Evolution and Trends in IoT Security

Rodrigo Román-Castro and Javier López, University of Malaga

Stefanos Gritzalis, University of the Aegean

The amount and diversity of devices that integrate connection capabilities continues to grow, and both the public and private sectors continue to explore various application areas and paradigms that involve these connected objects. Yet as the IoT field evolves, so too must its security capabilities. This article presents an analysis of IoT security issues and 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 recent years, this core idea 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 basic facilities like toilets. The IoT itself has also been given many different names, which refine and/or expand its scope. Examples include the Industrial Internet of Things (describing how IoT applies to the industrial and manufacturing sector) and the Internet of Everything (which includes the things alongside people, processes, data, and their connections). Moreover, the IoT has become closely related to other paradigms, either because they have similar core values (as is the case with machine-to-machine systems and cyber-physical systems), or because they make use

0018-9162/18/$33.00 © 2018 IEEE

of one another (as is the case with fog computing).

This fluidity is one of the factors that has influenced the development of security solutions. As described in the sidebar, “A Survey of Surveys,” researchers have explored how to provide security in 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 for 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 the underlying factors causing such evolution have also triggered various trends, which in turn exert great influence over the design and development of several security mechanisms and services.

The importance of the concept of security in the IoT is also evolving, and it has of course been increasing in recent years. This is clear when analyzing Figure 1, which shows the ratio of IoT articles that explicitly mention the term “security” 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 more detailed knowledge of security in the context of the past and present. By providing a detailed analysis on how the different IoT security areas have evolved over time, and what the current trends are that exert notable influence over them, we can plan and develop more optimal security mechanisms that are suitable to protect our connected future.

A SURVEY OF SECURITY SURVEYS

Because of the importance of the security of the Internet of Things, there have been several surveys in recent years that have tried to capture the state and challenges of this research field. Some surveys, like the seminal work by Sicari et al.,[15] focused on providing an overview of the security of the IoT as a whole. Other works, such as Weber and Studer[16] and Roman et al.,[17], focused their analyses on specific IoT aspects, such as legal challenges and IoT architectures, respectively. Finally, more recent work, like that of Hypponen and Nyman,[18] highlighted the multiple challenges associated with the Internet of (Consumer) Things, in which 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 looking to further explore a particular IoT security topic 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 (for example, 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 (such as anomaly detection through physical behavior analysis and local watchdogs).

As for the most important security challenges that the IoT faces, they range from the development (from cradle to 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 (such as 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, among others. Yet we must not lose sight of the non-technical issues, such as how to educate companies and users on the responsibilities associated with creating and owning what is essentially a macrocosm of microcomputers.

EVOLUTION OF IOT SECURITY

Before analyzing how all IoT security areas have evolved, we will summarize how their weight—that is,

