



EPOCHÉ & ESPRI

Side Channel Attacks CC, FIPS 140-2, EMV and PCI points of view

September 2010
11 ICCCT Turkey

The screenshot shows the website's navigation menu with links for EPOCHÉ & ESPRI, OUR SERVICES, SOLUTIONS, JOIN US, and CONTACT US. The main banner features a globe and the text "Your best companion to CC certification!". Below the banner is a search bar with a "GO" button. The content area includes a "WELCOME TO EPOCHÉ & ESPRI! Evaluation of IT security" section, a "A new face has arrived to the IT product security evaluation and testing arena ..." section with a "Click here to read more about us" link, and a "Request a free consultation" section with links for "CC and FIPS 140-2 training", "Evaluation and testing", and "Development best practices". At the bottom, there are three columns: "Our services" (The CC and FIPS 140-2 laboratory, "Click here to learn more"), "Solutions" (to implement the best security practices, "Click here to learn more"), and "Join us" (we are expanding and need your skills, "Click here to learn more"). There are also two logos: a yellow circular logo for "CERTIFICATION" and a blue diamond logo for "FIPS 140-2 VALIDATED".

Goal



E P O C H E & E S P R I

- This presentation provides a broad overview on the subject of side channel attacks as addressed by CC, FIPS 140-2, EMV and PCI.



Overview

- **Physical access to devices exposes risks:** the possibility of performing a successful side-channel attack could reveal the cryptographic algorithm secrets.
- **Side-channel attacks at the payment industry**
- **Side-channel attacks covered by standards:** The most transcendent of them are PCI, EMV, FIPS 140-2 and CC.
- **Standards grow up to considerate Side-channel Analysis**

Agenda

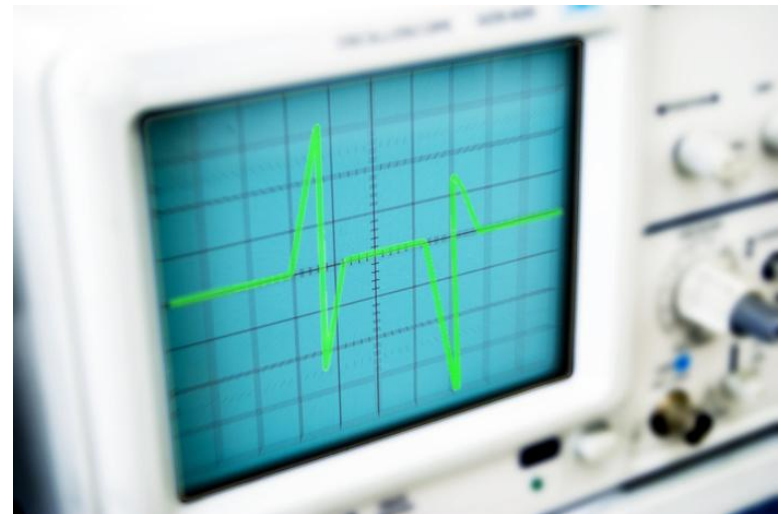


E P O C H E & E S P R I

- Introduction
 - Side-channel concepts
- CC overview
- EMV overview
- PCI overview
- FIPS overview
- Conclusions

1. Introduction – Side Channel Analysis

- New perception of encryption devices.
- Additional information can be gained from physical paths.
- Information used to break a system.
- Require considerable technical knowledge.



1. Introduction – Side Channel Analysis

Multiple attacks:

- Power Consumption Analysis:
 - Simple Power Analysis (SPA).
 - Differential Power Analysis (DPA).
 - Correlation Power Analysis (CPA).
- Electromagnetic Analysis:
 - Simple Electromagnetic Analysis (SEMA).
 - Differential Electromagnetic Analysis (DEMA).
- Timing Analysis.



1. Introduction – Side Channel Analysis

Countermeasures:

- “General purpose”
 - General Data-Independent Calculations.
 - Avoiding Conditional Branches.
 - Licensing Modified Algorithms.
- Against Timming Attacks
 - Add delays.
 - Time Equalization.



1. Introduction – Side Channel Analysis

Countermeasures:

- Against Power Analysis
 - Power Consumption Balancing.
 - Reduction of signal size.
 - Add noise.

