Security and Privacy Threats in IoT Architectures

Denis Kozlov
P.O.B. 35 Dept. of CS&IS
Mattilanniemi 2 Agora bldng
FI-40014 Univ. of Jyväskylä
+358 408 054290
denis.kozlov@jyu.fi

Jari Veijalainen
P.O.B. 35 Dept. of CS&IS
Mattilanniemi 2 Agora bldng
FI-40014 Univ. of Jyväskylä
+358 400 248127
jari.veijalainen@jyu.fi

Yasir Ali
Faculty of Information Technology,
Mattilanniemi 2 Agora bldng
FI-40014 Univ. of Jyväskylä
+358 414 904120
yasir.2.ali@student.jyu.fi

ABSTRACT
In this paper, we describe developments towards the Internet of Things (IoT) and discuss architecture visions for the IoT. Our emphasis is to analyze the known and new threats for the security, privacy and trust (SPT) at different levels of architecture. Our strong view is that the IoT will be an important part of the global huge ICT infrastructure ("future Internet") humanity will be strongly relying on in the future with relatively few data centers connected to trillions of sensors and other "things" over gateways, various access networks and a global network connecting them. While the infrastructure is globally connected, it is divided into millions of management domains, such as homes, smart cities, power grids, access points and networks, data centers, etc. It will evolve both bottom-up and top-down. An important question is what consequences a bottom-up and top-down construction of the IoT infrastructure has for the security, privacy and trust and what kind of regulation is appropriate. We review the currently emerging privacy regulation in EU.

Categories and Subject Descriptors
C.2.1 [**COMPUTER-COMMUNICATION NETWORKS**] *Network Architecture and Design*, D.2.11 [**SOFTWARE ENGINEERING**] *Software Architectures*, K.5.2 [**LEGAL ASPECTS OF COMPUTING**] Governmental Issues

General Terms
Design, Reliability, Security, Privacy, Legal Aspects

Keywords
IoT architecture, security, privacy, trust, energy consumption, Future Internet

1. INTRODUCTION
Mark Weiser wrote "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." [1]. He named such computing and communication technologies *ubiquitous computing.* Later during the 1990'ies IBM researchers introduced the term *pervasive computing* and Europeans (Philips) coined the term *ambient intelligence* (AmI) [2, p.3], all meaning roughly the same as ubiquitous computing. "In May 2000, the Information Society Technologies Advisory Group (ISTAG) commissioned the creation of four scenarios "to provide food for thought about longer-term developments in Information and Communication Technologies", with the intent of exploring the social and technical implications of ambient intelligence" [2, p.2]. Many FP5 and FP6 projects were launched in EU to investigate ambient intelligence since 2000. In Japan the term was ubiquitous networking, but the meaning roughly the same as that of AmI, pervasive/ubiquitous computing. Simultaneously, during the last ten years *Wireless Sensor Networks* (WSN) was made research into especially in USA, but also in Japan and Europe. WSN research was funded in part by the DoD that had military applications in mind, such as *smart dust*, tiny components that can organize themselves into a network, sense environment, process data, and communicate it to other components.

The Internet existed since the beginning of seventies, but it became a global ICT infrastructure around 1995 when WWW took off and its basic technology formed a homogeneous application level infrastructure. "Internet" is currently widely understood as various Web applications and globally accessible contents, although from the networking point of view this is a misconception; in a stricter sense the Internet is a publicly accessible global IP network (a network of networks).

The Internet of Things (IoT) emerged from "RFID tags everywhere" vision in Europe. "The connection of physical things to the Internet makes it possible to access remote sensor data and to control the physical world from a distance….A *smart object*, which is the building block of the Internet of Things, is just another name for an embedded system that is connected to the Internet. There is another technology that points in the same direction – the *RFID technology*. The RFID technology, an extension of the ubiquitous optical bar codes that are found on many every-day products, requires…" [3, p. 307]. The benefits of IoT services would come from the combination of data in the Web and the smart objects. CEC started to fund IoT projects in FP7, as well as Future Internet research. "Future Internet has become a federating theme for European research on communication networks and services" "The Internet of Things can be defined as "a worldwide network of uniquely addressable and interconnected objects, based on standard communication protocols."[4]. Thus in this parlance the IoT would be subsumed by the future Internet.

A parallel development to the above was *Machine-to-Machine communication* (M2M) [5]. As the term suggests, this concept stresses that the interaction takes place between machines, without a direct human control or an immediate reception of the data. Examples are the smart electricity meters that communicate their readings and other events directly to the server components over available mobile networks [6].

