Evaluating Open Source Security Software

SECRETS Project
(IST-2000-29289)

John Iliadis
R&D Unit
Intrasoft International

INTRASOFT INTERNATIONAL

Summary

SECRETS project aims at evaluating the use of open source security protocols, with respect to the efficiency and performance of the services they offer, by means of conducting specific experiments.

Protocols:

- *OpenSSL (SSL)*
- *FreeS/WAN (IPsec)*

Experiments drawn from:

- E-Commerce
- Mobile Communications
- Network Monitoring
- Intelligent Networks

General Approach

Adapt selected applications to operate with open source security software

Experiment with the use of open source security software in the selected applications, according to an evaluation methodology

Produce an evaluation report on the use of OpenSSL and FreeS/WAN

SECRETS Evaluation Framework

Evaluation of the developing organisations

- Capability and Stability of the organisations
- Support services for the products
- Ability to feed requirements into the developing process

Product evaluation

- Product Capability
  - Conformity verification
  - Interoperability
- Product Stability
- Product Maintainability

Application experiments

- E-Tender experiment (Intrasoft International)
- GPRS experiment (Motorola)
- Network monitoring experiment (Solinet)
- Intelligent network experiment (Alcatel)

Evaluation of the developing organisations (1)

Capability and Stability of the organisations

- The prehistory of the organisation, which will provide an insight on its quality,
- The official start of the Open Source project, and the work performed since then, in order to examine how active the organisation is,
- Licensing scheme under which the software package is distributed,
- The number of members and identity of the development team that contributes to the organisation.
- The commercial or not applications that use the product – in conjunction with the companies/organisations that interact with the specific organisation.

Evaluation of the developing organisations (2)

Support services for the products

- Maintenance and continuous update of a central Web site which is the reference for all the users of the product
- Documentation of the source code
- Installation support
- Releasing of support packages - Patches

Ability to feed requirements into the developing process

Product Capability

- *Conformity verification*

  the conformity of OpenSSL and FreeS/WAN to Netscape's SSL and IETF IPSec, respectively

- *Interoperability*

  the ability of OpenSSL and FreeS/Wan to successfully interoperate with other software implementations of the SSL and IPSec protocols

Product Stability

- a measure of how often a software changes and to what degree

Product Maintainability

the ability of a user of OpenSSL or FreeS/Wan to understand, maintain, use, and upgrade the software. Evaluation criteria:

- Available documentation,
- quality of the code,
- adherence of the code development to standards adopted by the developing organisation (if any).

Test Cases (1)

Intrasoft International: E-Tender – OpenSSL

- Installation and Configuration
- Identification, Authentication, Authorisation
- Integrity
- Confidentiality

Motorola: GPRS – FreeS/WAN

- Installation and Configuration
- Functional verification
- CPU utilisation (10 Mbps: up to 240% in peer, up to 900% in gateway)
- End-to-end delay (10 Mbps: up to 140%)
- Interoperability (Cisco IPsec)

Test Cases – Evaluation Metrics (2)

Alcatel: Intelligent Networks – OpenSSL

- Installation and Configuration
- Functionality
- Security
- Performance (3.5% overhead)
- Time critical parts

Solinet: Network Monitoring – OpenSSL

- Installation and Configuration
- Conformity verification
- Performance (40% overhead)

OpenSSL Evaluation

- Evaluation of the OpenSSL organisation
- OpenSSL Product Evaluation
- Conclusions

FreeS/WAN Evaluation

- Evaluation of the FreeS/WAN organisation
- FreeS/WAN Product Evaluation
- Conclusions

Evaluation Scale

Good

Fair

Poor

Evaluation of the OpenSSL organisation (1)

Capability and stability of the organisation = good

- Number of members and software releases indicate the organisation is actively promoting the use of OpenSSL
- Licensing scheme allows unrestricted and free use in commercial products.
- A high number of open source and commercial products already use OpenSSL

Evaluation of the OpenSSL organisation (2)

Support services for the products = fair

- User friendly navigation in OpenSSL web site
- Straightforward and documented OpenSSL installation procedure
- Structured documentation, but
  - Incomplete
  - Overlapping (documentation for old and new versions of the same functionality coexist)
- Poor patch installation guidelines. Expertise required.

