PV204 Term Project: Certificate Analysis

Tomáš Madeja, Tran Anh Minh, Ankur Lohchab

1. **Certificates** To implement the project on secure channel on certified smartcards following certificates have been selected for implementation.
   a. FM1280 V05 - EAL 5+
   b. Genuscreen 7.0 - EAL 4+
   c. TLX1280 - EAL 4

2. **FM1280 V05**
   a. **TOE Description**

   TOE is FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software, Secure smart card integrated circuit with dedicated software. TOE is intended for use in banking and finance market, electronic commerce or governmental applications. The certificate was issued by the Norwegian SERIT, and evaluated by Dutch evaluation facility (EVIT).

   TOE uses standard as well as OTP EEPROM, ROM; system and coprocessor, PAE, and CLA RAM. TOE supports various communication interfaces such as ISO/IEC 14443 Type A contactless interface, ISO/IEC 7816 contact interface, GPIO, SPI and High Speed SPI, I2C, and UART.

   TOE provides RNG, DES/TDES, AES, RSA, ECC and SHA1/SHA256 HASH as secure cryptographic services. DES and SHA only claim correctness, not security due to algorithms attack resistance. TOE claims the RNG provides high entropy true random numbers. TOEs driver provides CRC, EEPROM, and IO operations. TOEs driver services have not been made resistant against attacks.

   b. **Assumed Attackers Model** In accordance to the section 3.2 of the Security IC Platform protection profile, there are following threats to the TOE:

   - Inherent information leakage (T.Leak-Inherent).
   - Physical probing (T.Phys-Probing).
   - Malfunction due to enviromental stress (T.Malfunction).
   - Pysical manipulation (T.Phys-Manipulation).
   - Forced information leakage (T.Leak-Forced).
   - Abuse of functionality (T.Abuse-Func).
   - Deficiency of random numbers (T.RND).

   c. **Security Objective**
   - Security of RSA services for encryption and decryption (O.RSA).

- Security of ECC services for signature generation, signature verification, diffie-hellman key agreement, point multiplication and point addition (O.ECC).
- Security of the Triple-DES services for encryption and decryption (O.TDES).
- Security of the AES services for encryption and decryption (O.AES).

d. Testing and Evaluation

i. Delivery was supposedly checked during the evaluation.
ii. Independent vulnerability analysis was done based on design and implementation review of TOE, code review of crypto library and boot code, validation tests of security features, review of previous results considering "JIL Attack Methods for Smartcards and Similar Devices", penetration tests.
iii. Developer's tests were supposedly performed on: engineering samples (cards or Dual-In_line_package ICs), wafers, simulation tools to verify logical functions.
iv. Evaluator tests were performed using the developer's hardware testing tools and developers test cases. Addition tests were performed by augmenting existing tests by various parameters and supplementation.

e. Conclusion The report and security target specifies the expected threat model in a great detail. Together with the evaluation, it gives a semblance of idea as to the tests performed, and a setup is given in the appendix of the report. Tests performed are, however, all closed only to developers, and hence possibly not easily reproducible. This also hides any possible mistakes that could have been performed during testing. Errors in evaluation may have occurred as well, as the testing results are not given (likely due to closed nature of tests)**.**

3. Genuscreen 7.0

a. TOE Description

The product is develped by a German company genua and it was certified in Germany by Bundesamt für Sicherheit in der Informationstechnik (BSI). The TOE has two main functions – firewall and VPN. It uses the firewall function to monitor data traffic protect the LAN/Internet interface. The VPN function enables exchanging encrypted data between spread out company locations or public authority sites over the internet

There are two parts of product, one part runs on a number o f machines and works as network filters and other part runs on the machine to manage the network of firewall components. The product also contains cryptographic functionality and the cryptographic algorithms are part of the TOE. This includes a PRNG ("deterministic random number generator") of class DRG.3. However, the vulnerability assessment results stated in the

certificate do not include whether those cryptographic algorithms and their implementation are suitable for encryption and decryption.

Non-TOE components of the product: genucenter Management System: required hardware, operation system and server, genuscreen Firewall Components: required hardware, operation system and server, Legacy Hardware and Virtual genucenter.

b. **Assumed Attacker's Model** The threats to the TOE stated in the proposal are:
   - T.NOATUH - unauthenticated access to resources in protected network
   - T.SNIFF - access to sensitive data passing between the protected network
   - T.SELPRO - acess to TOE and reading, modifying or destroying security sensitive data on the TOE
   - T.MEDIAT - sending non-permissible data that result in gaining access to resources which is not allowed
   - T.MSNIFF - gaining access to the configuration or audit data
   - T.MODIFY - modification of the sensitive data passing between sensitive network
   - T.MMODIFY - modification of configuration or audit data

