SLOVENSKI STANDARD
SIST-TP CEN/TR 16670:2014

01-september-2014

Informacijska tehnologija - RFID, analiza groženj in ranljivosti

Information technology - RFID threat and vulnerability analysis

Informationstechnik - Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID

Technologie de l'information - RFID, Analyse de vulnérabilité et de menace

Ta slovenski standard je istoveten z: **CEN/TR 16670:2014**

ICS:

35.040.50	Tehnike za samodejno razpoznavanje in zajem podatkov	Automatic identification and data capture techniques

SIST-TP CEN/TR 16670:2014 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16670

June 2014

ICS 35.240.60

English Version

Information technology - RFID threat and vulnerability analysis

Technologies de l'information - RFID, analyse vulnérabilité et de menace

Informationstechnik - Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16670:2014 E

Contents

Page

Foreword

This document (CEN/TR 16670:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC Technologies”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This Technical Report is one of a series of related deliverables, which comprise mandate 436 Phase 2. The other deliverables are:

— EN 16570, *Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application systems*

— EN 16571, *Information technology — RFID privacy impact assessment process*

— EN 16656, *Information technology - Radio frequency identification for item management - RFID Emblem (*ISO/IEC 29160:2012*, modified)*

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

— CEN/TS 16685, *Information technology — Notification of RFID — The information sign to be displayed in areas where RFID interrogators are deployed*

— CEN/TR 16669, *Information technology — Device interface to support* ISO/IEC 18000-3

— CEN/TR 16671, *Information technology — Authorisation of mobile phones when used as RFID interrogators*

— CEN/TR 16672, *Information technology — Privacy capability features of current RFID technologies*

— CEN/TR 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

— CEN/TR 16674, *Information technology — Analysis of privacy impact assessment methodologies relevant to RFID*

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96 'RFID in Europesteps towards a policy framework'. This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardization work programme identified in the first phase.

This document will provide the additional information of the RFID application that will need to be provided to a citizen by accessing the source identified on the sign where the RFID application is operating. This information will be aligned with the details set out in the Recommendation, but some of this might not be available at the outset, a Technical Report is the preferred form of initial delivery to establish basic requirements.

1 Scope

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.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
blocker tag
tag forcing the reader to enter in its singulation algorithm

Note 1 to entry: The idea of the blocker tag that looks like a tag that we can have in our pocket, is to emit both '0' and '1' creating a collision and forcing the reader to enter in its singulation algorithm. If the blocker tag emits simultaneously '0' and '1' (that requires two antennas), the reader may never complete its algorithm. The blocker tag should be seen as a hacker device that is able to generate a denial of service in a legitimate system. We can even assess that a blocker tag has always a malicious behaviour since it cannot be selective and forbids the reading of one tag whereas it authorises the reading of the others. Moreover, the blocker tag works like a tag in a passive mode. So, it requires being in the reader field and it will protect only a small volume around itself. So a blocker tag can be considered as a malicious tag, which prevents a legal system to read legal tags or as a mitigation technique preventing an illegal reader to read a legal tag.

2.2
blocking
another way to produce a denial of service is to interfere during the anti-collision sequence

Note 1 to entry: Different devices have been developed.

2.3
cloning
impersonation technique that is used to duplicate data from one tag to another

Note 1 to entry: Data acquired from the tag by whatever means is written to another tag. Unless the technology and application require the interrogator to authenticate the RFID tag, cloning is possible. Cloning the unique chip ID presents a significantly bigger challenge for the attacker, but some researchers claim that this is possible. There is also a special case of cloning that needs to be considered where the application accepts multiple AIDC technologies. Cloning data from an RFID-enabled card can be replicated in magnetic stripe. In some payment card systems, information that might be

cloned from an AIDC card could be used in payment situations known as 'cardholder not present' for purchases made on the Internet or by telephone. In this case, the clone is virtual and requires no encoding on another RFID tag.

2.4
denial of service
preventing communication between the interrogator and the tags

Note 1 to entry: There are two main ways to accomplish a "denial of service". The first one is to create electromagnetic interferences, the second one is to insert a blocker tag in the communication.

