IPICS 2011
Intensive Programme on Information
and Communication Security

INTENSIVE PROGRAM ON INFORMATION COMMUNICATION SECURITY
IPICS 2011

Security in the Internet of Things

Author:
Ivan Gudymenko,
TU Dresden, Germany
ivan.gudymenko@gmail.com

Supervisor:
Michael Hutter
TU Graz, Austria
michael.hutter@iaik.tugraz.at

Abstract

The Internet of Things (IoT) is a very promising paradigm which can be seen as the process of integrating intelligence into the surrounding artefacts with their subsequent interconnection via the Internet in order to provide (possible new) services to the user. Despite bringing in undeniable benefits, it raises serious security and privacy concerns. This essay is devoted to the security peculiarities of the IoT domain. In order to address this issue, a general notion of IoT is briefly described and its technological cornerstones are discussed. The focus is made on the peculiarities of security threats in the resource-constrained IoT environment. The essay surveys the related work in the security area of IoT, discusses the proposed solutions and summarizes the inherent security vulnerabilities of IoT. The importance of taking privacy issues into account is outlined as well.

Introduction

With the current pace of technological progress, computing and telecommunications are experiencing substantial growth, which constantly introduces innovations, gives boost to new technologies and therefore enables implementation of the concepts, which were considered science fiction just a few decades ago.

The ever growing demand for mobility has stimulated the development of mobile telecommunications together with lightweight computing leading to the fact that, for example, mobile phones have become smaller and lighter at the same time possessing computational power and connectivity by far outweighing the ones of a desktop computer in the 90s.

However, that is by no means the end of the evolution process. A new era of intelligence-enabled environment where the surrounding artefacts are capable of performing processing and communication procedures to our benefit is steadily approaching. This gives birth to a number of qualitatively new paradigms and novel concepts, and marks the advent of so-called Ubiquitous Computing (UbiComp), which was envisioned by Marc Weiser back in 1991 in his seminal paper [1] and described as the process of "integrating computers seamlessly into the world at large" that allows them "to vanish into the background". This concept was further elaborated by Marc Stajano and referred to as "[...] a scenario in which computing is *omnipresent*, and particularly in which devices that do not look like computers are endowed with computing capabilities." [2].

In case such intelligence-enabled artefacts ("the things") are ubiquitously networked through the Internet, a related paradigm arises, which is referred to as "The Internet of Things" (IoT) and is regarded to be coined by Kevin Ashton in 1999 [3].

This essay is devoted to IoT, namely to the security challenges, which arise in IoT environments; considers inherent threats and possible solutions. At the beginning, the general notion of IoT is discussed together with its technological enablers. This forms the necessary basis for approaching the security implications of IoT, which are to a large extent determined by the peculiar features of IoT, such as the ubiquitous distribution of resource-constrained end devices, communication over the wireless interface, etc. The focus is made on the specific security vulnerabilities of IoT, the respective threats and possible countermeasures. Since IoT additionally raises serious concerns over individual privacy, which is closely related to security[1], this issue is shortly discussed as well.

The essay is organized as follows. Section 1 discusses the general concept of IoT highlighting different views of this notion. In Section 2, the technological cornerstones of IoT are discussed. Security implications of this domain are considered together with the specific attacks and possible countermeasures in Section 3. Section 4 briefly outlines the reasons for carefully considering privacy in IoT.

1 The IoT Paradigm

The concept of IoT is intuitively understood as interconnecting smart things via the Internet in order to provide certain services to the user. However, in order to explore this paradigm in more detail and to discuss inherent challenges to security in IoT environments, a deeper understanding of this notion is required. Therefore, this section highlights various definitions of this notion and discusses several views of IoT.

The authors of [4] describe the basic idea of IoT as "[...] the pervasive presence around us of a variety of things or objects [...] which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals". The difference between "things" and "objects" is however quite vague. On the one hand, "things" represent the simplest class of uniquely identifiable artefacts which can be addressed (mainly via the wireless interface). This is quite often associated with RFID (Radio Frequency Identification) tags attached to the various parts of surrounding environment that are worth being addressed and scanned. On the other hand, the same "things" can be described as simple nodes of a wireless network that are not only able to answer queries from a reading device (a "reader" in RFID networks) but can also *initiate* communication, i.e. act as peers in P2P networks.

