Research and Innovation Action for the Security of the Internet of Things: The SerIoT Project

Joanna Domanska[1], Erol Gelenbe[2,1], Tadek Czachorski[1], Anastasis Drosou[3], and Dimitrios Tzovaras[3]

[1] IITIS Polish Academy of Science, Gliwice, Poland
[2] Department of Electrical & Electronics Engineering, Imperial College London, UK
[3] ITI-CERTH, Thessaloniki, Greece

Abstract. The Internet of Things (IoT) was born in the mid 2010's, when the threshold of connecting more objects than people to the Internet, was crossed. Thus, attacks and threats on the content and quality of service of the IoT platforms can have economic, energetic and physical security consequences that go way beyond the traditional Internet's lack of security, and way beyond the threats posed by attacks to mobile telephony. Thus, this paper describes the H2020 project "Secure and Safe Internet of Things" (SerIoT) which will optimize the information security in IoT platforms and networks in a holistic, cross-layered manner (i.e. IoT platforms and devices, honeypots, SDN routers and operator's controller) in order to offer a secure SerIoT platform that can be used to implement secure IoT platforms and networks anywhere and everywhere.

1 Introduction

With roots in a globally connected continuum of RFID (Radio Frequency Identification and Detection)-based technology, the IoT[1] concept has been considerably extended to the current vision that envisages billions of physical things or objects, outfitted with different kinds of sensors and actuators, being connected to the Internet via the heterogeneous access networks enabled by current and future technologies [4]. Currently, IoT is emerging as the next big thing introducing the next wave of innovation with rather endless possibilities. For instance, it opens a huge window of opportunity for the creation of applications (e.g. automation, sensing, machine-to-machine communication, etc.), promises to improve and to optimize our daily life and forms the infrastructure that allows intelligent sensors and smart objects to communicate and work together [10].

Contrary to the application layer of the World Wide Web that was developed on the infrastructure of the Internet (i.e. the physical layer or network made up of switches, routers and other equipment), IoT becomes immensely important because it is the first real evolution of the Internet - a leap that will lead to revolutionary applications that have the potential to dramatically improve the way people live, learn, work, and entertain themselves. Today the IoT is well under way, with the potential for changing people's lives for the better, especially with regard to human safety and security [26]. It has created new application domains and already infiltrated and dominated a wide range of existing ones (e.g. Consumer Automotive, Telecommunications, Home and Building

[1] From now on, rather than write "the IoT" we shall simply say "IoT".

Automation, Data Center and Cloud, Consumer Devices, Industrial, Medical, Commercial Transportation). So, as Personal Computers (PCs) start to show revenue declines, IoT is rising as the next big wave after PCs, networking and mobile systems. Moreover, based on the "cloud" trend that expects "everything to be connected" to Cloud services, we can also refer to the so-called Internet of Everything (IoE) [36], which represents the open access to data from one or more monitoring and control systems by third-party applications to provide unique, additional value to stakeholders.

In this context, it is a commonplace in the research community and the IoT related industry that challenges in future IoT and IoE will be affected by issues, such as the lack of a shared infrastructure and common standards, the management of (big) data, including control and sharing, security, flexibility, adaptability and scalability, and of course the maintenance and update of the IoT network. While analysts agree that security concerns and the effective management of produced data need to be worked out before the IoT can be fully developed, there is little doubt that the long-range impact will be substantial.

2 Security and the IoT

With IoT's arrival, EU industry, homes and society are catapulted into the huge arena of security risks that accompany an untested yet already universal technology that directly manages our cyber-physical reality on a daily, and indeed second by second, way beyond the security issues that are faced by mobile telephony [2, 19, 20], by the early machine to machine systems [1, 41] or by software systems [14, 15, 21, 24].

However by thinking in an innovative and positive manner, the security threats to the IoT are also a great opportunity for industry and business, and for all those who will know how to harness security science and technology in order to counter the emerging threats in a cost effective manner, and who will market products to support the development of a thriving business that assures the safety and security of the IoT [5].

While today security technologies can play a role in mitigating risks connected to IoT security [27], we foresee problems and potential threats that are not limited to what has been developed until now. In currently developed systems, the data is not delivered using uniform, consistent technology; often conflicting protocols are used with unverified designs. Moreover, we tend to think of the maintenance cycle in a short term span, which may mean that updates to IoT systems are not compliant. Lack of standards for authentication and authorization, as and security standards, as well as standards for platform configurations, means that every vendor creates its own ecosystem. On top of that comes prevention from attack all the way from information stealing, physical tempering to problems we have not encountered in the pre-IoT world, like denial-of-sleep, synchronization and energy attacks [23, 34, 40]. Since today the IoT infrastructure is centralized and focused on a client/server model, *in fine* all communication needs to go either through mobile networks or the Internet even when the devices are physically close to each other, it is vulnerable to standard Internet attacks as well [21, 25]. Authentication relies on the central server that can be easily compromised. Thus, the model works well for small scale IoT but does not provide sufficient mechanisms for future, large scale IoT projects which incur very high costs.