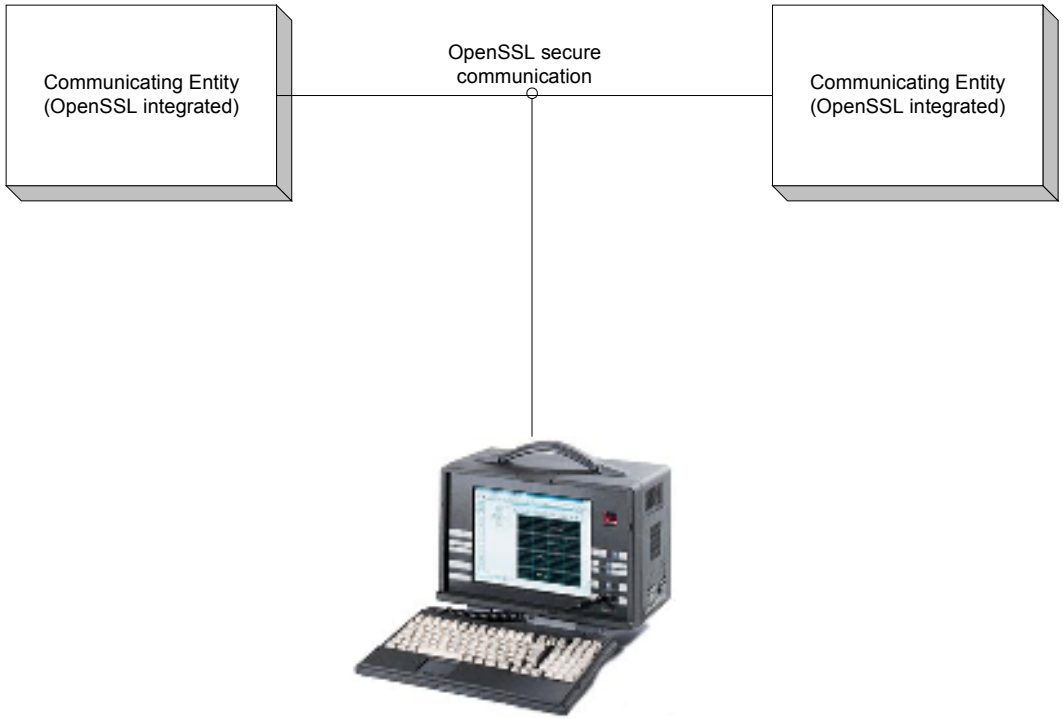
Evaluation of the OpenSSL organisation (3)

Ability to feed requirements into the developing process = good

- User support channels: Internet mailing lists
  - Rapid response to posted questions, within the open source community practices.
  - Rapid inclusion of reported bugs in the developing process, within the open source community practices.
- Replies posted in mailing lists provide accurate information

OpenSSL
software module evaluation (1)

