Building Trust in the Security and Privacy of RFID Systems[1]

Authors
Esteban Masobro Garcia, MSc (Royal Holloway, 2014)
Konstantinos Markantonakis, ISG, Royal Holloway

Overview

Radio Frequency Identification (RFID) technology offers a number of advantages that make it stand out amongst available automatic identification (Auto-ID) technologies. It has already been applied in many areas, from large retail stores to car immobilisers and even human beings. Nevertheless, the upcoming widespread adoption of RFID requires the incorporation of suitable privacy and security measures. Security protocols constitute a major mechanism to achieve that goal. However, it must be emphasised that their design is an error-prone task. Consequently, it is essential to have automated tools at our disposal that can formally verify, to some extent, those protocols. The importance of a proof of security is vital in a field where security and privacy are under the spotlight.

A Very Short Introduction to RFID Technology

It is the first job of this article to give a brief introduction to RFID technology. We will describe the general purpose, architecture and basic operation of a traditional RFID system.

RFID is an automatic identification (Auto-ID) technology. Tiny data-carrying devices known as RFID tags are attached to objects. Readers can interrogate those tags wirelessly so that the associated objects can be identified. For instance, those objects could be supermarket articles to be scanned at the checkout. Other Auto-ID technologies include barcode systems, optical character recognition, biometrics and smart cards.

RFID tag: small device which can transfer data by radio frequency. Commonly used to identify objects.

The architecture of a traditional RFID system can be described as comprising five components (see also Figure 1):

- *A large set of resource-constraint tags:*
  An RFID tag, in its simplest form, is a small and relatively cheap device which can transfer its data by radio frequency to a nearby reader. Tags can be either active or

[1] This article is to be published online by Computer Weekly as part of the 2015 Royal Holloway info security thesis series. The full MSc thesis is published on the ISG's website.

passive. Active tags have their own source of power, whereas passive tags extract their energy from the magnetic field created by the reader. This means that a passive tag is inactive while outside the reader's locality.

- *A computationally powerful backend system:*
  In the simplest scenario, the main purpose of the backend system is to receive the unique identifiers of the tags via the readers, and process this information. Examples of backend systems include the control computer of a robot or a PC.

- *A set of computationally powerful readers:*
  Readers can be stationary or mobile devices that can read several hundreds of tags per second. They request information from a tag and forward the responses to the backend database server. Messages from the server will also be delivered to the tag via the reader.

- *A communication channel between backend server and readers:*
  This channel is considered secure. Both readers and backend server, being powerful devices, are assumed to be able to afford the use of strong security mechanisms to protect data both at rest and in transit.

- *A communication channel between reader and tags:*
  This wireless channel is considered insecure. Transmitted information can be potentially eavesdropped. Furthermore, tags respond to any reader within reading range, whether that reader is legitimate or not. Finally, it is important to note that it is also possible that the tag holder is unaware of clandestine scanning.

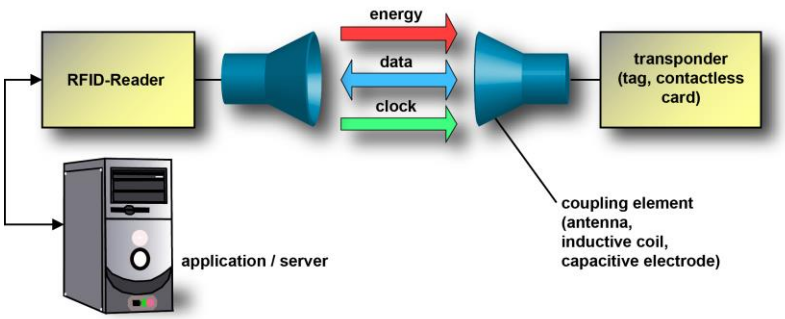

Figure 1: Architecture of an RFID System. This picture has been taken from Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiley, 3rd edition, 2010.

