secIoT10

1ST INTERNATIONAL WORKSHOP ON
THE SECURITY OF THE INTERNET OF THINGS
Tokyo (Japan), November 29, 2010
HELD IN CONJUNCTION WITH
INTERNET OF THINGS 2010

General Co-Chair's report from the SecIoT'10 Workshop

Written by Jim Clarke[1] and Rodrigo Roman[2]

[1]Waterford Institute of Technology, Ireland; [2]University of Malaga, Spain.

INTRODUCTION

The workshop proposal for the 1st Workshop on the Security of the Internet of Things, SecIoT'10 (http://www.isac.uma.es/seciot10) was submitted in 2Q 2010 and was accepted by the organizers of the prestigious Internet of Things 2010 conference being held in Tokyo, Japan in December 2010. A Program Committee of 30 members from around the globe was convened in late June 2010[1] and the call for papers was issued in July 2010[2]. As a result of the CFP, 17 full papers were submitted and 9 papers were accepted for the workshop[3].

The main focus of the 1st Workshop on the Security of the Internet of Things, SecIoT'10 (http://www.isac.uma.es/seciot10), was to address the most important security research issues that must be solved in order to protect the IoT. The workshop was focused on different security challenges that are related to the Internet of Things: From the protection and interoperability of the different actors and building blocks to the management of the information produced by the interactions between all entities. In particular, the topics of our workshop (which are thoroughly described in http://www.isac.uma.es/seciot10/theme.html) include the following:

- New security problems in the context of the IoT.
- Privacy risks and data management problems.
- Identifying, authenticating, and authorizing entities.
- Development of trust frameworks for secure collaboration.
- New cryptographic primitives for constrained "things".
- Connecting heterogeneous ecosystems and technologies.
- Legal Challenges and Governance Issues.
- Resilience to external and internal attacks.
- Context-Aware Security.
- Providing protection to an IP-connected IoT.
- Web services security and other application-layer issues.

[1] http://www.isac.uma.es/seciot10/comitee.html

[2] http://www.isac.uma.es/seciot10/cfp.html

[3] http://www.isac.uma.es/seciot10/papers.html

Moreover, authors of selected papers are invited to submit an extended version for possible publication in the "Protecting the Internet of Things" special issue of Wiley's Security and Communication Networks Journal. This international journal publishes original research papers on security and cryptographic mechanisms applied to all types of information and communication networks, and it is indexed in almost all important technical journal index systems, such as ISI, SCI, EI, SCOPUS, etc.

SUMMARY OF WORKSHOP

The 1st workshop on the Security of the Internet of Things was held in conjunction with the Internet of Things 2010 conference at the IBM building in Tokyo, Japan in November 29th, 2010. The workshop received 17 submissions from authors representing more than 15 countries around the world, and from those submissions 9 high-quality technical papers were accepted and presented at the workshop. Moreover, we were fortunate to have an extremely relevant invited paper that provided results from the ENISA study on the security of future scenarios of the Internet of Things.

The following paragraphs summarize the contents of the different presentations, alongside with the topics that were discussed by the audience (~30 academic researchers and members of the industry) after every presentation.

- Invited talk: Looking through the crystal ball - Identifying future security, privacy and social risks in a prospective IoT scenario. Speaker: Barbara Daskala, ENISA.

This invited talk summarized the results of a risk assessment analysis on a prospective scenario in air travel where IoT is an enabler for a plethora of improvements, novel services and business opportunities. As a result, the presentation discussed the general challenges for future IoT applications extending beyond the air travel scenario, and also provided a set of recommendations to be considered by various stakeholders when designing and deploying future IoT scenarios.

This talk generated the following discussions:

- What definitions are used for security and privacy, and what is the balance between these concepts? This generated a discussion on the existing nomenclature used to strictly define these concepts, and how security and privacy are intertwined.
- Did the study consider other aspects such as the supply chain (e.g. the lifecycle of RFID tags)? The answer was that they did consider such aspects in the study but at a high level in the detailed analysis of the risks and vulnerabilities. This data was then aggregated together with other information.

