Problem and Improvement of the Composition Documents for Smart Card Composed Product Evaluation

September 10, 2013

Jeonghoon Han (1st Author)

TTA (Telecommunications Technology Association), CIST (Center for Information Security Technologies) of Korea University

jhhan@tta.or.kr

Seungjoo Kim (Corresponding Author)

CIST (Center for Information Security Technologies) of Korea University

skim71@korea.ac.kr

Contents

01. Introduction

02. Problems

03. Improvement

Introduction

Introduction

About me…

Senior Research Engineer (jhhan@tta.or.kr)

Information Security Evaluation Department, Software Testing & Certification Laboratory
TTA (Telecommunications Technology Association)

PhD Course (xbtion4ever@korea.ac.kr)

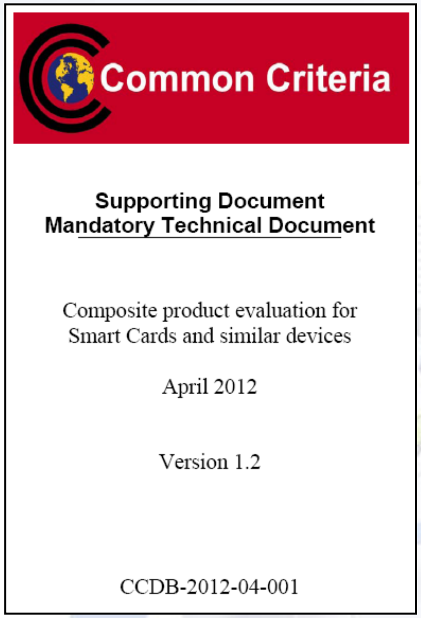
CIST (Center for Information Security Technology), Korea University

Corresponding Author (Professor. Seungjoo Kim, skim71@korea.ac.kr)

CIST (Center for Information Security Technology), Korea University

Introduction

About COMP...



Common Criteria

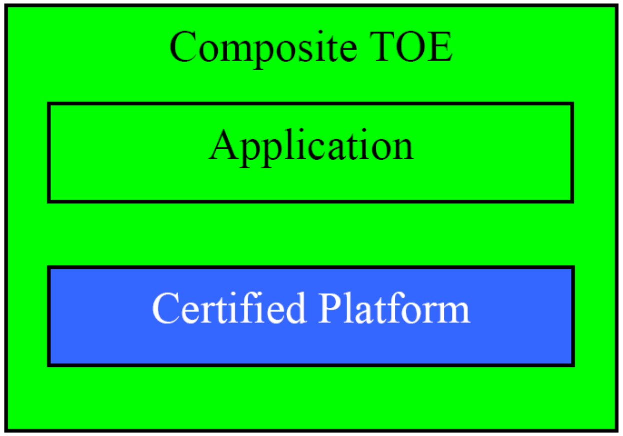
Supporting Document
Mandatory Technical Document

