



RFID Security Issues

by Andreas Krisch

Version: 1.0

1 Preface

In this paper we want to provide some thoughts on security issues concerning RFID systems and to highlight some of the areas that have to be considered regarding this topic.

To deal with security and RFID means to deal not only with security aspects of RFID systems but also with security aspects of anything or anyone affected by RFID systems. The widespread dissemination of identification technology and storage devices certainly has side effects and can lead to new threats in other areas and applications. Therefore the use of RFID challenges existing security systems, which have to be reviewed.

As with any other security measures, RFID security has to be a process rather than a singular event. This process should start at the technological basis, providing security mechanisms for applications built on this basis.

RFID security is not limited to technology but also has to deal with the question how secure it is to rely on information provided by RFID systems.

2 RFID Security Issues

Who controls what?

RFID Systems technically consist of RFID Tags, Readers, Communication Protocols, Information Systems, Networks, Lookup / Location Services and the like. These technical parts enable the collection of any amount of data in any quality on the tagged object or person. What is more this collected information can be searchable and accessible for a clearly defined group of persons or the general public.

The decision on who is allowed to collect data on tagged objects is taken by the person or organisation that mounts the tag on the object. In most of today's RFID Systems the data on the tag is accessible by anyone who is able to operate a RFID reader.

In current RFID applications the decision on who is allowed to access certain data is taken by the collector of the data. The collector can keep the data secret and protected or publish it and feed it into lookup and location services.

Finally the affected person (the person that owns or deals with the object) might be informed or not informed that the object in question is tagged, but in most of today's RFID applications has no means to do anything about it.

Are there new security threats?

Security threats stemming from RFID systems might not only be related to the technical components or the business processes they are intended for, but also might include any other security relevant situation. As some companies already prohibit the entrance to their buildings with camera equipped mobile phones to prevent industry espionage, security risks might also result from tagged objects. (Why not store commercial secrets on re-writeable RFID tags integrated into ones clothes?)

Therefore, unlike security risks stemming from other technologies (for example the use of personal computers), which can be addressed by securing the system one wants to operate, the usage of RFID technology will lead to dissemination of technology which cannot be controlled or secured by the affected parties.

Where to start?

Therefore security for RFID systems has to start at the very basis of the technology. Information on the tags has to be stored in a secure way. Communication protocols have to ensure secure communication. Information Systems have to use state of the art data protection mechanisms.

While it is important to analyse RFID security on basis of business processes, this is not enough due to the special characteristics of the technology. To implement security mechanisms (encryption, access control, ...) into every single part of RFID systems is key to enable not only the security of single business processes but to enable affected organisations or persons to build their security on this mechanisms.

Is security only a technical question?

While technically securing RFID systems to protect collected and stored information is one issue, a second one is securing a proper quality of the stored information. Given the example of tagged objects and the intelligent fridge that warns its users if a product has exceeded its best-before-date, the question arises how this date will be protected against alterations on the way of the product throughout the supply chain and who is responsible that this data is accurate.

This leads to some additional questions: Who owns and controls the data stored on the tag or collected in information systems? And is it secure to have this data controlled there? Under which jurisdiction is this information, in the EU or any third country?

If the data is stored and provided by the producer of an object: Does it constitute a risk that any access to the information can be monitored? Does it constitute a risk that this monitoring can include the movement of the object (via IP addresses for example, which are geographically assignable)? Does any of these risks change if the data is stored and provided by any other party?

The answer might be: It depends.

But if it depends, we will need mechanisms to make sure if we need to. Therefore it is important to implement means to verify who provides, alters, controls or is responsible for a given set of data. Information on a RFID tagged object can potentially be spread all over the globe and be connected via lookup services as needed. The challenge with this will be to separate accurate from inaccurate data. This will make the difference whether it is secure to base decisions on information provided by RFID systems or if the users get – spam-wise - flooded by irrelevant and unreliable data.