The advancements in RFID, communication technologies, and bulk of scientific literature produced in recent years on wireless sensor networks, altogether point towards the feasibility of the IoT at its various levels of architecture. But since these technologies

BODYNETS 2012, September 24-26, Oslo, Norway

DOI 10.4108/icst.bodynets.2012.250550

have been developed within the perspective of traditional Internet, need to be tailored according to new dimensions of resource-efficiency, scalability, security and privacy for the IoT [7].

The integration of sensors and smart things with the Web brought yet another term, *Web of Things* (*WoT*). Here the emphasis is more on the representation of the things in the Web and building applications using web technologies and smart objects [8, 9]. The Open Geospatial Consortium (OGC) standardized the architecture for integrating sensor networks with web services, by their Sensor Web Enablement Framework (SWE). A number of projects have implemented SWE so far, including Heterogeneous Mission Accessibility (HMA) project of ESA in Europe and NASA's OWS-4 [10, p.175-190].

Finally, after social media sites took off since ca. 2005, researcher began to think about combining "things" and social media facilities. This is sometimes called *Social Web of Things* (SWT). One direction is to deploy technologies that make it possible for people to share their smart objects [8]. One can also ponder scenarios, where the smart objects become members of the social media sites, can update their status, respond to queries, etc.

Valuable architecture work for the IoT is taking place within FP7, projects, including [11]. This work has a high relevance for our work at the detailed level, but we do not handle that level in this article.

In the sequel we will discuss especially architecture issues in the IoT and security, privacy and trust people would warrant towards IoT architectures. We will also address some SWT aspects. The paper is organized as follows. In section 2 we will present the overall architecture. Section 3 contains threat analysis, including EU regulation attempts towards IoT threats. Section 4 concludes.

2. OVERALL ARCHITECTURE

In this section we will discuss the overall architecture of the IoT scene. Authors of [5] express their view on the components of the IoT architecture: "To the authors, M2M represents a future where billions to trillions of everyday objects and the surrounding environment are connected and managed through a range of devices, communication networks, and cloud-based servers. There are three essential components to this "Internet of Things" vision...". The authors argue that there will be a continuum of devices from low-cost/low power to compute-rich/high-performance devices on the market. Second, the connectivity will be ultra-scalable. This means that the devices should be able to communicate among them and with the infrastructure. Third, the management of billions of devices should be based on cloud computing. The authors argue that centralized management and decision making should be imposed, although the system is highly distributed.

ISO has worked on the sensor network security. Because ISO, together with ITU, has addressed especially security we start with Figure 1. It shows a number of application areas of sensor networks. These kinds of applications would form the core of the new IoT infrastructure. In Figure 2 ensuing overall systems architecture is represented. The view of the authors of [5], and that presented in the ISO/ITU standard, match rather well. We must still remember that sensors are only a subset of smart objects of the IoT arena, although overwhelming in number.

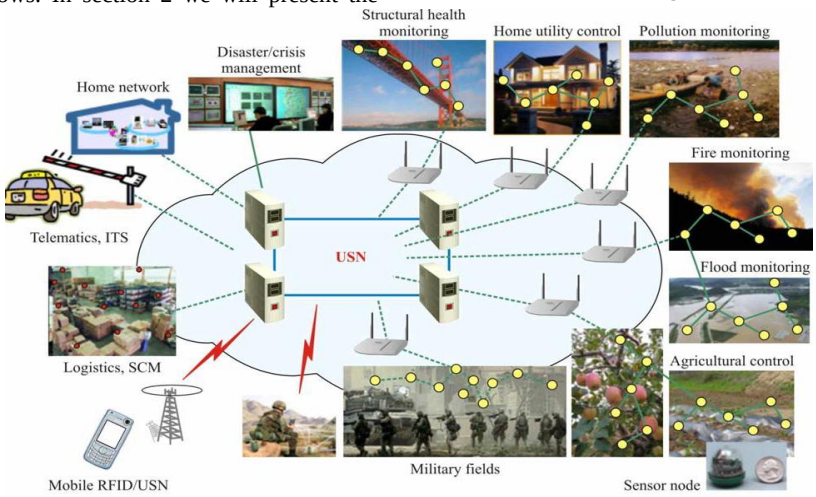

Figure 1. Application domains of IoT [12, Fig.1].

If we analyze the overall technical architecture in Figure 2, we can see roughly six levels there. At the bottom (L1) we have *sensors and actuators*, possibly embedded into objects to form bigger *smart objects*, like the car in the picture. Below, we will consider also the pure sensors and actuators to be smart objects. The smart objects can be mobile or fixed. There are three important points to consider when analyzing the bottom level. First, there are a huge number of smart objects, easily thousands of billions. This means that the IoT would be the biggest man-made system so-far in terms of number of entities. Second, they are necessarily heterogeneous, as concerns their size, functionality, protocol stacks, radios, operating systems (certain types of objects might not even have one), energy sources, identities, etc. Third, each smart object is owned by some organization or individual and controlled by the same or another organization or individual. There are millions of organizations and individuals controlling some subset of the smart objects in their *management domains*, or *spheres of control*. How this control is technically supported is a crucial issue from security, privacy and trust point of view. It is also absolutely crucial to find techniques that keep the need for manual management activities low.