Composite product evaluation for
Smart Cards and similar devices

April 2012

Version 1.2

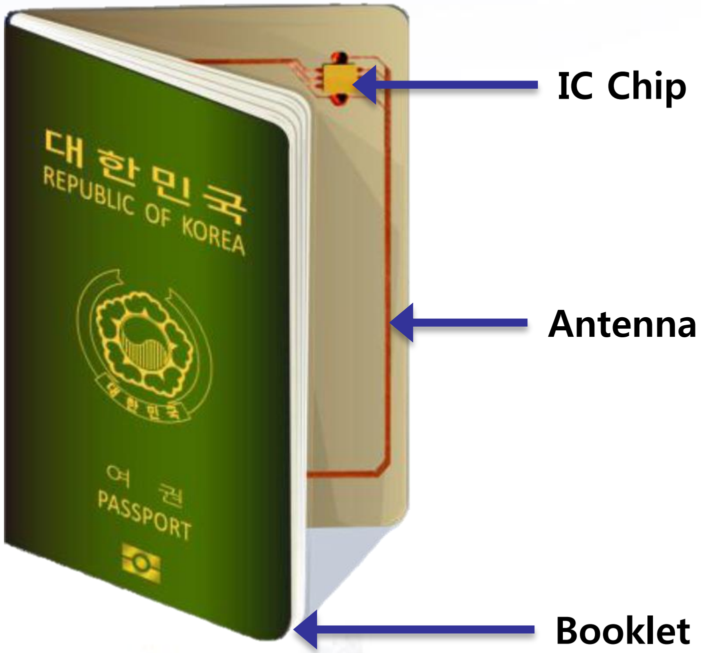
CCDB-2012-04-001



Composite TOE

Application

Certified Platform



Introduction

About presentation...

Problems(difficulties) in composite documents

Insufficient information…

- No exceptional cases of mandatory implementation requirements
- No way to verify integrity of certified platform TOE's software library

Improving problems of composite documents

Need to provide information about exceptional cases and integrity…

- To avoid applying unnecessary countermeasures of crypto functions
- To confirm that certified platform TOE's configuration is not modified

Problems

Problems – #1

ETR_COMP (from the platform TOE evaluation facility)
Guidance (from the platform TOE manufacturer)

Above composite documents enforce to apply the following countermeasure against perturbation attack on DES.

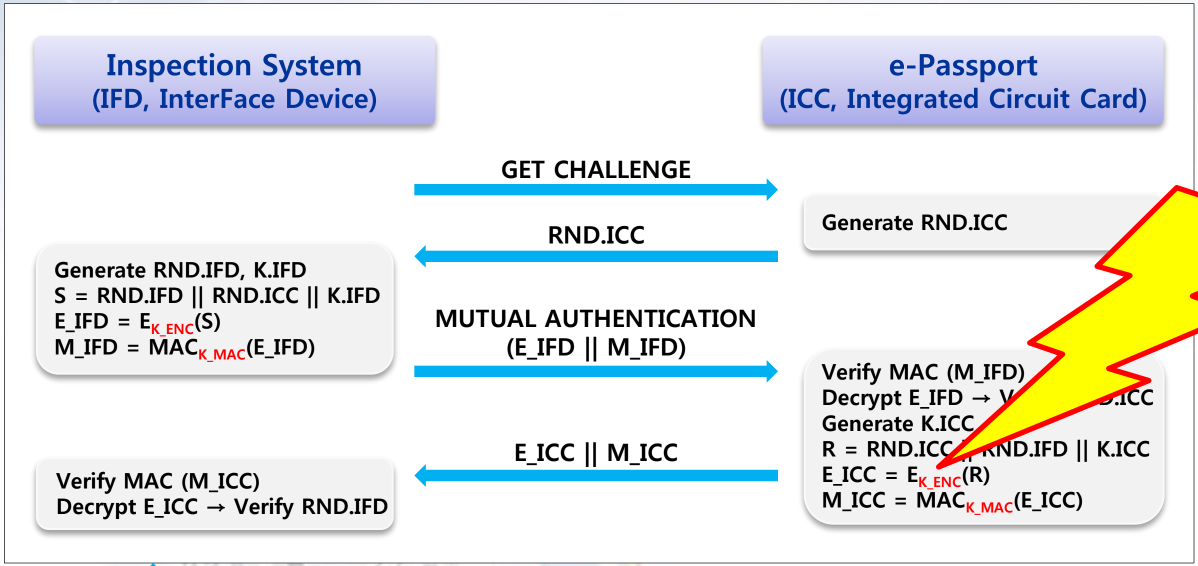
"It is MANDATORY … (countermeasure)."

If application developer can analyze attack potential about perturbation attack, it is easy to determine whether to apply the countermeasure. However, unfortunately, most developers can not do that.

So when evaluating smart card composite product, we have some difficulties.
In next slide, let me show you a case of the BAC mechanism in MRTD.