2.5
destruction
making the tag definitively unusable without using a logical kill function whenever such a function exist in the rfid protocol

Note 1 to entry: Destruction may refer to the reader too. Although this attack threats RFID system availability, it's different from deny of service because it can't reactivate and repair it. Destruction is considered as an attack when it's practiced without holder's knowledge. Two destruction types can be distinguished1) Hardware-and 2) Software destruction. While this can be seen as a security threat to the RFID operator, there are also situations where it might affect the individual. For example, if a public transport tag is accidentally damaged, then the individual's rights associated with it can be lost. In a similar manner as for tag removal, tag destruction can be used as a control to protect the privacy

2.6
eavesdropping
passive attack, which consists in remotely listening to transactions between a Real Reader and a Real Tag

2.7
guardian
special device developed by Melanie Rieback from a Dutch University to help citizens to communicate with their own contactless smartcards

Note 1 to entry: As an active device it can be turned into a blocking tag preventing an attacker to access such contactless cards. Thus, it can blur any pervasive reading by actively emitting a jamming signal in the sidebands of a typical RFID tag. Such a mechanism enables multiple functionalities:

— information can be sent to the reader or to the tag for secret key management, authentication, access control;

— monitoring of the RFID environment to warn of possible unsolicited reading;

— creation of collisions to prevent from the possible inquisitive reading.

As a consequence, the RFID guardian is a useful tool to ensure the privacy but it is also an efficient device to create denials of service. Whereas the blocker tag is designed to carry out a simple load modulation, the RFID guardian is an active device that requires batteries and that is able to emit is own signal. As a consequence, the distance of use is much larger.

2.8
jamming
creating a signal in the same range as used by the reader in order to prevent tags from communicating with the reader

Note 1 to entry: Because the RFID air interface protocol depends on radio signals, an attacker can exploit any such signals within the range of the communication between interrogator and tag

2.9
man in the middle
object or person interfering in the communication between a real reader and a real tag

Note 1 to entry: "Man in the middle" attack is often mistaken for relay attack. These are indeed similar but with the distinctive feature that in this attack the bit stream can be modified in the relay. Since the relay implies the adaptation of the modulation and of the bit coding by the Fake Reader or the Fake Tag for its use, it is not a problem to change some bits. This additional feature may take time but it will always be shorter than the timeout of the Real Reader.

2.10
RFID (1)
radio frequency identification
use of electromagnetic or inductive coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of an RF Tag

[SOURCE: ISO/IEC 19762-3]

2.11
RFID (2)
radio frequency identification
use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it

[SOURCE: RFID Recommendation C(2009) 3200 final]

2.12
relay attack
kind of Man in the Middle attack where fake reader and fake tag are used

Note 1 to entry: 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. Using this attack on cryptographic authentication schemes, the attacker would be able to convince both Real Reader and Real Tag to share a common secret key. The attacker would not be able to view in plaintext any subsequent communications. This is not needed as long as it can continue relaying the respective messages. The attack can be given an active twist by relaying the initial authentication sequence after which subsequent data is modified and relayed. Relay attacks involve two different devices and as a consequence two attackers that should coordinate each other except if the relay is really short (an arm's length for example). The device that will skim the data of the attacked person is the Fake Reader. The Fake Reader is linked via the relay to the Fake Tag, a Fake Tag that will reproduce the data of the Real Tag.

2.13
side channel analysis
analysis which allows to find secret information by using the analysis of the RF field during the processes made by the tag processor

2.14
side channel attack
attack which uses a Side Channel Analysis

Note 1 to entry: In a side channel attack, the information that is usually exploited includes timing information, power consumption or even electro-magnetic fields. This type of attack requires sufficient time, specialist equipment, and deep knowledge of the internal systems on which the cryptographic and other algorithms are implemented.

2.15
singulation
identifying an individual tag in a multiple-tag environment

2.16
skimming
active attack which consists in reading a tag

Note 1 to entry: It includes powering and modulation. It implies distance tag activation without consent of the operator of the application.

2.17
substitution
action of changing a real reader or tag by a fake one

Note 1 to entry: There are two kinds of substitution:

— Reader substitution: Reader substitution is a kind of smart jamming. During such an attack a Fake Reader radiates a RF magnetic field in order to perturb a communication between a Real Reader and a Real Tag. The goal of this perturbation is not to entirely block the communication but to transform the initial reader's message to access forbidden zones of the tag memory or to induce misusing of the tag. Depending of the goal of the attacker, all Real Reader's messages can be transformed or some messages can be kept unchanged (during initialisation protocol or Real Tag's authentication for example). A way of setting up such an attack is to make the Fake Reader speak louder than the Real Reader. This can be easily done if the Real Reader is far from the tag. The Fake Reader attacker has only to be nearer than the Real Reader. This attack is very complex to set up.