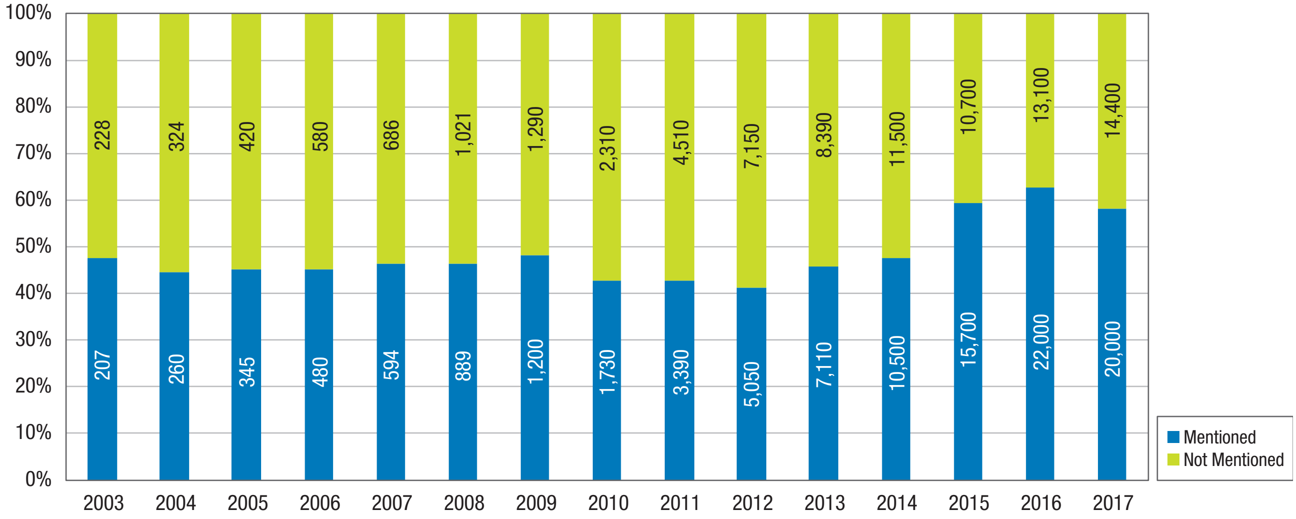

FIGURE 1. Internet of Things (IoT) research articles that explicitly mention the term "security."

their importance in relation to one another—have evolved from the year 2012 to late 2017. 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 recent years. For example, we can observe that the importance of major security areas such as privacy, authentication, trust, secure communications, intrusion detection, and access control, has been mostly stable. We can also observe that there are certain areas in which the importance has been growing, such as physical unclonable functions (PUFs) and security engineering. Moreover, there are other areas that have always been understudied, such as IoT forensics.

Linear evolution

There have been various IoT security areas in which the main long-term goals were relatively clear from the start: adapting existing and proven protocols and algorithms to the context of the IoT, and improving 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, for which software implementations were in fact available years ago for use in 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 continued steadily.

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 in which direct user-to-device and device-to-device authentication protocols are necessary. For this purpose,

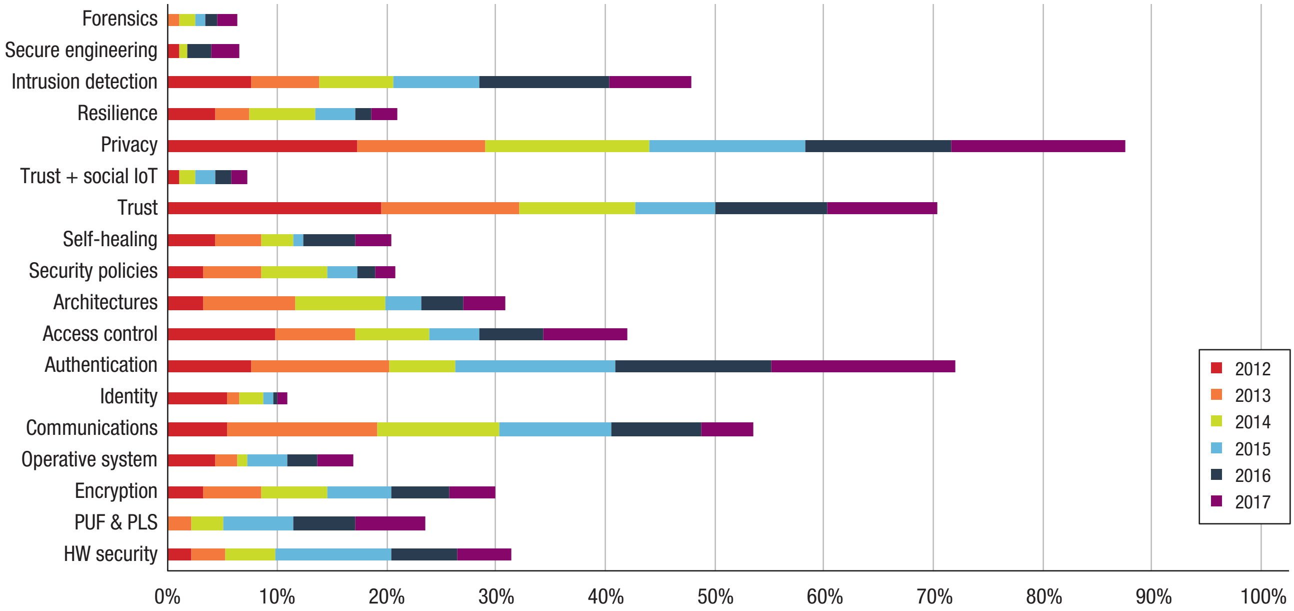

FIGURE 2. Evolution of the importance of every IoT security area.

existing ideas like user biometrics and out-of-band channels (specifically to 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 role-based access control (RBAC; based on entity roles) to other token-based solutions such as attribute-based access control (ABAC), for which integration is being actively explored.

