Electronic Communications of the EASST
Volume 17 (2009)

Workshops der Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen 2009 (WowKiVS 2009)

Security and Privacy Challenges in the Internet of Things

Christoph P. Mayer

12 pages

Guest Editors: M. Wagner, D. Hogrefe, K. Geihs, K. David
Managing Editors: Tiziana Margaria, Julia Padberg, Gabriele Taentzer
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Security and Privacy Challenges in the Internet of Things

Christoph P. Mayer

http://www.tm.uka.de/itm
Institute of Telematics
Universität Karlsruhe (TH), Germany

Abstract: The future Internet of Things as an intelligent collaboration of miniaturized sensors poses new challenges to security and end-user privacy. The ITU has identified that the protection of data and privacy of users is one of the key challenges in the Internet of Things [Int05]: lack of confidence about privacy will result in decreased adoption among users and therefore is one of the driving factors in the success of the Internet of Things. This paper gives an overview, categorization, and analysis of security and privacy challenges in the Internet of Things.

Keywords: Global Sensor Networks, Security, Privacy, Future Internet

1 Introduction

The Internet has undergone severe changes since its first launch in the late 1960s as an outcome of the ARPANET. The initial four-node network has quickly grown into a highly interconnected and self-organized network that builds the daily basis for business, research, and economy. The number of people using this worldwide network has exponentially grown up to about 1.5 bn and hereby makes up about 20% of the world population. This sheer number of end users – that does not even comprise servers and routers inside the networks – has changed our daily life and habits. With the miniaturization of devices, increase of computational power, and reduction of energy consumption, this trend will continue – the Internet of Things.

One of the most challenging topics in such an interconnected world of miniaturized systems and sensors are security and privacy aspects: without sureness that safety of private information is assured and adequate security is provided, users will be unwilling to adopt this new technology that invisibly integrates into their environment and life. Besides technical solutions to provide privacy and security, further instruments – like governmental and ethical institutions, that we will not cover here – need to get established and applied.

Having every 'thing' connected to the global future Internet and 'things' communicating with each other, new security and privacy problems arise, e. g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things'. Privacy of humans and things must be ensured to prevent unauthorized identification and tracking. Further, the more autonomous and intelligent things get, problems like the identity and privacy of things, and responsibility of things in their acting will arise. Up to now, corrupted digital systems were mostly not able to act in the physical world. This will change dramatically in a dangerous way that corrupted digital systems can now operate in and influence the physical world. What happens, once a corrupted thing killed a person?

The sequel of this paper is structured as follows: Section 2 performs an analysis of the components in the Internet of Things, their sensitivity to security and privacy, as well as an analysis of the state in research for topics considered as highly sensitive. In Section 3 two major components in the Internet of Things – Global Sensor Networks and RFID – are introduced and detailed on related security and privacy work. Three research results from other fields that we believe are worth investigating for the Internet of Things are introduced in Section 4. Finally, concluding remarks are given in Section 5.

2 Analysis of Security and Privacy

As the Internet of Things is a large field with diverse technologies used, we provide a categorization of topics and technologies in Section 2.1. The categorization serves as base to detail on the security and privacy sensitivity in the respective fields. Section 2.2 then looks into the state of research in the identified categories and details on topics that have insufficient research from our point of view.

2.1 Categorization and Sensitivity

Figure 1 shows a categorization of *topics* – inner items – and respective *technologies* used in each topic – outer items – that make up the Internet of Things. In our opinion the Internet of Things can be categorized into eight topics:

- *Communication* to enable information exchange between devices
- *Sensors* for capturing and representing the physical world in the digital world
- *Actuators* to perform actions in the physical world triggered in the digital world
- *Storage* for data collection from sensors, identification and tracking systems
- *Devices* for interaction with humans in the physical world
- *Processing* to provide data mining and services
- *Localization and Tracking* for physical world location determination and tracking
- *Identification* to provide unique physical object identification in the digital world