The next level (L2) in the architecture is *gateways* that communicate with many smart objects in their vicinity and relay the data to the access networks and vice verso. Such gateways are necessary for communication path establishment, if the communication range of the smart objects is small (say max 10 meters). The gateways can also perform various data processing tasks, in addition to the basic gateway functionality. *Access networks* form the next level (L3). They consist of fixed

infrastructure for mobile or fixed networks, or satellite-based systems. Currently they can be of Wi-Fi or LAN or 2G-4G telecom type of networks. The satellite-based systems consist of navigation satellite systems (GPS, Galileo, etc.), and satellite communication systems. In some cases smart objects can directly communicate with an access network (e.g. a car or mobile handset with a 3G network or a measuring station in the ocean with communication satellites), without a separate gateway. Access networks are usually local, regional or countrywide. They transfer data between the gateways/smart objects and *globally connected transmission network* (L4). In Figure 2 the latter is called Next Generation Network (NGN). In the current situation this can be the Internet, i.e. the global, public IPv4 network, but very soon the IPv6-based Internet. Its essence is that it is truly global and connects the access networks to each other with enough transfer capacity. What else it should offer has been discussed in the Future Internet projects in different parts of the world [13].

Finally, there must be components where the data is processed and stored and through which the actions taken at the bottom (i.e. at smart objects) are controlled. We would call this *service layer*, (L5) although in Figure 2 it is called USN middleware. Finally, the upmost level (L6) is the *application layer*. At this level the system offers various interfaces for the human users and possibly processing capacity. It was argued in [5] that the services should reside in the cloud, i.e. they should run inside data centers. This is not necessarily reasonable or possible in all cases for a number of reasons. First, an organization (e.g. a city) might want to keep the data produced by the smart objects, control of data production,

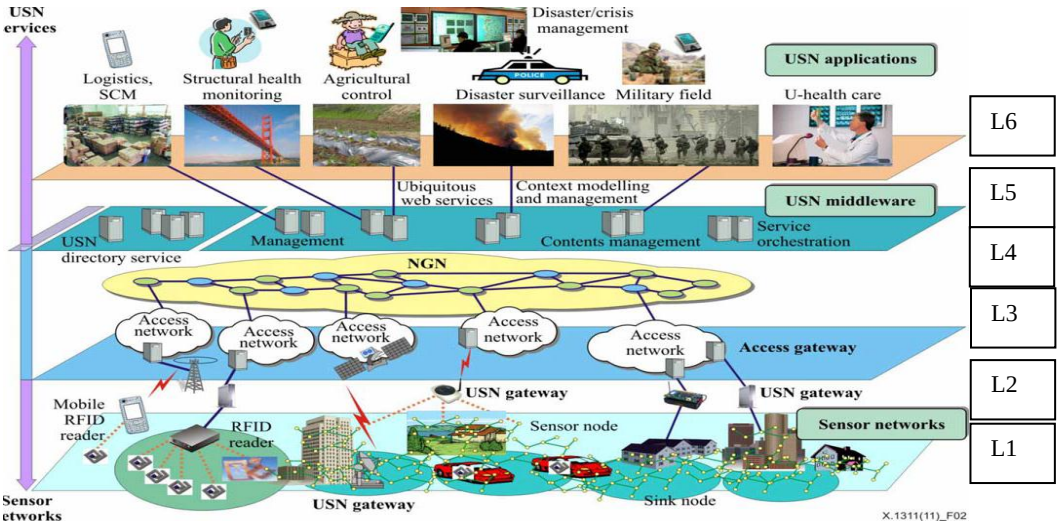

Figure 2. Overall architecture of USNs [12, Fig.2].

and control of the actuators inside the organizational boundaries that are regionally determined. If the organization does not have a private cloud, this would be done by smaller server installations on the city premises. Second, the data produced by the smart objects might be sensible from security and privacy point of view (e.g. medical/home data). It might be e.g. necessary to keep them inside a certain country and, thus, no data centers outside the country can be used for storage and processing. This situation is clearly expressed also in the above standard. The standard calls these spheres of control management domains.

The huge amount of data produced by the trillions of smart objects at the bottom might be processed at the highest levels, but there might be processing also at the lower levels, so that neither data, nor management domain borders are crossed. The number of levels in an instance of the architecture might be even one, in which case all entities would be smart objects at L1 and form necessarily an island. All data processing and remote control flow mediation could be at L1, in which case no data would leave the system. How many levels are needed in different application areas is clearly an issue for further study.

An important general consideration also for the IoT architectures is how they emerge and how the evolution and usage are controlled. Both fixed and mobile telecom networks are examples of top-down architectures that are fully specified by various organizations and deployed by operators. A user can only get access to the network if (s)he has made a contract with the operator. Users do not build the network infrastructure; they only control the usage of the terminal.

What parts of the architecture in Figures 1 and 2 could be constructed and offered bottom up? In IoT deployment the individual components are even much cheaper than a Wi-Fi access point. For this and further reasons we argue that in IoT architectures individuals will deploy a plethora of smart objects that they would control. The bottom level in some application areas (home, home utilities) could be clearly offered bottom-up by individuals, but local organizations might deploy e.g. flood, fire or structural health monitoring, or pollution monitoring infrastructure. Gateways (L2) would probably also be offered bottom up, and certain types of access networks, like LANs and WLANs. Some of the L1 and L2 entities might also be shared with others.

L3 is mainly controlled by organizations (companies and operators) and individuals. We do not expect radical changes in this landscape, even if new network technologies will be deployed.

The central transmission network (L4) should be deployed by operators or governments in a similar fashion as the current Internet is deployed and governed in interoperable pieces We do not anticipate big changes in at this level as concerns the regulation or the way this part of the physical infrastructure is built and operated in the near future.

Shaping L5 and L6 depend largely on viable business models and interest of the authorities to build applications and services that make use of smart objects. A necessary condition for the role of L5 and L6 is regulation that allows data and control flows between L1 and L5 and L6.

3. THREATS in IoT ARCHITECTURES

3.1 Threat scenarios for several levels

In general, threats are always related to a certain system architecture, sometimes called *System under Investigation*. The authors of [14, 4] presented a number of security scenarios for the Internet of Things. We map some of them to our layered architectural view.

Scenario 1: Disappearing computer, i.e. the user loses not just control but even *awareness* of what is actually going on with his/her computer. This ubiquitous scenario can be extended to an extreme scenario, where a person does not know what data is collected about him or her, by what sensors (L1), where and how they are sent (L2-L5), how processed (L5,L6), and whether some actuators would take an action towards him or her (L1).

Scenario 4: The home medical advisor. Secure transmission of critical sensor data from a patient to a health care center. In this case at level L1 sensors must be trusted, and a secured communication path must be constructed from the sensors sensing the patient to the applications at L6 through L1-L5. Sensor data must be correctly attached to the correct patient (L6), based on the identity of the sensing device or gateway. Data must be encrypted (end-to-end) while transmitted in order to guarantee its confidentiality, integrity and privacy (L1-L5). The applications storing and handling the data (L6) must enforce proper authorization, so that only relevant medical personnel have access to the data. Because sensors can rarely run sophisticated encryption algorithms, gateway must perform it.

Scenario 9: Networked cameras and microphones. Security of data captured and transmitted by public web-cameras and microphones. In this case the sensors are rather complicated and generate voluminous data streams. The privacy of persons captured is here the main issue. Who can access the data, what kind of operations can be performed on the data? (L5-L6).

Scenario 11: The Active Badge and other location systems. Privacy and security of location-based systems. This is large problem area and concerns all layers L1-L6. While transmitted, the positioning data should be encrypted (L1-L4). At L5 and L6 the data privacy must be preserved.

The above scenarios are all relevant for the current infrastructure, but also for the emerging IoT.

Das et al. [15] reviewed several security scenarios for pervasive computing that are related with security and privacy of networked services used by mobile terminals. Ioannidis [16] envisaged a scenario where a hacker could take a phone number off-line, in such a way that every time when this number is called it responds with the message "The telephone number you called is not available on the Vodacom network". This is an example where L3 component is intruded, i.e. a non-authorized person has grabbed control over some portion of the system.

Straub and Heinemann [4] presented four security scenarios for the Internet of Things. *Scenario 1: The mobile salesman.* Security of wireless connections available for a driver on a road. *Scenario 2: Passive Collaboration in Opportunistic Networks.* Security of peer-to-peer information sharing between people in a collaborative network. *Scenario 3: Patient Monitoring.* Security and privacy of personal data about patients in a hospital. *Scenario 4: RFID-Based Warehouse Management.* Security of storage and tracking goods within a plant and beyond. These scenarios span several layers L1-L6, but not all.