— Tag substitution: Tag substitution cannot be performed in the same way as reader substitution. Indeed, the attacker's tag cannot "speak" louder than the official Real Tag. The attacker has to use a powered RF device near the Real Reader and Real Tag to create a RF signal. This signal can then be superimposed on the official backscattered signal from the Real Tag leading to the cancellation of this signal from the Real Reader's point of view.

2.18
tag
RFID device having the ability to produce a radio signal or a RFID device which re-couples, back- scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer

[SOURCE: RFID Recommendation C(2009) 3200]

2.19
tag cloning
action of taking information from a real tag to create a fake tag with same functionalities

2.20
truncation
action of shortening (a number or a word) by dropping one or more digits or bits

3 Symbols and abbreviations

ALOHA	Probabilistic algorithm used for RFID tag singulation.
CCTV	Closed Circuit Television
CSP	Communications Service Provider
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DPP	Data Protection and Privacy
EAS	Electronic Article Surveillance
EPC	Electronic Product Code
ESO	European Standard Organisation
ETSI	European Telecommunication Standard Institute

FR	Fake Reader
NOTE 1	The reader used for the attack and not part of the application.
FT	Fake Tag
NOTE 2	The tag used for the attack and not part of the application.
HF	High Frequency
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Standard Organization
LF	Low Frequency
OCR-B	Optical Character Recognition type B (cf. ISO 1073-2).
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
RR	Real Reader
NOTE 3	The reader used in the application.
RT	Real Tag
NOTE 4…	The tag used in the application.
SIM	Subscriber Identification Module
SME	Small and Medium Enterprise
STF	ETSI Special Task Force
TID	Tag IDentifier
UHF	Ultra High Frequency
UII	Unique Item Identifier
UWB	Ultra Wide Band
WLAN	Wireless Local Area Network

4 Threats and Attack scenarios

4.1 Introduction

This clause analyses the various combinations of attacks to a RFID system comprising a RR and a RT, with the help of a FR, or a FT, or both a FR and a FT. Figure 1 summarises the combination of different readers and tags for a given attack.

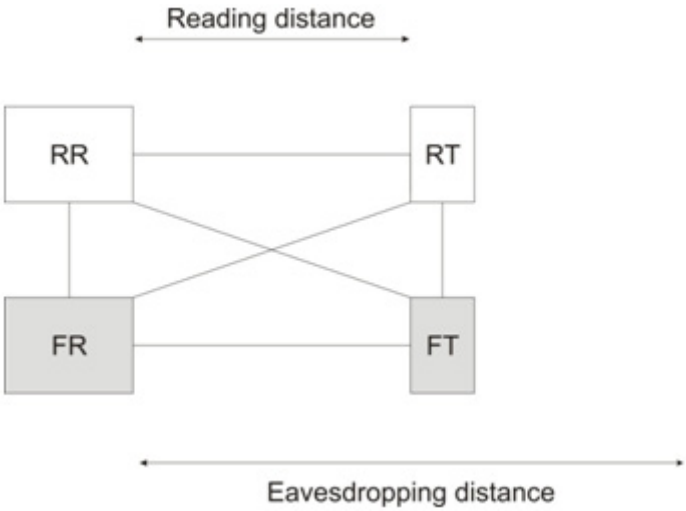

Figure 1 — Penetration Testing Framework: a proposed pictorial representation

4.2 Attacks to an RFID System with a Fake Reader

Three RFID devices are operating at the same time: RR + RT + FR.

A Fake Reader operating within the range of a RFID application, can perform two types of attacks:

— By generating radio waves at the same wavelength of the application it can generate interference with the application communication sequences, if sufficient energy is deployed (field strength in the vicinity of the RR). This prevents the exchange of data between RR and RT, and creates a denial of service.

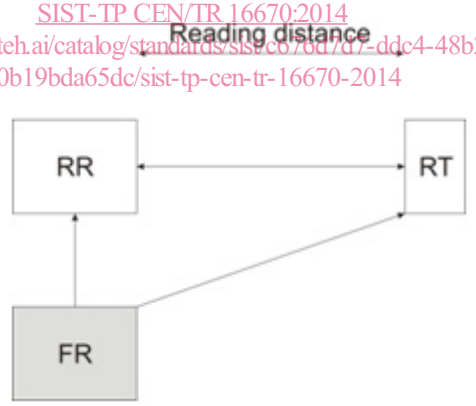

Figure 2 — FR used as interferer

— The reader can also listen (record the variation of the amplitude or the frequency during the communication) to the RF communication of the real RFID application. The FR is eavesdropping on the RFID application.

