EUROSMART

The Voice of the Digital Security Industry

JHAS, a success story

Amusec 2021

A bit of history…

JHAS has been created by Eurosmart in 2003

Eurosmart is a non-profit association founded in 1995 in Brussels

Eurosmart promotes security by design and supports security evaluation schemes

Eurosmart members are:

- **Designers and manufacturers of Secure Elements, semiconductors, smart cards, systems on chip, High Security Hardware & terminals**
- **Providers of Identity, IoT, Biometry, Payment, Mobile Connectivity solutions**
- **TICs, Laboratories, consulting companies, research organisations and associations**

Individual representatives are experts in the field of Digital security

What is JHAS ?

JHAS is an attack Working Group whose mission is to

own, maintain, and update the attack catalogue and the methodology to rate attacks against security IC hardware and embedded security firmware and software

JHAS individual representatives are WW recognized experts in Embedded Security, Tamper Resistance and related Attack Techniques

JHAS members are certification bodies, vendors, laboratories and issuers

Why an attack group ?

Ethical Hacking is an important piece of the cyber picture. It aims at anticipating what hackers will attempt once products & solutions are deployed in the field.

Ethical Hacking complements procedures, design rules, audits and automatic testing with concrete assessments about the security level of products & solutions

Security certifications @ substantial and high level should rely on Ethical Hacking with **penetration tests** run by independent 3rd party laboratories

But how to ensure that 3rd party laboratories run pertinent and comparable penetration tests ?

⇒ An **attack catalogue** gives the set of penetration tests that must be considered
⇒ A **rating methodology** enables fair and homogeneous conclusions of evaluations across laboratories

The JHAS attack group, how does it work ?

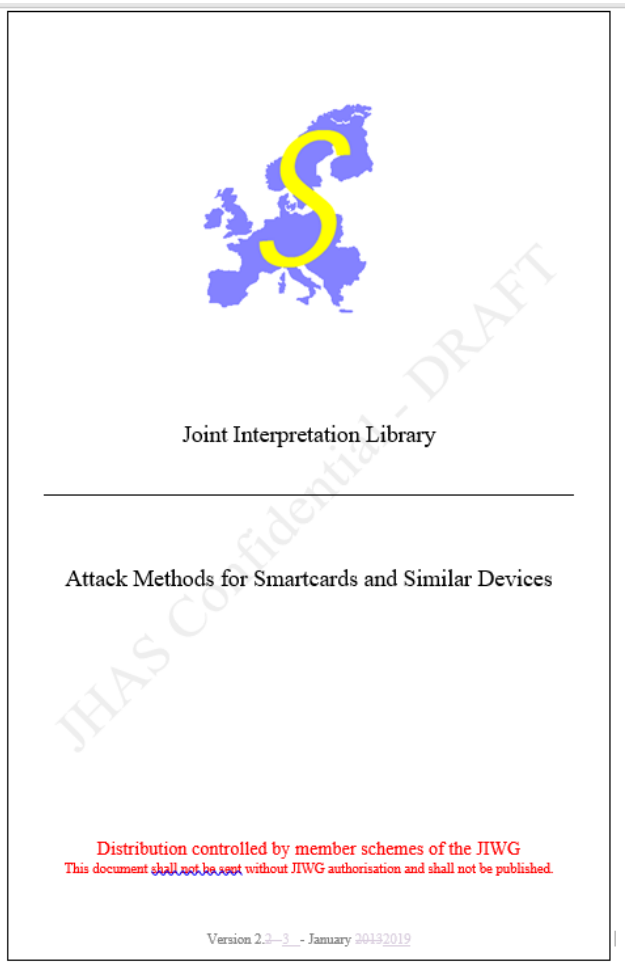
Experts from national security agencies, certification bodies, vendors, laboratories and issuers meet every 2 months to discuss State-of-the-Art attack paths, emerging attack techniques, and rating methodology

State-of-the-Art attack paths and emerging attack techniques remain highly confidential materials

The rating methodology measures cost and effort to identify (Identification) and to reproduce (Exploitation) a successful attack

The JHAS attack group, what outcomes?

For more than 19 years, JHAS has been feeding the SOG-IS , EMVCo, Mastercard, Visa,… with:

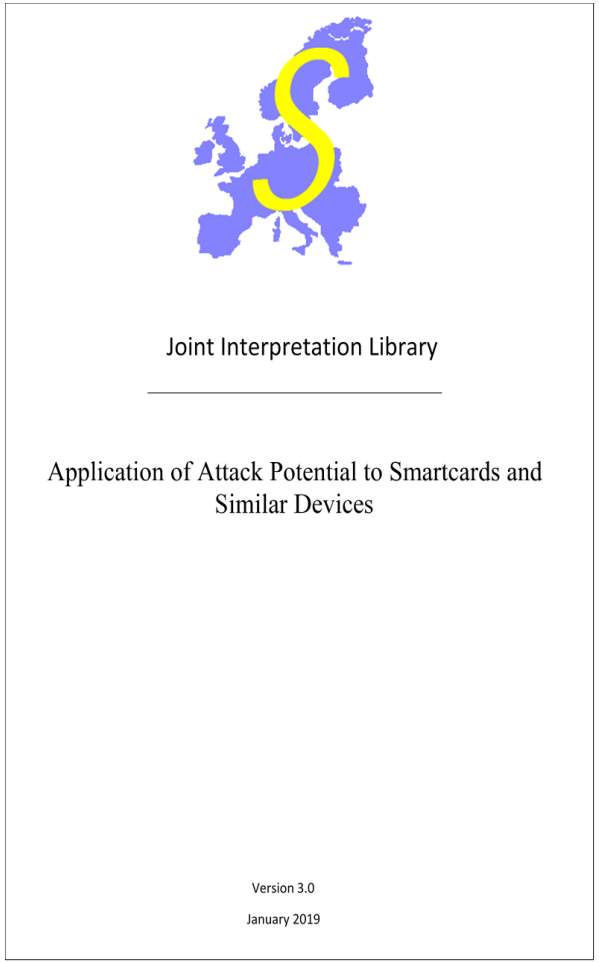

Joint Interpretation Library

Attack Methods for Smartcards and Similar Devices

JHAS Confidential - DRAFT

Distribution controlled by member schemes of the JIWG
This document shall not be sent without JIWG authorisation and shall not be published.

Version 2.2 – 3 - January 2013 2019


Joint Interpretation Library

Application of Attack Potential to Smartcards and Similar Devices

Version 3.0

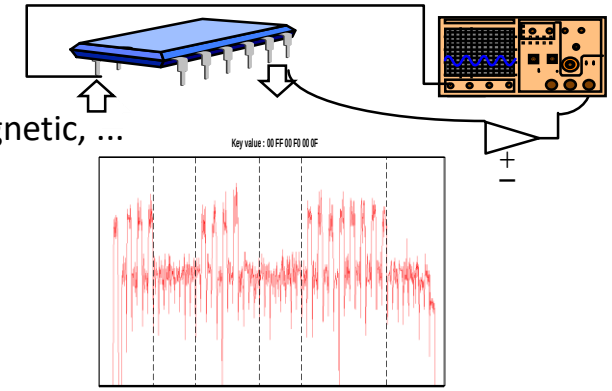
January 2019

EUROSMART
The Voice of the Digital Security Industry

The attack techniques discussed @ JHAS

- **Side-Channel Analysis***: Monitor analog signals on all interfaces and analyze:*

Time
Power
Electromagnetic, ...

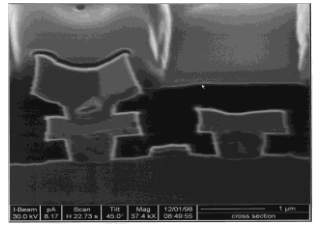


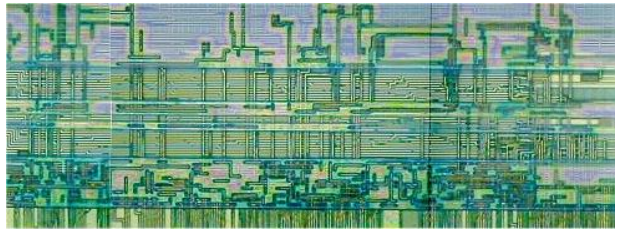
- **Fault Injection***: use of Laser, Glitchers, Flash light…*

to bypass protections and infer secrets.

- **SW attack***:* Malicious applets

- **Invasive manipulation***:*
  - Chip observation
  - Deposit probe pads on bus lines
  - Reverse ROM mapping
  - Disconnect RNG
  - Cut tracks
  - …





EUROSMART
The Voice of the Digital Security Industry

The JHAS rating table

Criteria	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months	6	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	*
Not pratical	*	*
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

EUROSMART
The Voice of the Digital Security Industry

The JHAS attack group, what results?

For more than 19 years,

Each high level Common Criteria certification of smart cards and similar devices issued by SOGIS members – French ANSSI, German BSI, Dutch NLNCSA and Spanish CCN – has relied on this 2 documents

Each EMVCo, Visa, Mastercard, JCB, GSMA, GlobalPlatform, IPA… certification of smart cards and similar devices has relied on this 2 documents

The impact of JHAS is worldwide:

Products certified by EMVCo, Visa, Mastercard, GSMA, GlobalPlatform,… are deployed worldwide
ID documents and ePassports of many countries WW are required to be Common Criteria certified by SOGIS

Thousands of products have been evaluated with JHAS' attack methods. As a matter of fact, they have escaped severe security crisis

Banking cards, ID documents, ePassports, GSMA certified SIM cards,… have proven to be secure products

What attack groups in the future ?

To make security certifications trustable, penetration testing by independent 3rd party laboratories must be part of the picture

Relying on a shared attack catalog is the most efficient way to ensure consistent and reliable evaluations across laboratories. This is particularly true when mutual recognition is sought, as mandated by the EU Cyberact

Since attack paths and attack techniques differ from one technology to another, such catalogs must be drafted by experts of each domain

Evaluations of Biometric solutions, Mobile apps, IoT devices, Cloud based services,… would deserve dedicated attack groups

Conclusion

The JHAS attack group has proven over years to efficiently fulfil its mission

The first EU certification scheme adopted @ EU level is the EU CC scheme that will rely on JHAS outcomes, just as SOGIS did during the past 17 years

Eurosmart advocates for the creation of dedicated attack groups as soon as mutual recognition of substantial and high level certificates is sought. In a first step, Eurosmart will create an ISAC as the legal entity to accommodate attack groups, starting with JHAS, ISCI WG1 and JDES

The creation of new attack groups will be discussed in the ISAC steering committee, where ENISA, EU commission, national security agencies of EU member states, vendors and laboratories will be represented