the Security of the Internet of Things”, *IEEE Computer*, vol. 51, pp. 16-25, 2018.
http://doi.org/10.1109/MC.2018.3011051
NICS Lab. Publications: https://www.nics.uma.es/publications

Evolution and Trends in the Security of the Internet of Things

Rodrigo Roman and Javier Lopez, *University of Malaga, Spain*

Stefanos Gritzalis, *University of the Aegean, Greece*

The field of the Internet of Things (IoT) has evolved in the last few years: the amount and diversity of devices that integrate connection capabilities is steadily growing, and both the academia and the industry have been exploring various application areas and paradigms that involve these connected objects. IoT Security has evolved as well, with security issues that have been actively researched coexisting with areas whose progress have been limited, plus other novel research areas that have gathered increased attention in the last years. It is the goal of this article to provide an analysis of this evolution of the different IoT security issues, alongside with an overview of the current and future trends in this area.

At its core, the idea of the Internet of Things (IoT) can be defined in one simple sentence: “a worldwide network of interconnected entities”. Yet, in these last years, this core concept has been expanded in a multitude of ways. One of the cornerstone concepts of the IoT, the ‘things’ themselves, has evolved to cover various types of devices: from simple RFID tags and wireless sensor devices to complex systems like connected cars, consumer devices such as TVs and cameras, and even facilities like toilets. The IoT itself also have been given many names, which refine and/or expand its scope. Examples include the Industrial Internet of Things (i.e. IoT applied to the industrial and manufacturing sector) and the Internet of Everything (i.e. things alongside with people, processes, data, and their connections). Moreover, the IoT has become closely related to other paradigms, either because they have similar core values (e.g. Machine-to-Machine, Cyber-Physical Systems), or because they make use of each other (e.g. Fog Computing).

This fluidity is one of the factors that has influenced over the development of security solutions. As seen in the “a survey of surveys” sidebar, researchers have explored how to protect the IoT paradigm since its inception, providing a multitude of security services. But security is not a monolithic concept: It evolves and changes alongside the field it protects. This evolution can be simple and linear, pursuing the optimization and integration of previously identified yet unsupported security mechanisms to the IoT ecosystem. It can also be reactive and adaptive: if the underlying ecosystem that security mechanisms are meant to protect keeps changing, the security mechanisms must then evolve in order to respond to these new circumstances. Beyond the evolution of specific IoT security areas, it is important to point out that all the underlying factors that have caused such evolution have also triggered various trends, which in turn exert a great influence over the design and development of several security mechanisms and services.