The basic operation in the simplest scenario is as follows. The tag is interrogated by a reader when it enters the reader's locality. The tag replies by sending its unique ID to the reader. The reader forwards the ID to the backend system. The backend system, having a database with information for all tags, is now able to identify the tag and optionally obtain related information about it. This protocol between backend system, reader and tag that we have just described can be seen in Figure 2.

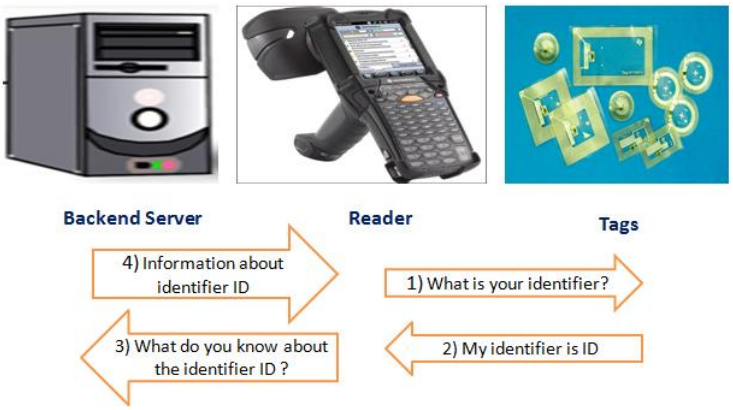

Figure 2: Basic Operation of an RFID System. The image of the backend has been taken from Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards*, *Radio Frequency Identification and Near-Field Communication*. Wiley, 3rd edition, 2010. The images of reader and tags are from RFID Journal, available at http://www.rfidjournal.com. Last accessed January 2015.

Why RFID Technology is Functionally Appealing

RFID is functionally very attractive. Indeed, this is shown by a number of salient characteristics, which include:

- *The identifier associated to an object is unique.* Tags are attached to objects, and the identifier of the object, which is stored in the tag, is unique. This is in contrast to barcodes, for instance, which identify the type of the object only.
- *It requires neither line-of-sight nor pre-established positioning*, which again provides an advantage over other Auto-ID technologies.
- *A reader can read hundreds of tags concurrently.* This can be advantageous to speed up identification in many applications, such as retail stores, where clients queue up at the checkout at peak times.
- *Tags have computing capability, even if constraint.* This allows the possibility of the implementation of functional mechanisms, including security ones. In particular, read/write operations can be made.
- *It is also noteworthy that RFID tags are very small.* For instance, the Hitachi Chemical Ultra Small Package UHF RFID tag is only 2.5 by 2.5 by 0.4 mm.
- *We finally note that RFID tags are potentially reusable.* Libraries constitute an example application where there is a business case to have tags which are not disposable.

Due to its functionality, RFID systems have already been deployed in many real-world applications, such as item-tracking in large retail stores, drug identification, pet identification, car immobilizer systems, and even in human beings. Like many technologies, this is a double-edged sword and brings with it much concern about privacy and ethics. Implantation in human beings, in particular, is a good illustration of unacceptable privacy invasion and ethical concerns generated by this technology.

Does RFID Security and Privacy Matter?

Despite its unquestionable functional advantages, RFID has not been widely deployed yet. Apart from the cost of the tags, which should continue to drop to make massive deployment possible, there are security and privacy issues that must be addressed. The nature of the response of the tag is crucial. In the basic scenario, the tag replies with its unique identifier, which is sent in the clear. Furthermore, this response is static. In other words, it does not change between tag interrogations. As will be evident in this section, this leads to such threats as information leakage or location tracking.

Moreover, tags can be quite small and thus go unnoticed. They are all-pervasive and respond to any reader that interrogates them. This alone poses privacy threats, which should also be addressed before large scale deployment of the technology. Figure 3 clearly shows how the privacy of Mr. Bob could be invaded if RFID technology was massively deployed in the absence of any security measures.