Evan Welbourne et al. in [5] outline IoT as "[...] a vision in which the Internet extends into our everyday lives through a wireless network of uniquely identifiable objects." The authors specifically consider an RFID system as the enabler of IoT since mass-produced RFID end devices (the tags) can be attached or integrated almost to every artefact equipping it with a certain degree of intelligence. This allows the artefacts data, which was previously "unknown" to the Web and inaccessible through the Internet, to be linked to and consequently used for various purposes, ranging from business and production processes to personal and social interaction.

The authors of [4] highlight yet another facet of IoT: " [...] a world where things can automatically communicate to computers and each other providing services to the benefit of the human kind". This raises a question of a so-called machine-to-machine communication (M2M)[2] since in this case the things are able to communicate not only to computers but also to each other. It leads in turn to the necessity of considering M2M security peculiarities in the environment where communication can happen without human intervention and be only infrequently interfered by humans for management and device configuration purposes.

Another definition of IoT found in [4] is: "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts". Taking the issues of M2M communication into account, this consequently determines the need to specifically consider the implications of so-called M2M privacy, which arises from the smart things "having identities" and possessing their own privacy derived from that of an individual [8].

Furthermore, IoT can be seen as "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [4]. In this case, it is underlined that the communication protocols should be standardized, which greatly facilitates the process of worldwide adoption and implementation of IoT and therefore encourages the process of moving from numerous local proprietary solutions to a *ubiquitous* ones with a qualitatively new level of interoperability.

[1] Security is an inalienable part of any mature privacy management solution (consider technical privacy enforcement, which is performed utilizing such security-related mechanisms as encryption and anonymization techniques, access control, etc.).

[2] See, for example, [6, 7].

2 The Technological Cornerstones of IoT

Technology is a decisive factor for enabling the realization of the IoT concept. According to [4], the following issues are going to build up IoT: the unique addressing schemes for objects, their representation, and storage of the exchanged information. Networking is surely going to be one of the main challenges as well. It is very likely that IPv6, namely the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN[1]), is going to be the main candidate for interconnecting intelligent things since it has a potential of leveraging the two basic concepts which brought success to the conventional Internet, namely packet switching and the "end-to-end" principle. The latter suggests that "[...] the behavior of the network should be determined by *what* is connected to it rather than by its internal construction [...]", and given the heterogeneity of end devices of IoT should help to "solve the problem of connecting heterogeneous devices rather than heterogeneous networks" [11].

According to [9], the adaptation between full IPv6 and the specific 6LowPAN format can be performed by so-called edge routers, which are situated at the edge of 6LowPAN islands delimiting the constrained IoT environment from the conventional Internet. This kind of transformation is described by the authors as transparent to the conventional IPv6 protocol stack, efficient and stateless in both directions. This greatly facilitates interoperability, optimization and management (including security management) of end devices.

From the communication medium point of view, the technological solutions supporting wireless communications are going to be predominant in this context as it is virtually impossible to provide for true ubiquity and unobtrusiveness using cable interconnection. Moreover, the possible spectrum of potential technologies will be concentrated in the area of lightweight communications since end devices (i.e. "things") are extremely resource-constrained in terms of computing, energy, and memory. That provides for interconnecting such resource-constrained devices, which eventually comprise the front-end of an IoT system as opposed to the back-end maintaining the support of background processes like heavy computation, global interconnection (via the Internet), billing, etc.

Among the possible candidates, Radio Frequency Identification (RFID) technology is fairly regarded as one of the main enablers of IoT. It deserves special attention for several reasons. RFID end devices (RFID tags) can be mass-produced and therefore are relatively cheap (an order of several cents). RFID technology has existed for several decades and has become established and mature in such fields as logistics, supply chain management, retail industry, etc. The inherent pervasiveness of RFID, the small size and low cost of end devices make it one of the main technological enablers of IoT for the nearest future. The authors of [12], for example, presented their approach to the realization of IoT using an RFID communication interface bridged with the IPv6 protocol, which is performed by a reader (the latter effectively acts as a gateway). In this case, an RFID reader acts as a "translator" from the IPv6 to a tag-specific communication interface. In order to establish a connection between an IPv6 device[2] ("a corresponding node" in [12]) and a specific RFID tag, the following is done: the corresponding node sends a message with the IP address of the tag[3]. The message is delivered to the reader in the interrogation zone of which the tag is currently situated. The reader performs mapping of the IP address of the destination (i.e. the tag's IP address) to the specific tag identifier, "translates" the message into a set of RFID specific commands, understandable by the tag, and sends the message to it. The answers of the tag undergo the inverse procedure and are sent to the corresponding node. Therefore, the reader acts as a router for the tags in its service area and the complexity of the system is shifted from resource-constrained tags to the corresponding reader (for more details on routing, see [12]). Figure 1 depicts the idea.