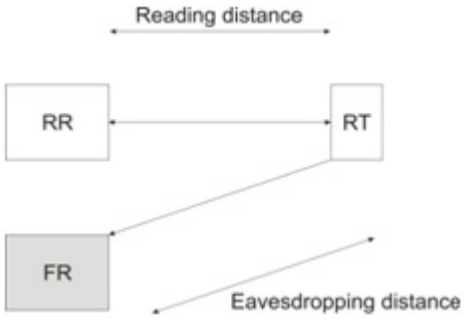

Figure 3 — FR used to eavesdrop RT's signal

NOTE An attack performed by a Fake Reader is not possible if there is no Real Tag in the environment, since a Real Reader will not respond to a Fake Reader.

4.3 Attacks to a RFID system with a Fake Tag

Three RFID devices are operating at the same time: RR + RT + FT.

If the FT talks to the RR at the same time then the RT, the RR will not determine which of the two tags will send the correct information creating a denial of service.

Figure 4 — Attack performed by a FT

NOTE An attack performed by a Fake Tag alone will be inoperative if there is no Real Reader in the environment, since no communication can exist between two tags.

4.4 Attacks to a RFID system with a Fake Reader and a Fake Tag

Four RFID devices are operating at the same time: RR + RT + FR + FT.

In this scenario, two attacks can be performed at the same time or independently:

— RT is activated by FR. FR writes the information collected from RT into FT creating a cloned tag;

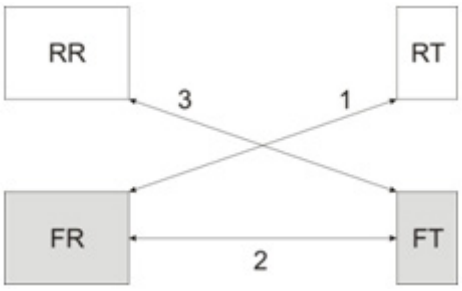

Figure 5 — Creating a cloned tag

— FT is activated by RR and responds with its own fake data creating a Man in the Middle attack.

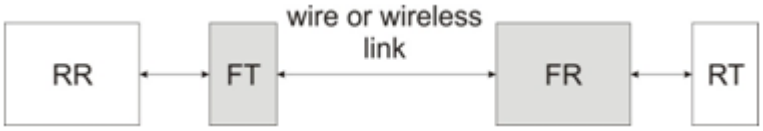

Figure 6 — Relay attack

4.5 Attack to a Real Tag with a Fake Reader and a Fake Tag

Since there is no communication possible between two tags, the attack can be performed only by the Fake Reader. See 4.6.

4.6 Attack to a Real Tag with a Fake Reader

A Fake Reader activates a Real Tag and writes new information in the Real Tag creating an **unwanted tag activation.** Real data may be modified without consent.

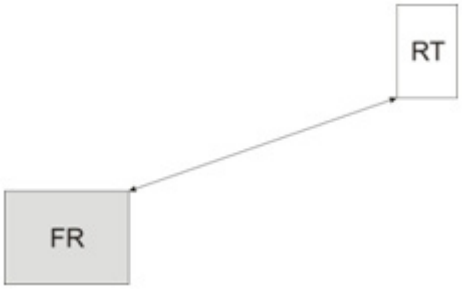

Figure 7 — Unauthorised tag activation

We can dissociate the activation side of the attack from the listening side. In that case, we need a first fake reader which only purpose is to activate the tag by sending it a transmitting signal. Another fake reader can be placed farther away just to eavesdrop the backscattered signal from the real tag. The spatial limitation of such an attack is given by the activation range. Some commercial systems make use of this approach by using different activation points to "illuminate" a wide area and place only one receiver to collect all the tags' responses. Special signal processing is set up to recover the antenna which activates the tag and therefore performs localisation.

4.7 Attack to a Real Reader with a Fake Tag

The Fake Tag can send false information to the Real Reader. The consequence can be similar to the case of an unwanted activation.