Wright et al. [2] discussed four dark scenarios of ambient intelligence and ubiquitous computing, i.e. 1) AmI vulnerabilities in the life of a typical family moving through different environments. It introduces dark situations in the smart home, at work and during a lunch break in a park. 2) An exploited vulnerability in the traffic system causes an accident, raising many different problems related to both travel and health AmI systems. This is also an example, where a non-authorized person gets control over a portion of infrastructure down to actuators (L1) through some upper layers. 3) A data-aggregating company that becomes victim of theft of the personal data which it has compiled from AmI networks and which fuel its core business. The final theft happens at L5 or L6. The scenario draws attention to the digital divide between developed countries with AmI networks and developing countries that do not have such networks. It further brings stressed the fact that if personal data gathered from sensors and from other sources is stored at L5, privacy can be jeopardized, even if all lower layers function properly. 4) AmI risk society from the studios of a morning news program. It presents an action group against personalized profiling, the digital divide at a global scale and related to environmental concerns, the possible vulnerabilities of AmI-based traffic management systems and crowd control in an AmI environment.

Dlamini et al. [17] identified several scenarios of attacks in the case of the Internet of Things. Scenario 1: exploitation of vulnerability in home electronic stoves, as well as taking control of an entire suburb's compromised vulnerable stoves (botnet of stoves), covertly and simultaneously switching them to maximum power for four or more hours while everybody is at work. This is again a scenario where the control over actuators at L1 is obtained by an unauthorized person. In this case all other layers might work properly, but in general it might also be the case that there are some further vulnerabilities at higher levels that open up control channel to the actuators. Scenario 2: compromised fake appointments through a healthcare system resulting in deaths. The effect becomes visible at L6, but also other layers might contain the actual vulnerability. Scenario 3: targeted DoS attacks organized by companies. For example, a Telco company with few subscribers organizes a targeted DDoS attack to bring down a dominant Telco company and hence improve its revenue as people switch to use its services. In this case the target system might function properly throughout.

Poslad [18] presented a number of security threats for mobile devices, i.e. sender masquerader, unauthorized access, DoS, communication access device lost, stolen or damaged, network loss, execute viruses, loss of confidentiality, local data corruption, message corruption, repudiation of sent or received messages. Among these the stolen or lost device belongs to the physical threat scenarios at L1. It is possible also for various sensors.

The ICT-FORWARD project provided an understanding of emerging and future information security threats and adversaries [18-21]. Within this project a sophisticated classification of emerging ICT threats and a number of scenarios have been elaborated. The list of threats consists of 28 items that are stratified into three major groups based on their priority and impact. The most important threats are considered to be associated with mobile devices and social networks, as well as the threats due to parallelism and scale. Among the threats with medium priority are routing infrastructures, DoS attacks, false sensor data, sensors and RFID, wireless communication and next generation networks. Examples of low-priority attacks are malicious hardware and IPv6 and direct reachability of hosts, as well as online games. Along with the threats ten major scenarios have

been described, i.e. election fraud, crashing the stock market for fun and profit, industrial espionage, smart grid, oil spill, fabrication take-over, the politician's phone, mass benchmarking through social networks, attack against an electric power station, attack on a water power station. Especially the latter two are examples of control loss at some level L1-L6 that result in actuators that are controlled by malicious people.

The authors of [22] discussed a "worms in a cloud" -scenario. Carr [23, p.14] reviewed the evolution of cyber-attacks from 2000 until 2009 and made some projections for the next years. The issues are classified into three categories, i.e. 1) DDoS arsenals (SYN, ICMP, GET/POST, UDP, applications back-end, bad protocol, connection floods, browser malware, P2P, DNS spoofing), 2) motivations (revenge, extortion, industrial or competitive sabotage, political activism, terrorism, theft), and 3) emerging issues (cloud attacks, VOIP, IPTV, defense mobilization).

The architecture presented in Section 2 contains many portions that are common with existing architectures. Consequently, the threats are similar. Based on the above scenarios we can draw a conclusion that for the Internet of Things the following security issues are of importance: eavesdropping, man-in-the-middle and other similar attacks, jeopardizing the data confidentiality and integrity, and last but not least, grabbing control of some components to malicious and unauthorized persons. DoS are possible against various components, as well as intrusion into system components that store data. Along with those well-known issues there are a number of new scenarios discussed in the next section.

3.2 Threats at the lowest level; energy issues

Cole and Ranasinghe [24] identified a number of attacks associated with RFID. For example, 1) cloning refers to the duplication of security features, so that they are likely to pass as authentic during inspection. 2) obfuscation connotes the use of misleading protection technologies. 3) tag omission, i.e. the abdication of the security features by counterfeit producers even if the corresponding genuine articles are equipped with protective measures; relies on low inspection rates among many categories of goods. 4) removal-reapplication attacks refer to the application of genuine security features from (mostly discarded) genuine products to counterfeit articles. 5) DoS attacks may be defined as "any event that diminishes or eliminates a network's capacity to perform its expected function". MacManus [25] discussed a number of issues related to RFID from the viewpoint of customers of shops. RFID threats are all relevant in IoT architecture relying of RFIDs.