The communication line between the reader and the tag is "not secured in a standard way" [12]. The reason for this is that a well-established IPsec protocol cannot be applied because the reader constantly performs the translation of the messages and should not be trusted. Therefore, a new security layer between the corresponding node and the target RFID tag is suggested in [12]. According to this concept, the tag and the corresponding node have to agree on a security suite to build up a secure connection. The reader, hence, solely passes the content of the messages and can only disturb but not compromise the end-to-end connection security. Security suits in this case define the security mechanism used (e.g. encryption or authentication) and specify the particular requirements for a tag, such as the ability to perform AES (Advanced Encryption Standard) or SHA-1 (the Secure Hash Algorithm).

In case RFID tags are further equipped with sensors, the opportunity of communicating the sensed information to the ambient readers arises (see the description of the Wireless Identification and Sensing

[1] For more details see, for instance, [9, 10].

[2] An IPv6 device can be any computing device supporting IPv6, e.g. a desktop computer.

[3] Tag items are assumed to be mobile and are expected to move through different reader fields and establish connection to the corresponding reader via their standard RFID communication protocol. That is why, Mobile IPv6 (MIPv6) is used for message routing from the corresponding node to the respective reader.

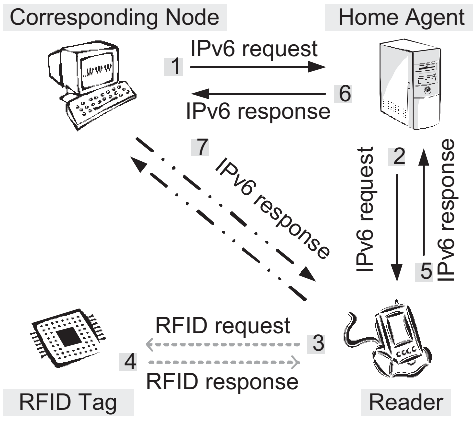

Figure 1: Communication between the corresponding node and the RFID tag. Taken from [12].

Platform (WISP) project in [13]). This enhances the capabilities of the IoT RFID-based system and enables the introduction of new services.

Most of the wireless communication between end devices in the IoT environments is going to have intermittent nature and take place over unreliable channels. This happens due to the high level of interference from other radio devices situated in close proximity to IoT artefacts and is aggravated by the fact that radio transmission is performed for the most part in the unlicensed frequency band, where the presence of other transceivers is even higher.

In this context, wireless personal[1] area networks (WPAN) may be of interest as they consider low-power communication for resource-constrained devices. For instance, IEEE 802.15.4 standard introduces a radio technology for low-power, low-data-rate applications and ”is intended to serve a set of industrial, residential, and medical applications with low power consumption and cost requirements” [14]. The standard specifies the two lower layers of the OSI[2] Reference model: the physical layer and media access control (MAC), and provides for a maximum data rate of 0.25 Mbit/s and range up to 10 meters [14]. According to [16], this standard is widely used and many companies are manufacturing IEEE 802.15.4-compliant devices. It has become a basis for a number of low-power radio stacks, such as ZigBee[3], WirelessHART[4] and 6LoWPAN [9, 10], due to its wide adoption and ubiquity. In particular, the IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) is the one to deserve special attention as it enables the use of IPv6 in low-power, low-bandwidth wireless networks with constrained processing capabilities. This technology has a very rich potential because, similarly to the conventional Internet, it should provide for interoperability[5], scalability, and reliability in such networks.

When it comes to widespread adoption and interoperability, a family of well-established 802.11 standards can be considered[6]. Whereas it is a perfect candidate for personal computers, smart phones and other handheld devices, a relatively high power consumption has prevented it from adoption into the world of embedded communication. However, the authors of [16] claim that the low-power versions of this popular standard have emerged recently thus paving the way for its integration into the environment of resource-constrained devices. For instance, in [17], it was mentioned that there already exist Wi-Fi modules which ”[...] can operate in a power-efficient fashion, and achieve multi-year battery life [...]”. This is achieved through the minimization of power consumption when data is not being transferred (in sleep mode) and by adding a set of flexible low-power states that is not available in existing conventional 802.11 modules.