Each topics has different technologies attached (outer items) that are used in the respective topic. Note, that the categorization given in this work is not strictly hierarchical in terms of topics and technologies. *Identification*, e. g., is actually a form of *Processing* that results from the use of *Sensors*. As we believe that *Identification* has a special role in the Internet of Things that is independent of physical world sensing, it is handled as a separate topic. Some technologies appear multiple times: RFID, e. g., is used as *Communication* technology, provides *Identification*, *Localization and Tracking*, RFID readers act as *Sensors*, and finally RFID tags and readers make up *Devices* in the Internet of Things. The manifold usage of RFID assigns it a special role that is detailed in Section 3.2.

The topics introduced are listed again in Table 1 and rated with respect to properties of security and privacy. The properties are taken from the CIA Triad (without *Non-repudiation*) and the Parkerian Hexad (without *Possession or Control* and *Utility*). The additional property *Regulation* represents the need for laws and regulations in this topic. For each topic the table contains the sensitivity for the respective property. As our categorization is not strictly hierarchical, sensitivity

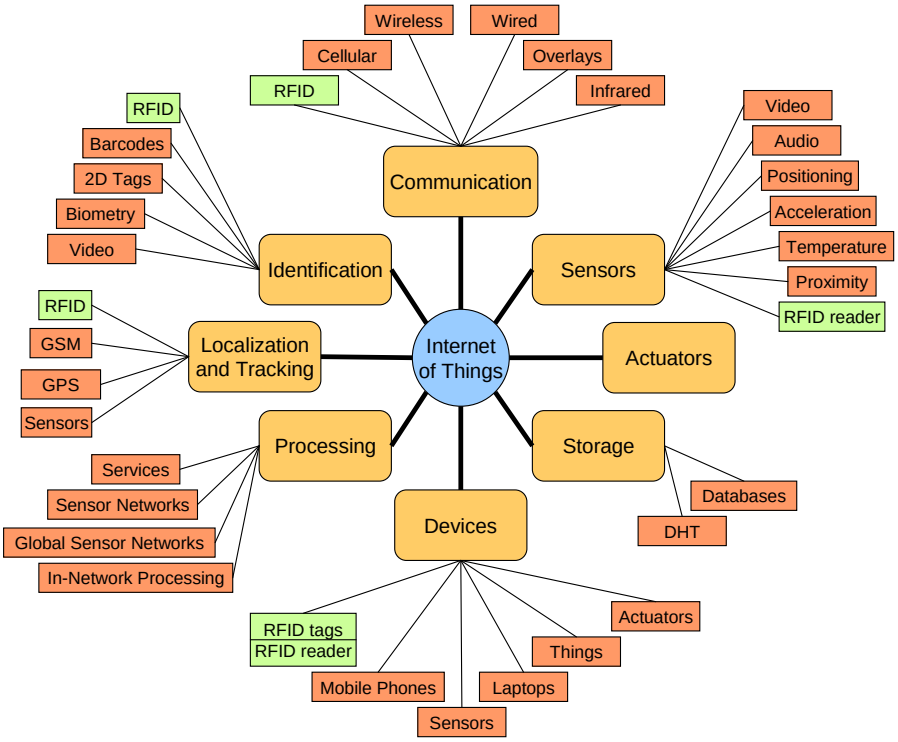

Figure 1: Categorization of topics and technologies in the Internet of Things

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	+++	+++	+++	++	+++	+
Sensors	+++	++	+	+++	+	+++
Actuators	+	+	+		+	++
Storage	+++	++	+++	+++	+	+++
Devices	+++	+	+	++	++	++
Processing	++	+	+	+++	+	+++
Localization/Tracking	+	+	+++	+++	+++	+++
Identification	++	+	+++	+++	+++	+++

Table 1: Sensitivity of topics in the Internet of Things to different security and privacy properties, and the need for laws and regulations (+ low sensitivity, ++ middle sensitivity, +++ high sensitivity)

sometimes is based on sensitivity of other properties. We will now describe the decisions for the chosen sensitivity values.