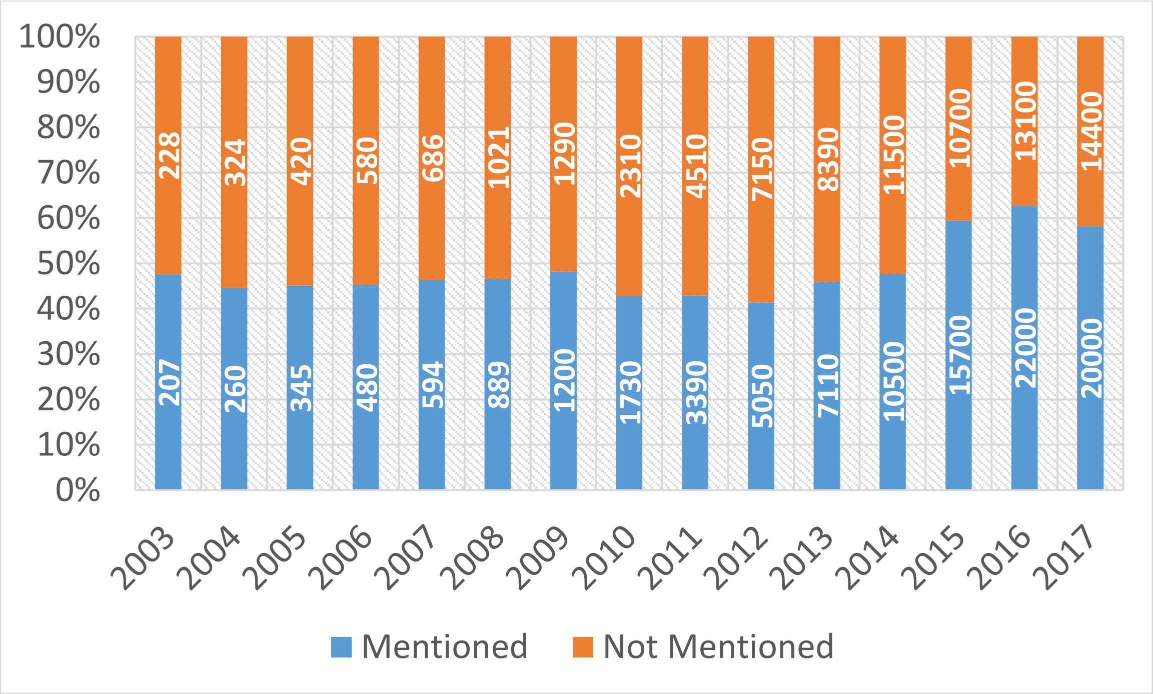

Figure 1 IoT research articles that explicitly mention the term “security”

The importance of the concept of security in the Internet of Things is also evolving, and it has been growing in these last years. This is clear when analyzing Figure 1, which shows the ratio of IoT articles that explicitly mention the term “security” in their text according to Google Scholar (as of December 2017). But as the importance of security is growing, and more attention is paid to the protection of the IoT ecosystem, it is essential to have a more detailed knowledge of our past and our present. By providing a detailed analysis on how the different IoT security areas have evolved over the years, and what are the current trends that exert notable influence over them, we can plan and develop more optimal security mechanisms that are suitable to protect our connected future.