Authors of [6] discuss privacy aspects of smart energy meters and suggest an architecture for better privacy protection. The authors of [26] argue that user query privacy could be broken by a WSN owner. Client might need query privacy from the WSN owner and operators, and there might arise need to make user's queries anonymous or pseudonymous within the sensor network, so that the user ends up with the desired data but the remaining actors including the controller, processor or the potential adversary do not learn from the communication. This privacy-by-design process would help reduce the privacy concerns not only at sensor network level but also at higher architectural levels. This is an interesting case where the control of the infrastructure is divided (owner-user). This might be rather common in smart cities or bottom-up portions of the IoT.

Source location privacy is the other danger area associated with sensor network level (L1) of the IoT architecture. It means "not letting the adversary know which sensor node sends data to a sink (the base station)" [27, p.391]. The authors of [28] argue that even though the data is encrypted, an adversary still can be able to extract information, by simply observing and analyzing the traffic pattern, given the fact that transmission detection in WSN is easy. They analyze a situation where the attacker can reveal the location of a particular node by analysis of the traffic. Thus, if the sensor can be related with a person, his or her location is exposed.

Tamara Bonaci et al. [29] discussed threat model for a node capture attack, and presented a framework for threat analysis and network response strategies in case of attack.

A portion of the smart objects are energy-poor, running on finite battery power. One attack form against them is *energy extortion*, during which they are forced to communicate with the gateway or other nodes more frequently than normal. The queries might be legal as such ("what is the current temperature"), but they are issued maliciously often. A kind of energy extortion attack is *sleep deprivation torture attack* that is common for wireless sensor networks [30, 31]. Another attack form related with limited power components is *jamming*, i.e. using so strong distortion signal in the area where the smart objects are deployed that they cannot communicate with the neighbors, gateway, base station, or navigation satellites, even if they used their maximum transmission power.

Electromagnetic pulse (EMP) is an all-devastating method against unprotected electronics. It can be caused e.g. by nuclear detonation in the atmosphere (c.f. a neutron bomb). Such a detonation would destroy ICT infrastructure in a wide area on Earth. There exist now also devices that can be used to destroy electronics in targeted objects, like cars. Similar devices could be used against smart objects in a limited area. Large scale EMP is a military measure, but the limited attack might be used by terrorists or criminals.

It is known, that the exchange of security protocol messages and encryption of the transmitted data consume energy. A general question in the IoT context is, when and where in the architecture is there really a need to encrypt transmitted or stored data and what kind of security protocols are needed at different levels of the architecture. Further, what measures and mechanisms are exactly required from the privacy protection point of view. These issues are related with many technical, organizational, and regulatory issues and are for further study.

3.3 Emerging EU legislation for IoT

Data protection is a fundamental right in Europe, enshrined in the basic legislation. EU directive 95/46/EC [32] is currently the reference text at the EU level which deals with safeguards against automated processing of personal data and its free flow within member states. EU directive 2002/58/EC [33] establishes the data protection and privacy in the electronic communication sector. Mandated by these two directives, member states have made national level set of rules for addressing the issues of data protection and security. After the 9/11 terror attacks in USA and further attacks in UK and Spain, the latter directive was amended by 2006/24/EC [34] that requires operators to retain identity information emanating from the communication events. It has now (Aug. 2012) been implemented in the member states, except in Germany.

EU commission is striving at single set of rules across Europe, including "the right to be forgotten, explicit consent for data processing, control of user over his or her personal data, making of EU rules applicable to the companies operating outside from

EU". These and further rights are included into a new regulation proposal for data protection [35]. The commission has set a two-year timetable for the implementation of the proposal through the European parliamentary system. Once approved, it will replace EU Directive 95/46/EC and the data protection laws of EU member states.

The legislators want to give the users unlimited access and control over their personal data and, thus, the processors and operators are burdened with additional transparency and accountability.

The definition of personal data has been widened to include everything related to a natural person, including online and location data. *Individual profiling* by aggregating data gathered from heterogeneous sources has been prohibited. Acquisition of *'apt-in consent in advance'* with the right to withdraw it subsequently, and *erasure of personal data when required* are emphasized, and this demands that the middleware of the IoT should be capable of deleting personal data including the object descriptors and the URLs of sensor nodes/RFID tags relating to him or her as and when required or at the end of agreed term. The data visibility in between applications without first receiving an explicit consent of the data subjects seems not legal now, which in turn could result in emergence of less innovative applications over time. New ways of making data anonymous or pseudonymous where possible could be employed to mitigate these problems.