Communication Research in communication protocols has come up with solutions that provide integrity, authenticity, and confidentiality – examples are TLS, or IPSec. Privacy needs have been tackled by different routing schemes like Onion Routing, or Freenet but unfortunately are not in wide use. An open issue – despite strong research – is disturbed availability through DDoS attacks. In regulations we currently see a low need.

Sensors The integrity and authenticity of sensor data is a current research target that can be handled, e. g., in the form of watermarking [JKK08]. Confidentiality of sensor data is a weak requirement, as an attacker can just place its own sensor physically near and sense the same values. Therefore, the need for sensor confidentiality at the sensor itself is low and confidentiality therefore relies on Communication confidentiality. Privacy in sensors mainly targets the physical world that is getting sensed. Mechanisms like face blurring in video data need to be employed to preserve the privacy of humans and objects in the physical world. The availability of sensors mostly depends on the Communication infrastructure. Regulations are necessary to preserve the privacy of people who are currently most often unaware of sensors – like video cameras – in their environment.

Actuators The Integrity, Authenticity, and Confidentiality of data send to an actuator mostly depends on the Communication security, therefore low sensitivity of the actuator itself is necessary. What must be assured, is that an attacker can not control the actuator (we will come back to this property when looking at Devices). Privacy in actuators is highly specific to the scenario, therefore we don't give a general rating on sensitivity. Whether availability of an Actuator is critical highly depends on the kind of actuator, but can generally be rated as sensitive. Regulations are similar to sensors and must assure that the use of actuators does not disturb privacy.

Storage Security mechanisms for storage devices are well-established, but employment is still weak. As storage of data is highly privacy-sensitive and reports on data breaches are common, regulations must be extended to provide adequate protection of user privacy. Availability of storage mostly depends on availability of *Communication* infrastructure and well-established mechanisms for storage redundancy.

Devices In the scope of devices integrity means that a device is free of malware. This property has also been called 'admissibility' [Sch06]. Ensuring admissibility is an open issue currently researched in *Trusted Platform Computing* (TPM) and highly sensitive. The authenticity of a device is mostly handled in the Communication part and there seen as connection endpoint. Confidentiality in a device goes with the integrity in ensuring that no third party has access to the devices internal data. This is normally ensured in case of device integrity. Privacy of devices depends on physical privacy and Communication privacy. Availability of a device depends on the devices integrity and reliability, and availability of the Communication part that connects the device.

Processing Integrity in the Processing of data for higher services and correlation is based on Device integrity and integrity of Communication. Furthermore, it depends on the correct design and implementation of algorithms for processing. As Processing can often be followed by Actuator actions it is sensitive in that an actuator may get incorrect commands. The Authenticity of

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability
Communication	2	2	3		1
Sensors	2			1	
Actuators					
Storage	3		3	1	
Devices	1				
Processing				1	
Localization/Tracking			3	1	2
Identification			3	1	2

Table 2: State of research for highly sensitive properties (1 research needed, 2 basic research available, 3 adequate research available)

Processing solely depends on the authenticity of the Device and authenticity of Communication, and therefore in itself is not sensitive to Processing. The property of confidentiality in Processing is only dependent on the integrity of the device, and – in case of distributed Processing – dependent on the integrity of the Communication. Processing is of major privacy and critical to Storage. Privacy preserving data mining is available, but regulations must be employed to make sure they are applied and applied correctly. The availability of Processing depends on the Device and Communication availability solely.