Problems – #1

Authentication and Key Establishment
(ISO/IEC 11770-2 Key Establishment Mechanism 6 using 3DES)



Inspection System
(IFD, InterFace Device)

e-Passport
(ICC, Integrated Circuit Card)

GET CHALLENGE →

Generate RND.ICC

← RND.ICC

Generate RND.IFD, K.IFD
S = RND.IFD || RND.ICC || K.IFD
E_IFD = E_{K_ENC}(S)
M_IFD = MAC_{K_MAC}(E_IFD)

MUTUAL AUTHENTICATION
(E_IFD || M_IFD) →

Verify MAC (M_IFD)
Decrypt E_IFD → V[illegible].ICC
Generate K.ICC
R = RND.ICC || RND.IFD || K.ICC
E_ICC = E_{K_ENC}(R)
M_ICC = MAC_{K_MAC}(E_ICC)

← E_ICC || M_ICC

Verify MAC (M_ICC)
Decrypt E_ICC → Verify RND.IFD

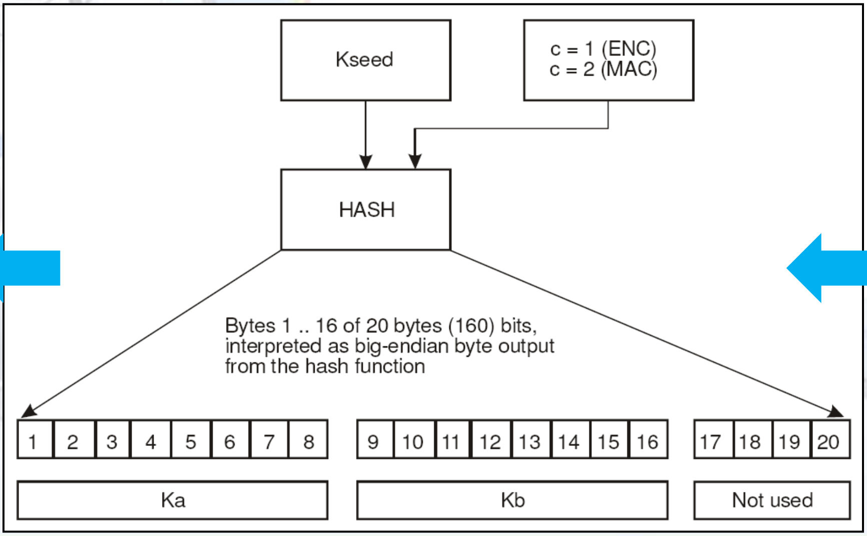
Key Derivation Mechanism
(Doc 9303 MRTD Part 1 - APPENDIX 5, 6)

```
MRZ =   P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
        L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Document number	= L898902C<,	check digit = 3
Date of birth	= 690806,	check digit = 1
Date of expiry	= 940623,	check digit = 6
MRZ_information	= L898902C<369080619406236	

H_{SHA-1}(MRZ_information) = '239AB9CB282DAF66231D C5A4DF6BFBAEDF477565'

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'


Kseed
c = 1 (ENC)
c = 2 (MAC)
HASH
Bytes 1 .. 16 of 20 bytes (160) bits, interpreted as big-endian byte output from the hash function
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
Ka
Kb
Not used

K_ENC (c='00000001')

K_a = 'AB94FDECF2674FDF'
K_b = 'B9B391F85D7F76F2'

K_MAC (c='00000002')

K_a = '7962D9ECE03D1ACD'
K_b = '4C76089DCE131543'

Problems – #1

When attacker has a victims’ MRTD,

The attacker doesn’t need to perform perturbation attack because he(or she) can read easily victim’s private information of the MRTD booklet.

When attacker doesn’t have a victims’ MRTD,

The attacker can’t operate BAC mechanism because he(or she) doesn’t know MRZ information.

Although the attacker know MRZ information, it is unfeasible for the attacker to perform perturbation attack on victims’ MRTD in real environment (e.g. immigration inspection in the airport)

In conclusion, application developers don’t need to apply the countermeasure against a perturbation attack on 3DES.

Problems – #2

Generally platform TOE includes software libraries related to cryptographic functions. Composite product evaluator shall confirm platform TOE’s integrity about that certified configuration is not modified.

However, there is not proper method to verify an integrity of the software libraries.

- Composite documents provide only version number of the software libraries

- Version number is not sufficient to confirm that certified platform TOE’s configuration is not modified

Improvement

Improvement

For improving the problem #1

It is inappropriate that the composition documents specify all possible exceptions. But, if following information is included in those documents, it could be very helpful to application developers.

Application Note:

Application developer could determine whether to apply the countermeasure as an attack potential in composite product's operational environment.

1. Necessity of perturbation attack
2. Possibility for an attacker to operate TOE's security features
3. Exploitability of obtained secret information, if 2nd step is possible

Improvement

For improving the problem #2

Most of software products provide a verification method of its integrity. (e.g. checksum or hash value of original image file)

To verify an integrity of the IC chip's software libraries, composition documents (ETR_COMP) should provide checksum(or hash) value and calculation method.

(Example)

Checksum: 85FF1D426F37C1B6067DBE834A2A76B543E5CA87617F395B428B1DFB1B761C47

Calculation method: SHA256

References & Bio

References

[01] Doc9303 “Machine Readable Travel Documents” Part1 “Machine Readable Passports” Volume 2 “Specification for Electronically Enabled Passports with Biometric Identification Capability” Sixth Edition, International Civil Aviation Organization(ICAO), August 2006

[02] Composite product evaluation for Smartcards and similar devices Version 1.2, CCDB-2012-04-01, April 2012

[03] Application of Attack Potential to Smartcard Version 2.8, CCDB-2012-04-002, April 2012

Bio & Acknowledgement

Jeonghoon Han

E-mail: jhhan@tta.or.kr

Jeonghoon Han received his B.S. (2007), M.S. (2009) in computer engineering from Sungkyunkwan University (SKKU) in Korea. After MS degree, He had worked at Korea Internet & Security Agency (KISA) from 2009 to 2011. At present, He is working for Telecommunications Technology Association (TTA) as CC evaluator and studying for information assurance under PhD course at Center for Information Security Technologies (CIST) of Korea University (KU). His research interests include side channel analysis, reverse engineering and information assurance.

Seungjoo Kim (Corresponding Author)

E-mail: skim71@korea.ac.kr
Homepage: www.kimlab.net
Facebook, Twitter: @skim71

Prof. Seungjoo Kim received his B.S. (1994), M.S. (1996), and Ph.D. (1999) in information engineering from Sungkyunkwan University (SKKU) in Korea. Prior to joining the faculty at Korea University (KU) in 2011, He served as Assistant & Associate Professor of School of Information and Communication Engineering at SKKU for 7 years. Before that, He served as Director of the Cryptographic Technology Team and the (CC-based) IT Security Evaluation Team of the Korea Information Security Agency (KISA) for 5 years. Now he is Full Professor of Graduate School of Information Security at KU, and a member of KU's Center for Information Security Technologies (CIST). Also, He has served as an executive committee member of Korean E-Government, and advisory committee members of several public and private organizations such as National Intelligence Service of Korea, Digital Investigation Advisory Committee of Supreme Prosecutors' Office, Ministry of Justice, The Bank of Korea, ETRI(Electronic and Telecommunication Research Institute), and KISA, etc. His research interests include cryptography, information security and information assurance.

The corresponding author (Seungjoo Kim) acknowledges the support of the IT R&D program (10043959, Development of EAL 4 level military fusion security solution for protecting against unauthorized accesses and ensuring a trusted execution environment in mobile devices) of KEIT/MOTIE and MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center)) support program (NIPA-2013-H0301-13-1003) supervised by the NIPA(National IT Industry Promotion Agency)

Thank you