Software module capability: Conformity verification

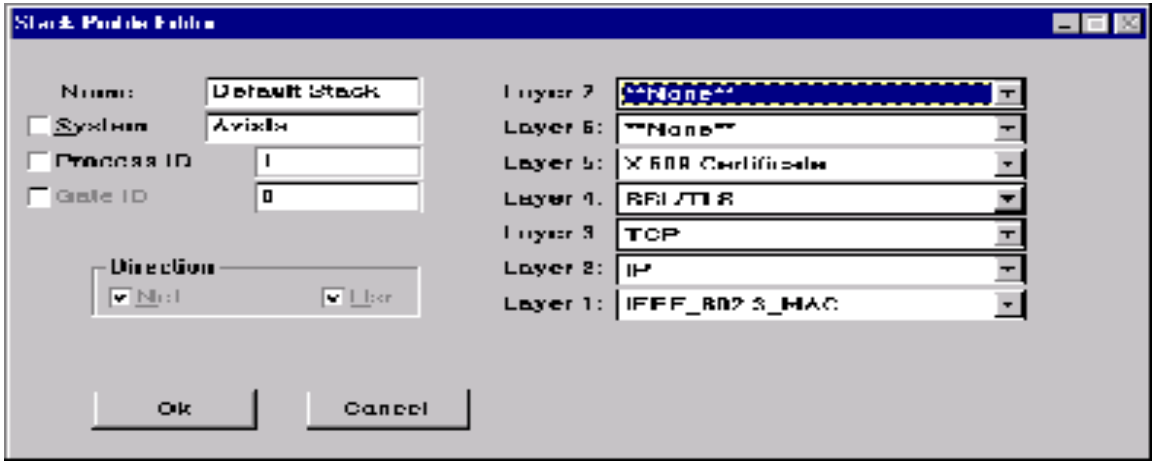


OpenSSL
software module evaluation (2)

Software module capability: Conformity verification (2)

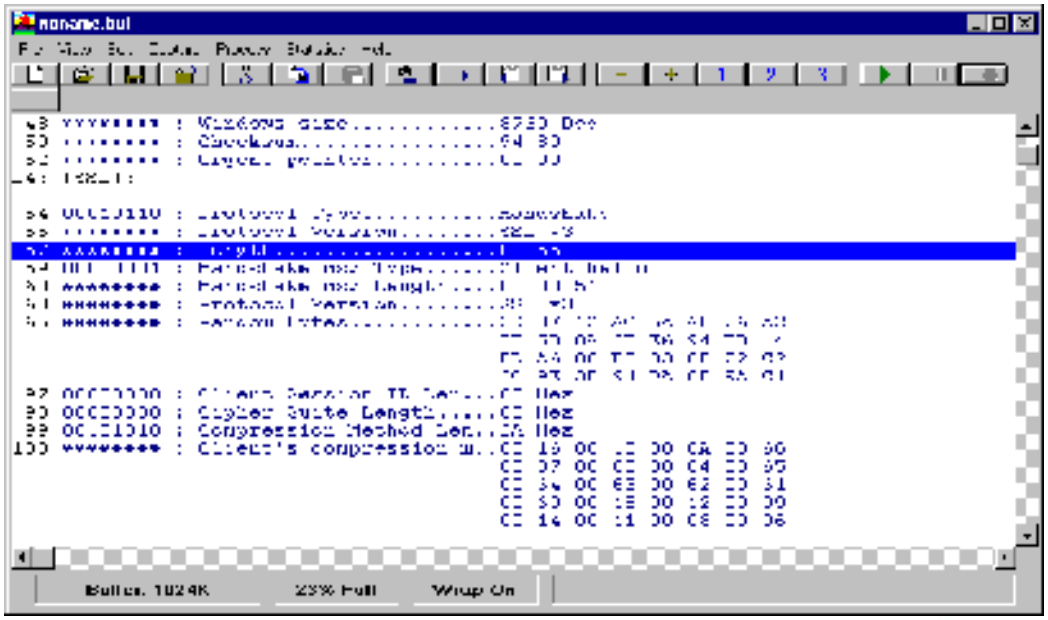
A8619 has been configured with

- IEEE 802.3 MAC protocol disassembly profile
- IP protocol disassembly profile
- TCP protocol disassembly profile
- SSL/TLS protocol disassembly profile
- X.509 certificate decoding profile



OpenSSL
software module evaluation (3)

Software module capability: Conformity verification (3) The OpenSSL protocol negotiation has been decoded properly using the relevant A8619 protocol disassembly profiles, verifying the conformity of the OpenSSL protocol to the relevant standards



Software module capability: Interoperability

- Interoperability with Microsoft Internet Explorer and Netscape Navigator
- Experimenting with Apache Web Server
  - Apache uses OpenSSL for SSL support, through the modSSL interface module
  - Apache used extensively (60% of Web Servers worldwide, Netcraft survey, November 2002)
  - modSSL backwards compatible to other OpenSSL interface modules