Within the purview of the current and proposed EU privacy legislations the sensors network level IoT architecture is generally prone to privacy breaches in many areas, including *'user query privacy' ,'location based privacy'* and *node capture attack* (cf. above).

Deployment of sensor networks at public spaces has its own perspective for privacy while taking in view the proposed EU regulation's concept of consent. According to M. Langheinrich [36] "users must be aware that they are being sensed ('notice'), users must be able to choose whether they are being sensed and be able to opt-out ('choice and consent'), and users must be able to remain anonymous ('anonymity and pseudonymity')". In this vein, the proposed EU regulation [35] bounds controllers and processors to notify data breaches within 24 hours' time, which would require efficient intrusion detection methods at all levels of IoT architectures.

4. CONCLUSIONS

We have discussed in this paper IoT architectures, especially from the security, privacy and trust point of view. We first present a tentative layered view on the architecture with six layers and then discuss how the IoT architecture might emerge and what actors can be at work at different layers to deploy the needed components. We argue that at the bottom layer that consists of smart objects, including sensors and actuators, individuals can also deploy them, not only companies or authorities. The same holds for WLANs or similar networking technologies. This requires that the technology is easy to manage and control. Should it be self-configuring or better not? We then analyze known and new security and privacy threats at different levels based on a literature review. One insight emerging from this analysis is that it is important to understand the management domains or spheres of control towards IoT architectures. Who controls what at which level? How this control is technically facilitated? What policies need to be enforced? In this vein we review the emerging EU legislation in the privacy and security area. It urges to take into account the privacy already while IoT systems are designed. The new EU regulation requires that an individual should be able to control data about him or she at all levels of the architecture. Many issues remain for further study. How is this kind of privacy control or a more general control technically supported? What are the acceptable risk levels? Energy aspects of security, privacy and trust also require more research. They are closely related with energy consumption of the entire future network infrastructure i.e. future Internet.

5. ACKNOWLEDGMENTS

The research was conducted in the Internet of Things program of TiViT (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT), funded by Tekes.

6. REFERENCES

[1] Weiser, M. 1991. The Computer for the 21st century, *Scientific American* **265**(3): 94-104.

[2] Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E. and Punie, Y. (Eds). 2008. *Safeguards in a World of Ambient Intelligence*, Springer Verlag.

[3] Kopetz, H. 2011. Internet of Things. Ch 13. *In Real-Time Systems: Design Principles for Distributed Embedded Applications.* 2nd Edition. Springer Verlag 2011, 307-323. DOI 10.1007/978-1-4419-8237-7_13.

[4] Straub, T. and Heinemann, A. 2008. Security for ubiquitous computing, In M. Mühlhäuser and I. Gurevych, *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises*, IGI Global, pp. 337-362.

[5] Wu, G., Talwar, S., Johnsson, K., Himayat, N., and Johnson, K.D. 2011. Recent Progress in Machine-To-Machine Communications, *IEEE Communication Magazine*. Apr. 2011, 36-43.

[6] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D. 2010. Private Memoirs of a Smart Meter. *Proc. of BuildSys* 2010 61-66. DOI:10.1145/1878431.1878446.

[7] Atzori, L. Iera, A., and Morabito, G., The Internet of Things: A survey, Computer Networks 54 (2010) 2787–2805.

[8] Guinard, G., Fischer, M. Trifa, V. 2010. Sharing using social networks in a composable web of things. In *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 702-707. IEEE CS. DOI=10.1109/PERCOMW.2010.5470524.

[9] Mattern, F. and Floerkemeier, C. 2010. From the Internet of Computers to the Internet of Things. In K. Sachs, I. Petrov, and P. Guerrero (Eds.): *Buchmann Festschrift*, LNCS 6462, 242–259, 2010. Springer-Verlag 2010.

[10] Botts, M., Percivaal, G., Reed, C., Davidson, J., Nittel, S., Labrinidis, A., Stefanidis, A. 2008. *GeoSensor Networks*, Springer Berlin / Heidelberg.

[11] IoT-A, Internet of Things –Architecture. Retrieved on June 20, 2012 from http://www.iot-a.eu/public/front-page.

[12] ISO/IEC 2012. *Information Technology – Telecommunication and Information exchange between systems*. International Standard, Final Draft, ISO/IEC 29180.

[13] Stuckman, P., Zimmerman, R. 2009. European Research on Future Internet Design. IEEE Wireless Communications Oct. 2009, 14-22.

[14] Stajano, F. 2010. Security Issues in Ubiquitous Computing. In H. Nakashima, H. Aghajan and J.C. Augusto (Eds).

