34

Evaluation of the security of distributed IT systems through ITSEC/ITSEM: experiences and findings

Ian Uttridge
Logica UK Limited, Stephenson House, 75 Hampstead Road,
London, NW1 2PL, UK. Tel: +44 171 637 9111. Email:
uttridgei@Logica.com
Gualtiero Bazzana
At the time of writing: Etnoteam, Via A. Bono Cairoli, 34 - Milano,
Italy.
At the time of final submission: Onion, Via L. Gussalli, 11 - Brescia,
Italy. Tel: +39 30 3581510. Email: gb@onion.it
Massimo Giunchi
At the time of writing: Etnoteam, Via A. Bono Cairoli, 34 - Milano,
Italy.
At the time of final submission: IMQ, Via Quintiliano, 43 - Milano,
Italy.
Tel: +39 2 507336. Email: imqittl@icil64.cilea.it
Gemma Déler
LGAI, P.O. Box 18, 08193 Bellaterra, Spain (Barcelona). Tel: +34
3691 9211. Email: lgai.ip@servicom.es
Stéphane Geyres
PSTI-Evaluation S.A., 150 Rue Nicolas Vauquelin, F-31100
Toulouse, France. Tel: +33 61.19.29.51. Email:
sgeyres@psti.mipnet.fr
Josef Heiler
TÜV Bayern, Westendstrasse 199, D-80686, München, Germany.
Tel: +49 89 5791 2257. Email: 100034.2201@CompuServe.com

S. K. Katsikas et al. (eds.), *Information Systems Security*

Abstract

This paper reports the experience matured within the SIPE Project (Synergic ITSEC/ITSEM Pre-Evaluation), which was part of the Infosec ‘93 work program. The SIPE Consortium developed European guidelines on the development and composition of security targets for distributed computer systems. The project established the practical application to such systems of the Information Technology Security Evaluation Criteria and Methodology (ITSEC (Commission, 1991) and ITSEM (Commission, 1993)) and was supported by the European Commission, DG XIII.

Keywords

Distributed systems, Composition, Security targets, Mutual recognition

1 INTRODUCTION

The current state-of-the-art of ITSEC/ITSEM is such that no doubt exists about the pragmatic feasibility of security evaluation for certification.

Given this maturity, there is now a need to:

- Sensitize the market, enlarging the audience of ITSEC/ITSEM topics in European industry.
- Cross-check evaluation approaches adopted by different countries in order to strengthen a common understanding of ITSEC/ITSEM concepts and definitions (this is a necessary step towards the mutual recognition of evaluation approaches throughout Europe).
- Benefit from the lessons learnt in evaluations by experienced organisations in order to speed up the knowledge transfer towards companies willing to offer services in the field of security evaluation, especially in those Member States that have been less active in this field so far.

A cost-effective way to reach these goals is to perform ITSEC/ITSEM pre-evaluation studies, involving several organizations of different expertise, characterised by:

- the involvement of companies that ensure a range of member States and expertise levels;
- the analysis of potential targets for pre-evaluations based on products developed by key industrial players from different parts of Europe;
- a strong information flow among partners, ensuring knowledge transfer, a common understanding of concepts and a similar approach to technical procedures used.

The SIPE Project (Synergic ITSEC/ITSEM Pre-Evaluations) was conceived to address these issues as part of the Infosec ‘93 work program, sponsored by the Commission of the European Communities (CEC), DGXIII. The consortium consisted of: Logica (UK), PSTI-Evaluation (France), TÜV Bayern (Germany), Etnoteam (Italy) and LGAI (Spain). The distributed product used as a basis of the SIPE work was Sesame (Secure European System for Application in a Multivendor Environment) (Sesame, 1993). Sesame is under development by ICL (UK), Groupe Bull (France) and SNI (Germany), under the auspices of the EC RACE program.

The project was organised around the following steps:

- development of security targets for a number of Sesame components by independent teams;
- independent parallel trial pre-evaluations of security targets towards an ITSEC level of E3;
- definition of guidelines for security target production, in particular for distributed systems;
- investigation of the feasibility of integrating component security targets of the distributed product into a single composite Target of Evaluation and definition of general guidelines for doing this.

2 A PRE-EVALUATION CASE STUDY - SESAME

Sesame is a distributed product offering a single point for logon, at which the user authenticates only once whatever application(s) he/she will be using. It offers the means to ensure that access to services is policed to the appropriate level of security. Sesame achieves this by means of a sophisticated access control technology which includes an Authentication Service and a Privilege Attribute Service. After successful authentication by an Authentication Server (AS), the user obtains an Authentication Certificate (AUC) which can be presented to a Privilege Attribute Server (PAS) to obtain proof of access rights in the form of a Privilege Attribute Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in ISO 10181-3 (ISO/IEC). Also see (Sesame, 1993).