Localization and Tracking Integrity of Localization and Tracking is especially based on Communication integrity. Furthermore, the integrity of reference signals used in Localization, e. g. GSM or GPS cell, need to be ensured. Likewise, the Authenticity depends on Communication authenticity and Device integrity. Confidentiality and privacy of localization and tracking data are of high importance to ensure user privacy and therefore highly sensitive. Confidentiality in this context means that an attacker is not able to reveal localization data and therefore is mainly based on Communication confidentiality. Privacy in Localization data means that (1) there is no way for an attacker to reveal the identity of the person or object the localization data is attached to and (2) that Localization and Tracking is not possible without the explicit agreement or knowledge. Availability of localization is important to ensure that the reference signals for localization are robust and can not be manipulated by an attacker. We think that regulations in Localization and Tracking are of high importance mainly in terms of privacy, as mentioned above.

Identification For Identification we see mainly the same sensitivities as for Localization and Tracking. One difference is the higher sensitivity in integrity. We think it is easier for an attacker to manipulate the identification process as it is to manipulate the localization process. This results mainly due to the technology used (e. g. RFID or biometry) that we think is more feasible for an attacker to manipulate than localization technologies (e. g. GSM).

2.2 State of Research

We will now look into the state of research for the properties rated highly sensitive in Section 2.1. Table 2 shows the properties rated as highly sensitive in Section 2.1 along with our rating of the state of research. For highly sensitive properties with a research rating of 1 we will explain in more detail why we think that research in this area is currently insufficient.

Communication Mechanisms for securing Communication are well-established but unfortunately seldom applied. Especially in small devices with weak processing power Communication security is often weak or missing. Availability of Communication is a big problem that is caused by botnets and DDoS attacks that exploit the best-effort service provided by IP.

Sensors A major problem in Sensors is privacy. This is mainly caused by people not knowing that they are being sensed. Langheinrich [Lan01] defines several guidelines to handle this problem in the design phase: (1) users must be aware that they are being sensed ('notice'), (2) users must be able to choose whether they are being sensed and be able to opt-out ('choice and consent'), and (3) users must be able to remain anonymous ('anonymity and pseudonymity'). As the user has no way to tell whether a ubiquitous system integrates these guidelines we believe that regulations must be employed.

Storage Mechanisms for integrity and confidentiality in Storage are well-established, but unfortunately often complex to employ. Privacy issues, however, are – besides Sensor privacy – one of the main privacy problems in the Internet of Things. Anonymization and pseudonymization mechanisms must be used to ensure that data does not contain information sensitive to privacy. Often, too much information is stored that is not necessary for the actual system, as mentioned lately by Schneier [Sch08].

Devices The integrity of devices – called 'admissibility' in [Sch06] – is an unresolved issue. Research in Trusted Platform Computing aims at protecting the integrity of devices. Although TPM modules have been built into laptops for some time now, fully TPM-capable operating systems are still missing.

Processing Mechanisms for data processing must assure sure that no sensitive information is available in processed data that is forwarded to untrusted Devices or Storage. Mechanisms for privacy preserving data mining exist [VBF+04] – e. g. adding noise – but are applied seldom. Regulations need to define a standard set of privacy preserving mechanisms that must be applied in Processing.

Localization and Tracking, and Identification For Localization and Tracking, as well as Identification we see the same research requirements: the privacy of users that are being localized, identified, or tracked. In all cases the user must be able to opt-out and be notified of the process. This has been defined by Langheinrich as 'Choice and Consent'.

To summarize, we see specific need for research in the availability of Communication due to DDoS and the best-effort service provided by IP. Furthermore, the Integrity of devices to make sure they are free from malware like spyware or rootkits needs more research. Finally, nearly all areas miss applicable mechanisms in privacy for the Internet of Things. The guidelines by Langheinrich are very helpful for system designers, but we suggest that (1) regulations are needed to ensure systems conform to these guidelines, and (2) mechanisms must be developed that provide users with possibilities in actively protecting their privacy instead of only relying on that systems in the Internet of Things respect their privacy and implement respective mechanisms.

3 Major players in the Internet of Things

We will now shortly detail on GSN Middleware and – more in-depth – on RFID technology. Besides background on RFID we will detail on GSN and RFID security in Section 3.1 and Section 3.2, respectively.

