JTEMS – A Community for the Evaluation and Certification of Payment Terminals

Jürgen Blum, Federal Office for Information Security (BSI), Germany

14th ICCC, USA
Outline

- Brief overview: What is JTEMS? Who are the members?
- Background and Expectations of group members
- Collaboration: Beginning + Improvements
- Results
- Future challenges
- Summary
What is JTEMS? A brief overview

- **JTEMS - JIL Terminal Evaluation Methodology Subgroup**
- **JIL Subgroup**: A Subgroup of the Joint Interpretation Library Working Group working under the European SOG-IS agreement
- Initially a Technical CC-Community for Writing PPs and an evaluation methodology for cashless payment terminals
- Members are payment schemes, certification bodies, labs and developers
- Since 2012 a Subgroup of the Technical Domain for Hardware Devices with Security Boxes:
  Significant proportions of security functionality depend upon a hardware physical envelope with counter-measures (a so-called "Security Box") against direct physical attacks (e.g. payment terminals, tachograph vehicle units, smart meters, access control terminals, HSM, etc.)
Members
Background (I)

- Previously approval practice of the payment schemes
  - Secure banking terminals are very important for payment schemes
  - Security evaluations conducted since many years
  - Define the security level from payment schemes’ perspective
  - Regulations are under complete governance of the corresponding scheme including fast responses to new attacks

- European payment systems established different evaluation methodologies

- Global payment systems have established Payment Card Industry (PCI) standard
Background (II)

- Existence of several payment systems/schemes within Europe:
  - Different requirements for payment terminals
  - Different evaluations for approval of devices
  - Cost intensive certifications within Europe as a consequence

- New legal framework (NLF) for Single European Payment Area (SEPA) for Cards:
  - Elimination of differences in requirements and standards used by payment systems
  - Implementation of interoperable system
  - Mutual agreements to underpin interoperability

- Payment schemes founded “Common Approval Scheme (CAS) initiative” to implement NLF
Background (III)

- CAS work items:
  - Scope of security relevant features for cards and payment terminals - CAS requirements - that must be evaluated
  - Commitment to common evaluation methodology for payment terminals: Common Criteria (CC)

- CAS initiated foundation of JTEMS as consortium of labs, certification bodies (CBs), developers and payment system representatives to:
  - Discuss technical aspects with experts in this area
  - Produce CC-supporting documents to interpret the CC according to the requirements of this special technical domain
  - Provide assurance that results of one evaluation can be used in approval processes of different payment schemes.

- Oriented on the smart card working groups ISCI WG1 and JHAS
Expectations of group members

- Payment systems
  - Cooperate closely towards pilot evaluations
  - Produce results that are helpful for their approval process
  - Maintain or improve system security
- Governmental CC schemes
  - Propagate the CC standard instead of a new proprietary scheme
  - Re-use results of the JTEMS activities for other areas of the CC
- Evaluation labs
  - Gain access to the new market of CC evaluations for banking terminals
  - Assure fair conditions with respect to evaluation efforts
  - Improve the efficiency of the evaluation process
- Vendors
  - Facilitate the approval of payments systems for their products
  - Better understand and influence a key process
Summary of starting conditions

Motivation:
- Payment schemes require security evaluations
- New legal framework: SEPA for Cards
- Success of voluntary initiative important for mutual recognition

Stakeholders:
- Stakeholders involved from the beginning

Forming the community:
- Die Deutsche Kreditwirtschaft, UK Card Association and Cartes Bancaires sponsored PP development and work of chairperson

Common understanding of participants:
- CC evaluation as basis for mutual acceptance by payment systems
- Purpose: Optimize CC for specific technical area
- Confidential forum with open minded participants
- Focus on technical work with CAS handling more political issues
Collaboration – The beginning

- First steps took time:
  - Controversies about POI PP with different VAN-levels in one PP
  - CAS requirements not fixed
  - Compliance of POI PP to PCI requirements not clear
  - Regulation for exchange of confidential information (NDA)
  - Work on JTEMS additional to day-to-day business
  - Vendors were sceptical about the whole procedure

- 1.5 years to attain major improvements:
  - Consensus for POI PP and preparation for certification
  - Successful involvement of vendors
Collaboration - Improvements

- Improved funding
  - GeSTE-Initiative combining labs of the French CC scheme, French vendors, academic resources, etc., founded and supported by public money