In order to overcome these issues we will seek to provide an efficiently programmable approach for flexible network management [32] a decentralized approach with peer to peer communication, distributed file sharing and autonomous device coordination, using the latest Blockchain technology [43], a distributed ledger that provides information about data transfers between parties in a secure, publicly verifiable, and efficient way. The properties the technology brings to the system come from the features of the method. By design, a Blockchain is distributed in an anonymous peer to peer network. All transactions (or data transfers) are public, auditable and recorded in blocks that are added to the top of the chain. There is no way to remove anything from a Blockchain, one can only add a modified version of a block. As it is decentralized, there is no authority that can be easily compromised. We plan to use the properties offered by Blockchain technology to help improve the shortcomings of IoT: keep immutable record of the history of smart devices, as well as improve the security and trust of messaging by leveraging smart contracts and cryptocurrencies transactions. This cutting edge technology has been already introduced by some companies in the field of IoT [33], but we plan to seek to improve some of its shortcomings and explore how we can bring it to the standardization bodies.

3 Objectives of the Project

The SerIoT project will address all the aforementioned challenges under a common framework based on the cooperative efforts and prior expertise of a strong interdisciplinary consortium, including the most important European key players in the IoT domain. We bring together star European technology companies such as DT/T-Sys. and ATOS together with highly competent SMEs such as HIS, HOPU, GRUVENTA, HIT and ATECH and world-leading European research organisations such as CERTH, JRC, TUB, ICCS, IITIS-PAN and TECNALIA, and universities such as Essex and TU Berlin, with savvy users such as OASA, Austria Tech and DT/T-Systems.

SerIoT aims to conduct pioneering research for the delivery of an open, scalable, secure and trusted IoT architecture that operates across IoT platforms, which will pave the way for the market uptake of IoT applications across different domains. Key enabling technologies, including Software Defined Networks, Secure IoT routers, Fog Computing, Analytics for improving embedded intelligence of IoT platforms and devices, Design-driven features for improving both resource efficiency and self-monitoring of next generation of “Things”, will be investigated in SerIoT, emanating from the market and industrial needs [35] for the delivery of safe and reliable IoT connected devices. SerIoT will consider a holistic approach in the formal definition of the end-to-end IoT network ecosystem, considering a multi-layered schema dealing with network, transport layer and perception layers. In this context, SerIoT technology will be installed, deployed and validated in emerging IoT-enabled application areas (i.e. Smart Transportation, Surveillance and Flexible Manufacturing/Industrie 4.0 as core business areas and Food, and Supply Chains) throughout its lifetime, enabling the conduction of pioneer R&D for the delivery of horizontal IoT end-to-end security platform in Europe.

With this overall ambition, the SerIoT project pursues a number of Technical Objectives which are listed below:

- To provide new means to understand the existing and emerging threats that are targeting the IoT based economy and the citizens' network. To research and analyse how Blockchain and distributed ledgers can contribute to improving IoT solutions. Moreover, to understand how to solve the know issues of IoT and blockchain.
- To introduce the concept and provide the prototype implementation of (virtualized) and self-cognitive, IoT oriented honeypots, easily configurable so as to meet the standards of and adapt to any IoT platform across domains (e.g. embedded mobile devices, smart homes/cities, security and surveillance, etc.) that will be both integrally connected with the core network components and centrally controlled, as well as that will have a transparent function within the network's total behaviour either it is active or passive.
- To deliver the design and implement the corresponding prototype of smart SDN routers [12] for the dynamic (i) detection of suspicious/high risk paths, (ii) re-planning and (iii) re-scheduling of the routing paths of the transmitted information in IoT networks over secure and (per user- or per case-) preferable connections, supporting among others the interference of the human (i.e. semi-supervised approach), when needed. Furthermore, this objective will design and implement a suitable substrate of fog nodes to support secure allocation of compute, storage and network resources for (i) localized processing of sensitive information, (ii) define the security requirements of a path coordinated by SDN, and (iii) enable secure communication with the core cloud.
- To introduce an extra, security dedicated, physical layer to the manufacturing of existing IoT platforms and devices so as to offer a secure-by-design architecture and monitoring capabilities for the sake of the network. To explore introduction of Blockchain as a security and privacy preserving layer for IoT. Along with improving the shortcomings of the existing efforts devoted to it.
- To optimize the information security in IoT networks in a holistic, cross-layered manner (i.e. IoT platforms and devices, Honeypots, fog nodes, SDN routers and operator's controller) that will be based both on dynamic and distributed processing of variable complexity by single network components (i.e. IoT platforms, devices and honeypots will perform lightweight processes while fog/cloud nodes and SDN routers will be shouldered with more heavy processes), as well as on a centrally located server/controller that will have the main control of the network and will collect, aggregate and appropriately fuse the transmitted data and produced metadata.
- To utilize and develop the appropriate technologies, so as to implement an efficient and robust Decision Support System (DSS) on the controller's side, where all data and metadata will be collected, for (i) the detection of potential threats and abnormalities, (ii) including a competent package of comprehensive and intuitive (visual) analytics (i.e. put the human in the loop for reasoning, hypothesis testing and interference in the decision making), and (iii) the generation of escalating mitigation strategies according to the severity of the detected threat.
- To enhance the inter-connection of heterogeneous devices by speeding up the communication processes and by selecting the optimal routing path for the transmitted information in terms of both security and travel time.

