PV204 Project Phase 1

- Nomit Sharma, Matěj Grabovský, Milan Šorf

Certified Products

- The Common Criteria Recognition Arrangement covers certificates with claims of compliance against Common Criteria assurance components.
- Chosen certificates by our team:
  - NXP JCOP 4 P71 (Nomit Sharma).
  - genuscreen 7.0 (Matěj Grabovský).
  - vinCERTcore v4.0.5.5733 (Milan Šorf).

Certificate: NXP JCOP 4 P71

- Developed in Germany.
- Evaluated in Netherlands.
- Valid till 25-07-2024.
- EAL6+ compliant.

Certificate: NXP JCOP 4 P71

- Target of Evaluation:
  - Smart Card Controller.
  - Test and Boot Software.
  - Cryptographic Primitives such as AES, 3DES for encryption and decryption and ECC for signature generation and verification.
- Assumed Attacker Model:
  - Applets without Native Methods.
  - Bytecode Verification.
  - Protected Storage of Keys.
  - Protection during Packaging, Finishing and Personalisation.

Certificate: NXP JCOP 4 P71

- Device Scrutinization:
  - Micro Controller protects from logical and physical attacks against data leakage.
  - Integrity and protection of application data and sensitive results.
  - TOE Security Functionality counters physical manipulation and probing.
- Security Assurance Requirement (SAR):
  - It ensures security of TOE during its development and production.
  - The developer shall provide a formal security policy model.

Certificate: NXP JCOP 4 P71

- Security Functional Components (SFR)
  - Java Card Virtual Machine and Object Management.
  - Configuration Management.
  - Card Content Management.
  - Cryptographic Functionality and Secure Box.
  - Random Number Generator.
  - Secure Data Storage and User Data Protection using PUF.
  - External Memory and Memory Management.
  - PIN Management.
  - Error Detection Code API.
  - Hardware Exception Handling and Module Invocation.

Certificate: NXP JCOP 4 P71

- Out of Scope of Certification
  - Java Card Applets.
  - Secure Box Native Library.
  - Crypto Library.
- Critical Evaluation and Conclusions
  - Well evaluated and approved evaluation results.
  - Detailed TOE evaluation.
  - Verdict of claimed assurance requirement is ‘Pass’.
  - The Security Target claims demonstratable conformance to the Protection Profile.

Certificate: genuscreen 7.0

- Distributed Packet Filtering Firewall System with VPN and IPsec capabilities.
- Developed by genua GmbH.
- Evaluated by German Federal Office for Information Security.
- EAL4+ compliant.

Certificate: genuscreen 7.0

- Target of Evaluation:
  - Software only – distributed *(genuscreen)* and central management *(genucenter)* part.
- Assumed Attacker Model (including Security Target):
  - Breakage, sniffing and modification of network, TOE and related data (configurations and audit data).
  - All components are physically secure.
  - Components were initialized exactly as required.
  - Reliable timestamps.
  - GUI used over a trusted network connected directly to the device.

Certificate: genuscreen 7.0

- Device Scrutinization:
  - Software on firewall components working as network filters.
  - Management system to manage network of firewall components.
  - SSH encrypted connection between genucenter and genuscreen.
  - Scrutinization performed by vendor and independent evaluator.
- Security Assurance Requirement (SAR):
  - From specifications till analysis.
  - Includes development architecture, user guidance, life cycle coverage, security objectives, testing and analysis.

Certificate: genuscreen 7.0

- 10 Security Functional Requirements (SFR)
  - Firewall and Network Separation.
  - IPsec and SSH.
  - Administration.
  - Identification and Authentication.
  - Audit.
  - General Management Facilities.
  - Random Number Generation.

Certificate: genuscreen 7.0

- Out of Scope of Certification
  - Hardware components.
  - Cryptocard usage.
  - Central management software in a virtual machine.
  - Remote maintenance feature.
  - Third-party VPN and IPv4 dynamic routing using OSPF.
- Subjective Evaluation
  - Reliance on OpenBSD and LibreSSL.
  - Wide range of functionality considered. Testing seems OK, but perhaps might have been more extensive.

Certificate: vinCERTcore v4.0.5.5733

- Developed and Evaluated in Spain.
- EAL4+ compliant.

Certificate: vinCERTcore v4.0.5.5733

- Target of Evaluation:
  - Software server.
  - Use of external user repository and IT products with HSM.
- Assumed Attacker Model:
  - Trusted external IT products and external components.
  - Trusted OS, SCA and HSM are used.
  - No physical access to TOE.
  - No malware can attack TOE from the same OS.

Certificate: vinCERTcore v4.0.5.5733

- Device Scrutinization:
  - More or less similar to assumed attacker model.
  - No further description apart from the set of assumptions.
- Security Assurance Requirement (SAR):
  - From basic design till vulnerability analysis.
  - Includes basic modular design, preparative procedures, development tools, security objectives and analysis of coverage.

Certificate: vinCERTcore v4.0.5.5733

- Security Functional Components (SFR)
  - Security Alarms.
  - Audit Data Generation and Review (Restricted and Selectable).
  - User Identity Association.
  - Potential Violation Analysis.
  - Cryptographic Operation.
  - Access Control.
  - User Data (Export and Import).
  - Data Integrity and Information Protection.
  - Identification and Authentication.

Certificate: vinCERTcore v4.0.5.5733

- Out of Scope of Certification
  - Hardware Security Model.
  - External Web Interface.
- Critical Evaluation and Conclusions
  - Independent testing covered 100 percent SFR and TSFI.
  - TOE does not present any exploitable vulnerabilities.
  - Since, description of the testing process is missing (as all attacks are covered by assumptions), the evaluation results are not convincing.

Thank You

Questions