Handbook of Ambient Intelligence and Smart Environments, Springer, pp. 281-314.

[15] Das, S.K., Agah, A. and Kumar, M. 2008. Security in Pervasive Computing, In H. Nemati (ed). *Information Security and Ethics: Concepts, Methodologies, Tools and Applications*, IGI Global, pp. 3627-3643.

[16] Ioannidis, S. 2008. Security and Privacy in a Networked and Mobile World. Retrieved on June 30, 2012 from http://www.ict-forward.eu/media/publications/fidis2008-presentation-forward.pdf.

[17] Dlamini, M.T., Eloff, M.M. and Eloff, J.H.P. 2009. Internet of things: emerging and future scenarios from an information security perspective. In *Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2009)*, Swaziland, 30 August-2 September 2009, pp. 6.

[18] Poslad, S. 2009. *Ubiquitous Computing: Smart Devices, Environments and Interactions*, John Wiley and Sons, pp. 386-392.

[19] Bos, H., Ioannidis, S., Jonssom, E., Kirda, E. and Kruegel, C. 2008. Future Threats to Future Trust, In *Proceedings of the Future Trust in Computing Conference*, Berlin, Germany: 2008, available at http://www.ics.forth.gr/dcs/Activities/papers/fot.pdf.

[20] Kruegel, C. and Ioannidis, S. 2009. On Looking FORWARD, ERCIM NEWS, vol. 76, Jan. 2009, pp. 62 - 63.

[21] Markatos, E., Ioannidis, S. and Kruegel, C. 2008. From the World of Security - A Word from the Experts Tracing the Changing Nature of Cyber-attacks, ENISA Quartely Review, vol. 4, p. 4.

[22] Biedermann, S., Katzenbeisser, S. 2011. Detecting computer worms in the cloud, In J. Camenish and D. Kesdogan (Eds.), *Open Problems in Network Security*, Lecture Notes in Computer Science 7039, 43-54.

[23] Carr. J. 2012. *Inside Cyber Warfare*. O'Reilly Media, Inc., Sebastopol, Calif. USA.

[24] Cole, P.H. and Ranasinghe, D.C. (Eds*). 2007. Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting*, Springer Verlag.

[25] MacManus, R. 2009. Should Consumers Fear the Internet of Things? Retrieved On June 7, 2012 fromhttp://www.readwriteweb.com/archives/rfid_fear.php.

[26] Carbunar, B. Yu, Y., Shi, W., Pearce, M, and Vasudevan, V. 2010. Query privacy in wireless sensor networks. *ACM Transactions on Sensor Networks*, Vol. 6, No. 2, Article 14. DOI=http://doi.acm.org/10.1145/1689239.1689244.

[27] Bao, F., Li, H. and Wang, G. 2009. Information Security Practice and Experience. *In Proceedings of the 5th International Conference IPSEC 2009*, Xi'an, China, 13-15.

[28] Ouyang, Y., Le, Z., Liu, D., Ford, J., and Makedon, F.2008. Source Location Privacy against Laptop-Class attacks in sensor networks. In *Proceedings of the 4th international conference on Security and privacy in communication networks*, 5, (Istanbul, 2008), ACM New York, available at http://dl.acm.org/citation.cfm?doid=1460877.1460884.

[29] Bonaci, T., Bushnell, L., Poovendran, R .2010. Node Capture Attacks in Wireless Sensor Networks: A system theoretic approach, *In Proceedings of Decision & Control (CDC), 2010, 49th IEEE conference on Digital Object Identifier*, Atlanta, GA, 6765-6772, DOI: 10.1109/CDC.2010.5717499.

[30] Martins, D. and Guyennet, H. 2010. Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. In *Proceedings of the 13th International Conference on Network-Based Information Systems*, IEEE Computer Society Press.

[31] Raazi, S.M.K., Pervez, Z. and Lee, S. 2011. Key Management Schemes of Wireless Sensor Networks: A Survey, In A.K. Pathan (ed). *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, CRC Press, pp. 297-316.

[32] European Parliament. 1995. Directive 95/46/EC on the *'Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data'*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[33] European Parliament. 2002. Directive 2002/58/*EC* on '*privacy and electronic communications*', available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF.

[34] European Parliament and the Council. 2006. Directive 2006/24/EC *'for amending Directive 2002/58/EC',* available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[35] European Commission. 2012. *Proposal for European Parliament and the Council (General Data Protection Regulation)*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[36] Langheinrich, M. 2001. Privacy by Design - Principles of Privacy-aware Ubiquitous Systems, In *Proceedings of the 3rd International Conference on Ubiquitous Computing*, Springer, pp. 273–291.