3 APPLICATION OF ITSEC/ITSEM IN THE INDUSTRIAL DOMAIN

3.1 Areas where guidance is needed

In ITSEC/ITSEM some features specific to distributed and portable systems are missing or not complete. Specifically in ITSEC/ITSEM very little information is provided about producing security targets for individual components of distributed systems so that they can be meaningfully integrated to give a composite security target. This point is based on the nature of the TOE and the major question: How do you evaluate a distributed, portable product, avoiding independent evaluations for each platform and re-evaluation of components?

In fact, the problem of the distribution of the product is an economic one: such a distributed and portable product is in fact a composite product, made of different components, which could be implemented on different platforms and evaluated at different time. As the business of IT moves more and more to the business of system integration, the need for composition, and thus of security target composition, becomes more and more important. On such products, intended as inter-related distributed components, there is only a limited experience on how such products could be evaluated, raising the following questions:

- How can a distributed and portable product be evaluated, taking into account the different individual components which can also be evaluated?

- How can a distributed and portable product be evaluated, re-using the evaluation results of the various components?

A logical evaluation approach seems to be:

- Break down a product for the most effective evaluation and produce security targets for the component parts of the composite, and then evaluate these component security targets;
- Produce the security target of the composite TOE, re-using the evaluation results of the individual components, and evaluate this security target.

There is thus a need for guidelines about the production of the security target for such composite products: re-using the security targets of the components. This composition issue looks very interesting from an industrial point of view, because it allows the re-use of work already done and practical experience on the composition theme is currently limited. To be able to compose security targets the most efficient structure and context for a composite security target was developed. Again guidelines on how to set up security targets are needed not only for composition aims, but also to guarantee mutual recognition.

3.2 Guidelines for the production of security targets

The security target of components of distributed products must contain specific information in order to allow their composition. The SIPE project demonstrated that the structure and the level of abstraction of the security targets could be rather different according to the different evaluators of the different countries. The different approaches taken were compared and resulting differences were analysed. The comparison showed that this variety is due, in general, to the following reasons:

- Different interpretations of the ITSEC requirements, where ITSEC does not provide precise enough information (for example the level of detail of the specification of the SEFs);
- Recommendations issued from each national scheme body. It generally concerns additional material recommended by the different national bodies.

The differences in the security targets sometimes led to differences in the pre-evaluation results of these security targets, which would lead to a different national certificate. This is why, in order to facilitate mutual recognition and to maximize the likelihood of obtaining the same evaluation results for a TOE in different nations, a harmonization of the production of security target among the different nations is needed.

The derived guidance (SIPE, 1994a) is composed of a template and guidelines on how to fill it (what information needs to be provided and with which level of detail). The template aims to help the sponsor in the process of writing security targets, simplify the process for evaluators and to give the Certification Bodies a basis for agreement and development of common procedures that lead to mutual recognition of evaluation results. The template and guidelines have been developed for the production of security targets to be evaluated at the E3 level and consider the possibility of having as a TOE a component of a larger system, product or even an upper level component giving special attention to the composition issue.

The Table of Contents of the resulting template follows (see (SIPE, 1994a) for further details):

- Introduction
    - Purpose of the Document
    - Target Evaluation Level
    - TOE Overview/Abstract
    - TOE Previously Evaluated
    - Document Layout
    - Terminology
    - Acronyms
    - References
    - Standards
    - Functionality Classes
- TOE Identity/Description
    - TOE Type
    - Evaluated Configuration
    - Schematic Diagram and local TOE Environment
        - TOE Interfaces Description
    - Objectives of the TOE
        - Security Objectives
        - Functional Objectives
    - Relation of the TOE with its Boundaries
        - Method of Use
        - Intended Environment
    - TOE Assumptions on Boundaries
        - Method of Use Assumptions
        - Environmental Assumptions
    - Threats:
        - Threats Covered by SEFs
        - Threats Covered by Method of Use and Environmental Assumptions
        - Not Covered Threats
- Security Enforcing Functions
    - Identification and Authentication
    - Access Control
    - Accountability
    - Audit
    - Object Reuse
    - Accuracy
    - Reliability of Service
    - Data Exchange
        - Identification & Authentication
        - Access Control
        - Data Confidentiality
        - Data Integrity
        - Non-Repudiation
    - Other Functions
- External Security Functions
- Security Mechanisms
- Strength of Mechanisms
- Correlation Tables
    - Secure Objectives vs. Threats covered by SEFs
    - SEFs vs. Threats covered by SEFs
    - SEFs vs. Security Mechanisms
    - Assumptions vs. Threats covered by Assumptions
    - Functional Objectives vs. ESFs
    - ESF vs. Security Mechanisms.