Another wireless technology which can be seen as the enabler of IoT is Bluetooth, particularly Bluetooth low energy (BT-LE), which is a part of Bluetooth v4.0 Specification [18]. It introduces the entire communication stack and according to [19], there is a number of chip vendors who are already producing BT-LE chips, e.g. Nordic, Texas Instruments, CSR, Broadcomm. The authors claim as well that most of the emerging mobile phones are going to be equipped with low-energy Bluetooth technology very soon,

[1] The term ”personal” is considered to be outdated because this type of networks has already been used as public communication technology as well.

[2] Open Systems Interconnection, see for instance [15].

[3] ZigBee® Alliance, http://www.zigbee.org/Home.aspx

[4] Wireless HART technology, http://www.hartcomm.org/protocol/wihart/wireless_technology.html

[5] A lot of communication solutions in this area are proprietary, which greatly impedes the process of interconnecting them into a single network.

[6] IEEE Standards Association, 802.11: Wireless LANs, http://standards.ieee.org/about/get/802/802.11.html

which is likely to provide for a sufficient basis to make it truly ubiquitous.

In literature, even the opportunity of interconnecting smart devices over the existing power line infrastructure is mentioned (see, for example, [16]). Power Line Communications (PLC) can enable for pervasive interconnection of electrical devices and have a benefit of providing the communicating devices with constant power supply. However, the authors of [16] claim that such solutions are domain-restricted because the modulated data signal is not able to traverse the electrical voltage transformers outside the electrical domain. Therefore, the possibility of inter-domain communication is largely limited. Moreover, interference levels in PLC channels are very high, which further aggravates the problem of using this type of communication for IoT.

Figure 2 depicts the most relevant communication technologies for IoT[1] with respect to the IP layering scheme[2].

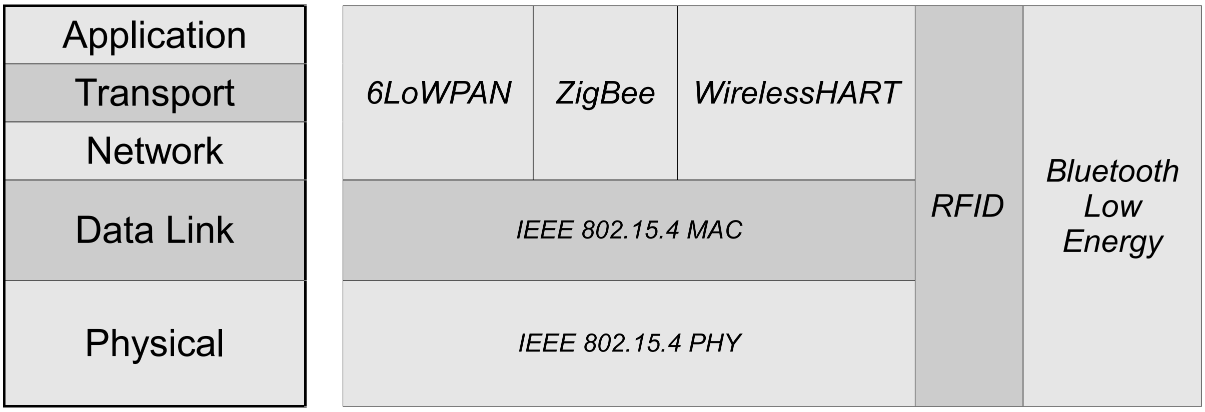

Figure 2: The most promising communication technologies for IoT and the IP stack layering scheme. Taken from [20].

Remark: RFID in this case implies not only the underlying physical principles of tag–reader communication but also readers interconnection via the backbone network, i.e. an RFID system in general (including the back-end).

3 Security Implications of IoT

IoT is going to introduce qualitatively new challenges to security. According to [4], the following issues determine particular security vulnerabilities of IoT:

1. Pervasive distribution of end devices.
2. Wireless communication.
3. Constrained resources.

3.1 Pervasive Distribution of End Devices

Given the pervasive distribution of end devices (e.g. mass produced RFID tags), it is hardly possible to physically isolate the components of the IoT network from the possible attackers and restrict the physical access to them. That in turn endangers the integrity and confidentiality of information stored on end devices and paves the way to availability violation[3].