- Assessing the Security of Internet Connected Critical Infrastructures (The CoMiFin Project Approach). Speaker: Neeraj Suri

This presentation primarily addressed the fundamental question of how to evaluate and assess the trustworthiness of Critical Infrastructure Protection mechanisms that are based on sensing nodes and communication overlays in the context of the Internet of Things. To quantitatively measure the level of quality of protection (QoP), the speaker stressed the need of defining appropriate, application-dependent metrics. In particular, the presentation focused on metrics for both the design phase (Trustworthiness by Design) as well as for run-time (Trustworthiness by Repair).

This talk generated the following discussions:

- What is the difference between proposed models and metrics? The speaker clarified such differences with a number of examples from the telecommunications providers SLA's and especially cloud services context.
- Is it algorithms that you are proposing? The speaker answered that yes, in the ideal situation (from the point of view of a scientist) such metrics should be included in real-world scenarios, but this is usually refuted by the industry people. From a conceptual viewpoint it is relatively easy to propose metrics. However, in actual deployed systems the issues of (a) proprietary nature of operational parameters, (b) lack of operation details of service specification interfaces, makes it very hard to realistically assess quantifiers, and/or to use these to direct response schema. Getting actual operational data is a key impediment to the use of deploying metrics.

- Accountability in the Internet of Things. Speaker: Rolf H. Weber.

Accountability of governing bodies in the Internet of Things is of major importance. This talk focused on how improving accountability requires the implementation of new general principles in order to provide for a stable and foreseeable legal framework on which business can rely.

This talk generated the following discussions:

- From the point of view of lawyers, what is the difference between "Internet" and "Internet of Things"? This comment spawned a discussion on how difficult is to grasp the concept of Internet of Things for non-technical people outside the area, and the existing issues that legal bodies face regarding the provisioning of legal frameworks in the digital world of today.
- What is a possible counter suggestion to criminal enforcement? The speaker suggested that one possibility is to make use of contracts-based enforcement.

- Privacy-Preserving Management of Personal Data For Assisted-Living Applications. Speaker: Gina Kounga.

The increasing proportion of elderly people in most industrialised countries introduces new challenges. One of these is the provision of efficient and cost-effective caring. The purpose of this presentation was to propose a solution providing a privacy-aware management of personal data in such scenarios. The proposed solution relies on a communication box, located at the individuals, which automatically protects individuals' privacy based on their consent.

This talk generated the following discussions:

- What is the actual state of your study, how it has been applied? The speaker explained the actual state of the prototype. This generated a small discussion on the different lessons that can be learnt from small prototypes and (controlled) real-world deployments.
- Is your future work going to broaden out to include the users? The answer was that the study at its present form did not fully included the users. After including the users, the researchers are confident that they can really study the benefits and security aspects of IoT.

- Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration? Speaker: Rodrigo Roman.

This talk focused on Wireless Sensor Networks, as they provide a virtual layer where the information about the physical world can be accessed by any computational system. In particular, the talk focused on whether the devices of a WSN should be completely integrated into the Internet or not, from the perspective of the security issues at the network level.

This talk generated the following discussions:

- It is really necessary to have an IP-connected sensor node? This question generated a discussion on the scenarios where sensor nodes should be directly accessible from the Internet, the real benefits on providing such connectivity, and the issue of (D)DoS attacks in those directly accessed systems.
- One particular comment raised the point that IP connectivity is important "after" a problem happens. This member of the audience provided the recovery times of IP-based power services as an example. Afterwards, the balance between IP networks weaknesses and IP recovery times was discussed, together with the existence of heterogeneous connectivity models in real world systems.

- A holistic approach to RFID security and privacy. Speaker: Evangelos Rekleitis.

RFID technology constitutes an important part of what has become known as the IoT In order to be able to secure the IoT in a cost-efficient manner we need to build security and privacy into the design of its components. This talk focused on the use of novel security and privacy mechanisms for fine granularity and context-aware information control in RFID systems.

This talk generated the following discussions:

- One question focused on the clarification of the different steps of the protocol. This question generated a small discussion on the usability and scalability of these kinds of security protocols, as it is necessary to apply brute force on the server side. In fact, one member of the audience pointed out how previous work in the area has formally modeled the security of such simple mechanisms.