Salient privacy and security threats include:

- *Information leakage*, where the tag discloses potentially sensitive information about the object it is attached to. For instance, a drug name that reveals an illness of the tag holder.
- *Location tracking*, where the owner of the tag is traced in time and space by the tags they carry.
- *Disclosure of information on past transactions*, where exposure of the contents of the memory of the tag provides an adversary with information to correlate past transactions involving the tag. As a result, the movements of the tag holder can be traced. This is possible because low-cost RFID tags cannot afford tamper-resistance. This threat requires that the attacker has access to the victim's tag. In some applications, such as tagged books in a library, this can be easily accomplished. The attacker can also have access to the tag if the victim throws it away, for instance, after use of the object to which it is attached.
- *Tag cloning:* Tag cloning naturally leads to counterfeiting. This is also an important issue which should be dealt with if RFID is to gain widespread adoption. The negative consequences of counterfeited products entering the supply chain are varied and include risks to consumers (e.g. fake drugs), revenue losses for corporations, and reduction of tax income for governments.
- *Unauthorised Tag Killing:* For legitimate reasons, it is possible for a reader to send a PIN-protected kill command to a tag. After receiving it, the tag becomes definitively inoperable. This can be done, for instance, at the checkout at a supermarket in order to ensure privacy once the customer leaves. If an attacker is able to enter the supermarket with a concealed device and succeed in killing a significant number of tags, business processes can be severely affected. Tags can also be killed by means of RFID zappers. These devices generate strong pulses that irreversibly damage the tag.

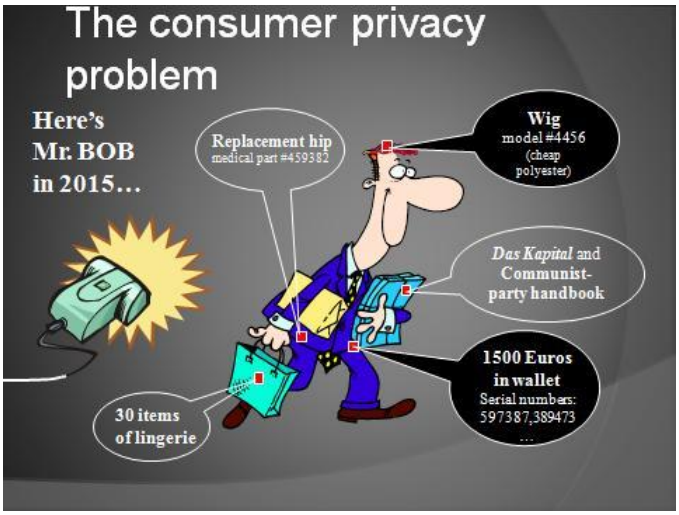

Figure 3: The Consumer Privacy Problem. This picture has been taken from A. Juels. *RFID Security and Privacy: A Research Survey*. IEEE Journal on Selected Areas in Communications, 24(2): 381 - 394, February 2006.

Security Protocols are a Major Weapon in our Armoury

In order to reduce security and privacy threats to acceptable levels, **a wealth of security protocols have been proposed.** These are meant to replace the simple protocol that implements the basic operation of the RFID system. See Figure 2 above.

It is evident that **the simple protocol is vulnerable to privacy breaches such as information leakage or location tracking:**

- **Information leakage:** An attacker eavesdropping on the wireless channel between reader and tag can learn the identifier ID of the tag. As a result, sensitive information can be revealed. For instance, it could be leaked that the tag holder has a replacement hip implanted, which is a clear invasion of his privacy. For this to be possible, of course, the attacker must have access to the relationship between the ID and its associated information.

- **Location tracking:** An attacker can track the tag holder in time and space by the tags he carries. The reason for this is that the response of the tag in the simple protocol is static. As a result, different responses can be easily correlated as they are always the same.

Fortunately, we can build a security protocol that addresses both issues. For example, for the first one, the tag could apply a cryptographic hash function to the ID, i.e. hash(ID), before sending it to the reader. The hashed identifier will look random to the attacker and information leakage will be prevented. However, this does not prevent the attacker from mounting a location tracking attack. To this end, he notes down the response(s) of one (or more) of Mr. Bob's tags. By concealing a number of readers at strategic locations, when a reader receives a response that matches one of those responses that the attacker noted down, the whereabouts of Mr Bob is known to the attacker.