– To introduce a methodology and to provide a tool-chain for automatic generation of design-driven security features, monitors and validators for IoT platforms and networks based on IoT architecture and behaviour model specifications.
– To validate these actions in both large- and small-scale representative real-case scenarios involving heterogeneous IoT platforms and devices in an EU wide testbed covering a wide variety of important areas.

SerIoT also aims to provide a useful open reference framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network in order to recognize suspicious patterns, to evaluate them and finally to decide on the detection of a security leak, privacy threat and abnormal event detection, while offering parallel mitigation actions that are seamlessly exploited in the background. Furthermore, the project will also address the role of networking, and in particular transmission control, media access control, bandwidth allocation, and routing, for anomaly detection and mitigation in the IoT. Thus, the **SerIoT System Architecture** is based on the expected work-flow of the system, broken down into several core architectural elements (see Figure 1).

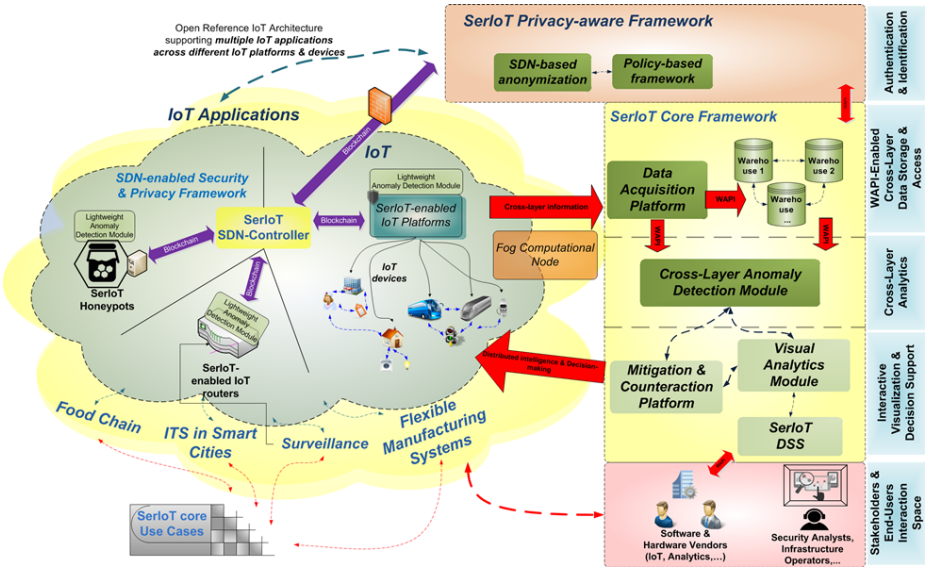

Fig. 1. Overview of SerIoT's planned architecture.

3.1 IoT Data Acquisition Platform

This layer is comprised of low-level IoT-enabled components that constitute the distributed IoT infrastructure backbone ranging from IoT platforms and devices, foreseen

SerIoT fog nodes including honeypots as well as normal computation engines and storage capabilities and the routers enriched with the Software Defined Network (SDN) framework of SerIoT.

The SDN framework will use an OpenFlow SDN-Controller that will specify and control routing paths for all given IoT applications. Similarly it will be possible to have specific SDN-Controller specialised to a single IoT application, or to groups of related IoT applications. The SDN-Controller will be a generic piece of software that may be incarnated for different IoT systems and it may be run on a given router for all routers in the SerIoT network, or it may be run remotely, as part of the core cloud or on a specific server. Thus, multiple SDN-Controllers may be running simultaneously for a complex set of IoT applications, even though some or all of the routers are common to some or all of the applications.

4 Smart Cognitive Packet Network (CPN) Flow Control and Data Acquisition

Smart network management of SDN [11, 12] will be considered for anomaly detection and mitigation [31, 38, 39].

The smart flow controller will be based on the Cognitive Packet Network (CPN) [17] and its Random Neural Network [13,22] based learning algorithm. The CPN Goal Function in this case will consider ecurity and attack acntivities over the network paths as a primary goal, but in the absence of attacks will follow paths that offer the best quality of service metrics, such as packet delay, packet desequencing which can significantly affect real-time applications, and end-to-end delay, which are important for IoT applications.

CPN routing, which is based on Reinforcement Learning using the specified Goal Function, will be used by the SDN routing engine, but it will also be distributed over selected network routers for measurement, observation, and threat detection purposes. These additional CPN nodes will also feed information to the SDN routing engines, as well as to the visual analytics modules. Thus, these CPN enabled nodes, will continuously gather information in order to conduct the routing and flow function. However, the data gathered in this manner will also feed into the Analytics module (e.g. network activity, attack-related information) in a distributed manner.

In this context a modular middleware will be employed building upon previous successful paradigms, i.e. WAPI API [42], for the implementation of the SerIoT data collection framework. The framework has been initially developed in WOMBAT project and was further extended in Vis-SENSE and NEMESYS projects [3]. This layer will feed the necessary information needed by the other architectural elements of the distributed SerIoT framework, which will deal with the ad-hoc anomaly detection and the centralized decision support framework, supported by the core cloud. These components will be coupled with innovative visual analytics techniques to further support decision making to the respective operators [29, 30]. In addition to the security monitoring, means for monitoring the energy consumption of the SerIoT network will also be introduced; indeed energy consumption has become an important issue in networks

in general [18, 28] since it is a significant component of the economic cost system operation, as well as significant from the point of view of CO2 impact.

