



SOGETI

SECURITY EVALUATION FACILITY

# Expertise-based security evaluation

*By Thomas Bousson, Sogeti*

# Agenda

- CC does not always fit
- The French touch
- Some results : TrueCrypt
- Conclusion

# CC does not always fit

- Some constraints
  - Timing
  - Cost
  - No access to the developer
- What assurance can I still get?

- Principles

- Fixed workload (35 man.days)
- Fixed timing (8 weeks)
- Expertise-based evaluation

- Called « CSPN »

*Certification de Sécurité de Premier Niveau*  
First Level Security Certification

- **The evaluation inputs**
  - A “ultra light” Security Target
  - Guidance
  - Documentation (option)
  - Source code (option)
  - Developers (option)

- **The evaluation tasks**
  - Security Target evaluation
  - Product's installation
  - Conformity analysis – security functionalities testing
  - Conformity analysis – documentation (option)
  - Conformity analysis – source code review (option)
  - Strength of Security functionalities
  - Vulnerability analysis
  - Ease of secure usage analysis
  - Developer interview (option)

- Evaluation output
  - ETR
  - Certificate by ANSSI

# TrueCrypt 6.0a

Results from the CSPN evaluation  
performed by Sogeti ITSEF

August 18<sup>th</sup> to September 2<sup>nd</sup>, 2008.

- **Open Source software**
- **Main features:**
  - Creates a virtual encrypted disk within a file and mounts it as a real disk.
  - Encrypts an entire partition or storage device such as USB flash drive or hard drive.
  - Encrypts a partition or drive where Windows is installed (pre-boot authentication).
  - Encryption is automatic, real-time (on-the-fly) and transparent.
  - Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
  - Hidden volume.
- **Scope of evaluation**
  - Software running on Windows XP SP3

# Evaluation highlights

- Cryptographic mechanisms analysis
- Security analysis
- Summary

# Cryptographic mechanisms

AES - Serpent - TwoFish - Cascades - XTS - PBKDF2  
- SHA-512 - Whirlpool - RIPEMD-160 - RNG()

- **Cryptographic algorithms conformity analysis**
  - Standard sequences for all algorithms
  - → no problem detected
- **Cryptographic source code review**
  - Whitebox analysis of RNG
  - Identification of problems
  - Analysis of ciphering contexts
  - → Possibility to mount one volume with different key files

- **Focused on new functionalities**
  - Current vulnerabilities
  - Secrecy traces seeking
    - In core space: program development querying the modified driver
    - In user space
  - Flaws seeking
    - Identification of potential vulnerable fields
    - Tool development handling volumes
    - Mutated volumes creation

# Evaluation Results

- **Cryptographics mecanisms analysis**
  - Standard tests sucessful
  - Volume mounting with different keys
- **Security analysis**
  - Secrecy seeking in core space
    - Password access in BIOS memory
  - Secrecy seeking in user space
    - Password in process memory
    - Key files path never deleted
    - Secondary key never deleted
  - Flaws
    - Strong conception
- **Recommandation**
  - Deny of service : patch ?
  - Avoid using keyfiles
  - Turn toward operating system fully encrypted

# CSPN vs CC

|                         | <b>CSPN</b>       | <b>CC</b>                             |
|-------------------------|-------------------|---------------------------------------|
| Approach                | Expertise         | Conformity & expertise                |
| Type                    | Tunnel Mode       | Iterative                             |
| Levels                  | 1                 | 7                                     |
| Workload                | Fixed 35 man.days | Variable > 3 months                   |
| Developer commitment    | Not necessary     | Necessary to provide all deliverables |
| Certificate recognition | France            | CCRA                                  |
| Certification rate      | 50%               | 90%                                   |

# Thank-you for your attention

Thomas BOUSSON

Sogeti ITSEF

[Thomas.bousson@sogeti.com](mailto:Thomas.bousson@sogeti.com)

<http://esec.fr.sogeti.com>