2. Points of View – CC

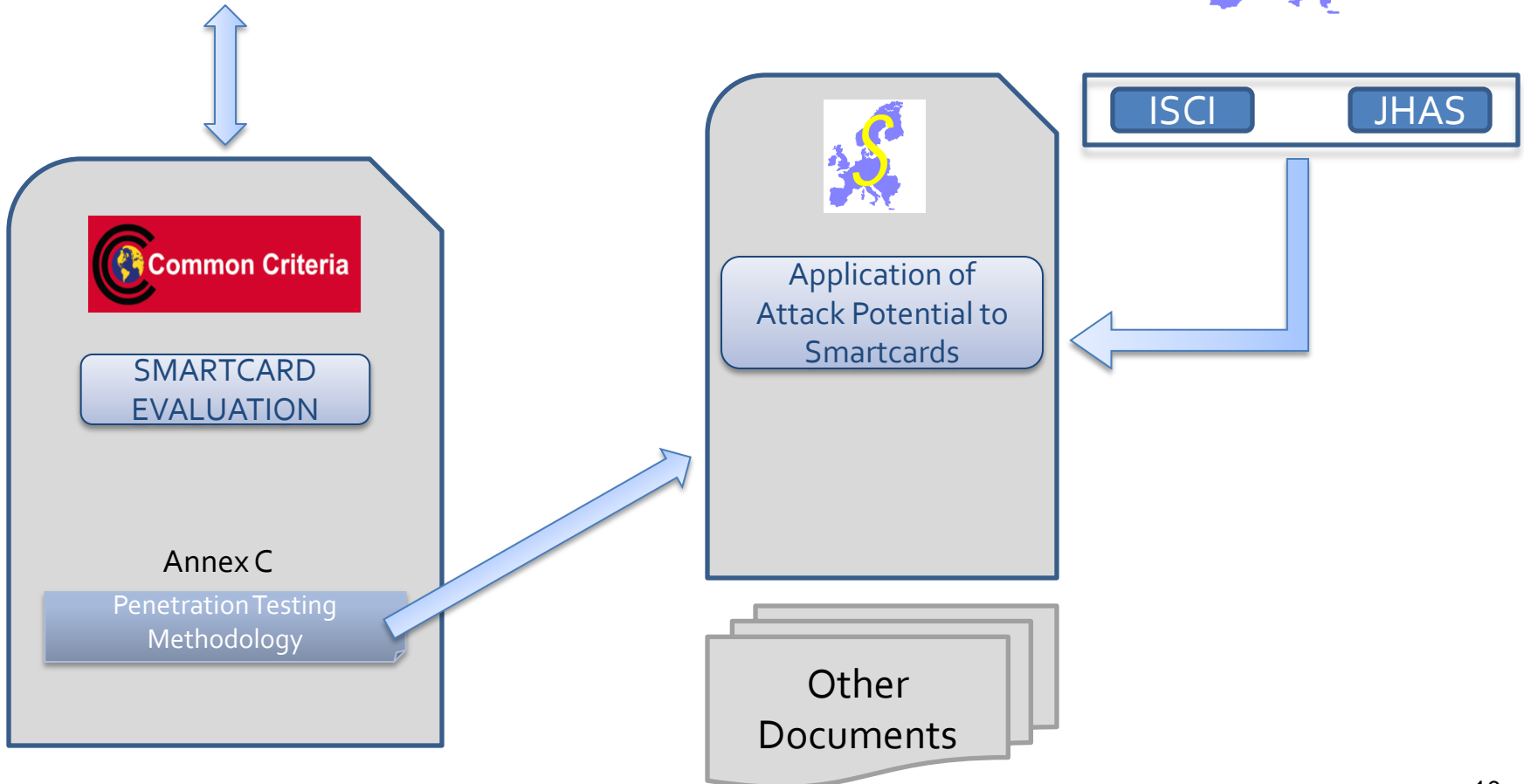


- CC as generic standard... ¿Side-channel analysis?
- Supported guidelines for concrete devices.
- Smartcards related supporting documents.