Software module capability: Interoperability (2)

- Interoperability problems located:
  - OpenSSL supports a Password Based Encryption method for private keys, that is not supported by all Web browsers (PBE-MD5-DES)
    solution: use other OpenSSL PBE methods for encrypting private keys to be used by Web browsers
  - Minor encoding ASN.1 errors, resulting in malformed certificates being parsed incorrectly
    solution: update OpenSSL, when ASN.1 encoding errors are fixed

Software module stability

OpenSSL product stability factor : 0,51

According to established software engineering practices, a product stability factor of 0,5 is considered to be adequate, for commercial software. Therefore, the open source OpenSSL software package is considered stable.

Software module maintainability (1)

- Few patches: patch factor 0,022 the influence of patches in maintainability is minor.
- 'Makefiles' available for automatic compilation and installation of the OpenSSL software package in a variety of operating systems.
- Distributions contain a text file where all changes, since the previous version, are described
- Online documentation available, comprising of:
  - Contributions by code authors,
  - Contributions by third parties,
  - Lately (Aug 2002), a book.

Software module maintainability (2)

Available documentation

- lack of consistency
- lack of an integrated Table of Contents, or Master Document
- semantic overlaps
  - two or more authors covering the same subject
  - documentation is available, covering older and newer versions of the source code
- No documentation on the code structure

Conclusions on OpenSSL

OpenSSL Organisation

- Capability and stability of the organisation = *good*
- Support services for the product = *fair*
- Feeding requirements to the developing process = *good*

OpenSSL Product

- Conformity verification = *good*
- Interoperability = *good*
- Stability = *good*
- Maintainability = *fair* (for open source community practices)

Evaluation of the FreeS/WAN organisation (1)

Capability and stability of the organisation = fair

- The FreeS/WAN development team consists of experienced software developers and engineers.
- The FreeS/WAN software package is already widely used.

Evaluation of the FreeS/WAN organisation (2)

Support services for the products = poor

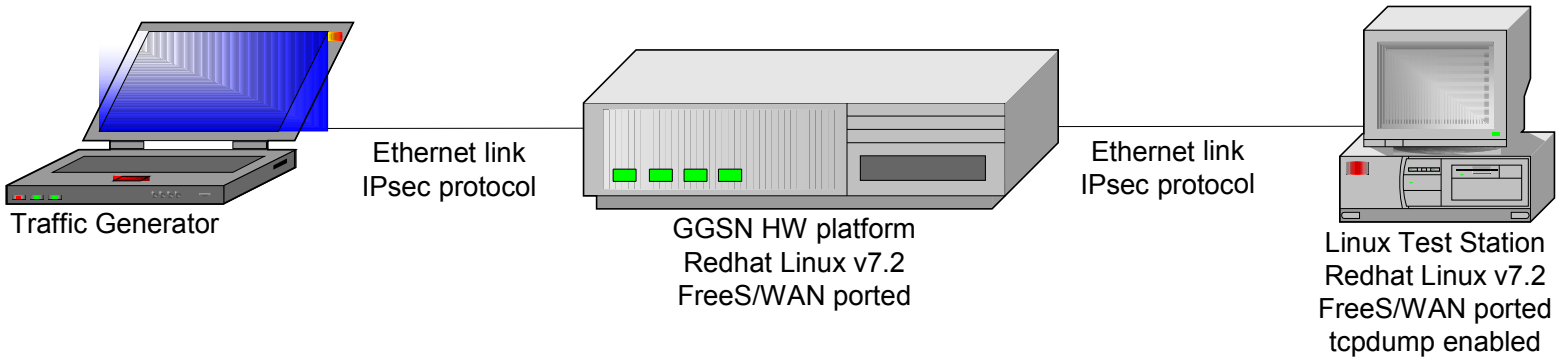
- Navigation in the FreeS/WAN web site is not user friendly
- Documentation provided is not structured and requires advanced experience on several issues (e.g Linux, configuration files etc.)
- Documentation provided does not contain
  - configuration examples
  - detailed installation guidelines
  - patch installation guidelines