Finally, other examples include the areas of trust and privacy. Both areas have been heavily researched, again mostly using the mechanisms developed for sensor networks as a first step, and then evolving based 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, intrusion detection systems (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 work in this area has focused on exploring what privacy means in the context of the IoT, and what mechanisms can be integrated. Some work has 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 more thoroughly explore how such services could be further developed, to avoid problems in the near future.

One of the IoT's main issues is identity management. As described above, there have been several attempts aimed at integrating 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" or "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 (for example, Street_light_#654A), but it is important to know what are my features (a street light, located in Málaga University). However, such concepts are mostly underdeveloped, with work focused 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.

FORTUNATELY, THE FIELD OF SECURE SOFTWARE ENGINEERING IN IOT HAS FINALLY STARTED TO TAKE OFF.

There are other areas, like secure management and self-healing, that were identified early on to be vital for the safe development of the IoT.[2] These security services are necessary 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 immaturity of the IoT, there were initially very few published works on these subjects, and it is only recently 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, defined as the ability of managers and IoT entities themselves to understand the state of their surroundings. This is achieved by securely integrating various IT management platforms, and through the use of other strategies such as distributed agents. Second, the definition of predictive systems: which describes 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: this describes mechanisms that allow the system itself to react against failures. At present, these mechanisms have been based on functionality replication, such as the use of containers (including dockers) to rapidly deploy supporting services close to IoT devices.

Finally, there are various areas for which development has been and is very limited, such as secure software engineering, security and usability, and forensics. Here again, the main reason is that 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 with these areas are crucial for developing robust and vulnerability-free IoT software, for reducing management errors when interfacing with IoT environments, and for facilitating the analysis of attacks against IoT elements, respectively. If these aspects of security are not broadly available, we are left with an ecosystem of vulnerable things. Fortunately, the field of secure software engineering in IoT has finally started to take off, with work underway to analyze how to model security and privacy requirements and risks in this context. Usability research has been less developed, with only a few surveys highlighting how usability might help to improve the perception of security and privacy. As for research in forensics, most has focused on explaining why we need forensics, and only recently have some researchers begun exploring 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 PUFs 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 hardware 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 hardware components (such as gyroscopes) and others based on hardware extensions. Moreover, other research has begun 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 challenges that go with these novel approaches, they are mostly related to how to take advantage of the resources that are available to IoT objects (such as hardware elements, surroundings, and so on) in order to implement these PUFs/PLS, and 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: first, the integration of social networking concepts into the IoT, such that objects that have "friends" and "social links"; and second, because IoT objects are aware of the social networks of their owners, they can then use this information to create a sort of "parallel" social network with other IoT objects. The main goal of these two approaches is the same—reduce the uncertainty of the interactions between different IoT entities.

In the past two years, various researchers have developed simple social IoT trust models through various means, including inheriting existing social network connections and employing existing trust factors—such as reputation, recommendation, experience, knowledge—or using a combination of the two, along with other factors such as context information. This concept has now been applied to some initial proof of concept implementations, including: trustworthy crowdsourcing, in which device communities are formed based on social links; and service composition, in which 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 blockchain, and other related technologies such as smart contracts. These technologies provide support for various operations—including token exchange, metadata storage, and execution of computer programs, amongst other services—in a trusted and decentralized way. 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 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

A variety of IoT security issues affect its successful deployment and adoption, and such issues of course continue to expand as the IoT's reach itself expands. Nevertheless, several security trends have emerged to help handle and mitigate certain challenges and risks the IoT technologies present. These include expanding our ability to detect and handle vulnerabilities and to minimize mistrust in IoT, establishing trusted third-party gateways, and integration of broad security mechanisms.