2. Points of View – CC



EPOCHE & ESPRI



2. Points of View – CC



Application of Attack Potential to Smartcards

- Work input from ISCI and JHAS.
- Distinction between identification and exploitation phases.
- Factors: Elapsed time, Expertise, Knowledge of the TOE, Access to the TOE, Equipment needed, Disposition of samples.
- Attack potential calculation.
- Examples of attacks methods.
- Application of examples for evaluation of a TOE.

2. Points of View – CC



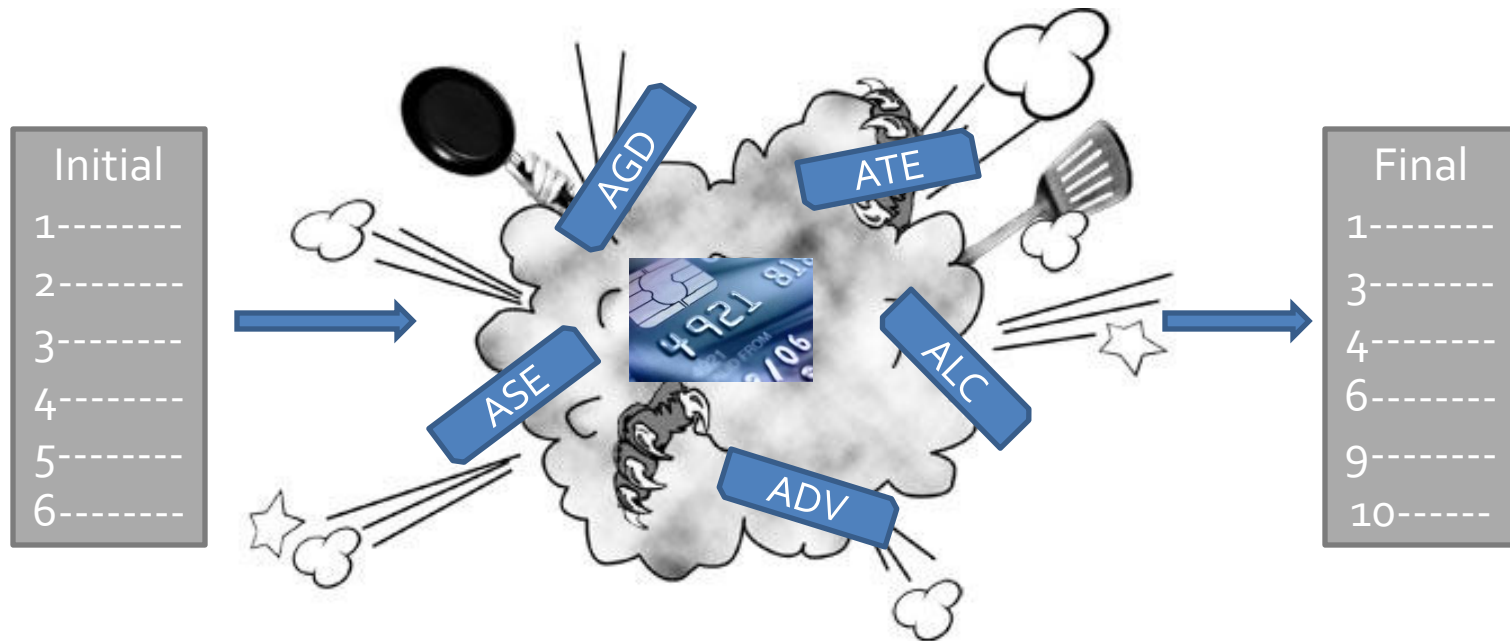
Application of Attack Potential to Smartcards

- Side-channel-related attacks:
 - SPA/DPA
 - High Order DPA
 - EMA

2. Points of View – CC



- Methodology:



2. Points of View – EMVCo



- What is EMV?
- Interaction at physical, electrical, data and application levels.
- Support the work of the ISCI group.
- Common security evaluation methodology.

2. Points of View – EMVCo



- Laboratories perform security evaluations using EMV Security Guidelines.
- EMVCo recognizes the methodology used in Common Criteria.
- Delta CC evaluations are allowed.
- The level of Assurance Requirement is **High** as described in the JIL document *Application of Attack Potential to Smartcard*.

2. Points of View – EMVCo



- Evaluation reports:
 - Complete vulnerability analysis against the threats discussed in the JIL group.
 - Residual vulnerabilities.
 - Conclusions based on JIL document “Application of Attack Potential to Smartcard”
 - Sufficient reporting of penetration testing.
 - Demonstration of equivalence to EAL₄+

2. Points of View – PCI



- Open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.
- PCI mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards.

2. Points of View – PCI



- Three main security standards:
 - DSS (Data Security Standard): is intended to help organizations protect customer account data.
 - PA-DSS (Payment Application Data Security Standard): ensure that vendor's payment applications support compliance with PCI-DSS.
 - PTS (PIN Transaction Security): physical and logical security requirements for all payment security devices.



2. Points of View – PCI



- Evaluation process.
 - PCI-recognized laboratories
 - PCI forms
- Payment Security Devices: Evaluated using the requirements at the Physical and Logical sections.
- A specific requirement related to side-channel attack for each kind of devices.
- Considerations given at the work of JIL.



E P O C H E & E S P R I

2. Points of View – FIPS

- What is FIPS 140-2?
 - Security Requirements for Cryptographic Modules
 - Four levels.
- Single-chip CM.
- *Physical security*: Nothing related to side-channel analysis.
- *Mitigation of other attacks* section includes the unique reference to side-channel attacks.
- No guidance.



EPOCHES & ESPRI

2. Points of View – FIPS

FIPS 140-3 perspective

- New section: *Physical Security – Non-invasive attacks.*
- Applied to Level 3 and Level 4, to Single-chip CM.
- Level 3: Protect the module's CPSs against non-invasive attacks of Annex F, explaining mitigation techniques.
- Level 4: Undergoing of testing.



2. Points of View – FIPS

FIPS 140-3 perspective

- Annex F *Non-invasive attack Methods* include:
 - CPA/DPA/SPA
 - SEMA/DEMA
 - TA

Non-Invasive Attack Methods	Security Functions / Algorithms
SPA and SEMA	Approved or Allowed asymmetric cryptographic algorithms
DPA and DEMA	Approved or Allowed symmetric cryptographic algorithms
TA	Approved or Allowed asymmetric cryptographic algorithms Approved or Allowed symmetric cryptographic algorithms Authentication mechanisms that control access to the module