Again, our security protocol can be improved so that this second threat is addressed. A commonly used technique involves randomizing tag responses. In other words, they will never be the same. For instance, the Randomised HashLock Scheme is a well-known protocol where the tag response is given by (r, hash(ID,r)), where r is a random number generated by the tag. Consequently, the attacker will no longer be able to correlate the responses of the tag, and, as a result, will no longer be able to track the tag holder.

Nonetheless, we want to emphasise that there are a myriad of other possible attacks. Furthermore, to date and to the best of our knowledge, **no protocol has been found that can be considered ideal for the purposes of security, privacy, scalability and requirements on tag**. Indeed, there is always a trade-off between, on the one hand, the security and privacy offered, and, on the other hand, the scalability of the resulting RFID system, or the requirements on tag. Scalability is important if the system is to perform efficiently when it contains a large number of tags. High requirements on tag can have a significant impact on the cost of the system.

"Dead Tags Tell no Tales" *– Ari Juels*

Are security protocols the only technical solution proposed to address security and privacy issues in RFID systems? No, they are not. Non-protocol proposals have also been suggested.

Let us consider one of them, namely, killing the tags. The reader sends a PIN-protected command to the tag, which becomes definitively inoperable after receiving it. It is clear that this measure is effective in enforcing privacy. For example, we could kill a tag at checkout. However, apart from technical obstacles, such as PIN management, there are several functional disadvantages. For instance, if tags are killed at the checkout, they will not be operable for smart appliances at home.

As a result, alternative non-protocol proposals have also been suggested. All these non-protocol proposals, though, require some involvement from the user. For instance, for tag killing, the user should bear PIN management.

Can you Verify the Security and Privacy of a Protocol?

We have seen that security protocols are a major mechanism to mitigate security and privacy threats to RFID systems. Unfortunately, their design is an error-prone task. As Roger Needham stated "they are three line programs that people still manage to get wrong". **If these protocols could be formally verified, the confidence in the security and privacy of the corresponding systems would increase substantially.**

Security Protocol Design is an Error-Prone Task

In 2008, the Single Sign-On (SSO) protocol used in the SAML-based Single Sign On for Google Applications was shown flawed by Alessandro Armando et al using the tool SATMC. Single Sign-On enables users to sign in once only and then access several applications.

What was the issue? It was possible for a dishonest service provider to impersonate a user at another service provider. The flaw was quickly reported to Google and to the Computer Emergency Response

Researchers in academia and industry have not been unaware of this issue, and a number of tools for the automated formal verification of security protocols have been developed.

By way of example, we can consider one of these tools, namely AVISPA, the predecessor of yet another tool, AVANTSSAR. AVISPA stands for Automated Validation of Internet Security Protocols and Applications, and includes:

- A modular formal language to model security protocols and the security properties to be verified. The language is HLPSL, short for High Level Protocol Specification Language.
- Four different validation backends which offer a number of automatic protocol analysis techniques.

The architecture of the AVISPA tool is shown in Figure 4 below:

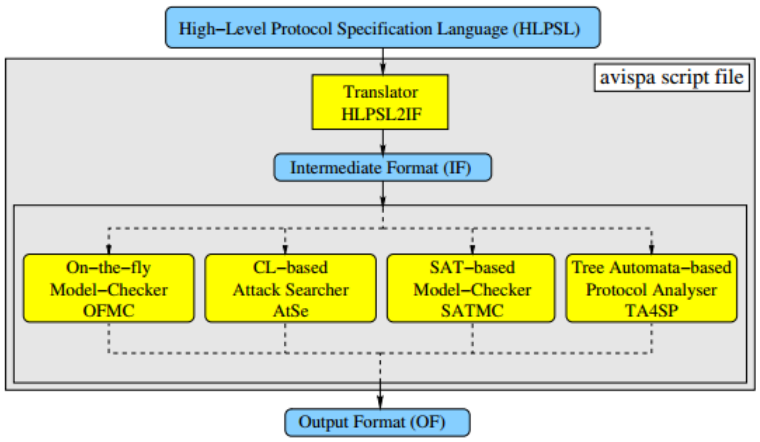

Figure 4: The Architecture of the AVISPA Tool. This picture has been taken from Laurent Vigneron. *Tutorial: A Tool Helping to Design Cryptographic Protocols*. 4th Conference on Security and Network Architectures (SAR). Available at the website of the AVISPA project, AVISPA Talks, http://www.avispa-project.org/talks/tutorialSAR2005-Vigneron.pdf. June 2005. Last accessed January 2015.

Let us examine the architecture in closer detail:

- Using HLPSL, the user of the tool models a target security protocol and the security properties to be verified. This model is input into the tool.
- Then, the HLPSL2IF translator translates the HLPSL specification to IF, which stands for Intermediate Format. IF models an infinite-state transition system.
- After that, the IF specification is input into up to four different validation backends, which search the state system to find attack states where the security properties to be verified are violated.
- Finally, the output of each backend indicates whether the protocol goals have been achieved. Furthermore, if an attack trace is found, it is also shown.

The Needham-Schroeder Public-Key Protocol (NSPK) is a well-known example of the error-prone nature of security protocol design, and the successful application of these tools. Seventeen years after its publication, it was shown flawed and subsequently fixed by Gavin Lowe using the Casper/FDR tool.

It was thought that the protocol met the mutual authentication security property. In other words, both parties in the protocol have assurance of each other's identities at the moment the protocol ends successfully. Unfortunately, a man-in-the-middle attack is possible that invalidates this claim. To this end, two sessions are needed. The first one between one of the honest entities, say Alice, and the attacker. The second one between the attacker and the other honest entity, say Bob. Once the second session finishes, Bob believes that he is communicating with Alice, when he is actually communicating with the attacker. The interested reader will learn that the attack would not have been possible if Bob had included his identity in the second message of the protocol. In fact, this fix is an example of the application of one of the Abadi and Needham's principles for the prudent design of cryptographic protocols.

Figure 5 shows the output of the AVISPA tool for NSPK and NSPK-fixed. For the former, see on the left, the tool reports that the protocol is unsafe. In addition, an attack is also found and shown. For the latter, see on the right, the tool reports that the protocol is safe.

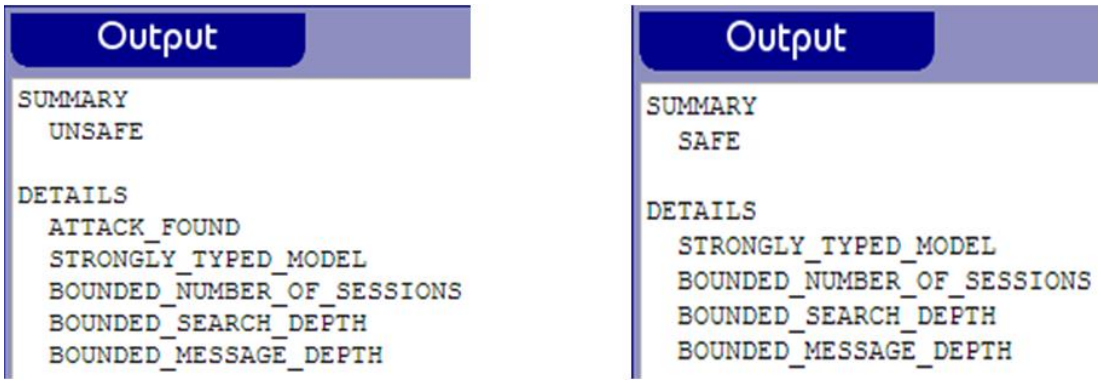

Figure 5: Output of the SATMC Backend of the AVISPA Tool for NSPK and NSPK-fixed.