SEVERAL SECURITY TRENDS HAVE EMERGED TO HELP HANDLE AND MITIGATE CERTAIN CHALLENGES AND RISKS THE IOT TECHNOLOGIES PRESENT.

Mistrust in IoT

One of the main factors affecting how IoT security is perceived is the realization that IoT objects can themselves become adversaries. This situation was to be expected, as existing Internet hosts can be owned by malicious entities, or be remotely controlled through the exploitation of vulnerabilities. As IoT objects become first-class citizens of the Internet, they can also be exploited in a similar way. This issue gained broad attention through the advent of the Internet of (vulnerable) consumer things, and the rise of botnets such as Mirai—these issues truly put this threat into the spotlight, triggering the current trend of mistrusting the integrity of IoT devices and infrastructures.

One clear effect of this trend was the application 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, thereby making use of online tools such as Shodan, which is a 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.

ONE APPROACH IS TO MAKE USE OF THE VERY SAME GATEWAYS THAT CONNECT THE THINGS WITH THE INTERNET.

Another effect was the influence on the research surrounding the security of IoT devices themselves. One example is the ongoing integration of trusted execution environments, such as ARM TrustZone, in constrained IoT devices.[8] Not only do 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 (namely, gateways) perform the attestation on behalf of a relying party.

One final effect related to this trend is the growing importance of the intrusion detection systems (IDS) domain for the IoT. Before, most research 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" concept propelled the integration of other mechanisms, including the deployment of honeypots and other mitigation techniques based on software-defined networks—wherein malicious traffic is redirected to analyzers. Aside from these, other theoretical and practical work has focused on optimizing the behavior of IDS from a holistic point of view, including the placement of 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 rise to another trend that is gradually touching all areas of IoT security: the need for 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 they 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 in which 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, in that things can move between different trusted gateways without compromising the end-to-end security. This is especially useful in fog computing/MEC scenarios, in which 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, and any entity that seeks to access the devices' services must first exchange information with the authorization provider to retrieve an access token. Then, the entity uses the token to communicate directly with the device. Finally, the area of privacy also benefits from the existence of this concept, because researchers have focused on the creation of privacy helpers—assistants that act as representatives of the objects, implementing privacy services and shielding the objects' identities and data—which have been 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, among other reasons. Therefore, with this perspective, things and remote entities must not be aware of each other, thus the gateway must act as an intermediary that accesses IoT objects through their local interfaces (such as MQTT, CoAP, Modbus/TCP), and provides services to external entities through well-defined remote interfaces (such as 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

Another ongoing trend 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, but we also consider the integration of novel security mechanisms in existing IoT platforms. These range from IoT platforms developed by various industrial consortiums and foundations like OneM2M and the Open Connectivity Foundation (such as OM2M and IoTivity), to other platforms developed under the umbrella of European research projects (such as FIWARE).

There are now 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 these can be applicable to existing security protocols and components. One clear example of this is the IETF RFC 7925, which provides an IoT-specific DTLS/TLS profile. Such a 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 they provide a method for securing communication in a multicast group of IoT devices.

THE GATEWAY ALSO TAKES THE ROLE OF A SECURITY MANAGER, ANALYZING AND MANAGING THE SECURITY OF THE LOCAL IOT ENVIRONMENT.

Other IoT protocols, 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 advanced 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 (namely, 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, unlinkable M2M transactions, among other benefits. Still, it is evident that more work is needed 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 IoT security research field 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, as current IoT ecosystems are synonymous with vulnerable environments in which security is quite limited. In fact, current IoT devices are sold with lousy security, leading to vulnerabilities that will "affect flesh and blood."[14] Therefore, it is crucial to promote both the creation and integration of tools to help companies design, deploy, integrate, and continuously assess basic security practices within IoT-linked devices at a negligible cost, as well as to establish the legal frameworks that will facilitate this whole process. C

ABOUT THE AUTHORS

RODRIGO ROMÁN-CASTRO is a post-doctoral security researcher 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. Roman-Castro has a doctoral degree in computer science from the University of Málaga. He is a member of IEEE. Contact him at roman@lcc.uma.es.

