brightsight®

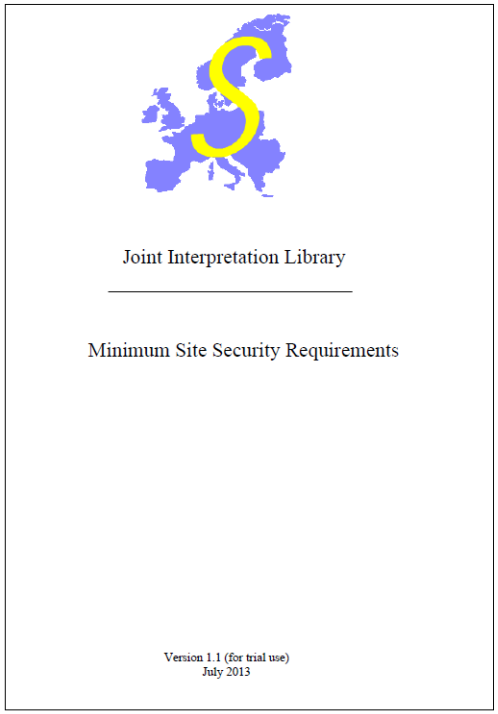
your
partner
in security
approval

Experience with the JIL document: ‘Minimum Site Security Requirements’

Peter van Swieten
+ 31 15 269 2500
swieten@brightsight.com
www.brightsight.com

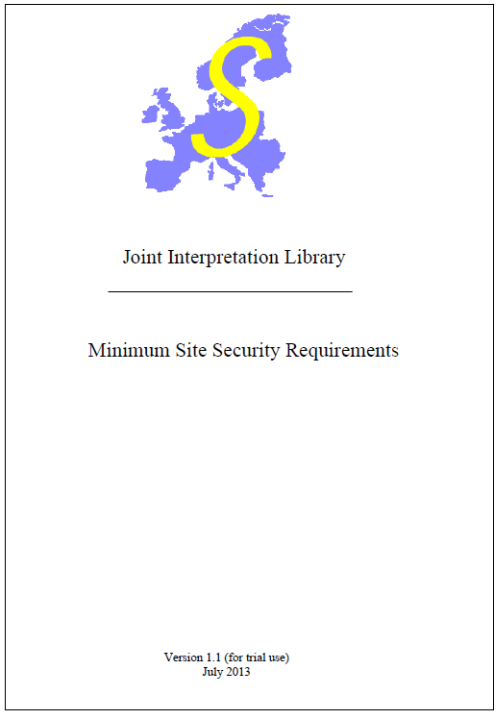
Who, why, when and what? (1)

- Who?
  - ISCI-WG1
- Why?
  - Common Criteria states site security measures have to be ‘sufficient’.
  - Improve harmonization of site security requirements among schemes and labs in relations to this ‘sufficient’
- When?
  - 2 year trial phase (July 1st, 2013): Mandatory to Common Criteria evaluated smartcard and similar devices, including related software.



Who, why, when and what? (2)

- What?
  - Defines many requirements for site security.
  - Requirements are concrete by inclusion of implementation details
  - Some requirements are optional where others are mandatory.
  - Specifically aimed at EAL4+ evaluations and higher where the attacker has a high attack potential (AVA_VAN.5).


Joint Interpretation Library

Minimum Site Security Requirements

Version 1.1 (for trial use)
July 2013

Contents of the presentation

- Brief look into the actual MSSR requirements
- Experiences in applying the MSSR requirements
- Pros and cons of the MSSR approach

MSSR = The JIL ‘**M**inimum **S**ite **S**ecurity **R**equirements’ document

Brief look into the actual MSSR requirements (1)

9.1.2.3 Destruction and disposal of material

Finished goods, semi-finished goods, rejected material, or parts of it that contain the TOE or its parts and that are no longer needed shall be destroyed in a way that remains cannot be used in any meaningful way that might affect the confidentiality of the TOE.

Example:

Wafer, single dies, and packaged chips are shredded in a rolling mill so that every edge of each and any die is cut 3 times.

Masks/Reticules are re-etched in order to remove the pattern or shredded in a rolling mill.

The destruction process is recorded on CCTV.

Confidential and strictly confidential documentation of the TOE on paper or optical disks are shredded according to at least

Brief look into the actual MSSR requirements (2)

In case physical keys are used to access the development area (i.e. where the key is the only access control measure) this area shall have a locking system independent from other areas. Such keys shall be kept secured in a safe place (e.g. key boxes, safe), with access only to authorized persons. Any withdrawal of a key shall be logged.

Brief look into the actual MSSR requirements (3)

9.4.6 Network security management

Objective: To ensure protection of information in networks and protection of the supporting infrastructure.

Only authorized people shall have access to electronic information and data related to the TOE.

The entry point into the development area's network shall be protected at the network boundary by a mechanism that restricts network traffic to a **minimum**, defined in a policy.

Regulations for the segregation of network segments depending on their security categorization shall be defined. Networks for development activities shall be separated from networks for other (e.g. office) applications either physically or by VLAN technologies, protected by access control measures and appropriate firewall rules.

Experiences in applying the MSSR (1)

- Examples are very useful
  - Evaluator: understand the extent of the requirement
  - Developer: clearer in what is expected
- Creating a site audit check list becomes easier. However:
  - The JIL document is extensive (60 pages)
- Developers using ‘a different approach’ to realize security objectives are allowed to do so but have to demonstrate that their level of protection is at least the same.

Experiences in applying the MSSR (2)

- Recently started applying MSSR in:
  - The site security part of a product evaluation
  - Several site certifications including:
    - A development site
    - Network administration sites

- The projects above are expected to complete this year, I will get back to you next year with the results.

Pros and cons of the MSSR approach (1)

Pros (1):

- CC ALC_DVS requires that security measures must be sufficient.
- MSSR defines what is sufficient
  - ➔ Improves harmonization between labs/schemes
    - ➔ Levels involved costs between labs/schemes
    - ➔ Improves re-usability of results between labs/schemes

- MSSR defines what is sufficient
  - ➔ More clear what is expected and at what level
    - ➔ Lower risk for developer.
    - ➔ Lower risk for evaluator.
      - ➔ Both improve cost efficiency

Pros and cons of the MSSR approach (2)

Pros(2):

- Alternative purposes:
  - The MSSR can be used as an educational means.
  - To lower the risk of a site audit the MSSR can be used by the developer to check their (subcontracted) sites.

Cons

- The 'Minimum Site Security' document is extensive (~ 60 pages)
  - ➔ Potentially higher cost. When?
    - ➔ If the developer has to implement new/additional measures or improve existing measures.
    - ➔ If the evaluator has more to check and/or report.

Questions?