3.1 Global Sensor Network Middleware

A lot of work has been performed in the last years about middleware architectures that connect sensors and sensor networks into the global infrastructure of the Internet [Oll07, AHS06, FJK+05, GKK+03] and therewith enable advanced sensing applications. Security aspects in the work on middleware have mostly been derived from security needs that arise when connecting multiple heterogeneous networks over the Internet – the topic of Connection in our categorization. However, the new security and privacy issues that arise when integrating the physical with the digital world in the Internet of Things need to be covered by future research. In the following, work in security and privacy in Global Sensor Network Middleware systems is detailed on shortly.

IrisNet The IrisNet Architecture [GKK+03] for distributed sensing uses Webcams as sensors. Security is based on the assumption that 'the entire worldwide sensor web is administered by a single, universally trusted authority'. It therefore can be secured using communication security mechanisms. To counter privacy concerns in the video data IrisNet implements face blurring. As one scenario in IrisNet is monitoring of free parking-lots, if is a good example that anonymization does not necessarily limit data utility.

HiFi The HiFi [FJK+05] specifies a hierarchical architecture of 'levels'. Data is forwarded from the lowest level – actual sensor data sources like RFID or sensor networks – over intermediate levels upwards. Levels perform specific tasks: the lowest level 'cleans' the data and only forwards data items that comply to a specific quality standard (like RFID signal strength). Higher levels 'smooth' and 'validate' data. Privacy and access control is implemented using SQL views for the specification of authorization policies.

ETRI Ubiquitous Sensor Network An analysis of security threats in the ETRI project is given in [KLR07]. The following security requirements are identified: *Threats toward applications* like unauthorized users acquiring sensing data, applications disrupting the functionality of the sensor network by reconfiguring sensor nodes, and performing Denial-of-Service attacks through large numbers of sensing requests. *Threats from corrupted sensor networks* that provide invalid sensing data, therewith distorting application results. *Threats from external objects* like eavesdropping. Furthermore, replay attacks and man-in-the-middle attacks are possible when an attacker positions itself between the application and a layer of the middleware system.

3.2 RFID

An RFID tag is a small integrated circuit that contains a unique ID that identifies this special item – not only the item group as done with barcodes. RFID readers can query the tags and receive the unique item ID. The ID is then the entry key into a database that contains additional information about the item. Often, the ID is built in a hierarchical form that contains, e. g. the manufacturer, the group class, and the item ID.

The RFID market is growing rapidly with 1.02 bn tags sold alone in 2006, and a $5.20 bn

market value in 2008 [DH08]. These numbers are predicted to grow and RFID tags posing an important technology in the Internet of Things. With current passive RFID tags having no sensing capabilities, the sensors in an RFID scenario are the RFID readers. Future RFID tags will incorporate advanced sensing and communication capabilities, so the sensor part will also be available in the RFID tag itself.

As RFID tags identify unique items, privacy issues arise as the tracking of items – and with this tracking of the person who carries, wears, has implanted the item – becomes possible. Therefore, different cryptographic techniques have been proposed with the goal that only authorized parties are able to reveal the real ID of the tag. A good overview of such techniques is given in [PM07]. As different RFID tags exist (e. g. active, passive, semi-active) with different computational capabilities, different mechanisms exist for security and privacy.

Security and privacy in RFID systems has been defined as [Ban08]:

- **Security**: 'The ability of the RFID system to keep the information transmitted between the tag and the reader secure from non-intended recipients.'
- **Privacy**: 'The ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from non-intended recipients.'

RFID tags have the ability to perform basic operations like XOR, simple hashing, calculating Pseudorandom Functions (PRFs), and to participate in challenge-response protocols. Therewith a number of protocols have been proposed that employ challenge-response protocols between a RFID tag and RFID reader. An RFID reader has access to a database system that includes all tag IDs and additional information, depending on the protocol. Physical mechanisms to preserve RFID privacy is detailed in Section 3.2.1 and cryptographic RFID protocols in Section 3.2.2.

