FACULTY OF
INFORMATICS
Masaryk University

Analysis of Security Certificates

Team Supercalifragilisticexpialidocious

Anh Minh Tran
Ankur Lohchab
Tomáš Madeja

Certificates

1 Thinklogical TLX1280

2 genuscreen 7.0

3 FM1280 V05

Thinklogical TLX1280 Matrix Switch

- EAL 4
- Optic fiber switch that uses multimode fiber optics.
- Transmit and receive a digital video pulse stream without alteration or interpretation of the original signal.
- Embedded keyboard, mouse, USE 1.1, USB 2.0 (high speed up to 480 Mbps), and audio signals are also transmitted.
- 1280 x 1280 routing system, 40 Data Input and Output Cards (32 optical input and output ports each).
- Data Input and Output Cards to connect with single or multiple ports.

Thinklogical TLX1280 Matrix Switch

Security Functional Components

Security Functional Requirements	
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

Security functional requirements are similar to the PSSPP

Thinklogical TLX1280 Matrix Switch

Security Objectives

Security Objective	
O.CONF	No access of info
O.CONNECT	No sharing of information

Security Objective Environment	
OE.EMISSION	Limited electromagnetic radiation
OE.MANAGE	Install and manage as per directions
OE.NOEVIL	Authorised user non hostile
OE.PHYSICAL	Physical security of devices
OE.SCENARIO	Attached device vulnerability not TOE concern

Thinklogical TLX1280 Matrix Switch

Attacker Model

Threat	Definition
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy.
T.ATTACK	An attack on the TOE may violate the security policy
T.RESIDUAL	Residual data may be transferred between different port groups in violation of data separation security policy.
T.STATE	State information may be transferred to a port group other than the intended one.

Thinklogical TLX1280 Matrix Switch

Testing & Evaluation

Testing	
Developer Test followed by Evaluator Test	No details of the type of test and methodology
Evaluators tested sample of Developer tests	Evaluator asses that developer have performed test correctly

Thinklogical TLX1280 Matrix Switch

Review

- Attacker model details are missing.
- No details of evaluation procedure.
- Test performed too generic, details missing.

Certificates

1 Thinklogical TLX1280

2 genuscreen 7.0

3 FM1280 V05

genuscreen 7.0

- Main functions:
- monitoring data traffic
- protecting LAN/Internet interface (firewall)
- enabling the exchange of encrypted data (VPN)
- Optional SIP relay functionality consists only of the software (on CD or USB) and its documentation checksum of software on CD/USB provided cryptographic algorithms are part of TOE, e.g. RNG

- EAL 4+
- Evaluated by developer and an independent evaluator
- test procedures = scripts in Ruby, Perl or Shell
- Developer: local and live tests
- Independent eval.: only live tests but with additional vulnerability tests
- Details on the tests are not provided

genuscreen 7.0

Security Functional Components

- 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

TOE Scurity	Functionality
SF_PF	Packet Filter
SF_NS	Network Separation
SF_IPSEC	IPSec Filtering
SF_SIP	SIP Relay
SF_IA	Identification and Authentication
SF_AU	Audit
SF_SSH	SSH Channel
SF_ADM	Administration
SF_GEN	General Management Facilities

genuscreen 7.0

Security Objectives

Security Objectives	
O.AUTH	The TOE must assure that only administrators can change the packet filter, VPN and SSH configuration.
O.MEDIAT	The TOE must mediate the flow of all data between all connected networks.
O.CONFID	The TOE must assure that data transferred between the networks protected by firewall components is kept confidential unless explicitly configured otherwise.
O.INTEG	The TOE must assure that data transferred between the networks protected by firewall components cannot be modified unnoticed unless explicitly configured otherwise.
O.NOREPLAY	The TOE must assure that data transferred between the networks behind the firewall components cannot be reinjected at a later time unless explicitly configured otherwise.
O.AUDREC	The TOE must provide an audit trail of security-related events, and a means to present a readable and searchable view to administrators, service users and revisors.
O.AVAIL	The TOE must optionally provide a fail over solution where the services of a failing system are taken over by a peer machine.

genuscreen 7.0

Threats

Threats	
T.NOATUH	Anonymous user enters a system without athentication
T.SNIFF	An anonymous user might gain access to the sensitive data passing between the protected networks. Attack method is packet inspection of Internet traffic.
T.SELPRO	An anonymous user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used.
T.MEDIAT	An anonymous user might send non-permissible data that result in gaining access to resources which is not allowed by the policy. The attack method is construction of IP packets to circumvent filters.
T.MSNIFF	An anonymous user might gain access to the configuration or audit data passing between the management system and a firewall component. Attack method is packet inspection of Internet traffic.
T.MODIFY	An anonymous user might modify the sensitive data passing between the protected networks. Attack method is packet interception and modification of Internet traffic.
T.MMODIFY	An anonymous user might modify the configuration or audit data passing between the management system and a firewall component. Attack method is packet interception and modification of Internet traffic.

genuscreen 7.0

Assumptions

Assumptions	
A.PHYSEC	The management system and the firewall components of the TOE are physically secure. Only administrators have physical access to the TOE. This must hold for the management system and the firewall components.
A.INIT	The TOE was initialised according to the procedure described in the docu-mentation.
A.NOEVIL	Administrators, service users and revisors are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.
A.SINGEN	Information can not flow between the internal and external network, unless it passes through the TOE.
A.TIMESTMP	The environment provides reliable timestamps.
A.ADMIN	Administrators, service users and revisors using the administrative GUI on the management system or the firewall components work in a trusted network directly connected to the system.
A.HANET	The environment provides a physical separate network for TSF data transfer for the optional high availability setup.
A.REMOTE_AUTH	The server for external LDAP authentication of genucenter administrators and revisors is located in a secure network.

Certificates

1 Thinklogical TLX1280

2 genuscreen 7.0

3 FM1280 V05

FM1280 V05

Physical protection
Watch Dog Timer
Security Controller
Environment Detection Circuits
Light Sensor
Clock Frequency Monitor
Temperature Sensor
Voltage Sensor
Glitch Sensor
Active Shielding

Memory
OTP EEPROM
EEPROM
ROM
System RAM
Coprocessor RAM
PAE RAM
CLA RAM

Interface
ISO/IEC 14443 Type A contactless
ISO/IEC 7816 contact
GPIO
SPI
High Speed SPI
I2C
UART

FM1280 V05

Coprocessors
TRNG
CRC-CCITT
DES/TDES
AES
PAE for RSA
PAE for ECC
HASH (SHA1/SHA256)
Chinese Domestic Algorithm

Algorithm
RNG
DES/TDES
AES
RSA
ECC

FM1280 V05

Attacker/Threat Model

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

Security Objectives	
O.RSA	Encryption, decryption
O.ECC	Signature generation and verification, DH, point multiplication and addition
O.TDES	Encryption, decryption
O.AES	Encryption, decryption

FM1280 V05

Testing & Evaluation

Developer Tests
Engineering samples
Wafers
Simulation tool

Evaluator Tests
SFI
SFI interfaces
Security mechanisms
Developer tests
Augmented developer tests

Vulnerablity Analysis
Deign and Implementation review
Code review of crypto lib
Code review of boot code
Validation tests of features
Review based on “JIL Attack Methods for Smartcards and Similar Devices”
Penetration tests

Thank You