E P O C H E & E S P R I

2. Points of View – FIPS

FIPS 140-3 perspective

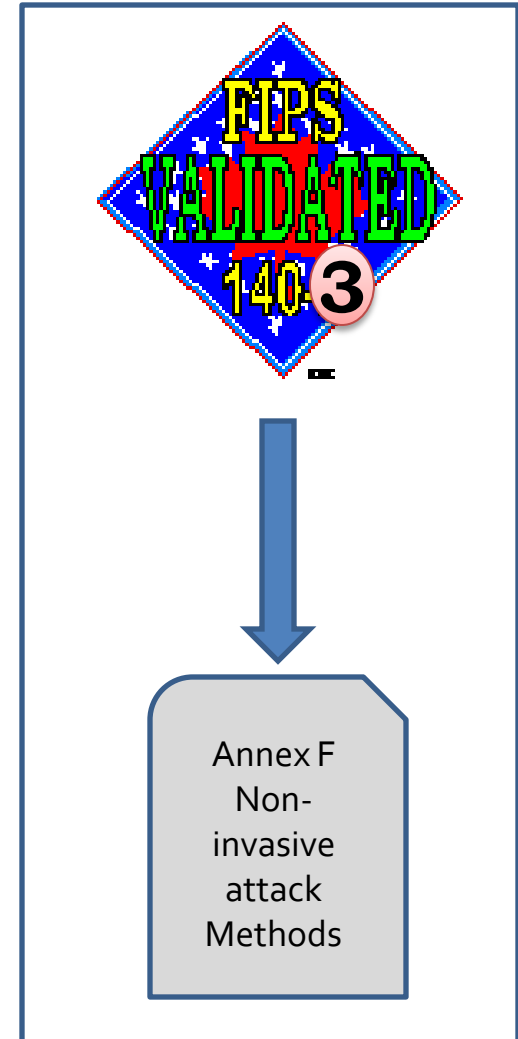
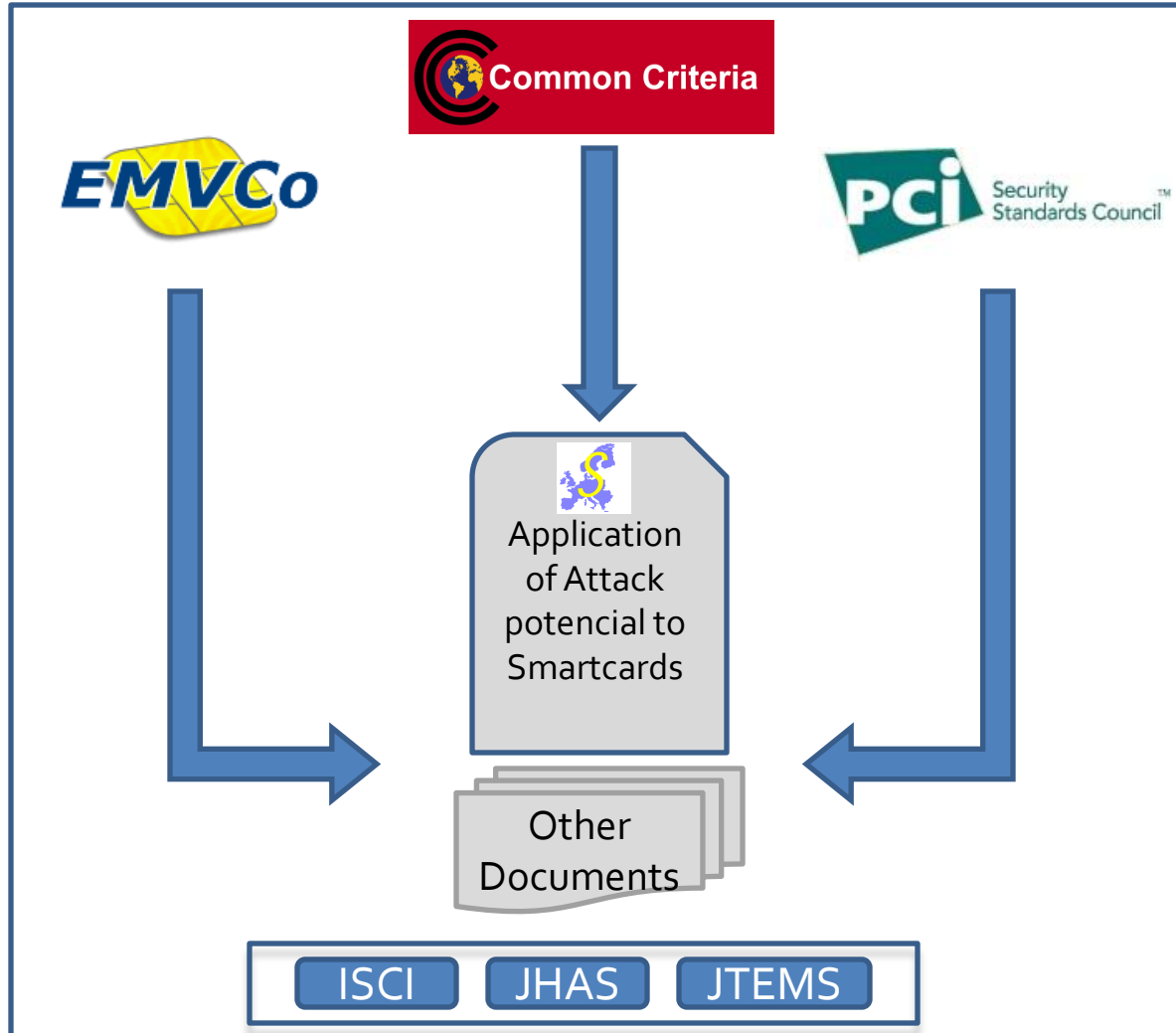
- Approach from FIPS 140-3 to the Smartcard CC evaluation community.



3. Conclusions

- Side-channel analysis activate alerts at the main security standards and groups.
- **Applies to a wide range of devices.**
- Work of JIL group is the cornerstone.
- FIPS creates its own methodology following guidelines of CC.

3. Conclusions





EPOCHE & ESPRI

QUESTIONS



Álvaro Ortega Chamorro

Epoche and Espri S.L.

eval@epoche.es