Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SAFE RFID AUTHENTICATION PROTOCOL FOR INTERNET OF THINGS

[1]DONGFENG XU, [2]YAN CHEN

[1] College of Informatics, South China Agricultural University, Guangzhou 510642, China
[2] College of Engineering, South China Agricultural University, Guangzhou 510642, China

ABSTRACT

Internet of Things (IoT) is the evolution of related technologies and applications such as Internet and mobile networks. Future research into IoT will focus on generic technology, information security, and critical applications. Based on IoT, the existing RFID system security mechanisms are analyzed, with a focus on cryptographic protocols. Investigate the weaknesses or flaws in these protocols, and then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed. A mutual authentication protocol of RFID system using synchronized secret information is put forward..

Keywords: *Internet of Things; Security Architecture; Radio Frequency Identification; Privacy Protection; Authentication protocol.*

1. INTRODUCTION

The Internet of Things (IoT), an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established.

The Internet of Things is an information architecture facilitating the exchange of goods and services in global supply chain networks. For example, the lack of certain goods would automatically be reported to the provider which in turn immediately causes electronic or physical delivery. From a technical point of view, the architecture is based on data communication tools, primarily RFID-tagged items (Radio-Frequency Identification). The IoT has the purpose of providing an IT-infrastructure facilitating the exchanges of ''things'' in a secure and reliable manner. The most popular industry proposal for the new IT-infrastructure of the IoT is based on an Electronic Product Code (EPC), introduced by EPC global and GS. The ''things'' are physical objects carrying RFID tags with a unique EPC; the infrastructure can offer and query EPC Information Services (EPCIS) both locally and remotely to subscribers. The information is not fully saved on an RFID tag, but a supply of the information by distributed servers on the Internet is made available through linking and cross-linking with the help of an Object Naming Service (ONS). The ONS is authoritative (linking metadata and services) in the sense that the entity having – centralized – change control over the information about the EPC is the same entity that assigned the EPC to the concerned item. Thereby, the architecture can also serve as backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and receive information from the Internet to facilitate their adaptive functionality. The central ONS root is operated by the (private) company VeriSign, a provider of Internet infrastructure services. The ONS is based on the well-known Domain Name System (DNS). Technically, in order to use the DNS to find information about an item, the item's EPC must be converted into a format that the DNS can understand, which is the typical, ''dot'' delimited, left to right form of all domain names. Since EPC is encoded into syntactically correct domain name and then used within the existing DNS infrastructure, the ONS can be considered as subset of the DNS. For this reason, however, the ONS will also inherit all of the well-documented DNS weaknesses, such as the limited redundancy in practical implementations and the creation of single points of failure.

The 'Internet of Things' is a vision of a ubiquitous Internet where every day physical objects are integrated into information networks. This aims to provide an interconnected infrastructure supporting new and innovative services based on widespread access to contextual information about objects in the physical world.

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

One of the main requirements for the 'Internet of Things' is that objects must have a unique identity, which would make them practically addressable when exchanging information. RFID tokens, such as EPC tokens, have sufficiently long identifiers to allow for unique identities to be assigned to individual items, rather than to groups of items as is currently done with barcodes. RFID tokens are also easy to integrate into many objects as they do not need to be visible or adhere to a specific form factor.

With the advancement in networking and multimedia technologies enables the distribution and sharing of multimedia content widely. In the meantime, piracy becomes increasingly rampant as the customers can easily duplicate and redistribute the received multimedia content to a large audience. Insuring the copyrighted multimedia content is appropriately used has become increasingly critical.

Although encryption can provide multimedia content with the desired security during transmission, once a piece of digital content is decrypted, the dishonest customer can redistribute it arbitrarily[2, 3].

2. FORMAT OF MANUSCRIPT

The described technical architecture of the IoT has an impact on the security and privacy of the involved stakeholders. Privacy includes the concealment of personal information as well as the ability to control what happens with this information. The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession.

2.1 Technology of the Internet of Things

The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them even knowing about it and would leave their data or at least traces thereof in cyberspace. Further aggravating the problem, it is not anymore only the state that is interested in collecting the respective data, but also private actors such as marketing enterprises.

Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.

Data authentication: As a principle, retrieved address and object information must be authenticated.

Access control: Information providers must be able to implement access control on the data provided.

Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

Private enterprises using IoT technology will have to include these requirements into their risk management concept governing the business activities in general.