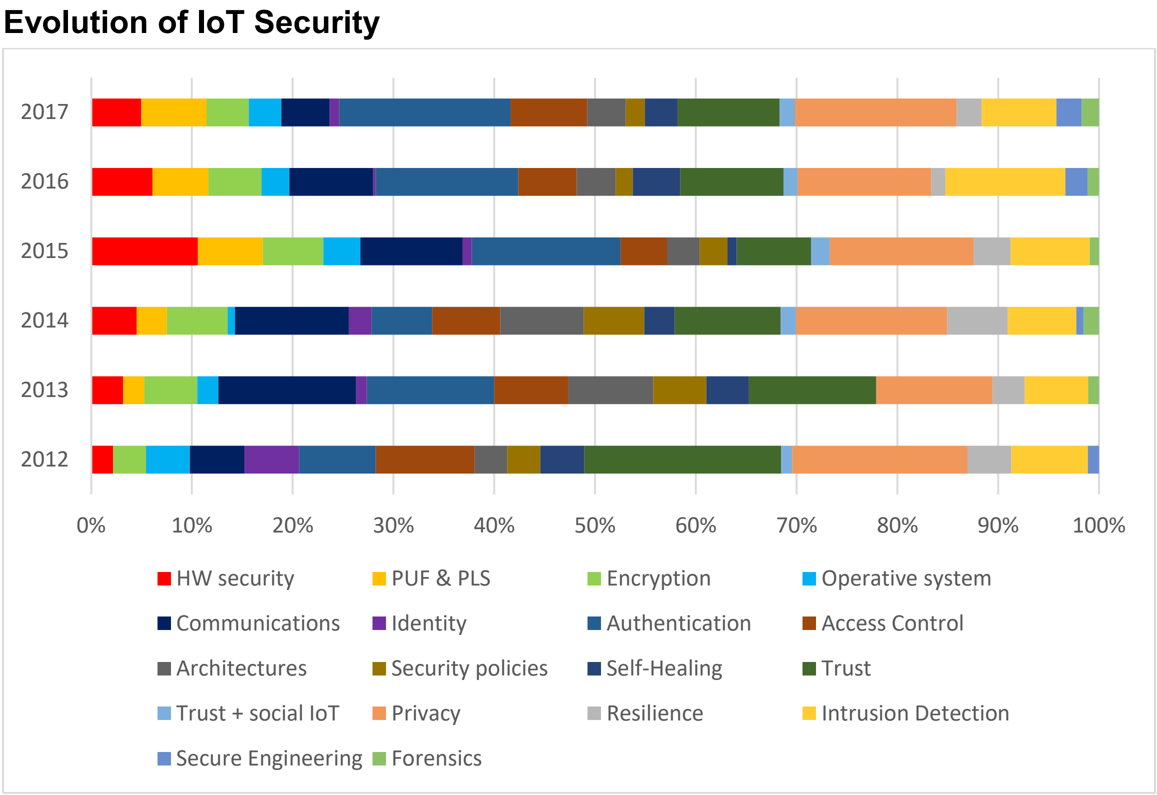

Figure 2. Evolution of the importance of every IoT security area

Before analyzing how all IoT security areas have evolved, we will summarize how their weight (i.e. their importance in relation to each other) have evolved from the year 2012 to the present. This information is shown in Figure 2, which was created by compiling and analyzing all articles indexed in the Scopus database that explicitly define IoT security mechanisms. From this figure we can derive what IoT security areas have been prioritized by the research community in the last years. For example, we can observe that the importance of major areas such as privacy, authentication, trust, secure communications, intrusion detection, and access control, has been mostly stable in the last years. We can also observe that there are certain areas whose importance has been growing, such as physical unclonable functions (PUF) and security engineering. Moreover, there are other areas that have been always understudied, such as IoT forensics.

Linear evolution

There have been various IoT security areas where the main long term goals were relatively clear from the start: to adapt existing and proven protocols and algorithms to the context of the IoT, and improve their performance as much as possible. As seen in Figure 2, most of these areas have been actively researched in comparison to other areas.

One clear example of this is the area of *cryptographic primitives*. There are certain primitives, such as elliptic curves, whose software implementations were in fact available years ago for sensor network devices. Those initial implementations were considered too cumbersome for these constrained devices. Yet several advances in the design and implementation of those primitives, like lightweight curves and optimized algorithms, have greatly reduced their memory overhead and energy consumption. This enables the implementation of protocols like key agreement (ECDH) and digital signatures (ECDSA) at the sensor level, and even the integration of more advances protocols like bilinear pairings in more powerful hardware. These improvements are not limited to the realm of software implementations, as research and development of cryptographic primitives and trusted computing integrated in low-powered hardware has steadily continued in the last years.

Another example of this linear evolution can be found in the authentication and authorization areas. At first, user-to-service and device-to-service authentication protocols were adapted from existing protocols designed for the building blocks of the IoT paradigm, like wireless sensor networks. Later, various researchers started the integration of existing federated identity and authentication protocols, such as OpenID and OAuth2. While these protocols facilitate the communication between users/devices and services, there are certain use cases like smart cities and industrial services where direct user-to-device and device-to-device authentication protocols are necessary. For this purpose, existing ideas like user biometrics and out-of-band channels (i.e. take advantage of the physical surroundings) were applied to this context. As for authorization and access control, the availability of better primitives has facilitated the jump from simpler access control mechanisms like RBAC (based on entity roles) to other token-based solutions such as ABAC, whose integration is being actively explored.

Finally, other examples include the areas of *trust* and *privacy*. Both areas have been heavily researched in the last years, again mostly using the mechanisms developed for sensor networks as a first step, and then evolving on the specific needs of the IoT. Regarding trust mechanisms, there have been advances in three major topics: the definition of trust models, the integration of such models in generic trust architectures designed for cloud-powered IoT infrastructures, and their application in various areas such as access control, IDS, data collection, and usability. Still, there is the need to further improve these mechanisms and to facilitate the integration of trust in existing IoT architectures. As for privacy mechanisms, most works in this area have focused on exploring what privacy means in the context of the IoT, and what are mechanisms that can be integrated. Some works have focused on data privacy, studying how users can effectively protect their data using mechanisms such as homomorphic encryption – which allows computation on encrypted data. Other researchers are focused on exploring other known dimensions of this problem, such as location privacy, group anonymity, plausible deniability / anonymity, and privacy-aware low level mechanisms.

Understudied subjects

Several IoT security areas have received little or no attention until recently. It is then necessary to explore in deep how such services could be further developed, in order to avoid problems in the near future.