- New cooperations outside of JTEMS:
  - Vendors agreed on a better coordination founding the Secure POS (Point Of Sale) Vendor Alliance (SPVA)
  - Payment schemes founded steering committee (OSeC) for coordination of activities relating to CC-based evaluations of banking terminals
Summary of improvements

- **Activity:**
  - More activities of some participants (e.g. GesTE) motivated the whole group

- **Mutual Trust:**
  - Payment schemes gained confidence in multiple recognition of evaluation results
  - European and global payment schemes trust CBs to oversee evaluation
  - Participants bring in their experiences – problems with intellectual properties openly discussed

- **Benefits:**
  - Vendors appreciate the influence on the evaluation methodology and other activities
  - CBs test new concepts for improvement of CC in this technical domain
  - Labs recognize the benefit in improving standards and develop a mutual understanding for testing of state-of-the-art attacks
Results (I)

- Issue, evaluation and certification of PP
  - Point of Interaction "POI-PED-ONLY", Nov 2010, V2.0
  - Point of Interaction "POI-COMPREHENSIVE", Nov 2010, V2.0
  - Point of Interaction "POI-OPTION", Nov 2010, V2.0

- Issue of supporting documents
  - CEM Refinements for POI Evaluation, June 2011, V1.0 (for trial use)
  - Application of Attack Potential to POIs, June 2011, V1.0 (for trial use)
  - Attack Methods for POIs, June 2011, V1.0 (for trial use)

- Link to the PP and supporting documents:
  - www.sogisportal.org (except the confidential “Attack Methods for POIs”)
Results (II)

- Evaluation and certification of products
  - Two certified products and one product whose certification is almost completed; Certificates are granted by BSI and CESG
  - One ongoing certification with NLNCSA as certification body
  - Products and their evaluations / certifications are presented by the labs to payment scheme representatives. Residual weaknesses are discussed.

- Links to the security targets and certification reports:
  - www.bsi.bund.de/zertifizierung
  - www.cesg.gov.uk/servicecatalogue/CCITSEC
Results (III)

- Payment schemes need additional information regarding residual vulnerabilities => “ETR for Risk Management” issued by the lab, its underlying template is issued by JTEMS
- List of interpretations of supporting documents (FAQ) helps to avoid redundant discussions
- Discussions and decisions about how to perform site visits for “Final Assembly” and “Intial Key Loading” Sites (to be continued); major difference to PCI DTS
- Terms of Reference (ToR) Update:
  - Classification of information and results is decided by the JTEMS
  - Rules for distribution are recommended by JTEMS
  - Publication is made by JIWG
Results (IV)

  - As result of discussions how to handle new attack methods against payment terminals as shown at the Black Hat Europe 2012
  - Goal of the JIL document:
    - “... to set a framework shared between SOGIS qualified participants, allowing monitoring, analyzing and ending with a common conclusion on any new attack or any new event that may impact Common Criteria evaluations.
    - The objective of this process is to allow an efficient and common reaction, analysis and response.”

- Liaison with Japan referring JTEMS
Future challenges

- Integration of PCI DTS 4.0 in the POI PP and its supporting documents => Goal: Approval by PCI
- Integration of two optional PCI modules: “SRED (Secure reading and exchange of data)” and “Open Protocols”
- Modular approach: Base PP + additional modules
- Reduction of the PP complexity, diminish the number of SFRs; a high number of SFRs was the consequence of different VAN-levels in one PP

=> A subgroup develops proposals for modified PP and supporting documents, sponsored by the approval schemes

- Inclusion of hardware boxes as JTEMS topic
Summary (I)

- Promising starting conditions:
  - External pressure
  - Technical work items
  - Sponsorship for crucial positions and deliverables
  - Stakeholder representatives with technical background

- Established collaboration:
  - Open discussions without issues with intellectual property
  - Trust in each other has been established
  - Relationship to other communities (OSeC/CAS, JIWG, SPVA) clarified and accepted
  - Esteem of each participant
Summary (II)

- Increased importance of CC:
  - Establishment of a new technical area
  - Innovative cooperation with payment systems

- Encouraging pilot results
  - Improved product quality

- Next steps are clear:
  - Optimization of the PP and its supporting documents
  - Integration of PCI DTS 4.0 and optional modules
  - Optimization of the developer documentation, the evaluation and the certification processes
Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jürgen Blum
Godesberger Allee 185-189
53175 Bonn

juergen.blum@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de