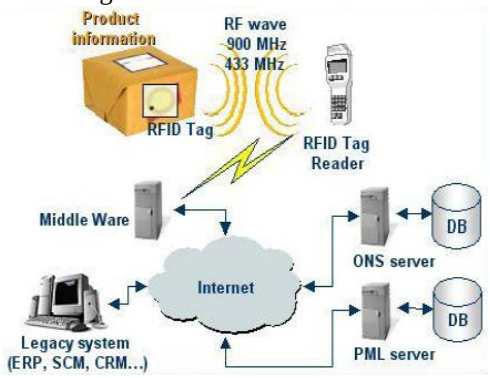

Figure 1: The System Of Internet Of Things

2.2 RFID in the Internet of Things

The European Commission is aware of the security and privacy issues related to the RFID and the IoT. In a Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification the European Commission invites the Member States to provide for guidance on the design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data.

In particular, the Recommendation outlines measures to be taken for the deployment of RFID application to ensure that national legislation is complying with the EU Data Protection. Member States should ensure that industry in collaboration with relevant civil society stakeholders develops a framework for privacy and data protection impact assessments (PIA); this framework should be submitted to the Article 29 Data Protection Working Party within 12 months. Industry and civil society stakeholders are in the process of establishing the requested framework PIA until late 2009. The objectives of the PIA are designed to identify the implications of the application on privacy and data protection, to determine whether the operator has taken appropriate technical and organizational measures to ensure respective

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protection, to document the measures implemented with respect to the appropriate protection, and to serve as a basis for a PIA report that can be submitted to the competent authorities before deployment of the application. Presumably, the framework should serve to determine a common structure and content of reports. In particular, RFID application description and scope, RFID application governing practices, accountability and analysis and resolution seem to be of importance. Furthermore, operators are asked to conduct an assessment of the implications of the application implementation for the protection of

Mid summary: takeaway points from last slides. RFID is assigned to several topics. Being unaware of this dual-use can end up badly, Same with IP addresses! Used as locator and identifier. Now research into ID/Locator split. Point is not to take RFID apart technically, but be aware of the multi-se when developing protocols, S&P currently done per technology, not per topic.

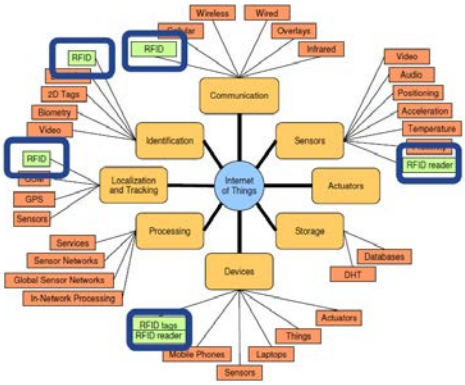

Figure 2: The Internet Of Things Technology And RFID

User-oriented RFID applications are also expected to experience growth on the back of increased deployment of NFC. One of the main goals of NFC is to facilitate ad-hoc communication between the user and tagged objects and the NFC Forum has therefore specified several standards that can enable user-oriented services [16]. The main specification that could enable such services is the NFC Data Exchange Format (NDEF), which defines a common data format for NFC-forum compliant devices and the four types of NFC Forum-compliant RFID tokens. The NFC Record Type Definition (RTD) specifies the format and rules for building standard record types based on the NDEF data format. The RTD specification provides a way to efficiently define record formats for new applications and gives users the opportunity to create their own applications adhering to NFC Forum specifications.

Standard RTDs are currently specified for storing text strings in multiple languages, storing Uniform Resource Identifiers (URI) and triggering a specific action (such as starting an application). As an example of how to apply NDEF and RTDs the NFC Forum provides a Smart Poster specification, which defines how to put URLs, SMSs or phone numbers on an NFC token. The Smart Poster RTD builds on the RTD mechanism and NDEF format and uses the URI RTD and Text RTD as building blocks.

2.3 EPC global Network

The equations are an exception to the prescribed primarily RFID-tagged items (Radio-Frequency Identification). The IoT has the purpose of providing an IT-infrastructure facilitating the exchanges of ‘‘things’’ in a secure and reliable manner. The most popular industry proposal for the new IT-infrastructure of the IoT is based on an Electronic Product Code (EPC), introduced by EPC global and GS. The ‘‘things’’ are physical objects carrying RFID tags with a unique EPC; the infrastructure can offer and query EPC Information Services (EPCIS) both locally and remotely to subscribers.

The fulfillment of customer privacy requirements is quite difficult. A number of technologies have been developed in order to achieve information privacy goals. This Privacy Enhancing Technologies (PET) can be described in short as follows Number equations consecutively.

Virtual Private Networks (VPN) are extranets established by close groups of business partners. As only partners have access, they promise to be confidential and have integrity. However, this solution does not allow for a dynamic global information exchange and is impractical with regard to third parties beyond the borders of the extranet. Transport Layer Security (TLS), based on an appropriate global trust structure, could also improve confidentiality and integrity of the IoT. However, as each ONS delegation step requires a new TLS connection, the search of information would be negatively affected by many additional layers.