One of the main issues of the IoT is *identity management*. As aforementioned, there have been several works whose aim was to integrate existing identity protocols, such as OpenID, into the IoT, plus various efforts from multiple standard bodies and consortiums to define identity architectures and naming schemes for the IoT – although most of these definitions exist within disconnected silos. Yet beyond the basic concept of identity (who I am), there are various aspects that need to be explored in this context, such as core identity (what I am), association identity (who I am associated with / who is my owner), and location identity (where I am)[1]. These notions can facilitate the creation of multiple IoT applications, as in many IoT scenarios it is not important to know who I am (Street_light_#654A) but what are my features (A street light, located in Málaga University). However, such concepts are mostly underdeveloped, with punctual works on the notion of identity as a set of properties (based on mechanisms like attribute certificates), and the definition and delegation of an identity within personal area networks.

There are other areas, like *secure management* and *self-healing*, that were early identified as vital for the safe development of the IoT[2]. These security services are necessary in order to provide an accurate picture of the status of the virtual world and to make the IoT as fault tolerant and resilient against attacks as possible, respectively. However, mainly due to the lack of proper IoT deployments, there were in the beginning very few works on these subjects, and it is only in the last few years that they have started to gain momentum. Current research efforts in these areas are mostly focused on three aspects. First, the provision of situational awareness, where managers and IoT entities themselves are able to understand the state of their surroundings. This is currently being achieved by securely integrating various IT management platforms, and by using other strategies such as distributed agents. Second, the definition of predictive systems: models that analyze the state of the resources, detect errors, and find potential alternatives. For this, various strategies such as machine learning are being explored. Third, the introduction of reactive systems: mechanisms that can allow the system itself to react against failures. At present, these mechanisms have been based on functionality replication, such as the use of containers (e.g. dockers) to rapidly deploy supporting services close to IoT devices.

Finally, there are various areas whose development have been and is very limited, such as *secure software engineering*, *security and usability*, and *forensics*. Again, the main reason is simple: these security areas are clearly linked to the development and deployment of complex IoT applications, which were not available until recently. Yet the security principles and services associated to these areas are crucial in order to develop robust and vulnerability-free IoT software, to reduce the management errors when interfacing with of IoT environments, and to facilitate the analysis of attacks against IoT elements, respectively. If they are not broadly available, what is left is an ecosystem of vulnerable things. Fortunately, the field of secure software engineering in the IoT has finally started to take off, with works that analyze how to model security and privacy requirements and risks in this context. Usability has been less developed, and only certain surveys have highlighted how usability might help to improve the perception of security and privacy. As for forensics, most works also focused on explaining why we need forensics, and it is only until recently that some researchers have started to think how it should be implemented[3].

Bold approaches

Finally, there are various concepts and approaches that, regardless of their novelty, are actually disruptive when applied to the context of the IoT.

For example, various researchers are exploring the applicability of concepts such as *physical unclonable functions* (PUF) and *physical-layer security* (PLS) in the context of the IoT[4]. A PUF is a physical element that provides hardware fingerprints that are easy to evaluate but hard to predict – the HW equivalent of a one-way function. On the other hand, PLS mechanisms, such as cooperative jamming, use the physical features of the wireless transmission medium to secure the communication channel against eavesdropping adversaries without relying on private keys. At present, there have been various prototype implementations of both PUFs and PLS, some of them based on off-the-shelf HW components (e.g. gyroscope) and others based on HW extensions. Moreover, other works have started to explore the applicability of PUFs and PLS mechanisms for the implementation of security services like device authentication and key distribution in local networks of constrained devices. As for the hard problems of these novel approaches, they are mostly related to a) how to take advantage of the resources that are available to IoT objects (e.g. HW elements, surroundings, etc) in order to implement these PUFs/PLS, and b) their actual strength in terms of security and entropy.