3.3 Guidelines for the composition of composite security targets

Guidelines were produced on how to compose distinct security targets into a sensible composite security target (SIPE, 1994b), based on the re-use of the security targets of the components. The guidance is based on the following underlying ideas:

- identification of overall composite security target features ('black box' view of composite);
- gathering security target features from component security targets;
- composition process of security target features divided into steps, each followed by a validation step in order to verify the final composition results ('white box' view of composite).

The inputs needed for applying the composition method are:

- architectural design documentation of the composite;
- security targets for the previously evaluated components being composed.

It is important to note that the method can be applied, provided that the following assumptions are satisfied:

- The available component security targets should be structured according to what is described in the SIPE security target template. If not, additional information requested by such a template will have to be extracted from the architectural design documentation of the composite.
- For those components identified in the architectural decomposition to be correlated to the security target, but for which there is no available security target (for instance, unevaluated components), the method assumes that all the component security and functional features, required to harmonise the composition, can be extracted from the design documentation.

The method has proven to be applicable for all the intended composite assurance level (provided the assurance level of the composite is compatible with the component assurance level). Specifically security targets at different levels of evaluation differ only in the granularity of information (rigor of description): extra information, requested if the composite was at a higher level, would be extracted from the design documentation. There follows a high level description of the method.

Definition of composite security target features

The definition of the overall composite security target features must be provided, in order to allow validation of the work during the composition. Such description of the composite security target will be performed in a top-down way, extracting the security features of the composite component from its design documentation; the following information is derived (see (SIPE, 1994b) for further details):

- the type of the composite;
- the evaluated configuration;
- the schematic diagram and local composite component environment;
- the objectives of the composite component (security and functionality objectives);
- the composite component boundaries (in terms of intended method of use and environment);
- the threats;
- the Security Enforcing Functions (SEFs);
- the External Security Functions (ESFs) (see the first bullet point of section 3.4);
- the security mechanisms implemented in the composite (ITSEC optional section).

Gathering security target features from component security targets

During this stage all the component security features (such as method of use, threats and ESFs) are gathered from component security targets (if available) or architectural design documentation.

Composition process

The purpose of the composition process is to integrate and validate all the information for the security target of the composite. The composition of security targets is based on:

- independently developed definition of features of a composite security target (such as SEFs);
- each composition will be followed by a 'validation process'.

The composition process follows the structure of the SIPE security target template. Each step of the composition process corresponds to the filling in of a section of the security target template of the composite. For each step consisting of a composition of several sources of information (component security targets and design documentation) a validation process is undertaken in order to ensure the consistency of the resulting security target and its evaluatability. Specifically, it could be simply a check of consistency (for terminology, acronyms, references, standards and functionality classes referenced) or a check of compatibility of the configurations, or a check of completeness of the component functional objectives versus the design documentation.

In other cases, it could be a binding analysis in order to investigate the ability of the set of features to work together in a way that is mutually supportive and provides an integrated and effective whole (this is the case of composite functional/security objectives, method of use assumptions, ESFs, SEFs and security mechanisms). Again validation could also be performed by a suitability analysis in order to determine whether the security features (such as SEFs, ESFs, mechanisms) will in fact counter the identified threats and whether the threats are countered by the security features. To gain a better understanding of which features of component security target contribute to which security features of the composite security target, see (SIPE, 1994c).

3.4 Findings from the case study

During the SIPE project, the distributed, portable and composite Sesame product has been used to gain experiences on a pragmatic case study. Such a case study allowed the SIPE partners to highlight various technical issues which first emerged from the nature of a distributed system and then from different interpretations (national driven) of ITSEC/ITSEM.

The main issues emerged and analysed during the SIPE project, proposing for each of them a solution or recommendations, are as following:

- **Categorisation of Functionality**: This issue arises when it is taken into consideration the future integration of a TOE when writing its security target. It concerns the need to include the component 'core-functionality' in their corresponding security targets, and the way to do it, in order to enable the composition phase. Such 'core-functionality' are those functions that are externally visible and which contribute to build the security of the overall system. For these functions a new term was introduced, the 'External Security Functions' (ESFs).
- **Level of Abstraction of Security Target**: As the security targets can have different levels of detail/abstraction (currently ITSEC/ITSEM give little guidance about this), it appears that more guidance on writing security targets is needed because this variety might have consequences on the evaluation process and results and make the composition process less harmonized. The solution proposed is to reduce the range for abstraction of security targets by the production of a template that includes guidelines about how to fill it, taking into account several cases.
- **Portability of TOE:** To avoid multiple evaluations of portable TOEs, the evaluation deliverables and result should be as 're-usable' and as modular as possible. The Sponsor does not want to have separate security targets for each evaluated configuration, but rather a generic security target for its product, which could be instantiated for each platform. In this case a problem arises, because such a generic security target, independent on any platform, does not contain all the information needed to perform a complete evaluation (for instance, the penetration testing cannot be performed). Currently the ITSEC gives no guidance on how security targets should be written for end-system products which are portable across many architectures, so that re-use of evaluation results can be optimised.
- In order to maximise portability of the TOE and re-use of evaluation results, the following recommendations should be used:
  - Do not list specific machines or operating systems as required platforms.
  - Precisely specify the services you need from the hardware and operating system.
- **Relevance of ITSEC/ITSEM Headings for Distributed Products**: For distributed components and composed product there is the need to extend the conventional notion of SEFs, because the recommended ITSEC SEF headings are not suitable. As ITSEC/ITSEM do not prevent the use of other headings for the classification of SEFs, if a new heading is required, then it should be clearly stated why the recommended headings are not appropriate for the classification of this SEF.
- **Strength of Mechanism:** It is difficult to have strength of mechanism where the exact

mechanism type is not known. There are three reasons for which it seems to be very difficult to claim a strength of mechanism for a distributed and portable product like Sesame:

- What should be the composition function of the different component strengths of mechanism? If we choose, for the Sesame security target, the lowest strength of mechanism of its components, it would certainly not reflect the truth (e.g. the composition of two components which have both a basic strength of mechanism could generate a high strength of mechanism as a result of composition).
- The concept of strength of mechanism is not applicable for every mechanism. This is the reason why the Common Criteria (ISO/IEC, 1994) defines two types of mechanisms: type A mechanisms, for which it is relevant to consider a strength of mechanism (e.g. encryption mechanisms), and type B mechanisms, for which this concept is not applicable (e.g. access control mechanisms).
- For a portable component, the mechanism type is not known in some cases, and the strength of mechanism depends on the specific implementation. Thus it may not be relevant to define a strength of mechanism for a generic product which claims to be independent of a particular implementation. The solution proposed is for each component i, which depends on optional mechanisms j, a function must be defined which gives the strength S_i of component i as a function of the strength S_j of component j:

  $S_i := f(S_j)$

- In the easiest case, this function could be a statement like "If the strength of j is high, then the strength of i is also high". But more complex mathematical functions are possible. The elaboration of the function $S_i := f(S_j)$ must be done during the composition of component i. The actual calculation of the result will be done on the integration of the components to an overall product.

4 CONCLUSIONS

In summary, the benefits gained during the SIPE project are (further details can be found in (SIPE, 1994c)):

- **Technical Results**: Major technical results, which will be of benefit to the European security community at large, have been achieved from the project and include:
  - Technical basis for addressing the evaluation of distributed systems.
  - Improvements to the ITSEC and ITSEM, from the distributed system viewpoint and from a general viewpoint. This includes identifying exactly what 'composibility' means in terms of evaluations under the ITSEC.
  - International scope for the composition method developed since it does not depend on any security evaluation criteria: the security target of a distributed product/system obtained by applying the composition method can be used as a reference in any security evaluation (according to ITSEC/ITSEM, to the Common Criteria (ISO/IEC,

1994), etc.) from the fact that the considered criteria are based on a security target or alike.

    - Identify the need and propose solutions for modular evaluations of products, systems and components for which the results (security targets, evaluation results) can be reused.

- **Contribution to Sesame**: The Sesame consortium has benefited from SIPE:
    - Ideas and means for future improvement of the Sesame product and its documentation.
    - Development of security targets for some Sesame components.
    - Pre-evaluation of some of the Sesame security targets.
    - Assessment of suitability of Sesame documentation for full evaluation.
- **Estimation of Costs** for a full evaluation of a Sesame component.
- **Knowledge Transfer**: There were many benefits to the expert and novice evaluators, sponsors and to the continued evolution of evaluation in Europe, including, mutual understanding of general security topics, evaluation criteria and methods in different European countries which will contribute to mutual recognition.
- **European Awareness on Security Evaluation**: The project has helped European countries, new to IT security evaluation, to progress in the field. In fact, the novice evaluators from Italy and Spain are now deeply involved in the development of their own national schemes.
- **Additional Project Outcome**: The original goal of the project was to address the evaluation of distributed systems/products. However, during the course of the project, it became clear that such distributed systems are only a special case of a more general case, that is composed systems/products. As a consequence, the method and template developed by the project address various aspects of composition and distribution, such as:
    - Reusability of component security targets;
    - Reusability of evaluation results;
    - Modular, hence more cost-effective evaluations;
    - Portable products.

5 FUTURE DEVELOPMENTS

The SIPE project found that there are several areas which should be developed further, including:

- Further experimentation and refinement of the composition method and template.
- Full evaluation of all or part of Sesame, in particular using the harmonised approach developed in the project.
- Investigation of the impact of the security target template and composition method on the emerging Common Criteria.
- Investigation of the possibility of developing a set of guidelines which are based on the security target template and composition method and would help to design a composible product or component with security features.
- Investigation of the expansion of the guidelines to other associated domains such as safety.

6 REFERENCES

Commission of the European Communities (1991*) Information Technology Security Evaluation Criteria (ITSEC) - Version 1.2,* CEC.

Commission of the European Communities (1993*) Information Technology Security Evaluation Manual (ITSEM) - Version 1.0,* CEC.

Sesame (1993) *Secure European System for Application in a Multivendor Environment, An Introduction - Issue 1.2.*

ISO/IEC DIS 10181-3 *Information Technology - Security Frameworks in Open Systems- Part 3: Access Control.*

SIPE Consortium (1994a) *Guidelines for Developing Security Targets for Distributed Systems - Issue A.*

SIPE Consortium (1994b) *Guidelines for the Composition of Security Targets - Issue A.*

ISO/IEC/JTC1/SC27/WG3 (1994) *The Common Criteria.*

SIPE Consortium (1994c) *Final Management Report - Issue A.*

7 BIOGRAPHIES

Ian Uttridge is an IT and Security Consultant in Logica's Government Division and was Project Manager for the SIPE project. Logica is one of the UK's Commercial Licensed Evaluation Facilities (CLEF). Ian has worked in IT security for 11 years, developing the first high assurance secure operating system to be formerly certified by the UK Government, leading security R&D, implementation and evaluation activities and participating in pan-European collaborative projects.

Massimo Giunchi, since 1991, has worked for the Sw Technology and Engineering Department at Etnoteam. As a consultant he worked in telecommunications, covering topics like: sw development methodologies, testing methods, definition of documentation standards, process improvement and definition of quality systems. In 1995 he joined the Italian Certification Body (IMQ), where he is involved, in the definition of services for the Certification of IT products/systems according to ITSEC/ITSEM and in collaborative research projects, concerning IT certification services.

Gualtiero Bazzana has acted in the SIPE Project as part of his R&D work in the Sw Technology and Engineering Area of Etnoteam. He is currently a Partner and Consulting Director of Onion, which specialises in the fields of communications, technologies and consulting. He has acted as Project Manager in important projects in sw development/testing/evaluation for major companies in Europe. He has been involved in research collaborative projects, concentrating in sw engineering and IT security. He is author of more than 30 publications, including books and refereed papers.

Gemma Déler is head of the IT and Projects area in LGAI where Card Systems testing, evaluation and assessment is performed - security is important. Member of the Ad-hoc group defining the National Evaluation and Certification Scheme for IT since June 1994. Member of standardisation committees, (National, European and International): Convenorship of the

National Committee for Card Systems and delegate in CEN and ISO. Member of AENOR CTN 71: IT, and CTN 71/SC 27: Security. Member of ATI (Asociacion de Tecnicos en Informatica) working group on Security.

Stéphane Geyres is head of the Security Evaluation Activity at PSTI-Evaluation, Toulouse, France, one of the French ITSEC Evaluation Facilities. As the former Technical Leader of the ESPRIT SCOPE (Software CertificatiOn programme in Europe), his research interests are in software products evaluation in general and in security evaluation in particular. His current investigations are related to the evaluation of authentication solutions for real information highways contexts.

Josef Heiler has been with T¼V since 1990 working in the Institute for Quality and Safety in Electronics Engineering. His major assignments include: evaluating the security of personal computer networks, safety testing of medical equipment, industry automation systems and real time data processing for digital analysis and synthesis of speech and medical laboratory data acquisition.

Thanks go to Jeremy Wilde (Logica) for his ideas and support in starting-up the SIPE Project. Our thanks also go to Belinda Fairthorne, Robin Lee, Piers McMahon, Tom Parker (ICL), Hiep Doan, Hassan Ratni (Groupe Bull), Per Kaijser (SNI), Fabienne Hantz (PSTI), and Gianni Rumi.