3.2.1 Physical Mechanisms

Kill Codes Kill codes permanently disable the tag and therefore prevent reading and tracking. This is especially useful for items that need tracking in the supply-chain only and not after customer purchase. RFID applications like easy item reshipment are made impossible.

Faraday Cage Putting an RFID tag into a faraday cage makes it impossible to read the tag. Enables the user to decide when reading should be possible. A faraday cage renders ubiquitous services impossible.

Blocker Tag The Blocker Tag [JRS03] performs jamming that makes unauthorized readers think that a large number of different RFID tags are present. A blocker tag is placed besides the actual RFID tag, therefore it can be easily applied and removed.

3.2.2 Cryptographic Protocols

Randomized Hash-Lock Protocol A database contains the IDs of all tags ID_i, $i \in \{0 \ldots n\}$. The RFID reader queries the tag a to start the protocol. The tag calculate $x = h(ID_a|r)$ using a hash function $h(x)$, his ID ID_a, a random number r, and transmits $\{x, r\}$ to the server. As the server knows the IDs of all keys ID_i, he calculates $y = h(ID_i|r)$ for every i and compares $x =^? y$. If x matches y the correct ID ID_a is found. As the protocol runs in $O(n)$ it can put heavy load at the server.

Hash Chain based Protocols The YA-TRAP [Tsu06] protocol requires loose time synchronization between server and readers, tags aren't required to have clocks. In initialization every tag i is assigned a triple $\{K_i, T_0, T_{max}\}$, K_i is a tag-specific identifier used as tag ID and cryptographic key, T_0 is an initial timestamp, e. g. the time of manufacture, and T_{max} is the top value of timestamps and corresponds to the maximum lifetime of the tag. Every timestamp T_r with $r \in \{0 \ldots max\}$ gets a hashtable $HASHTABLE_r$ created in the server database. For every tag i the values of $HMAC_{K_i}(T_r)$ are inserted into the tables $HASHTABLE_r$, i. e., for every tag i with key K_i every hashvalue in every timestamp T_r is precomputed and stored.

The protocol goes as follows: the reader sends the current timestamp T_r to the tag. The tag remembers the current timestamp as $T_t = T_r$, computes $H_r = HMAC_{K_i}(T_t)$ and sends back H_r to the reader. The server now knows T_r and H_r which is the current timestamp and the hashvalue for the tag in the current timestamp. It looks into the hashtable $HASHTABLE_r$ that contains all hashes for the current timestamp T_r. By querying H_r of the $HASHTABLE_r$ the server can retrieve K_i which corresponds to the ID of tag i.

4 Research from other Domains

The current Internet has failed in many ways to provide adequate security and privacy. We present three research results that are worth considering in the Internet of Things. We shortly present these approaches and motivate in investigating them for the use in the Internet of Things.

4.1 Information Accountability

Since first information systems have been set up and the Web has taken its way to reach millions of people, the dilemma of privacy in the digital world has begun. Using the same techniques to protect privacy of people – and maybe the privacy of 'things' in the Internet of Things – will maybe end in the same results: uncontrolled information flow and uncontrolled privacy. The current large-scale databases storing personal data will get filled up even more in the days of the Internet of Things and record our every steps. As Schneier warns in [Sch08] we have quite no way of controlling the collection and use of personal data. Worse, lots of data is linked to personal information – which is often not necessary. All of this data is collected and stored, but not deleted, which inevitably result in data garbage that goes uncontrolled.

Weitzner et al. present a new concept to privacy which they call *Information Accountability* [WAB+08]. The main principle of information accountability is not to try to prevent the leakage of data – and being helpless once data leaks – but rather being able to control the usage of the data. Therewith being able to call persons to account that misuse the data – which is not able with the current concept of privacy that is based on keeping information secret.