4.1 Ad-hoc Anomaly detection Platform

This layer will deal with the design and implementation of a modular information network security component stack, which will support the provision of a number of security mechanisms that will be executed across IoT devices, honeypots and routers. Lightweight techniques fully exploiting the capabilities (single core versus multiple CPU cores) of each IoT device (accessed through the corresponding IoT platform) will be investigated for the identification and prediction of abnormal patterns [37]. Lightweight and robust anomaly detection techniques based on local traffic characteristics such as dynamic changes in queue lengths and second order properties of traffic will be regularly measured and probed by smart probe "cognitive packets" sent out by the SDN controller, feeding into the SDN-Controller's routing decisions. Analysis of wireless communication links based on research based evidence and performance data will also be used to feed the anomaly detection functions. These smart probe packets will bring back the information to the SDN-Controller's Cognitive Security Memory (CSM), which will be used for periodic or on-demand routing updates, to eliminate lack of security and points of failure (e.g. intelligently route traffic when an attack has been identified) and bottlenecks stemming from the network intrusion attempts. This data will also be forwarded to the Analytics modules for confirmation (or the opposite), which will in turn come back to the SDN-Controller's CSM. Any alert at the CSM level that is clearly denied by the Analytics module will be removed, while alerts that are either confirmed or not denied clearly will be acted upon for greater security. Between updates from the Analytics module, the CSM will remain under the influence of the most recent information it has received, although it may not react to this immediately. This may lead to some reactions or re-routing under some false alarms, but the principle followed is that it is better to react than to discover a security breach after it has done its harm.

4.2 Interactive Visual Analytics and Decision Support Tools

This architectural layer will deal with the interactive decision support tool kits that will be delivered to the end-users (i.e. IoT network operators) of the SerIoT system. It will be composed of advanced information processing mechanisms, fully utilizing the raw measurements from the SerIoT IoT-enabled data collection infrastructure (i.e. devices, routers and honeypots), which will be able to effectively detect potential abnormalities at different levels of the IoT distributed network in the spatiotemporal domain. To support decision making in terms of analysing the root cause of attacks [9] in the IoT infrastructure, a novel visual analytics framework will be researched and developed dealing with the effective management and visualization of data.

4.3 Mitigation and Counteraction Platform

This component is responsible for orchestrating, synchronizing and implementing the decisions taken by the aforementioned DSS. Apart from a central processing unit, it

will involve specific software on the network components (i.e. SDN routers, honeypots and IoT devices), remotely handled.

5 Overall Approach for SerIoT

SerIoT has adopted an agile, trans-disciplinary requirement engineering, modelling and design methodology, which includes the following aspects: (i) End-user and stakeholder requirements engineering and refinement, (ii) Architecture and system analysis and refinement [6–8, 16], (iii) IoT-related research and innovation to implement the architecture, (iv) Prototype technical development and integration plus testing, (v) Creating pilot examples in large-scale business oriented applications (OASA and DT), (vi) Multi-level performance evaluation and end-user validation acceptance based on the fullfillment of Key Performance Indicators (KPI), and (vii) Lessons learned and concrete efforts towards standardization and market take-up of SerIoT results. It is therefore crucial for the successful outcome of the SerIoT project that a clear well-structured methodology be used. Thus, the overall methodology proposed involves five phases.

5.1 Phase One

Framework Design and Preparation (embodied in WP1 and WP2). This phase marks the beginning of the project and includes the identification of state-of-the-art technologies relevant to the project objectives, through existing knowhow of project partners and existing solutions. The output of this phase will be a comprehensive set of requirements, recommendations and guidelines covering all scientific and implementation aspects of the project. It also includes the conception of a business environment that can provide the framework for commercial exploitation of the envisioned framework along with its exploitable products. It involves market analysis, technology assessment, valorisation and business modelling for successful penetration in the emerging market around IoT.

5.2 Phase Two

Technical Development and Innovation (WP3 and WP6) will proceed in parallel with Phase One, where the definition of the SerIoT architectural framework takes place, this phase will involve the conceptual design and implementation of the envisioned IoT ecosystem. It includes the development of the architectural elements in accordance with their high-level functional, technical and interoperability specifications. The agile process followed in SerIoT will address in a unified way the whole reference chain, including end-users as well as business scenarios (defined in the previous phase) and system requirements, Thus, allowing for holistic implementation of the envisioned framework and tool sets (SDN-controller and secure router, design-driven self-monitoring of IoT devices, ad-hoc honeypots, cross-layer anomaly detection and analytics, mitigation engine, IoT reference malware warehouse infrastructure, etc). The output of this phase is the effective definition of the SerIoT specifications to operational architectural elements by following a UML based approach and preparing the groundwork for the transfer of the SerIoT approach to real-world environments.