Another interesting approach is the notion of a *social IoT*, and its implications in regards to trust management[5]. In fact, there are two interpretations of the social IoT concept: a) the integration of social networking concepts into the IoT, with objects that have "friends" and "social links", and b) IoT objects are aware of the social networks of their owners, thus they can use that information to create a sort of "parallel" social network with other IoT objects. The main goal of these two approaches is the same: to reduce the uncertainty of the interactions between different IoT entities. In the last two years, various researchers have developed simple social IoT trust models through various means: by inheriting existing social network connections, by employing existing trust factors (e.g. reputation, recommendation, experience, knowledge), or using a combination of the two – including other factors such as context information. Afterwards, this concept has been applied to some initial proof of concept implementations: trustworthy crowdsourcing, where device communities are formed based on social links, and service composition, where social IoT-derived trust is used to select the most optimal components for a particular interaction.

Finally, researchers are also currently exploring the applicability of *distributed ledger technologies*, such as blockchains, and other related technologies such as *smart contracts*. These technologies provide support for various operations in a trusted and decentralized way, such as token exchange, metadata storage, and execution of computer programs, amongst other services. These operations can be used by IoT networks to securely implement various services, including tracking physical and digital items, and the creation of marketplaces where IoT objects can autonomously buy and sell their services. There are also both research and commercial solutions that use these technologies in order to provide various security primitives and services, such as decentralized access control management and secure decentralized firmware updates. Nevertheless, there are still a multitude of issues to tackle in this context, like the need to have cost-effective blockchains, the existence of potential yet understudied attacks, and other factors such as low transaction throughput, high fees, and low scalability[6].

Trends in IoT Security

Mistrust on the IoT

One of the main factors that have affected how IoT security is perceived is the realization that IoT objects can become adversaries themselves. This situation was to be expected: Existing Internet hosts can be owned by malicious entities, or remotely controlled due to the exploitation of vulnerabilities. And as IoT objects become first-class citizens of the Internet, they also can be exploited in a similar way. Yet it was the advent of the Internet of (vulnerable) consumer things, and the rise of botnets such as Mirai, that truly put this threat into the spotlight. This situation triggered the current trend of **mistrusting the integrity of IoT devices and infrastructures**.

One clear effect of this trend was the application of the concept of *vulnerability scanners* in the context of the IoT. As IoT objects and platforms might have (un)known vulnerabilities, it is essential to discover them before they are exploited by adversaries. These vulnerability scanners aim to work not only at a local level, analyzing IoT components (devices, middleware, platforms) within the deployment site, but also at a remote level – making use of online tools such as SHODAN (i.e. search engine for Internet-connected devices)[7]. The detection mechanisms used by these scanners usually incorporate analysis of signatures of known vulnerabilities, yet most research in this area aims to go higher: to be able to uncover dormant flaws. For this purpose, techniques such as fuzzy analyzers are being explored, where inputs are pseudo-randomly created and tested until an abnormal state is triggered. There are still various challenges to be overcome in these approaches, such as guiding the evolution of the fuzzy inputs, and designing and deploying the test oracles that certify the existence of an abnormal state.

Another effect was the influence over the research on the *security of the IoT devices* themselves. One example is the ongoing integration of trusted execution environments, such as ARM TrustZone, in constrained IoT devices[8]. Not only they enable the creation of execution environments for security-critical applications and functions, but they also serve as a root of trust, storing credentials and facilitating secure booting and code integrity testing. Another example is the area of IoT operative system security. This area mostly shifted from the development of lightweight secure mechanisms to the integration of better attestation mechanisms, which can be used to remotely analyze the integrity of IoT software components[9]. At present, more scalable-friendly, efficient attestation strategies are being explored. Examples include aggregated attestation mechanisms, which efficiently tests all leaf nodes in a hierarchical architecture, and tiered attestation mechanisms, where edge routing entities (i.e. gateways) perform the attestation on behalf of a relying party.

One final effect related to this trend is the growing importance of the domain of *intrusion detection systems* (IDS) for the IoT. Before, most works on IDS for the IoT focused on the development of isolated detection components, studying the applicability of existing mechanisms such as pattern detection, information fusion, game theory, anomaly mining, and others. The advent of the "IoT as an adversary" angle propelled the integration of other mechanisms, including the deployment of honeypots and other mitigation techniques based on software-defined networks – where malicious traffic is redirected to analyzers. Besides, other theoretical and practical works have focused on optimizing the behavior of IDS from a holistic point of view, including the placement and interactions between the diverse detection agents, and the cooperation between different IoT deployments when a malicious IoT entity is detected – although related aspects such as threat intelligence management are still underdeveloped[10].