4.2 Cryptographic Identifiers

Cryptographic Identifiers [MC04] are used within several newer networking protocols to prove ownership of an address. The IPv6 Secure Neighbor Discovery (Send), e. g., uses Cryptographically Generated Addresses to prevent address spoofing, as possible in the Address Resolution Protocol (ARP) used in LANs. Furthermore, given the large size of Overlay identifiers, the use of Cryptographic Identifiers can there be used to prove the ownership of ones identifier. The Host Identity Protocol (HIP), e. g., bases its security highly on Cryptographic Identifiers.

The Cryptographic Identifiers as RFID IDs would enable tags to prove that they really own

the ID. With current RFID solutions mainly deployed in self-contained systems, the need to ownership proof does hardly arise. Having public databases that store all information about a tags and are publicly queriable, brings up the problem of tag ID spoofing as an attacked can gather all tag information from the database and then prepare a tag that spoofs its identity as some other tag. Cryptographic Identifiers can help detect tags that spoof their ID as other tags. Furthermore, the scheme can be deployed for sensor nodes that take part in an overlay network where identifiers are long enough to use Cryptographic Identifiers. These nodes can then prove ownership of their identifier. This allows to detect rogue sensors that spoof as another tag and possible give out corrupted sensing data.

Cryptographic Identifiers are based on asymmetric-key cryptography and therefore have a large overhead compared to symmetric-key cryptography in terms of computational power and key-size. As it has been shown that sensor nodes can be able to perform asymmetric-key cryptography [BZ05], the use of Cryptographic Identifiers in sensor nodes is possible. RFID tags are quite some time away from performing asymmetric-key cryptography, but will eventually be able. Therefore, interesting results are to arise when using the RFID tags ID in combination with Cryptographic Identifiers.

4.3 Key Extraction from Wireless Channel Characteristics

As a large part of communication in the Internet of Things will occur over wireless channels – that are susceptible to eavesdropping – key establishment is necessary to provide confidential communication. The work of Mathur et al. [MTM+08] provides the establishment of a common cryptographic key for two users by the use of characteristics of the wireless channel. As the wireless channel characteristics for a communication context between A and B are the same *only for exactly* A and B, it is possible to use this characteristic to extract bits from stochastic processes. These bits can then be used to form a symmetric cryptographic key. So, A and B independently calculate the *same* symmetric key for the communication between A and B – solely through the fact that A talks to B and B talks to A.

This scheme seems promising when it comes to wireless communication in the Internet of Things, because (1) it is based only on symmetric-key cryptography, and (2) it would be expensive to establish key infrastructures or distribute keys in the Internet of Things that is made up of such large numbers of ‘things’.

5 Conclusions

The Internet of Things is quickly coming closer. The incremental deployment of the technologies that will make up the Internet of Things must not fail what the Internet has failed to do: provide adequate security and privacy mechanisms *from the start*. The introduction of e-passports, e. g., has been pushed by politics into deployment with – back then – insufficient privacy mechanisms [JMW05]. We must be sure that adequate security and privacy is available *before* the technology gets deployed and becomes part of our daily live.

In this paper we presented a categorization of topics and technologies in the Internet of Things with analysis of sensitivity and state in research to different security and privacy properties. We see this (1) as a basis for coming up with an integrated systems approach for security and privacy in the Internet of Things, and (2) as stimulator for discussion on the categorization and sensitivity rating in the Internet of Things. Furthermore, we presented research in security and privacy for

two major technologies in the Internet of Things – GSN and RFID – and finally pointed out research from other fields in computer science that is worth considering for use in the Internet of Things.

Acknowledgements: The author thanks Oliver P. Waldhorst for comments on an early version of this paper and the anonymous reviewers of GSN09 for their valuable comments. The work presented in this paper was done as part of the SpoVNet Project that is funded by the Landesstiftung Baden-Württemberg under the initiative BW-FIT.