5.3 Phase Three

The Integration and Validation (WP7 and WP8) phase after the realisation of the SerIoT prototype components will include the following activities: (i) Individual Component/Module Configuration and Adaptation, will take place including experimental verification in the virtual testing environment towards integration int the SerIoT framework. (ii) Prototype integration and iterative testing, in with a specific integration methodology addressing interdependencies, hierarchy, software and hardware implementation, test-bed plans, etc., followed by system integration. Integration should assemble all architectural elements and iteratively deployed into real-life demonstration sites (DT, OASA, etc.).

5.4 Phase Four

This comprises Demonstration and Evaluation (WP8). Due to the agile approach we will adopt, this phase will be run almost in parallel with design, development and integration activities, and focus on fine-tuning and validation of the whole framework as well as on the assessment of the demonstration phase of the project. Thus, this phase is concerned with the iterative deployment of the end-to-end IoT framework in the business scenarios of SerIoT (OASA, DT) as well as the overall project evaluation (lessons learned). This should be followed by activities that address follow-up project achievements. Overall activities will include as (i) System Acceptance involving the execution tests, the recording of findings and the addressing of identified shortcomings. Furthermore, laboratory integration tests will be conducted in order to identify potential leaks and bugs of the prototype system prior its deployment and evaluation in realistic conditions. (ii) Validation of the whole system against the user requirement specifications and the developed business and exploitations plans. (iii) Evaluation of the entire project and its foreground along with tangible achievements compared to the initial project objectives, with adequate focus on technical evaluation (i.e. KPIs), user acceptance and impact assessment.

5.5 Horizontal Activities

These include Project Management, Dissemination/Exploitation and Standardization (WP9 and WP10). This work comprises all the horizontal activities of the project including (i) Overall Project Management (administrative, scientific and technical), (ii) Dissemination and Exploitation of SerIoT results by consortium partners during and after the end of the project, (iii) Standardization activities stimulating seamless connectivity with existing industrial bodies and initiatives in the domains addressed in the project and will be in line with the guidelines from the related standardization bodies and (iv) Sustainability of exploitable SerIoT products, based on a concrete strategy (IoT market analysis)" SWOT, CBA/CEA analysis stemming from Large-scale trials, detailed business plan, etc.).

5.6 Use Case 1: Surveillance

This Use Case will target the exploitation of the system on multimedia data streaming from surveillance networks and from proprietary sensor networks (e.g. cameras, registration points, etc.), that render valuable "loot" for fraudulent hackers or unauthorized companies or individuals. In this case, sensitive information related to personal data, and protected by privacy legislation, become available in the interconnected IoT and are obtained via unauthorized access and then are forwarded via the rerouting/bypassing of the information on secure paths. This Use Case will be combined with the next one regarding Intelligent Transport Systems in Smart Cities to demonstrate security scenarios in the context of Autonomic Sensor Systems. Examples of such autonomous systems related to SerIoT include critical infrastructures that can effectively monitor external facilities (Athens Pilot Concept I), and the case where embedded intelligence in IoT devices (e.g. placed on parts of a manufacturing system) can automatically notify storage areas and services to improve maintenance planning and worker safety. These are core impacts stemming from the Flexible Manufacturing domain, which SerIoT targets in particulat by our partner DT/T-Sys. This Use Case will be also demonstrated through the infrastructure and public services offered by OASA, the largest transport authority in Greece.

5.7 Use Case 2: Intelligent Transport Systems in Smart Cities

This Use Case focuses on the analysis and definition of security solutions for Intelligent Transport Systems (ITS) integrated in a Smart City where ITS stations can be vehicles, but also mobile persons, other transportation infrastructures, etc. The term ITS refers to the application of Information and Communication Technologies (ICT) to road transportation to support and enhance various applications. The main concept is to integrate computers, electronics, wireless communications, sensors, and navigation systems such as Global Navigation Satellite Systems (GNSS), to enable the collection and distribution of information to and from the vehicles. One of the main standardization activities in ITS is specific to Vehicle to Vehicle communications where generic ITS stations (e.g. cars or a roadside platform) exchange information in a secure way through Dedicated Short Range Communication (DSRC), also called ITS G5 in Europe. A key aspect of such an example of Cooperative-ITS (C-ITS) is the establishment of "trust" between participating systems and devices. The C-ITS security framework (for cars and infrastructure stations) is mainly based on the Public Key Infrastructure (PKI) concept and is currently defined at the EU level in the C-ITS deployment platform.

While the use of PKI for a specific vehicle based ITS application like Collision Avoidance is well defined and described in specification documents, the secure and safe integration of ITS stations in the Smart City and transport systems is still a subject of investigation. We will explore the security framework for such applications beyond the ones prescribed at the EU level, through C-ITS deployment, namely the buses provided by OASA, and ATECH's contribution of roadside ITS stations. IoT security solutions will be integrated to ensure that the evolution of ITS will not generate security risks or vulnerabilities when different means of communication and devices are integrated. In addition, cyber-physical aspects are quite relevant in ITS and a security breach can

generate not only loss of data but also risks to physical safety, including possible loss of life. Thus, the related security requirements will differ from generic IoT security requirements, as the reaction time of the cyber-physical components are very short and the related security solutions must react very quickly.

