General Data Protection Regulations

RFID Threats and Vulnerabilities – Part 1

An overview of the **RFID Threats and Vulnerabilities Identified in CEN/TR 16670**

Not all threats are as obvious as these. It is important to gain an understanding of the threats and vulnerabilities to your RFID applications, and how these could affect privacy and data protection.

CONVERGENT SOFTWARE

General Data Protection Regulations

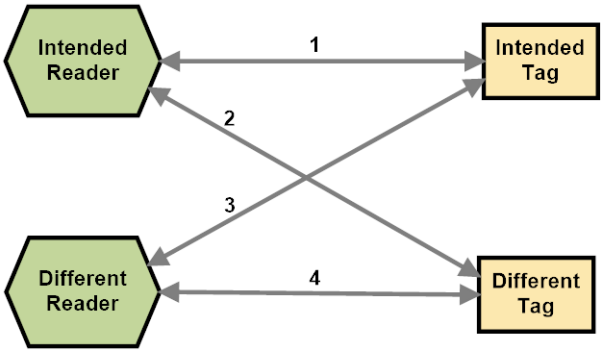
RFID Threats and Vulnerabilities – Part 1

CEN/TR 16670, *Information technology — RFID threat and vulnerability analysis* was developed as part of the European Commission Mandate M/436 on the subject of Radio Frequency Identification Devices (RFID) in relation to data protection, information security and privacy. This was seen as a subject-matter precursor to the development of the General Data Protection Regulation.

CEN/TR 16670 was a lab-based research project undertaken by RFID experts using real RFID tags and readers. The objective was to establish some facts about threats and vulnerabilities. Here is the scope of the report:

> The scope of the Technical Report is to consider the threats and vulnerabilities associated with specific characteristics of RFID technology in a system comprising:
> - the air interface protocol covering all the common frequencies;
> - the tag including model variants within a technology;
> - the interrogator features for processing the air interface;
> - the interrogator interface to the application.
>
> The Technical Report addresses specific RFID technologies as defined by their air interface specifications. The threats, vulnerabilities, and mitigating methods are presented as a toolkit, enabling the specific characteristics of the RFID technology being used in an application to be taken into consideration. While the focus is on specifications that are standardized, the feature analysis can also be applied to proprietary RFID technologies. This should be possible because some features are common to more than one standardized technology, and it should be possible to map these to proprietary technologies.
>
> Although this Technical Report may be used by any operator, even for a small system, the technical details are better considered by others. In particular the document should be a tool used by RFID system integrators, to improve security aspects using a privacy by design approach. As such it is also highly relevant to operators that are not SME's, and to industry bodies representing SME members.

The work is built on the classic communications model of Alice, Bob and Eve, where Alice and Bob are legitimate parts of the communication, and Eve is an interloper. For the purposes of explaining this for RFID, we have created this figure adapted from CEN/TR 16670 to avoid terms like "real" and "fake". The figure identifies four channels of communication:



1. This is the intended reader in the system, reading the tag presented to it.
2. This is the reader in the system reading a different tag, e.g. a tagged product from another retailer, a contactless card within range but not intended to be used for payment (now known as card clash). It could also be with a cloned tag.

CONVERGENT SOFTWARE

3. The intended tag being read by a different reader. This could be a malicious read (such as eavesdropping) or accidental, where the signal from a nearby reader within the system communicates with the tag (sometimes a problem within warehouses). There is also a write communication to change data on the tag.
4. When combined with a malicious (3) read the reader writes data to the tag to create a clone.

Let's look at some of the content of CEN/ TR 16670, by pulling together some points about some of the threats and vulnerabilities.

Denial of Service
This is defined as "preventing communication between the interrogator and the tags". Mechanisms include blocker tags or creating electromagnetic interference by active jamming. The vulnerability is in the air interface protocol and at the reader level.

If denial of service is invoked in the intended communication channel (1 in the model above) then it interferes with the RFID application and can be used for theft or disrupting the application, e.g. when a tag is expected. However if used in communication channel 3 it can be a privacy enhancing feature to protect a tag or card held by a person from malicious readers.

Skimming (unauthorised reading)
This is defined as an "active attack which consists in reading a tag" implying tag activation without consent of the operator of the application and the holder of a tag or smartcard. It is invoked in communication 3. Given that there are relatively few RFID protocols, and even fewer obvious ones for a particular type of application, skimming can be achieved using standard off-the-shelf products.

At one extreme the fear of skimming of contactless cards has resulted in lots of sales of RFID wallets (some with uncertain efficacy). While at the other extreme RFID operators of many applications deny that skimming can take place; have they not understood the black swan theory? Passport authorities take skimming seriously and employ a two-factor reading procedure requiring an OCR character string or 2-D bar code to be read, which then enables the chip to be read. CEN/TR 16670 goes on to point out a potential weakness of one of these features.

Eavesdropping
This is defined as a "passive attack, which consists in remotely listening to transactions between a Real Reader and a Real Tag". This differs from skimming in that it is applied at the protocol level to record the variation of the amplitude or the frequency during the communication to the RF communication of the real RFID application. While it is undertaken in communication channel 3 in our model, the intrusive "reader" is some form of analytical radio device such as a spectrum analyser.

Man-in-the-Middle / Relay
These two attacks are related, but slightly different. A classic Man-in-the-Middle attack is invoked in communication channel 1 in our figure. It requires the attacker to place a device, or devices, logically

between the legitimate tag and reader convincing each end point device that the communication is as intended, when the entire communication is controlled by the attacker. A wrong assumption about a relay attack is that all the devices have to be present and in view of the legitimate user. This is because the communication link within the attack does not depend on the RFID air interface protocol of the real tag and interrogator.

The relay attack is based on a specific weakness of the RFID tags that has the possibility to activate the device without the consent of the user. Indeed, a user is not able to switch off his tag. Thus an attacker can, therefore, access the tag discreetly, without knowledge of its owner, and relay information through a communication link between the tag and a remote Fake Reader. The reader will assume that the tag, and by implication the user, is in close vicinity and provides access to the attacker. A good example of a relay attack involving access control is provided here.

It is even possible to create a relay attack by using two NFC-enabled smartphones using standard features: one as a reader and another as a tag emulator. These features are available in most NFC enabled smartphones and can be applied to a number of RFID protocols. The relay attack requires the firmware on the phone to be modified and a simple app to link via WiFi to a server. It is also possible to do further manipulation of the data for a man-in-the-middle attack. We won't provide details of the source material presented at a research conference.

The threats and vulnerabilities identified in TR 16670 have different impacts depending on the RFID application, protocol, and even the products being used. To understand the real risks a privacy impact assessment, based in EN 16571:2014 *Information technology - RFID privacy impact assessment process* should be undertaken. Convergent Software Ltd. has developed compliant software to make this work easier and to produce consistent results.

In Part 2, we will look at some of the realities of read range found by the experts who developed CEN/TR 16670.