Trust and security of the Internet of Things (IoT)

BIC Discussion Paper **30 August 2012**

James Clarke[1]

Neeraj Suri[2]

Abhishek Sharma[3]

[1] Waterford Institute of Technology, Ireland

[2] TU Darmstadt, Germany

[3] BIC IAG and Beyond Evolution Tech Solution Pvt Ltd., India

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction – Description of a topic that requires INCO

There is still considerable RTD required by international communities for the trust, privacy and security research challenges arising from the constitution of the IoT architectures, infrastructures, communications, devices, objects, applications and services. In this short report, we present an overview of how to go about addressing this in future RTD work, specifically in Europe and beyond, regarding trust, privacy and security of the Internet of Things with a view towards enabling international cooperation efforts around the globe to solve these major research challenges. More details can be found in the SecurIT 2012 paper at [1].

There are a number of widely used definitions for Internet of Things, including the following:

“Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Interconnected objects having an active role in what might be called the Future Internet.” source: Internet of Things in 2020 - Roadmap for the Future. May 2008 [2]

“Objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment and/or use actuators to interact with it”. source: Internet of Things – An action plan for Europe. June 2009 [3]

“A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols - Physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.” source: Internet of Things – Strategic Research Roadmap. September 2009 [4]

However, all IoT definitions revolve around the same central concept: “a world-wide network of interconnected objects” with the following attributes: existence, sense of 'self', connectivity, interactivity, dynamicity, and sense of environmental awareness.

The Stakeholders involved.

In order to identify the stakeholders, it is necessary to identify the research challenges that need to be addressed. As shown in Figure 1, there are a number of top level security research challenges. In summary, the challenges are the following:

Protocol and network security

To deal with the large number of objects with significant heterogeneity. This would involve improved cryptography to make them operate in smaller environments requiring faster operation while keeping same levels of security so far. A Key management infrastructure is needed for the open configuration of IoT, in which the new systems need to be able to manage the keys in objects of small size where the current certificate based systems wouldn't work. The current Internet protocols are not usable in these environments.

Figure 1 – Security research challenges in IoT

Data and Privacy

As carrying multitudes of objects can bring up a lot of privacy issues as they are not operating in an isolated way. This area can be addressed by using Privacy by Design (user should be able to decide which of his/her information and how it is being used); Privacy by Default (right to be forgotten); transparency (he should know when it is being used), and improved data and information management.

Identity management

Identity management must be taken from a different perspective in IoT in which objects will have a core identity and yet a temporary identity must be possible. ID management systems should encompass Identification (how to define the identity of a "Thing"); Authentication (infrastructure that allows mutual authentication based on Centralized, Distributed, Local, Global, Attributes); and Authorization based on delegation (e.g. stethoscope) and granularity (e.g. classroom provides class schedule to everyone, syllabus only provided to students).

Trust and governance

Trust and governance is required in order to obtain trust between the different objects (and from the user perspective). For the IoT, a trust management system is especially required inside in order to gain trust management from the user perspective. From the system perspective, governance is very important where policies should be contained and where the policies vs. control is dealt with.

Fault tolerance

As the perimeters of the networks do not exist any more in IoT. Therefore, attackers will be all around and there is a need to provide solutions with the following attributes - Secure by default (Patch Tuesday?), Internal State and the ability to provide self - defence recovery.

Also shown in Figure 1, there are two special **"foundational challenges",** including those related that are **Properties / Application-specific**. These are basic properties that all challenges must consider (e.g. Interoperability, Scalability, Resilience) and to the high-level, application-specific security mechanisms that make use of all the challenges above (e.g. Secure discovery of services); and **Architecture**. Within a system, it is necessary to provide some architectural support to integrate the different security services.

Benefits, Success Metrics and need for INCO on topic

Benefits:

The benefits of proposed strategy derived based on INCO are:

- The research and technological development of IoT capabilities that will work in a trustworthy and secure manner across borders.

Success metrics:

- Achieving considerable impact from international partners in realising IoT technologies.
- Increased number of collaborative projects in progress.
- Sharing of resources and capabilities in the required areas.
- Taking into account cultural aspects of different users of IoT technologies and systems.

The Need for INCO:

IoT research and technological developments are taking place at different levels around the globe and it would be more efficient and effective to pool these resources together.

Approach - bi-lateral, multi-lateral or combination of both:

The authors would suggest to start with bi-lateral with countries very much engaged in these research areas and move to a more multi-lateral approach when the levels of research cooperation begins to grow exponentially. This suggestion is made from a more practical perspective as the building of international cooperation is difficult when using a bi-lateral approach as it takes significant time for all of the parties to come together to try to align their activities and priorities. Therefore, it is even more difficult for a multi-lateral approach when building a longer term strategy in as complex an area with so many research challenges as proposed within this short paper.