Two core aspects will have to be taken into consideration: (a) Vehicles and drivers will be connected through multiple wireless technologies such as Cellular Networks, Bluetooth, Wi-Fi,etc. (b) The security of the ITS station and the exchange of information (including personal data) will have to be protected in this heterogeneous context. (c) Beyond cars, people on the streets and other roadside nodes could also be connected to ITS stations Thus, widening the current concept of ITS station and its collaborative functionalities. This Use Case will also be coupled with the Surveillance Use Case (monitoring of an infrastructure) and will be instantiated in the large-scale IoT-enabled systems that are described below.

Bilbao Pre-Demonstrator and Real World Scenarios This pilot offers an intermediate step between early validation of algorithms in a laboratory environment, and the actual exploitation of the system in real world environments as in the next three use-case pilots. In particular, all applicable systems of the SerIoT solution will be tested in the controlled environment of the Bilbao park before being exploited on the streets of Athens so as to significantly facilitate the early detection of faults, bugs, etc., to minimize any risk to the public, and thoroughly and repeatedly check certain cases with no time restriction or environmental disturbances. The TECNALIA private test track is a fully instrumented permanent test site for Automated Vehicles composed of two Renault Twizzy automated vehicles, a private (dedicated) test track with central station (with I-to-V and Vehicle-to-Vehicle communication) and a driving platform simulator. This scenario will help validate some of the individual and cooperative manoeuvres in the vehicles: overtaking, intersection lane change and roundabouts. Dual mode services, such as control of automated functions and sharing techniques between vehicle and driver, can be tested. technology providers from the consortium will participate in this demonstrator.

Transport for Athens Pilot Concept I Audio permanent sensors and cameras wil be installed in public transport vehicles and depots to detect illegal or unwanted activities such as window scratch graffiti, graffiti, potential security incidents, and unsolicited activities (such as begging, in-vehicle music playing, etc.). This low-cost network of microphones and cameras, coupled with an “security incident control center”, will have the capability to detect selected image frequencies for graffiti and scratch graffiti, and detecting and recognizing sound patterns that indicate security incidents or unsolicited activities. This in-vehicle and depot systes will have capabilities of audio feedback, in order to deter and avert unwanted and illegal actions. The central system will identify the vehicle in which an incident takes place and give the operators required information for incident management.

Transport for Athens Pilot Concept II The installation of engine sensors in buses and trolleybuses (potential extensions to Metro will also be investigated during pilot

designs), aims to enable the access to engineering data in order identify potential future breakdowns and create engineering log of required data, in order to plan maintenance activities, using the secure and safe IoT ecosystem of SerIoT. Both of the "Athens Pilot" Use Cases will be organized by OASA with ICCS and CERTH for the application development and integration in liaison with project partners ATOS, HOPU and DT/T-Sys.

C-ITS Stations Vienna Pilot Concept III Use of existing and installed C-ITS stations in a living lab environment with additional security elements of SerIoT for the monitoring of security risks and attacks form the connected sensors and external C-ITS dynamic communication links. Enable and support fast recognition of "insecure ITS stations" or other external users and contribute data reports and logs to the clarification of the "unclear situation" in terms of severity of the risk and the consequences for the extended and distributed C-ITS network (e.g. options could range from closing one network channel of the ITS station, temporarily close the receiving channel, temporarily shut down the C-ITS station, to report to central operators to close all "linked stations" down in "hibernation mode" till certain conditions are met again and operational capacity can be resolved). Generate for the operator additional recommendations and hints for regular network operation and propose improvements for regular and stable operations. ATECH has access to ITS stations in the Vienna Living lab environment and will offer the expertise and resources from there in order to set up the aforementioned scenario.

5.8 Use Case 3: Flexible Manufacturing Systems

This Use Case will deal with Flexible Manufacturing Systems (Industry 4.0), which concern a sophisticated approach for enabling connected industry to create value and novel business models. This Use Case will provide monitoring and detection of physical attacks to wireless sensor networks in the context of the Industry 4.0 and will be mainly supported by DT/T-Sys. and the testbed provided by UEssex. There will be two concrete scenarios, which will be instantiated in DT/T-Sys. infrastructure:

- Attack on an intelligent automatic warehouse such as those that are planned by Amazon. In this use case the warehouse is operated by wireless connected robots, which collect the purchase lists automatically and bring the goods to the packing stations. Since all data communication is wireless, many attack vectors may be used for breaking or jamming the communication line. Within SerIoT, techniques such as anomaly detection at SDN and device levels will be utilized for the early identification of such attacks.
- This use case is also an example of dealing with a critical infrastructure, where some of the components, actors or sensors are linked by wireless technology such as W-Lan or Bluetooth. Jamming attacks can disturb the communications, so that the supply of critical resources such as energy or water can be impacted seriously. The monitoring and detection system of SerIoT will be also utilized here to demonstrate the feasibility of mitigating such attacks, and tested in OASA pilots, in DT/T-Sys., and perhaps in other contexts.