Bibliography

[AHS06] K. Aberer, M. Hauswirth, A. Salehi. A Middleware for Fast and Flexible Sensor Network Deployment. In *Proceedings of the 32nd International Conference on Very Large Databases*. Pp. 1199–1202. Sept. 2006.

[Ban08] J. Banks. Understanding RFID Part 9: RFID Privacy and Security. http://www.rfidnews.org, May 2008.

[BZ05] E. Blaß, M. Zitterbart. Towards Acceptable Public-Key Encryption in Sensor Networks. In *Proceedings of 2nd International Workshop on Ubiquitous Computing*. Pp. 88–93. May 2005.

[DH08] R. Das, P. Harrop. Complete RFID Analysis and Forecasts 2008-2017. http://www.IDTechEx.com/forecasts, 2008.

[FJK+05] M. Franklin, S. Jeffery, S. Krishnamurthy, F. Reiss, S. Rizvi, E. Wu, O. Cooper, A. Edakkunni, W. Hong. Design Considerations for High Fan-in Systems: The HiFi approach. In *Proceedings of the CIDR Conference*. Pp. 290–304. Jan. 2005.

[GKK+03] P. Gibbons, B. Karp, Y. Ke, S. Nath, S. Seshan. IrisNet: An Architecture for a Worldwide Sensor Web. *IEEE Pervasive Computing* 2(4):22–33, Dec. 2003.

[Int05] International Telecommunication Union. The Internet of Things. ITU Report, Nov. 2005.

[JKK08] H. Juma, I. Kamel, L. Kaya. On Protecting the Integrity of Sensor Data. In *Proceedings of 15th IEEE International Conference on Electronics, Circuits and Systems*. Pp. 902–905. Sept. 2008.

[JMW05] A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-passports. In *Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Pp. 74–88. Sept. 2005.

[JRS03] A. Juels, R. L. Rivest, M. Szydlo. The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy. In *Proceedings of 10th ACM Conference on Computer and Communications Security*. Pp. 103–111. 2003.

[KLR07] M. Kim, Y. Lee, J. Ryou. What Are Possible Security Threats in Ubiquitous Sensor Network Environment? *Lecture Notes in Computer Science* 4773:437–446, 2007.

[Lan01] M. Langheinrich. Privacy by Design - Principles of Privacy-aware Ubiquitous Systems. In *Proceedings of Ubicomp*. Pp. 273–291. Oct. 2001.

[MC04] G. Montenegro, C. Castelluccia. Crypto-based Identifiers (CBIDs): Concepts and Applications. *ACM Transactions on Information and System Security* 7(1):97–127, Feb. 2004.

[MTM+08] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *Proceedings of MobiCom*. Pp. 128–139. Sept. 2008.

[Oll07] Ollero et al. AWARE: Platform for Autonomous Self-deploying and Operation of Wireless Sensor-actuator Networks Cooperating with Unmanned AeRial vehiclEs. In *Proceedings of IEEE International Workshop on Safety, Security and Rescue Robotics*. Pp. 1–6. June 2007.

[PM07] R. D. Pietro, R. Molva. Information confinement, privacy, and security in RFID systems. In *Proceedings of ESORICS*. Pp. 187–202. Dec. 2007.

[Sch06] B. Schneier. Updating the Traditional Security Model. http://www.schneier.com/blog/archives/2006/08/updating_the_tr.html, Aug. 2006.

[Sch08] B. Schneier. The Future of Privacy. Presentation at RSA Conference Europe, Oct. 2008.

[Tsu06] G. Tsudik. YA-TRAP: Yet Another Trivial RFID Authentication Protocol. In *Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. Pp. 196–200. Mar. 2006.

[VBF+04] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, Y. Theodoridis. State-of-the-art in Privacy Preserving Data Mining. *ACM SIGMOD Record* 33(1):50–57, Mar. 2004.

[WAB+08] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. J. Sussman. Information Accountability. *Communications of the ACM* 51(6):82–87, June 2008.