DNS Security Extensions (DNSSEC) makes use of public-key cryptography to sign resource records in order to guarantee origin authenticity and integrity of delivered information. However, DNSSEC could only assure global ONS information authenticity if the entire Internet community adopts it.

Onion Routing encrypts and mixes Internet

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

traffic from many different sources, i.e. data is wrapped into multiple encryption layers, using the public keys of the onion routers on the transmission path. This process would impede matching a particular Internet Protocol packet to a particular source. However, onion routing increases waiting times and thereby results in performance issues.

Private Information Retrieval (PIR) systems conceal which customer is interested in which information, once the EPCIS have been located. However, problems of scalability and key management, as well as performance issues would arise in a globally accessible system such as the ONS, which makes this method impractical.

It is important that an RFID tag having been attached to an object can – at a later stage – be disabled in order to allow for customers to decide whether they want to make use of the tag. RFID tags may either be disabled by putting them in a protective mesh of foil known as a ''Faraday Cage'' which is impenetrable by radio signals of certain frequencies or by ''killing'' them, removing and destroying them. However, both options have certain disadvantages. While putting tags in a special cage is relatively safe, it requires that every tag from every single product is put in that cage if a customer desires so. Chances are that certain tags will be overlooked and left with the client and that he/she could still be traced. Sending a ''kill'' command to a tag leaves room to the possibility of reactivation or that some identifying information could be left on the tag. Furthermore, businesses may be inclined to offer clients incentives for not destroying tags or secretly give them tags. Instead of killing tags, the dissolution of the connection between the tag and the identifiable object could be envisaged. The information on ONS is deleted to protect the privacy of the owner of the tagged object. While the tag can still be read, further information with potential information concerning the respective person, however, are not retrievable.

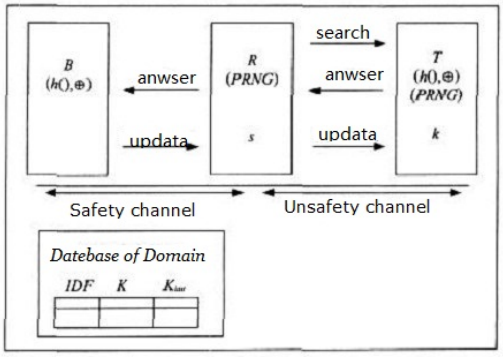

Figure 3: The RFID System Architecture Of This Paper

3. SECURITY FOR THE INTERNET OF THINGS

Current Internet security protocols rely on a well-known and widely trusted suite of cryptographic algorithms: the Advanced Encryption Standard (AES) block cipher for confidentiality, the Rivest-Shamir-Adelman(RSA) asymmetric algorithm for digital signatures and key transport, the Diffie-Hellman(DH) asymmetric key agreement algorithm, and the SHA-1 and SHA-256 secure hash algorithms. This suite of algorithms is supplemented by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC).Adoption of the ECC algorithms has been slowed by significant IPR concerns, but publication of RFC 6090 and recent IPR disclosures may encourage adoption.

The Internet of Things (IoT) will present new security challenges in cryptographic security, credentialing, and identity management. Currently available cryptographic techniques require further analysis to determine applicability in the Internet of Things. Credentialing presents significant challenges in the current Internet and these challenges will be exacerbated by the sheer number of devices and the expected limitations in user interfaces. Identity management is currently oriented towards either user or device identity; in the Internet of Things making an implicit or explicit mapping between IoT device identities and Internet user identities may be required. Network security devices, such as firewalls and network guards, will be essential to meet security requirements. Security will be in tension with usability, privacy, and devices' constrained resources.

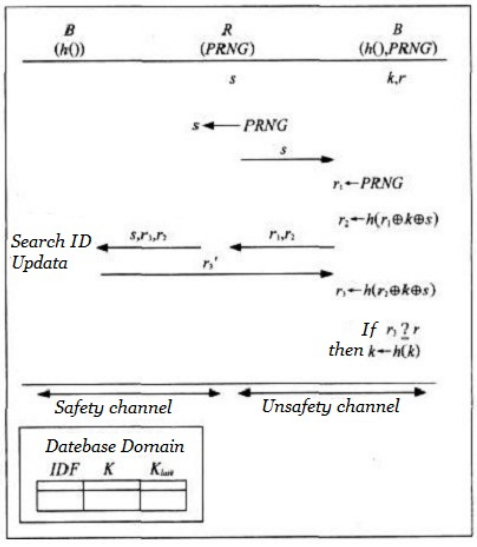

Figure 4: The RFID Authentication Protocol In This Paper

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the IoT, the most devices will not be associated with a single person. A house only needs one toaster even if it serves a family of four. There may be a need to map device identities to groups of people (e.g., the adults in that family of four) in ways that are not commonly performed today. The security challenges for the IoT are daunting. It is essential that early IoT protocols include mandatory to implement security features, even if those features stretch the capabilities of such devices. Automated key management is always a challenge, but it is even more critical that IoT protocols do not rely on pre-shared keys. Credentialing/registration of devices will also be a challenge, but pairing protocols are well-understood and provide one possible solution set.