Timeline/roadmap:

In figure 2, the challenges are configured into a timeline as introduced by *Internet of Things: Strategic Research Roadmap* [5] and the *Towards a Trustworthy Information Society Think-Trust report* [6]. As seen in the figure underneath the timeline, there are a number of research items (e.g. trust management, access control (delegation) and governance) that don't easily fit yet into the timeline and the research community needs to

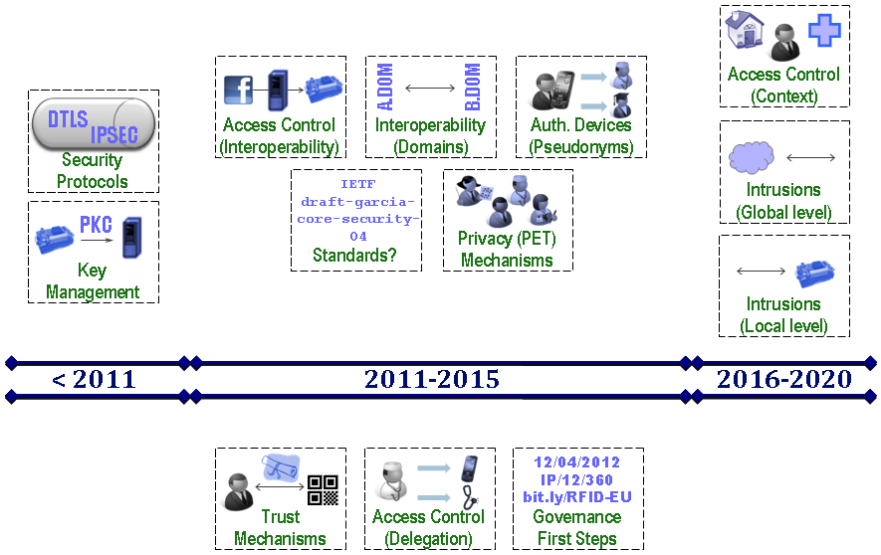

Figure 2 – Research challenges in a timeline

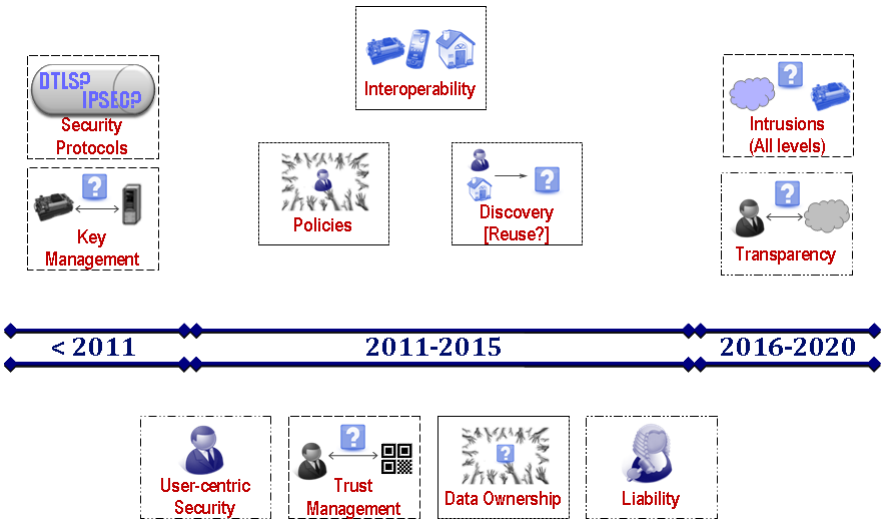

Figure 3 – Future research challenges required in timeline

urgently work together closely to determine when and how these challenges should be addressed for IoT.

Although a considerable amount of research has already been undertaken for IoT, there needs to be considerable more research carried out in particular with respect to trust, privacy and security elements. It should be noted that while the data here is as accurate as the authors could conclude from their research and interactions in the aforementioned events and documents, there could be existing studies already being carried out on these items not included here (e.g. in an European project, where public deliverables are sometimes limited), or there may be additional challenges not considered in detail within our analysis. Therefore, this paper is being used to draw feedbacks from the INCO research communities on these topics in which readers and listeners could certainly clarify something and to share their knowledge with the authors and other attendees. Figure 3 depicts research areas where we are lagging behind in the timeline formation.

References

[1] Clarke, J., Suri, N., Sharma A., Lopez, J., Roman Castro, R., Trust & Security RTD in the Internet of Things – Opportunities for International cooperation, SecurIT 2012, Kerala, India, 14-16th August 2012, ACM Publications.

[2] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[3] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[4] http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

[5] Vermesan, O., et al. 2011, Internet of Things Strategic Research Roadmap, published by The IoT European Research Cluster — European Research Cluster on the Internet of Things (IERC). http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf

[6] Foley, B., Sullivan, K., et al., 2010. Towards a Trustworthy Information Society - Report of the RISEPTIS Advisory Group, published by the FP7 Think-Trust project. http://www.think-trust.eu/riseptis.html

About the Main Author

James Clarke has been working for the Waterford Institute of Technology (WIT) in the Telecommunications Software and Systems Group (TSSG), since February 2005. Prior to joining WIT-TSSG, Mr. Clarke worked at LAKE Communications in Ireland for eight years and Grumman Corporation in the United States for eight years. Since January 2011, Mr. Clarke has been the project coordinator of a European Framework Program 7 Co-ordination action entitled 'BIC ', which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. Previous to this, Mr. Clarke coordinated the successful FP7 INCO-Trust project. More information can be found at http://www.tssg.org/about/people/james-clarke/.