Evaluation of the FreeS/WAN organisation (3)

Ability to feed requirements into the developing process = poor

- Communication channel with users and developers: Internet mailing lists
  - response time is not adequate, for a commercial organisation
  - difficult to track related postings

FreeS/WAN
software module evaluation (1)



Software module capability: Functional Verification

- Use of the tcpdump and ethereal tools
- Verification of the ISAKMP negotiation
- Verification of the FreeS/WAN encryption

FreeS/WAN
software module evaluation (2)

Software module capability: Interoperability (1)

- FreeS/WAN does not implement single DES and Diffie-Helman group 1 (768-bit) because they are insecure.
  - Solution: Avoid configuration related to single DES and Diffie-Hellman group 1

- RFCs define two modes for IKE negotiations including the main mode and the aggressive mode. FreeS/WAN does not implement aggressive mode.
  - Solution: If the default option of the other peers is the aggressive mode the user should configure them for main mode

Software module capability: Interoperability (2)

- FreeS/WAN provides perfect forward secrecy (PFS) by default, which is more secure and cost effective. However, some other implementations turn PFS off by default.
  - Solution: Users should either disable PFS in FreeS/WAN, or enable PFS in the other peers

- The IKE protocol allows several types of optional messages. FreeS/WAN ignores optional messages. Problems may arise if the other end relies on the use of optional messages.
  - Solution: Modifications to the source code of FreeS/WAN

Software module capability: Interoperability (3)

- Concerning FreeS/WAN interoperability with Windows 2000 IPSec, a problem with respect to IKE was reported.
  - Solution : FreeS/WAN has changed (from version 1.92 and on) the handling of this.

- **General rule for interoperate with FreeS/WAN**
  - main mode for IKE negotiation
  - triple DES encryption
  - Diffie-Hellman Group 2 (1024-bit) or Group 5 (1536-bit)
  - Perfect Forward Secrecy enabled

Software module capability: Interoperability (4)

- Discrepancies in IPSec terminology used in IPSec implementations
  - Solution: Developers should be aware of the discrepancies in terminology, and interpret the terms they meet, depending on the IPSec implementation they are using.
- IPSec is a peer to peer protocol. IPSec clients cannot provide IPSec services for subnets residing behind them, only IPSec gateways can.
  - Solution: If there is a need to support a subnet behind an IPSec implementation, use an IPSec gateway instead of an IPSec client

FreeS/WAN software module evaluation (6)

Software module stability

- Unexpected communication problems may emerge with VPN clients that use DHCP and NAT.
- FreeS/WAN has restricted functionality concerning shared secret authentication. The FreeS/WAN organisation counter proposes RSA for authentication purposes. However, no IPSec standard has yet been implemented for user authentication.
- No support for X.509 or other certificates
- No support for single DES encryption
- No support for AES encryption

Software module maintainability

- FreeS/WAN does not provide any documentation regarding the architecture of the software module.
- A source code walk-through is required, to understand the functionality of the FreeS/WAN software subsystems.
- An initial source code walk-through we performed, indicated that the source code is not well structured, and that comments are not used throughout the code, thus reducing its maintainability.
- Although the size of the FreeS/WAN patches is not too big, their number is quite big (more than 15) during the FreeS/WAN project period having a detrimental effect on software maintainability.

Conclusions on FreeS/WAN

FreeS/WAN Organisation

- Capability and stability of the organisation = *fair*
- Support services for the product = *poor*
- Feeding requirements to the developing process = *poor*

FreeS/WAN Product

- Functional verification = *good*
- Interoperability = *fair*
- Stability = *fair*
- Maintainability = *fair*

…for more info

For more info, visit

http://laplace.intrasoft-intl.com/secrets/

INTRASOFT INTERNATIONAL

Q&A