- Towards a Model for Security and Privacy in the Internet of Things. Speaker: Sasa Radomirovic.

The presentation proposed a high-level, work-in-progress description of a model which will allow the research community to reason about security and privacy of communication protocols in the Internet of Things and identify the next steps necessary towards a complete formal model. In fact, the presentation defended that from a security and privacy perspective, the Internet of Things is to be considered as a fusion of an operating system and a network.

This talk generated the following discussions:

- One of the foundations of the paper was to make use of previous knowledge on the relationship between Internet technologies and malware to deduce how the security of the Internet of Things would evolve in the Future. One member of the audience pointed out how malware evolved due to the existence of a (shady) business model, and this generated a small discussion on this topic.
- The paper presented the concept of "digital crumbs": the small bits of information about us that can be put together in order to create a picture of our lives. This concept generated a discussion on the protection of IoT-generated information.

- An epistemology of information technology models for pervasive computing. Speaker: Jim Clarke for Michel Riguidel.

This paper provided a thought-provoking analysis that introduced the digital realm as a dynamic, Darwinian ecosystem. In particular the presentation analyzed the emergence of the concept of pervasive computing, and developed an account of information and communication technologies (ICT), their evolution, and a roadmap for their potential future development. Moreover, the presentation also introduced the cluster of projects that were used as an inspiration for this paper, the Future Internet Assembly.

This talk generated the following discussions:

- Most of the questions revolved around how non EU countries could participate to the Future Internet Assembly mechanisms. Everyone was invited to participate to this open process, and were redirected to the FIA website, http://www.future-internet.eu/

- Optimization of Public Key Cryptography (RSA and ECC) for 8-bits Devices based on 6LoWPAN. Speaker: Antonio J. Jara

The contribution of this paper was an analysis of security mechanisms for IoT applications, specifically of RSA and ECC algorithms in 6LoWPAN nodes. In particular, the paper proposed an implementation of multiplication operations for RSA and ECC based on bit shifting, which improved the overall throughput of these public key cryptography algorithms.

This talk generated the following discussions:

- Which Montgomery multiplication and Montgomery reduction methods are you using? This question sparkled an analysis of the different methods that can be used to perform modular multiplication with an odd modulus.
- The availability of an open source implementation of these optimizations was discussed, and the speaker pointed out that they might be provided in the near future.

- Efficient and Side-Channel Resistant RSA Implementation for 8-bit AVR Microcontrollers. Speaker: Zhe Liu.

The RSA algorithm is the most widely used public-key cryptosystem today, but it is difficult to implement on embedded devices due to the computation-intense nature of its underlying arithmetic operations. The speaker provided an optimization for small microcontrollers, based on a new variant of the hybrid method for multiple-precision multiplication, which improved all existing RSA implementation for sensor nodes.

This talk generated the following discussions:

- Can this technique be used with the optimizations presented in the previous paper? This question produced a small discussion on this subject between the speaker and the presenter of the previous paper.

CONCLUSIONS AND NEXT STEPS

In the closing discussions, after raising the question of which were the most relevant security issues for the future of the IoT, very interesting discussions took place, which are summarized below:

1. How do we make sure that security for IoT is built in at the right time? A very real danger is that developments go ahead, but later we find out it isn't possible to fix things due to costs associated with random updates, software improvements for IoT devices, etc. An example of this is the car manufacturers area, where they may find it isn't possible to perform on the spot updates for security related patches within future automobiles services, and thus making all the research a waste of time and money.
2. Following the previous discussion, we analyzed the problem of a fault tolerant IoT, and whether the existence of underlying (and partially unsolvable) problems would influence the survivability of the IoT after a phase transition occurs and the IoT becomes one of the inherent elements of our society.
3. How do we educate people in security, and what are the costs involved in educating people? As a part of this discussion, a study in Switzerland was cited where students are being taught security and privacy aspects at an early age.

It was decided due to the success of the workshop that there would be a 2nd international workshop on Security of IoT in 2011/12. The organizers would discuss possible venues for consideration and inform everyone. Lessons learned would be taken into account and the workshop would be co-located again with a major event as this was felt to contribute to the success of the event.