Privacy concerns may provide incentives for adoption for technologies designed to prevent information leakage in military/intelligence environments. Privacy issues are also expected to be significant. Our experiences with Smart Grid demonstrate the sensitivities of exposing electricity usage associated with a home or business. The IoT has the potential to expose the precise application of that energy demand, further violating the privacy expectations of the population. In combination with these privacy issues, compromises in the IoT protocol suites are likely to require establishing a security perimeter that monitors and restricts IoT devices. Older technologies from the military and intelligence communities, such as "network guards", once used to prevent information leakage may be needed once again.

4. CONCLUSION

With the emergence of an Internet of Things, new regulatory approaches to ensure its privacy and security become necessary. In particular, attacks have to be intercepted, data authenticated, access controlled and the privacy of customers (natural and legal persons) guaranteed. The nature of the IoT asks for a heterogeneous and differentiated legal framework that adequately takes into account the globosity, verticality, ubiquity and ethnicity of the IoT. Internet of Things (IoT) is the evolution of related technologies and applications such as Internet and mobile networks. Future research into IoT will focus on generic technology, information security, and critical applications. Based on IoT, the existing RFID system security mechanisms are analyzed, with a focus on cryptographic protocols. Investigate the weaknesses or flaws in these protocols, and then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed. A mutual authentication protocol of RFID system using synchronized secret information is put forward.

Currently available cryptographic techniques require further analysis to determine applicability in the Internet of Things. Credentialing presents significant challenges in the current Internet and these challenges will be exacerbated by the sheer number of devices and the expected limitations in user interfaces. Identity management is currently oriented towards either user or device identity; in the Internet of Things making an implicit or explicit mapping between IoT device identities and Internet user identities may be required. Network security devices, such as firewalls and network guards, will be essential to meet security requirements. Security will be in tension with usability, privacy, and devices' constrained resources.

The content of the respective legislation has to cover the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

ACKNOWLEDGEMENTS

This work was supported by the Natural Science Foundation of Guangdong Province，China (No.S2011010001933).

Corresponding author: YAN CHEN

REFERENCES:

[1] P. Barreto, H. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In M. Yung, editor, Proceedings of Crypto 2002, volume 2442 of LNCS, pages 354–68. Springer-Verlag, Berlin, 2002.

[2] M.R. Rieback, B. Crispo and A.S. Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, Vol. 5, Issue 1, pp 62-69,January 2006.

[3] Y. Tana, M. Sata, "Asymmetric fingerprinting based on 1-out-of-n oblivious transfer", *IEEE Communications Letters*, Vol. 14, No. 5, 2010, pp. 101-111.

[4] Ari Juels, RFID Security and Privacy: A Research Survey, *IEEE Journal on Selected Areas in Communications*, Vol. 24, 2006, 381–394, at 383.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] Benjamin Fabian, Secure Name Services for the Internet of Things, Thesis, Berlin 2008, 30/31.

[6] Lu Yan，Yan Zhang，Laurence T. Yang，The Internet of Things, New York/London 2008.

[7] K. Osaka, T. Takagi, K.Yamazaki and Takahashi. An Efficient and Secure RFID Security Method with Ownership Transfer. Conference on Computational Intelligence and Security, pp 1090-1095, November 2006.

[8] C. Mulliner. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. 1st Workshop on Sensor Security, March 2009.

[9] A. Mitrokotsa, M.R. Rieback and A.S. Tanenbaum. Classifying RFID Attacks and Defences. Information Systems Frontiers, Springer, July 2009.

[10] G. Roussos, S.S. Duri, C.W. Thompson. RFID Meets the Internet. *IEEE Internet Computing*, Vol. 13, Issue. 1, pp 11-13, January 2009.

[11] A. Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, Vol. 24, Issue 2, pp381-394, February 2006.

[12] P. Rotter. A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing Magazine*, Vol. 7, Issue2, pp70-77, April 2008.

[13] B. Song. RFID Tag Ownership Transfer. 4th Workshop on RFID Security - RFIDSec08, July 2008.

[14] S. Garfinkel, A. Juels and R.Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, Vol. 3, No. 3, pp 34-43 2005.

[15] Avoine Gildas, Oechslin Philippe. RFID traceability: a mulilayer problem. Financial Cryptography. March 2005: 125-140.