Trusted Gateways

The vulnerable nature of things and the existence of malicious IoT objects also gave birth to another trend that is gradually touching all areas of IoT security: **the need of a closely located trusted third party that can execute security services, or even protect the IoT objects themselves**. Such trusted third parties are assumed to have more resources than the things themselves, thus are able to implement security services on behalf of the devices they supervise. There are various strategies for the instantiation of these trusted third parties. One approach is to make use of the very same gateways that connect the things with the Internet, as many devices implement Internet protocol optimizations like 6LoWPAN that need to be translated in order to provide network connectivity. Other approaches plan to use the computing resources provided by novel paradigms like Fog Computing and Multi-Access Edge Computing (MEC).

There are various areas where this concept has been applied. One example is the area of *key management schemes*. In some cases, part of the key negotiation process is delegated to trusted gateways located between the things and the central servers. Some of these schemes also have a positive side effect: things can move between different trusted gateways without compromising the end-to-end security. This is especially useful in Fog/MEC scenarios, where a mobile entity (a car) travels around a local environment (a town). Another example of the trusted gateway concept is in the area of *authorization*. Here, either the owner of the devices or the trusted gateways act as the authorization provider: any entity that wishes to access the devices' services must first exchange information with the authorization provider in order to retrieve an access token. Then, the entity can use such token to communicate directly with the device. Finally, the area of *privacy* also benefits from the existence of this concept: there are several works that focus on the creation of privacy helpers – assistants that act as a representative of the objects, implementing privacy services and shielding the objects' identities and data – deployed in these gateways.

A more extreme view on the subject of a trusted third party is the idea of a "gateway for things", such as the 'guardian' concept[11]. Here, IoT objects are deemed too dangerous to be directly connected to the Internet, either because they are too weak against attacks from powerful adversaries, or because they pose a great danger when controlled by such adversaries, amongst other reasons. Therefore, under this perspective, things and remote entities must not be aware of each other, thus the gateway must act as an intermediary: accessing IoT objects through their local interfaces (e.g. MQTT, CoAP, Modbus/TCP), and providing services to external entities through well-defined remote interfaces (e.g. REST, SNMP). The gateway also takes the role of a security manager, analyzing and managing the security of the local IoT environment.

Integration of Security Mechanisms

There is another ongoing trend that is helping to fill an important gap in IoT security: **the integration of security mechanisms in existing IoT protocols and architectures**. Within this trend, we include not only the standardization of security configurations and mechanisms under the umbrella of the IoT, or the inclusion of extensions that provide additional protection to IoT-related protocols such as MQTT: we also consider the integration of novel security mechanisms in existing IoT platforms. Such platforms range from IoT platforms developed by various industrial consortiums and foundations like OneM2M and the Open Connectivity Foundation (e.g. OM2M, IoTivity), to other platforms developed under the umbrella of European research projects (e.g. FIWARE).

At present, there are various standard organizations and bodies, such as the IETF, IEEE, and ISO/IEC, that are pursuing the development of IoT security standards and recommendations[12]. Some of them can be currently applicable to existing security protocols and components. One clear example of this is the IETF RFC 7925, which provides a DTLS/TLS profile specifically designed for the IoT. Such profile provides communication security by using not only pre-share keys but also mutual certificates based on ECDH, ECDSA, and AES. Other researchers are developing extensions of DTLS/TLS that, even if not standardized, either do not break the protocol or provide a compatible alternative for specific scenarios. Such extensions enable the integration of novel mechanisms such as mutual authentication through implicit certificates (ECQV), or provide a method to secure communication in a multicast group of IoT devices.

Other IoT protocolos, such as CoAP and MQTT, have also received the attention of the research community on this regard[13]. As expected, several researchers have developed specific optimizations for the integration of DTLS and CoAP/MQTT, so they could be integrated in more constrained devices. Other, more advances integration efforts also exist. For example, there are various proof-of-concept implementations that have explored the integration of CoAP/MQTT with security concepts such as adaptive encryption (i.e. the strength of the secure channel adapts to the criticality of the exchanged information). Other authors have explored the creation of specific security components, which, for example, extend existing MQTT architectures with access control rules based on security policies. Moreover, other authors have also explored the integration of standard web authentication protocols like OAuth2 with CoAP/MQTT.