   On the other hand, TOE is assumed to work under the following conditions:
   - A.PHYSEC - the system is physically secure
   - A.INIT - initial configuration was according to the documentation
   - A.NOEVIL - responsible, competent and trained administrators, service users and revisers
   - A.SINGEN - firewall components provide the only connection for different networks
   - A.TIMESTMP - the IT environment must supply reliable timestamps for the TOE
   - A.ADMIN - administrators, service users and revisors use the administrative GUI only from a trusted network directly connected to the system.
   - A.HANET - physical secure separate network for server establishment and transfer for optional high availabity setup
   - A.REMOTE_AUTH – server for external auth. Is located in a secure network

The proposal of the product does not specify methods by which it would protect the system and itself against the mentioned attacks.

c. Security Assurance Rationale

- ALC_FLR.2 Flaw reporting procedures
- ASE_TSS.2 TOE summary specification with architectural design summary
- AVA_VAN.4 Methodical vulnerability analysis

d. Security Functional Requirements claimed by TOE

Firewall SFP: It is concerned with the creation, modification, deletion and application of firewall security policy rules; it also provides protection against unauthorized access to the platform running the firewall components

Network Separation SFP

* **IPSec SFP:** including requirements on some cryptographic operations
* **IKE SFP:** cryptographic functions in relations to the key management of the VPN connections
* **SSH SFP:** requirements associated with the flow control functions in relation to the communication between the management system and the firewall components, (includes cryptographic operations)

SIP Relay

Identification and Authentication: related to identification and authentication of administrators, service users and revisors.

Audit: audit capabilities of the TOE

General Management Facilities

e. **Evaluation** The product was tested in the developer's laboratory and also by an independent evaluator - securevera GmbH in an evaluation facility recognized by the certification body of BSI. The test procedures are executable scripts (Ruby, Perl or Shell). The developer uses two kinds of tests: Local tests and Live tests. Local tests need the developer environment and were executed inside the developer systems. During the test by the independent evaluator, the main focus was on the implemented SIP Relay, the management system, cryptographic functions, random number generator (RNG) and its entropy source (part of OpenBSD kernel) functions. The repetition of the developer testing was performed in the developer laboratory. Evaluator has also done an independent vulnerability analysis and designed additional vulnerability tests. The documentation of the product was tested as well.

f. **Conclusion** The report and security target probably specified all necessary fields. As a customer, e.g. being a company which searches for such product, I would probably trust the result of certification. However, I would personally appreciate more detail on the assumed treat model, because it was difficult for me to immediately imagine concrete scenarios which are in the scope of evaluation and which are not. Also, there are no details on techniques the product uses to acquire the stated security functionality or details on the used methodology of the tests, e.g. how they simulated the attacks. But overall, I think that as a customer, I would be satisfied.

4. TLX1280 Matrix Switch Security Target

a. **Description** The TOE is a 1280 x 1280 routing system, which provides connection of 1280 optical inputs located on the upper and lower card cage ports to any or all of the 1280 optical outputs located on the same upper and lower card cage ports. The TOE consists of 40 Data Input and Output Cards having 32 optical input and output ports. The Input and Output Cards installed in the upper and lower card cages can be used to connect any of the 1280 inputs, in one direction, to any output or multiple outputs.

b. Assumed Attacker's model No assumption about the attacker's model are explained in the Certificate Report. However as per threat model, the major threats are :

- The TOE may be delivered & installed in a manner that violates security policy.
- An attack on TOE may violate security policy.
- Residual data may be transferred between different port groups in violation of data separation security policy.
- State information may be transferred to unintended port group.

c. Testing and vulnerability analysis

The evaluator vulnerability analysis was based on both public domain sources and the visibility of the TOE given by evaluation process. The vulnerability analysis took into consideration the Enhanced –Basic attack potential.

Evaluators have devised set of tests to test potential vulnerabilities to TOE. The vulnerability analysis states that in its intended environment no exploitable vulnerabilities are present.

Developer's test and Evaluator's test have been carried out to ensure the TOE has desired behaviour. **No details about the type of test and mechanism are explained in the Certificate Report**.

d. Security Functional Components (SFRs)

- The TOE shall not violate the confidentiality of the information which it processes. Information gathered within the peripheral shall not be accessible by any other connection.
- No information shall be shared between switches computers and peripheral set via the TOE in violation of data separation SFP.
- The TOE shall meet the appropriate national requirements for electromagnetic emission.
- TOE doesn't encrypt optical, wired network connections. The switch, the transmitter, the receiver and the optical connections from the Switch to the

transmitter and receiver and the wired network connection has to be physically secured.

- Most of the TOE Security functional requirements are similar to the PSSPP.
  - FDP_ETC.1 - Export of user data without security attributes
  - FDP_IFC.1 - Subset information flow control
  - FDP_IFF.1 - Simple security attributes
  - FDP_ITC.1 - Import of user data without attributes

e. **Conclusions**

As per my opinion, there are various shortcomings in the Certificate Report. The details about the attacker model are missing. There are no details about evaluation procedure. As per the Certificate Report the evaluators just independently tested a sample of developers test and verified that the TOE behaves as specified. However, the detailed description about the methodology of test and the outcomes is missing.