Having physical access to end devices enables an adversary to perform so-called implementation attacks targeted on obtaining the cipher keys[4] residing in their memory. These attacks fall into several categories [20]:

- Side-channel attacks (timing analysis, power analysis, electromagnetic analysis, or acoustic attacks)

[1] The technologies depicted in Figure 2 are relevant for UbiComp as well (see Introduction).

[2] IP layering is provided for comparison purposes to visually represent the approximate position of each technology with regard to the classic IP layering scheme.

[3] Consider an example of shielding, for instance, an RFID tag by wrapping it into aluminium foil or simply destroying its antenna, which renders it inoperable and consequently prevents a reader from getting response from the compromised tag.

[4] Cipher keys are usually utilized for encryption and authentication of information transmitted over the wireless interface (in order to achieve, for example, confidentiality, integrity, etc.).

- Fault analysis;
- Reverse engineering.

Side-channel Attacks

There are several types of side-channel attacks [21]:

1. *Timing analysis.* Timing behavior of cryptographic implementations can leak information about the secret key. That is: the decryption time can be correlated to the values of the input ciphertext and reveal the key[1] if no special countermeasures have been undertaken.
2. *Power analysis*:
   - Simple power analysis. Secret key extraction by visual inspection of one or a few power-consumption traces produced during the execution of cryptographic procedures. See [22] for details.
   - Differential power analysis. Targeted at an intermediate value of the cryptographic algorithm that depends on the secret key using statistical analysis. More on this type of attacks can be found in [23].
3. *Electromagnetic analysis.* This kind of side-channel attack exploits correlations between secret data and variations in power radiations of electromagnetic field emitted by cryptographic devices [24]. According to [21], it allows attacks from a distance (far-field measurements).
4. *Acoustic attacks* [25]. Similarly to power analysis, the secret key can be gained through analysis of acoustic oscillations made by hardware while performing cryptographic operations. For more details, see [25].

According to [21], randomizing techniques or masking can be used to remove the dependences between the actual cryptographic operations and the revealing factor (power consumption, electromagnetic emissions, etc.).

Fault Analysis

Fault analysis is based on the principle of fault induction into implementations of cryptographic algorithms in order to reveal internal states of the latter and consequently deduce the key. According to [21], there exist several types of fault-analysis attacks:

1. *Non-invasive.* Package encapsulating the circuitry is left untouched and only working conditions are modified (e.g. high temperature, exposure of an RFID tag to a strong electromagnetic field, etc.)
2. *Semi-invasive.* Involves decapsulation of an RFID package, i.e. physically opening it and performing, for example, optical fault injection.
3. *Invasive.* This type of fault analysis implies establishing electrical contact to the chip with its modification.

The possible countermeasures are shielding (passive[2] or active[3]) and redundant computation with final parity check [21].

Reverse Engineering

Sometimes proprietary solutions to a large extent rely on the secrecy of the utilized cryptographic algorithms (so-called "security by obscurity"). However, according to [26], "any algorithm given to users in form of hardware can be disclosed even when no software implementation exists and black-box analysis is infeasible". Reverse engineering implies reconstructing the key by using a combination of circuitry image analysis and protocol analysis. An example of a successful attack can be breaking the proprietary CRYPTO-1 cipher used for transport ticketing (like the one in Amsterdam, London, Boston, Los Angeles, etc.) and access control [27, 21]. The key can be revealed within 0.1 seconds using an algebraic attack presented in [28].

[1] For example, square and multiply operation takes more time than the multiply one, which can be associated with 1 and 0 values of the utilized key respectively.

[2] An additional protective surface on top of the circuitry.

[3] Integration of sensors to detect the attempts of intrusion and act accordingly, e.g. reset the chip's configuration, delete sensitive data, etc.

3.2 Wireless Communication

A wireless nature of communication greatly facilitates eavesdropping and paves the way to a number of other attacks on wireless interface, which in case of RFID systems are the following [20]:

- Jamming (interruption of the communication between the reader and the tag; affects availability);
- Extension of the reading range beyond the norms defined in the respective standard (in order to covertly skim a remote tag; affects confidentiality);
- DoS attack using the blocker tags (preventing the anticollision algorithm from working properly by introducing a so-called blocker tag, which simulates collision[1]; affects availability);
- Relay attack (an undetected use of a remote tag in order to simulate the fact that it is situated in the proximity of a reader[2]; affects confidentiality and integrity).

The possible countermeasures in this case would be the utilization of encryption (against eavesdropping) and authentication (against, for example, relay attacks).