As for the integration of security mechanisms in existing IoT platforms, we have to consider that many of these platforms follow a component-based design. Here, the interactions and dependencies between the components are well defined, thus new components can be easily integrated. For example, the IoTivity platform can be extended with attestation modules, which can be used not only to bootstrap trusted relationships, but also to update components of the IoTivity platform. This platform can also be extended with coarse-grained access control through the integration of access control policies specific to resource attributes, and service isolation through the integration of Linux containers. Another platform, FIWARE, can also be extended with the Idemix anonymous credential system – which provides privacy-preserving, unlikable M2M transactions, amongst other benefits. Still, it is evident that more work is needed in order to improve the overall security of these platforms, as many areas such as intrusion detection are still underrepresented.

After our analyses, we can conclude that the field of IoT security research is alive and well: all major IoT security areas, including previously underrepresented ones, are being explored; the amount of research keeps growing; and both existing and novel mechanisms are being implemented and deployed. However, this is clearly not enough: nowadays, IoT ecosystems are synonymous with vulnerable environments, whose security is quite limited. In fact, current IoT devices are sold with lousy security, which leads to vulnerabilities that will "affect flesh and blood"[14]. Therefore, it is crucial to promote not only the creation but also the integration of the tools that will help companies to design, integrate, and continuously assess basic security principles into their IoT devices at a negligible cost, and even the legal frameworks that will facilitate this whole process.

Acknowledgments

This work was partially supported by the Spanish Ministry of Economy and Competitiveness through the IoTest project (TIN2015-72634-EXP/AEI), which is cofinanced by the European Regional Development Fund.

References

1. K.-Y. Lam and C.-H. Chi. "Identity in the Internet-of-Things (IoT): New Challenges and Opportunities". In Information and Communications Security (ICICS'16), Lecture Notes in Computer Science, Springer, vol

9977, pp. 18-26, November-December 2016.

2. I.G. Smith, O. Vermesan, and P. Friess, A. Furness (eds.). “The Internet of Things 2012 - New Horizons”. IERC Cluster Book 2012, http://www.internet-of-things-research.eu.
3. M. Conti, A. Dehghantanha, K. Franke, and S. Watson. “Internet of Things security and forensics: Challenges and opportunities”. In Future Generation Computer Systems, vol. 78, Part 2, pp. 544-546, 2018.
4. D. Mukhopadhyay. “PUFs as Promising Tools for Security in Internet of Things”. In IEEE Design & Test, vol. 33, no. 3, pp. 103-115, 2016.
5. W. Abdelghani, C.A. Zayani, I. Amous, and Florence Sèdes. “Trust Management in Social Internet of Things: a Survey”. In 15th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society (I3E’16), Lecture Notes in Computer Science, Springer, vol 9844, pp. 430-441, September 2016.
6. J. E. Ferreira et al. “A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack”. In Security and Communication Networks, In Press, 2018.
7. K. Simon, C. Moucha, J. Keller. “Contactless Vulnerability Analysis using Google and Shodan”. In Journal of Universal Computer Science, vol. 23, no. 4, 2017.
8. C. Shepherd et al. “Secure and Trusted Execution: Past, Present, and Future - A Critical Review in the Context of the Internet of Things and Cyber-Physical Systems”. In IEEE Trustcom/BigDataSE/ISPA’16, pp. 168-177, August 2016.
9. T. Abera et al. "Things, trouble, trust: On building trust in IoT systems". In 53nd ACM/EDAC/IEEE Design Automation Conference (DAC’16), pp. 1-6, June 2016.
10. B.B. Zarpelão, R.S. Miani, C.T. Kawakani, and S.C. de Alvarenga. “A survey of intrusion detection in Internet of Things”. In Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.
11. H. Tsunoda and G. M. Keeni. “Feasibility of societal model for securing Internet of Things”. In 13th International Wireless Communications and Mobile Computing Conference (IWCMC’17), pp. 541-546, June 2017.
12. A. Meddeb. "Internet of things standards: who stands out from the crowd?". In IEEE Communications Magazine, vol. 54, no. 7, pp. 40-47, 2016.
13. G Perrone, M Vecchio, R Pecori, and R Giaffreda. “The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices”. In 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS’17), pp. 246-253, April 2017.
14. B. Schneier. “IoT Security: What’s Plan B?”. In IEEE Security & Privacy, vol. 15, no. 5, pp. 96-96, 2017.