JAVIER LÓPEZ is the director of the Network, Information and Computer Security Lab (NICS), at the University of Málaga. He is the Spanish representative in the IFIP TC-11, co-editor in chief of the International Journal of Information Security (IJIS), and a member of the editorial boards of, among others, IEEE Wireless Communications, and Computers & Security. Lopez's research interests focus on information and communications security. Lopez has a doctoral degree in computer science from the University of Málaga. He is a Senior Member of IEEE and ACM. Contact him at jlm@lcc.uma.es.

STEFANOS GRITZALIS is the director of the Lab of Information and Communication Systems Security (Info-Sec-Lab), at the University of the Aegean. Gritzalis's research interests focus on information and communications security and privacy. He has a doctoral degree in information and communications security from the University of Athens. He is a Senior Member of IEEE and ACM. Gritzalis has been involved in several national and EU funded R&D projects, and he is an editor-in-chief, editor, editorial board member for more than 15 journals. Contact him at sgritz@aegean.gr.

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," *Proc. Information and Communications Security* (ICICS 16), 2016, Lecture Notes in Computer Science, Springer, vol. 9977, pp. 18-26, November-December 2016.
2. I.G. Smith et al., editors, *The Internet of Things 2012 - New Horizons*, IERC Cluster Book, 2012; www.internet-of-things-research.eu.
3. M. Conti et al., "Internet of Things Security and Forensics: Challenges and Opportunities," *Future Generation Computer Systems*, vol. 78, part 2, 2018, pp. 544-546.
4. D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," *IEEE Design & Test*, vol. 33, no. 3, 2016, pp. 103-115.
5. W. Abdelghani et al., "Trust Management in Social Internet of Things: A Survey," *Proc. 15th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society*, (I3E 16), 2016, Lecture Notes in Computer Science, vol. 9844, Springer, pp. 430-441.
6. J. E. Ferreira et al., "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks*, vol. 2018, Article ID 9675050, 27 pages, 2018.
7. K. Simon, C. Moucha, and J. Keller, "Contactless Vulnerability Analysis Using Google and Shodan," *J. 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," *Proc. IEEE Trustcom/BigData* (SE/ISPA'16), 2016, pp. 168-177.
9. T. Abera et al., "Things, Trouble, Trust: On Building Trust in IoT Systems," *Proc. 53rd ACM/EDAC/IEEE Design Automation Conf.* (DAC 16), 2016, pp. 1-6.
10. B.B. Zarpelão, et al., "A Survey of Intrusion Detection in Internet of Things," *J. of Network and Computer Applications*, vol. 84, 2017, pp. 25-37.
11. H. Tsunoda and G.M. Keeni. "Feasibility of Societal Model for Securing Internet of Things," Proc. 13th Int'l Wireless Communications and Mobile Computing Conf. (IWCMC 17), 2017, pp. 541-546.
12. A. Meddeb, "Internet of Things Standards: Who Stands Out from the Crowd?," *IEEE Comm. Magazine*, vol. 54, no. 7, 2016, pp. 40-47.
13. G Perrone et al., "The Day after Mirai: A Survey on MQTT Security Solutions after the Largest Cyber-attack Carried Out through an Army of IoT Devices," *Proc. 2nd Int'l Conf. Internet of Things, Big Data and Security* (IoTBDS 17), 2017, pp. 246-253.
14. B. Schneier, "IoT Security: What's Plan B?," *IEEE Security & Privacy*, vol. 15, no. 5, 2017, pp. 96-96.
15. S. Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, 2015, pp. 146-164.
16. R.H. Weber and E. Studer, "Cybersecurity in the Internet of Things: Legal Aspects," *Computer Law & Security Review*, vol. 32, no. 5, 2016, pp. 715-728.
17. R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266-2279.
18. M. Hypponen and L. Nyman. "The Internet of (Vulnerable) Things," *Technology Innovation Management Review*, vol. 7, no. 4, 2017, pp. 5-11.