It is, however, extremely difficult to provide for protection against jamming attacks. Klaus Finkenzeller, for example, states that for the RFID domain there are practically no countermeasures available[3].

3.3 Constrained Resources

Last but not least, constrained computational and energy resources (especially in case of passive devices, e.g. passive RFID tags) do not allow for utilization of complex security mechanisms, which can ensure confidentiality and integrity of data residing in end devices and transmitted over an inherently insecure wireless channel. However, lightweight implementations of cryptographic algorithms can be utilized in this case. For example, in [30, 31], it was shown that AES (Advanced Encryption Standard [32]) and ECC (Elliptic Curve Cryptography [33]) are already feasible for RFID and it is just a matter of costs whether to implement cryptographic algorithms in RFID tags. Moreover, there exists a set of lightweight cryptographic algorithms specifically designed for the domain of resource-constrained devices, such as PRESENT, HIGHT, TEA, etc. (see [34] for more details).

4 Privacy Concerns in the IoT

Along with numerous benefits, which IoT is going to enable, serious concerns over individual privacy arise. The authors of [8] claim that the reason for this is that thanks to the omnipresent intelligence-integrated artefacts, the process of sampling and distribution of information in IoT can be practically carried out anywhere. Moreover, ubiquitous connectivity through Internet access aggravates the problem because, unless special mechanisms are considered (encryption, authentication, etc.), personal information might become worldwide available.

It is important to realize that IoT is going to pose a qualitatively new privacy challenge, which, if not properly addressed and handled, may greatly impede the adoption of IoT systems. For more information on this issue, see, for example, [8].

Conclusion

In this essay, the security peculiarities of IoT were discussed. In order to effectively address this issue, the general notion of IoT was explored from several perspectives together with the possible spectrum of technological solutions, which can be regarded as IoT enablers. Last but not least, privacy implications of IoT should be specifically considered along with security issues.

Summarizing, it can be stated that the IoT paradigm is going to change the perception of computing and networking bringing in novel services, which are going to have substantial influence on our everyday life. It is, however, of high importance to carefully consider security and privacy along with the issues of

[1] The simulation of collision depends on the anticollision algorithm used. According to [29], there are two established anticollision algorithms in RFID systems: the binary search tree algorithm and the slotted ALOHA. In the first case, the blocker tag misleads the reader by simultaneously sending "0" and "1", thus simulating a collision at each bit location of its serial number. In case of ALOHA, the blocker tag keeps sending its serial number in each available time slot and therefore preventing the other tags from answering the reader's query.

[2] Relay attack can be used to attack the tag carrying out the transactions that are subject to charges (e.g. RFID tickets, RFID-enabled paying cards, etc.).

[3] Klaus Finkenzeller. Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities, http://www.rfid-handbook.de/downloads/Finkenzeller_Systech-Bremen-2009_v1.0.pdf

direct functionality of IoT systems in order to prevent the scenario of pervasive surveillance described by George Orwell in his novel "1984" [35].

References

[1] Mark Weiser. The Computer for the 21st Century. *Scientific American*, February 1991.

[2] Frank Stajano. *Security for Ubiquitous Computing.* John Wiley & Sons, LTD, 2002.

[3] Kevin Ashton. That "Internet of Things" Thing. http://www.rfidjournal.com/article/view/4986, June 2009. Accessed on 01.11.2011.

[4] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[5] Evan Welbourne, Leilani Battle, Garret Cole, Kayla Gould, Kyle Rector, Samuel Raymer, Magdalena Balazinska, and Gaetano Borriello. Building the internet of things using rfid: The rfid ecosystem experience. *IEEE Internet Computing*, 13:48–55, 2009.

[6] Geng Wu, S. Talwar, K. Johnsson, N. Himayat, and K.D. Johnson. M2M: From Mobile to Embedded Internet. *Communications Magazine, IEEE*, 49(4):36 –43, April 2011.

[7] Inhyok Cha, Y. Shah, A.U. Schmidt, A. Leicher, and M.V. Meyerstein. Trust in M2M Communication. *Vehicular Technology Magazine, IEEE*, 4(3):69 –75, sept. 2009.

[8] Ivan Gudymenko, Katrin Borcea-Pfitzmann, and Katja Tietze. Privacy Implications of IoT. In *Workshop on Privacy, Trust and Interaction in the Internet of Things*, November 2011. Accepted.

