This is a free page sample. Access the full version online.

Irish Standard Recommendation
S.R. CEN/TR 16670:2014

Information technology - RFID threat and vulnerability analysis

© CEN 2014 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

S.R. CEN/TR 16670:2014

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
CEN/TR 16670:2014	2014-06-04

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2014-06-21	35.240.60
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

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

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TR 16670:2014 E

This is a free page sample. Access the full version online.

Contents

Page

Foreword 4
Introduction 5
1 Scope 6
2 Terms and definitions 6
3 Symbols and abbreviations 9
4 Threats and Attack scenarios 10
4.1 Introduction 10
4.2 Attacks to an RFID System with a Fake Reader 11
4.3 Attacks to a RFID system with a Fake Tag 12
4.4 Attacks to a RFID system with a Fake Reader and a Fake Tag 12
4.5 Attack to a Real Tag with a Fake Reader and a Fake Tag 13
4.6 Attack to a Real Tag with a Fake Reader 13
4.7 Attack to a Real Reader with a Fake Tag 13
5 Vulnerabilities 14
5.1 Introduction 14
5.2 Denial of service 14
5.3 Eavesdropping 14
5.4 Man in the Middle 15
6 Mitigation measures 15
6.1 Introduction 15
6.2 Mitigation measures for secured RFID Devices 15
6.2.1 Mitigation measures for tags 15
6.2.2 Mitigation measures for readers 15
6.2.3 Mitigation measures for the Air Interface Protocol 15
6.3 Mitigation measures against attacks 15
6.3.1 Introduction 15
6.3.2 Eavesdropping 15
6.3.3 Skimming 15
6.3.4 Relay attack 16
6.3.5 Denial of Service 16
7 Conclusions 16
Annex A (informative) **Attack scenarios** 18
A.1 Amusement parks takes visitors to RFID-land 18
A.1.1 Introduction 18
A.1.2 Threat scenarios 18
A.1.3 DPP objectives of relevance 19
A.1.4 Security objectives of relevance 19
A.1.5 Privacy objectives of relevance 20
A.2 Purpose of Use and Consent 20
A.2.1 Purpose 1 20
A.2.2 Purpose 2 (with explicit consent) 21
A.2.3 Purpose 3 (with no explicit consent 21
A.3 Multi-tag and purpose RFID environment for Healthcare 22
A.3.1 Scenario description - Emergency 22
A.3.2 The hospital RFID environment 22
A.3.3 Arrival at the hospital 23
A.3.4 Treatment at the hospital 24
A.3.5 The value of the drug prescribed 24
A.3.6 Returning home 24
A.3.7 The home RFID environment 24

This is a free page sample. Access the full version online.

A.3.8 Drug repeat prescription and out of date drug recycling 25
Annex B Original Test Set ups and Results 26
B.1 Test Area 26
B.2 Equipment 26
B.3 Overview of the Tests 27
B.3.1 Introduction 27
B.3.2 Range tests 27
B.3.3 Write Tests 27
B.3.4 Illicit Reading 27
B.3.5 Eavesdropping 28
B.3.6 Detection inside buildings 28
B.3.7 Combined EAS/RFID systems 28
B.4 Test procedures and results 28
B.4.1 General 28
B.4.2 Reading range 30
B.4.3 Write range 37
B.4.4 Illicit reading 41
B.4.5 Eavesdropping 46
B.4.6 Detection inside buildings 47
B.4.7 Combined EAS/RFID system 48
B.5 Analysis of results 48
B.6 Conclusions 49
Annex C Additional Test Set ups and Results 50
C.1 Introduction 50
C.2 Scope of tests 50
C.3 Documenting the results 50
C.4 Equipment required for additional tests 50
C.5 Description of tests 51
C.5.1 Activation distance for HF system 51
C.5.2 Activation distance for UHF system 52
C.5.3 Eavesdropping tests for HF system 53
C.5.4 Eavesdropping tests for UHF system 55
C.6 Test results 56
C.6.1 Equipment utilised during the tests 56
C.6.2 Description of Tests 56
Bibliography 70

This is a free page sample. Access the full version online.

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*

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

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

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation