Rating Attack Potential for Smartcards

Alain MERLE, CEA-LETI

Technical manager of CESTI LETI

on behalf of ISCI (JHAS) group

The ISCI group

(International Security Certification Initiative)

cea

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

gemalto

PHILIPS

Giesecke & Devrient

Trusted Labs

viaccess
a France Telecom company

ATMEL

TÜViT

infineon

T · · Systems ·

SiVenture
A division of NDS

TNO

ST

RENESAS
Everywhere you imagine.

MasterCard
Worldwide

SERMA TECHNOLOGIES

SRC
security consulting

Riscure

cea
leti

ISCI objectives

- Standardize the evaluation practice for smartcards
  - Common understanding and interpretations
  - Comparable results of evaluations (including Vulnerability Analysis)
- Promote the evaluation/certification practice

Why a specific table for smartcards ?

- High challenging area
  - Smartcard is ***the*** security device
  - Intensively used in R&D for attack/protection
  - State of the art evolving extremely quickly
  - Powerful attacks not necessarily "***costly***"
- VLA.4 products must be secure
  - Resistant to known attacks
- Defining potential vs state of the art

Rating table

V2.0

Factors	Identification	Exploitation
Elapsed Time		
Expertise		
Knowledge of the TOE		
Access to TOE		
Equipment		
Open samples		

Modified factors

New factor

tion of
cation and
Exploitation

V1.0

Factors	Identification	Exploitation
Elapsed Time		
Expertise		
Knowledge of the TOE		
Access to TOE		
Equipment		

Rating table

V2.0

Factors	Identification	Exploitation
Elapsed Time		
Expertise		
Knowledge of th		
Access to TOE		
Equipment		
Open samples		

V1.0

Factors
Elapsed Time
Expertise
Knowledge of th
Access to TOE
Equipment

Rating

$R_{Final} = R_{Identification} + R_{Exploitation}$

Identification: Rate the effort to *demonstrate* that the attack is possible

- Produce a ***script***
- Could be limited to a step (ex a subkey)

Exploitation: Rate the effort to *perform* the full attack (ie execute the script)

- Could be estimated

Rating table: Elapsed time

V2.0

Factors
Elapsed Time
Expertise
Knowledge of the T
Access to TOE
Equipment
Open samples

< 1 hour	0	0
< 1 day		
< 1 week		
< 1 month		
> 1 month		
Not practical		

Better definition of “**Not practical**”

- Related to the attack path
- Related to application specificities
- Attacker’s time and not evaluator’s time
- Removing the 3 months duration

V1.0

Factors
Elapsed Time
Expertise
Knowledge of the T
Access to TOE
Equipment

< 1 hour		
< 1 day		
< 1 week		
< 1 month		
1 m < time < 3 m		
Not practical	0	0

Rating table: Expertise

V2.0

Factors
Elapsed Time
Expertise
Knowledge of the TOE
Access to TOE
Equipment
Open samples

Layman	0	0
Proficient		
Expert		
Multiple Expert		

New level: **Multiple expert**

- Multi steps attacks
- Distinct expertises
- Ex: ***hardware*** and ***cryptography***

V1.0

Factors
Elapsed Time
Expertise
Knowledge of the TOE
Access to TOE
Equipment

layman		
Proficient	2	2
Expert	5	4

Rating table: Knowledge of the TOE

V2.0

Factors
Elapsed Time
Expertise
Knowledge of the TOE
Access to TOE
Equipment
Open samples

Public	0	0
Restricted (FSP)	2	2
Sensitive (HLD/LLD)	4	3
Critical (IMP)	6	5
Very critical hardware design	**9**	**na**

V1.0

Factors
Elapsed Time
Expertise
Knowledge of the TOE
Access to TOE
Equipment

Very critical hardware design

- For hardware, “source” data base

requires the use of “bespoke” tools

Rating table: Access to the TOE

V2.0

Factors
Elapsed Time
Expertise
Knowledge of the TO
Access to TOE
Equipment
Open samples

< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

V1.0

Factors
Elapsed Time
Expertise
Knowledge of the TO
Access to TOE
Equipment

< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

Rating table: Equipment

V2.0

Factors
Elapsed Time
Expertise
Knowledge of the TOE
Access to TOE
Equipment
Open samples

None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6
Multiple Bespoke	**7**	**8**

V1.0

Factors
Elapsed Time
Expertise
Knowledge of t
Access to TOE
Equipment

Multiple equipments

- Apply only for ***distinct*** types of equipments
- Multiple specialized = Bespoke
- New level: Multiple bespoke

Rating table: Open samples

V2.0

Factors	Identification	Exploitation
Elapsed Time		
Expertise		
Knowledge of the TOE		
Access to TOE		
Equipment		
Open samples		

Public	0	
Restricted	2	
Sensitive	4	
Critical	6	

V1.0

Factors		
Elapsed Time		
Expertise		
Knowledge of the TOE		
Access to TOE		
Equipment		

Open samples: Why ?

- Related to composite evaluations: SW put on certified HW
- 2 types
  - HW loaded with test software implementing no security features
  - Samples loaded with known secrets (or enabling loading)
- Objective:
  - Calibrate (or tune) the benches to be sure to test the SW countermeasures
  - Save evaluator’s time
    - Split the complexity
    - Verify quickly the success of an attack (subkey)

Open samples: How to rate ?

- Values
  - Defined according to the classical protection rules (Public, Restricted, Sensitive, Critical).
  - Value is given by the IC evaluation (ETR Lite)
- Rating: $\mathbf{R_{Final} = MIN\,(R_{With}, R_{Without})}$
  - Main effect on ***time*** factor
  - If needed both types could be included

$\mathbf{R_{With}}$	$\mathbf{R_{Without}}$
• Use resources ***spent*** by the evaluator • Add the “open sample” factor value	• Estimate the attackers resources • Don’t use “open sample” factor

Resistance: Unchanged

Range of values	Resistance to attacker with attack potential of	SOF rating	Compatible with
0 - 15	No rating	No rating	FAIL
16 - 24	Low	Basic	VLA.2
25 - 30	Moderate	Medium	VLA.3
>= 31	High	High	VLA.4

Conclusion

- The rating table
  - Result of years of use by all the actors
  - Better reflects the state of the art (attacks, tests, evaluation practice)
- Extensive work done on examples
  - Verify the rating of “standard” attacks
  - Give landmarks
- A step for
  - Common understanding of evaluations practice
  - Standardization over various countries, CB, labs
- Future work
  - CC V3 compatibility
  - Continuous work

Thank you for your attention

Questions ?