[9] Carsten Bormann Zach Shelby. *6LoWPAN: The Wireless Embedded Internet.* Wiley, 2009.

[10] J.W. Hui and D.E. Culler. Extending IP to Low-Power, Wireless Personal Area Networks. *Internet Computing, IEEE*, 12(4):37 –45, july-aug. 2008.

[11] Neil Gershenfeld, Rafi Krikorian, and Danny Cohen. The Internet of Things. *Scientific American*, 10:76–81, Oct 2004.

[12] S. Dominikus, M. Aigner, and S. Kraxberger. Passive RFID Technology for the Internet of Things. In *Internet Technology and Secured Transactions (ICITST)*, pages 1–8, November 2010.

[13] M. Philipose, J.R. Smith, B. Jiang, A. Mamishev, Sumit Roy, and K. Sundara-Rajan. Battery-free Wireless Identification and Sensing. *Pervasive Computing, IEEE*, 4(1):37 – 45, 2005.

[14] J.A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile. IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks. *Network, IEEE*, 15(5):12 –19, sep/oct 2001.

[15] J.D. Day and H. Zimmermann. The OSI reference model. *Proceedings of the IEEE*, 71(12):1334 – 1340, dec. 1983.

[16] Jean-Philippe Vasseur and Adam Dunkels. *Interconnecting Smart Objects with IP.* Morgan Kaufmann, 2010.

[17] Daniel M. Dobkin and Bernard Aboussouan. Low Power Wi-Fi$^{\mathrm{TM}}$ (IEE 802.11) for IP Smart Objects. http://www.gainspan.com/docs2/Low_Power_Wi-Fi_for_Smart_IP_Objects_WP_cmp.pdf, 2009. Whitepaper, GainSpan Corporation.

[18] Bluethooth SIG. Specification of the Bluetooth technology. Covered Core Package version: 4.0, June 2010.

[19] Markus Isomki et al. Connecting BT-LE sensors to the Internet using IPv6. In *Interconnecting Smart Objects with the Internet Workshop*, March 2011.

[20] Ivan Gudymenko. Protection of the User's Privacy in Ubiquitous RFID Systems, 2011. Master thesis, in progress.

[21] Michael Hutter. RFID Security, 2011. IPICS-2011 summer school.

[22] Siddika Berna Örs, Maria Elisabeth Oswald, and Bart Preneel. Power-Analysis Attacks on an FPGA–First Experimental Results. In Springer, editor, *Cryptographic Hardware and Embedded Systems – CHES 2003* , volume 2779 of *Lecture Notes in Computer Science*, pages 35 – 50. Springer Verlag, 2003.

[23] Elisabeth Oswald Stefan Mangard and Thomas Popp. *Power Analysis Attacks Revealing the Secrets of Smart Cards.* Springer, 2007.

[24] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '01, pages 251–261, London, UK, 2001. Springer-Verlag.

[25] Adi Shamir and Eran Tromer. Acoustic cryptanalysis: on nosy people and noisy machines. http://www.cs.tau.ac.il/~tromer/acoustic/, 2004. Preliminary proof-of-concept presentation.

[26] Karsten Nohl, David Evans, Starbug Starbug, and Henryk Plötz. Reverse-engineering a cryptographic RFID tag. In *Proceedings of the 17th conference on Security symposium*, pages 185–193, Berkeley, CA, USA, 2008. USENIX Association.

[27] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, CARDIS '08, pages 267–282, Berlin, Heidelberg, 2008. Springer-Verlag.

[28] Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime. Cryptology ePrint Archive, Report 2009/137, 2009. http://eprint.iacr.org/.

[29] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication.* Third Edition. A John Wiley and Sons, Ltd., 2010.

[30] Michael Hutter, Martin Feldhofer, and Johannes Wolkerstorfer. A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines. In *WISTP*, pages 144–159, 2011.

[31] Michael Hutter, Marc Joye, and Yannick Sierra. Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation. In *AFRICACRYPT*, pages 170–187, 2011.

[32] NIST. Specification for the Advanced Encryption Standard (AES). FIPS 197., November 2001.

[33] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):pp. 203–209, 1987.

[34] T. Eisenbarth and S. Kumar. A Survey of Lightweight-Cryptography Implementations. *Design Test of Computers, IEEE*, 24(6):522 –533, nov.-dec. 2007.

[35] George Orwell. *1984*. Signet Classic, 1950.