5.9 Use Case 4: Food Chains

Food Chains can illustrate end-to-end security across communication channels, i.e. Transport Layer Security, Datagram TLS protocol, etc., by addressing device authentication mechanisms, the detection and avoidance of DoS and replication attacks, as well as early detection of the interruption of IoT devices (critical functionality), while the requirements related to the mobility of these devices will be explored, for instance when they are deployed in an environment where no protection is available by design. Since many food items are perishable and can only remain in shops for a certain time before they become unfit for consumption, replacing printed "deadlines" by IoT devices on packages will communicate to shop managers when a deadline is reached and flash a red LED indicator for the shop managers and customers, offering "on board sensing and communications" for food. This Use Case will be supported by third parties that will join the SerIoT consortium and interconnected to the project through the EU wide test-bed supported by UEssex.

6 Conclusions

As we move towards the IoT and the IoE, we are opening our most vital physical systems that support our daily life, to possible security and privacy breaches, and attacks that can impede and impair all of our common daily activities. Thus, in this paper we have outlined the EU H2020 SerIoT project which addresses the IoT Security Challenge by developing, implementing and testing a generic IoT framework based on a specific adaptation of the concept of smart Software Defined Networks, augmented with secure routers, advanced analytics and user friendly visual analytics. The SerIoT project will create a unique and portable software-based SerIoT network to spearhead Europe's success in IoT security. The SerIoT project has thus formulated major Scientific and Technological Objectives which will also help us monitor overall progress based on specific quantitative and qualitative indicators relevant to each objectives. These advances will also be evaluated in individual laboratory test-beds and in an integrated EU wide test-bed, which will be interconnected and demonstrated via significant use cases by our industry partners.

Acknowledgement

This research was partially supported by funding from the H2020-IOT-2016-2017 (H2020-IOT-2017) Program under Grant Agreement 780139 for the SerIoT Research and Innovation Action.

References

1. 3GPP: Study on machine-type communications (mtc) and other mobile data applications communications enhancements (release 12) (Dec 2013), `http://www.3gpp.org/DynaReport/23887.htm`, 3GPP TR 23.887

2. Abdelrahman, O.H., Gelenbe, E.: Signalling storms in 3G mobile networks. In: IEEE International Conference on Communications (ICC'14). pp. 1017–1022. Sydney, Australia (Jun 2014)
3. Abdelrahman, O.H., Gelenbe, E., Gorbil, G., Oklander, B.: Mobile network anomaly detection and mitigation: The NEMESYS approach. In: Proc. 28th International Symposium on Computer and Information Sciences (ISCIS'13), LNEE, vol. 264, pp. 429–438. Springer, Paris, France (Oct 2013)
4. Bera, S., Misra, S., Vasilakos, A.V.: Software-defined networking for internet of things: A survey. IEEE Internet of Things Journal 4(6), 1994–2008 (2017)
5. Collen, A., Nijdam, N.A., Augusto-Gonzalez, J., Katsikas, S.K., Giannoutakis, K.M., Spathoulas, G., Gelenbe, E., Votis, K., Tzovaras, D., nd M. Volkamer, N.G., Haller, P., Sanchez, A., Dimas, M.: Ghost - safe-guarding home iot environments with personalised real-time risk control. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.) Proceedings of the 2018 ISCIS Security Workshop. Springer (2018)
6. Czachorski, T., Domanski, A., Domanska, J., Pagano, M., Rataj, A.: Delays in ip routers, a markov model. In: Czachorski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.) Computer and Information Sciences ISCIS 2016. vol. 659, pp. 185–192. Springer CICIS (2016)
7. Czachórski, T., Grochla, K., Pekergin, F.: Diffusion approximation model for the distribution of packet travel time at sensor networks. In: Cerdà-Alabern, L. (ed.) Wireless Systems and Mobility in Next Generation Internet, 4th International Workshop of the EuroNGI/EuroFGI Network of Excellence. pp. 10–25 (2008)
8. Domanski, A., Domanska, J., Pagano, M., Czachorski, T.: The fluid flow approximation of the tcp vegas and reno congestion control mechanism. In: Czachorski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.) Computer and Information Sciences ISCIS 2016. vol. 659, pp. 193–200. Springer CICIS (2016)
9. Drosou, A., Kalamaras, I., Papadopoulos, S., Tzovaras, D.: An enhanced graph analytics platform (gap) providing insight in big network data. Journal of Innovation in Digital Ecosystems 3(2), 83–97 (2016)
10. Elhammouti, H., Sabir, E., Benjillali, M., Echabbi, L., Tembine, H.: Self-organized connected objects: Rethinking qos provisioning for iot services. IEEE Communications Magazine 55(9), 41–47 (2017)
11. Francois, F., Gelenbe, E.: Optimizing secure sdn-enabled inter-data centre overlay networks through cognitive routing. In: Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), 2016 IEEE 24th International Symposium on. pp. 283–288. IEEE (2016)
12. Francois, F., Gelenbe, E.: Towards a cognitive routing engine for software defined networks. In: Communications (ICC), 2016 IEEE International Conference on. pp. 1–6. IEEE (2016)
13. Gelenbe, E.: Learning in the recurrent random neural network. Neural Computation (1), 154–164 (1993)
14. Gelenbe, E.: Keeping viruses under control. In: International Symposium on Computer and Information Sciences. pp. 304–311. Springer (2005)
15. Gelenbe, E.: Dealing with software viruses: a biological paradigm. information security technical report 12(4), 242–250 (2007)
16. Gelenbe, E.: A diffusion model for packet travel time in a random multi-hop medium. ACM Transactions on Sensor Networks (TOSN) 3(2), 10 (2007)
17. Gelenbe, E.: Steps towards self-aware networks. Communications of the ACM 52(7), 66–75 (July 2009)
18. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity 2015(June), 1:1–1:15 (2015)