Dr. Rodrigo Román-Castro is a post-doctoral security researcher working at the University of Málaga. His research is focused on protecting Internet of Things ecosystems in various contexts, such as critical infrastructures and Fog Computing networks. Contact him at roman@lcc.uma.es.

Prof. Javier López is the Director of the Network, Information and Computer Security Lab (NICS), University of Málaga. Prof. Lopez is the Spanish representative in the IFIP TC-11, Co-Editor in Chief of International Journal of Information Security (IJIS), and member of the Editorial Boards of, amongst others, IEEE Wireless Communications, and Computers & Security. Contact him at jlm@lcc.uma.es.

Prof. Stefanos Gritzalis is the Director of the Lab of Information and Communication Systems Security (Info-Sec-Lab), University of the Aegean. Prof. Gritzalis has been involved in several national and EU funded R&D projects, and he is an Editor-in-Chief or Editor or Editorial Board member for more than 15 journals. Contact him at sgritz@aegean.gr.

SIDEBAR: A survey of security surveys

Because of the importance of the security of the Internet of Things, in the last years there have been several surveys that have tried to capture the state and challenges of this research field. Some surveys, like the seminal work by Sicari et al.[1], focused on providing an overview of the security of the IoT as a whole. Other works, such as Weber and Studer[2] and Roman et al.[3], focused their analyses on specific IoT aspects, such as legal challenges and IoT architectures, respectively. Finally, more recent works, like Hypponen and Nyman[4], alerted of the multiple challenges associated with the Internet of (Consumer) Things – where traditional appliances and other, more unusual devices (showerheads, sex toys) are connected to the Internet. Due to space constraints, the references included in this article are limited, thus we recommend interested readers that want to further explore a particular IoT security topic to read these surveys in detail.

Most surveys agree that, for the development of security mechanisms, the specific features of the IoT (heterogeneity, connectivity, physicality, constraints, scale) create challenges, but in some cases also opportunities. The physicality of the "things" and their (usually) limited resources create various complications in applying and adapting known security principles, sometimes forcing researchers to think outside the box (e.g. user authentication through ECG). On the other hand, there are several factors, such as the predictability of physical processes and the existence of neighbor things, that can be used to implement more optimal security mechanisms (e.g. anomaly detection through i) physical behavior analysis and ii) local watchdogs).

As for the most important security challenges that the IoT faces, they range from the development (from the cradle to the grave) of secure IoT devices in terms of hardware and software, to the secure cooperation of heterogeneous IoT platforms and ecosystems, plus other challenges such as the continuous integration of better security mechanisms in the most commonly used IoT protocols (e.g. 6LoWPAN, TLS, CoAP), the definition of a more granular, user-friendly AAA infrastructure, and the inclusion of mechanisms that facilitate the self-management of the devices through anomaly detection and automatic reconfiguration, amongst others. Yet we can't lose sight of the non-technical issues, such as how to educate companies and users on the responsibilities associated to creating and owning what is essentially a macrocosm of microcomputers.

References

1. S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead". In Computer Networks, vol. 76, pp. 146-164, 2015.
2. R. H. Weber, and E. Studer. "Cybersecurity in the Internet of Things: Legal aspects". In Computer Law & Security Review, vol. 32, no. 5, pp. 715-728, 2016.
3. R. Roman, J. Zhou, and J. Lopez. "On the features and challenges of security and privacy in distributed internet of things". In Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.
4. M. Hypponen and L. Nyman. "The Internet of (Vulnerable) Things". In Technology Innovation Management Review, vol. 7, no. 4, pp. 5-11. 2017.