Adapting Automated Formal Verification to RFID Systems

Tools for the automated formal verification of security protocols have been designed to deal with security protocols in general. However, security protocols for RFID systems feature some special characteristics, which are not always supported by existing tools. Sometimes, if they are, it is only in a limited way. Consequently, the aim and main contribution of Chapter 6 of the full report is to attempt to identify a number of these special characteristics and examine to what extent they are currently covered in existing tools. In other words, we provide suggestions for the improvement of these tools to better capture the requirements of the RFID field.

Let us consider some of these suggestions:

- **Support for the exclusive-or operator:** This operator is widely used amongst security protocols for low-cost RFID tags. Nonetheless, some tools do not support its use. One such example is the SATMC backend of the AVISPA tool.
- **Support for Diffie-Hellman exponentiation:** Support for this operator would prove advantageous once public key cryptography becomes affordable for low-cost RFID tags. Even though public key cryptography has been considered expensive, work is ongoing to reduce that cost**.**
- **Support to model different adversarial capabilities:** In the RFID environment, it would prove useful if the tool offered the possibility to restrict or add to the capabilities of the adversary. For example, low-cost RFID tags are not tamper-resistant. Consequently, it would be important that the tool could model an attacker's ability to compromise the contents of a tag, including secret data.
- **Support for location tracking analysis:** One of the main factors hindering widespread deployment of RFID technology is the threat to privacy. In particular, the possibility of the tag holder being tracked in time and space is a main issue. As a result, support for the automated formal verification of location tracking in security protocols for low-cost RFID tags is highly desirable. Unfortunately, it is rarely found amongst existing tools.
- **Support for an expressive modelling language:** Some protocols for low-cost RFID tags cannot be modelled unless the language of the tool is expressive enough to provide flow control constructs such as if-then-else.

Final thoughts

In this article, we have tried to justify and motivate the importance of both RFID technology and its associated security and privacy issues. We have highlighted the relevance of security protocols as a powerful technological mechanism to mitigate them. Furthermore, we have argued that if we could verify the correctness of those protocols, our trust in the security and privacy of the system would be significantly increased. In the light of such facts, researchers have developed several automated tools. Nevertheless, we have also observed that these tools have not been specifically designed to cover the special characteristics of protocols in the RFID environment.

It is our view that there is sufficient evidence to anticipate the progressive improvement of these tools to better meet the requirements of security protocols for RFID systems. There are two main reasons that support this statement. The first one is that there is an interest from the authors of the tools to incorporate additional features into them. The second one is that there is a need for confidence in the security and privacy of RFID systems. Indeed, recommendations by authorities to incorporate security and privacy into RFID systems have been made, both in Europe and in the US.

With this aim in view, formally verified security protocols represent an invaluable technological mechanism. However, we must not forget that technological solutions alone are not sufficient. Management measures must also be applied. Furthermore, legislators should also lay down rules to address misuse of the technology. We firmly believe that this

Biographies

Esteban Masobro received his BSc in Computer Science from the Polytechnic University of Catalonia in 1992. Since then, he has worked for Tecnocom as a software analyst, programmer and responsible for a number of projects in the banking industry. For the last eight years, he has focused on a software application monitoring online banking transactions for malicious activity. This application runs on the mainframe of the Europe's leading savings bank. This year, he has completed Royal Holloway's MSc in Information Security. His interests include Cryptography and Smart Card Security. He is also currently exploring the options to work on a PhD in Information Security.

Dr Konstantinos Markantonakis M.Sc., Ph.D., MBA is currently a Reader in the Information Security Group. His main research interests include smart card security and applications; secure cryptographic protocol design and analysis, Public Key Infrastructures (PKI), key management, mobile phone security, embedded system security. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects. He has worked as a Multi-application smart card Manager for VISA EU, responsible for multi-application smart card technology for southern Europe. Following from the he worked for Steer

Davies Gleave**,** responsible for advising transport operators and financial institutions on the use of smart card technology. He continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators, technology integrators.