19. Gelenbe, E., Görbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., Lyberopoulos, G.: Nemesys: Enhanced network security for seamless service provisioning in the smart mobile ecosystem. In: Information Sciences and Systems 2013, pp. 369–378. Springer (2013)
20. Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., Lyberopoulos, G.: Security for smart mobile networks: The nemesys approach. In: Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on. pp. 1–8. IEEE (2013)
21. Gelenbe, E., Hernández, M.: Virus tests to maximize availability of software systems. Theor. Comput. Sci. 125(1), 131–147 (1994)
22. Gelenbe, E., Hussain, K.F.: Learning in the multiple class random neural network. Neural Networks, IEEE Transactions on 13(6), 1257–1267 (2002)
23. Gelenbe, E., Kadioglu, Y.M.: Energy life-time of wireless nodes with and without energy harvesting under network attacks. In: Advances in Cyber-Security: An ISCIS International Workshop. Springer (2018)
24. Gelenbe, E., Kaptan, V., Wang, Y.: Biological metaphors for agent behavior. In: International Symposium on Computer and Information Sciences. pp. 667–675. Springer (2004)
25. Görbil, G., Abdelrahman, O.H., Pavloski, M., Gelenbe, E.: Modeling and analysis of RRC-based signalling storms in 3G networks. IEEE Transactions on Emerging Topics in Computing 4(1), 113–127 (2016)
26. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Computer Science 5, 39–47 (2011)
27. He, D., Chan, S., Qiao, Y., Guizani, N.: Imminent communication security for smart communities. IEEE Communications Magazine 56(1), 99–103 (Jan 2018)
28. Jiang, H., Liu, F., Thulasiram, R.K., Gelenbe, E.: Guest editorial: Special issue on green pervasive and ubiquitous systems. IEEE Systems Journal 11(2), 806–812 (2017)
29. Kalamaras, I., Drosou, A., Polychronidou, E., Tzovaras, D.: A consistency-based multimodal graph embedding method for dimensionality reduction. In: 2017 IEEE International Conference on Data Science and Advanced Analytics (DSAA). pp. 351–360 (Oct 2017)
30. Kalamaras, I., Drosou, A., Tzovaras, D.: A multi-objective clustering approach for the detection of abnormal behaviors in mobile networks. In: Communication Workshop (ICCW), 2015 IEEE International Conference on. pp. 1491–1496. IEEE (2015)
31. Kalkan, K., Gür, G., Alagöz, F.: Defense mechanisms against ddos attacks in sdn environment. IEEE Communications Magazine 55(9), 175–179 (2017)
32. Kalkan, K., Zeadally, S.: Securing internet of things (iot) with software defined networking (sdn). IEEE Communications Magazine (2017)
33. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C.P.A., Sun, Z.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal 4(6), 1832–1843 (2017)
34. Lu, X., Spear, M., Levitt, K., Matloff, N.S., Wu, S.F.: A synchronization attack and defense in energy-efficient listen-sleep slotted mac protocols. In: Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on. pp. 403–411. IEEE (2008)
35. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S.: Internet-of-things-based smart cities: Recent advances and challenges. IEEE Communications Magazine 55(9), 16–24 (2017)
36. Melcherts, H.E.: The internet of everything and beyond. Human Bond Communication: The Holy Grail of Holistic Communication and Immersive Experience p. 173 (2017)
37. Papadopoulos, S., Drosou, A., Tzovaras, D.: A novel graph-based descriptor for the detection of billing-related anomalies in cellular mobile networks. IEEE Transactions on Mobile Computing 15(11), 2655–2668 (2016)

38. Pavloski, M., Gelenbe, E.: Attacks on the signalling systems of mobile telephony. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.) Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Springer (2018)
39. Pavloski, M., Görbil, G., Gelenbe, E.: Counter based detection and mitigation of signalling attacks. In: Proc. 12th International Conference on Security and Cryptography (SECRYPT'15). pp. 413–418. Colmar, Alsace, France (Jul 2015)
40. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., Brooks, R.: The sleep deprivation attack in sensor networks: Analysis and methods of defense. International Journal of Distributed Sensor Networks 2(3), 267–287 (2006)
41. Ratasuk, R., Prasad, A., Li, Z., Ghosh, A., Uusitalo, M.A.: Recent advancements in M2M communications in 4G networks and evolution towards 5G. In: Proc. 18th IEEE International Conference Intelligence in Next Generation Networks (ICIN). pp. 52–57. Paris, France (Feb 2015)
42. Yan, L., Da, G.: Study of wapi technology and security. In: Web Society (SWS), 2010 IEEE 2nd Symposium on. pp. 716–719. IEEE (2010)
43. Zohar, A.: Bitcoin: under the hood. Communications of the ACM 58(9), 104–113 (2015)