

NESSIE

Project Number IST-1999-12324
Project Title NESSIE
Deliverable Type Report
Security Class Public
Deliverable Number D05
Title of Deliverable Dissemination and Use Plan

Nature of the Deliverable

Document reference NES/DOC/KUL/WP7/D05/1
Contributing WPs WP7
Contractual Date of Delivery Y1M06
Actual Date of Delivery Y2M01
Editor Keith Howker

Abstract The planned routes for uptake of NESSIE results into standards and products is described.

Keywords

Disclaimer The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Document Control

Document History

Changes have been incorporated in line with comments in earlier drafts.

This is the first issue of this document

Changes forecast

Any substantial changes to plans will be included in a Version 2.:

- exploitation
- dissemination in general
- standardization opportunities

1, Introduction

This document outlines the dissemination and exploitation activities of the project. It may be claimed that this is in fact the prime goal of the project, and that the technical activity is the means to realize it.

The NESSIE mission is to put together a public portfolio of strong cryptographic primitives for use by the information economy and society that the IST programme is designed to foster. This portfolio is to be obtained through open, transparent call and evaluation processes carried out by the project.

In addition to simply making the project results available for general use and exploitation, the project partners will actively support their adoption into appropriate international standards.

The majority of the partners are from academic institutions and do not themselves have direct routes to exploitation of the project results; the exploitation intentions of the industrial partner, Siemens AG¹, are described below.

The project has already contributed to the *defacto* international standardization through its contribution to NIST's AES² process.

2. Background

The project supports several main priorities identified in the 1999 Work Programme. It will provide building blocks that are essential to overcome the bottlenecks that prevent the development of the information society by recommending and establishing trust in strong cryptographic primitives. In addition, these results will support interoperability and standards and will support European policies in the area of data security, data protection, and privacy.

The project can produce the necessary critical mass to build confidence in, and European support for, a set of primitives, which would not be possible at the national level.

One of the most important objectives of this project is to ensure the acceptability of the results of the project, that is, to convince software developers and users to integrate the recommended primitives into applications.

The final step of the dissemination process is the input of the results into standardisation in a way that maximises the likelihood of uptake.

3. Dissemination

The Project Industry Board was established to create visibility of the work of NESSIE in the commercial sectors and to ensure alignment between the requirements of industry and the technical orientation of the project. The board is being consulted during every stage of the project.

The project will also use the opportunities offered by the Fifth Framework Programme to make its work and results known and to interact with other projects that can use NESSIE's results.

1 Siemens AG is the only industrial participant following the withdrawal of Fondazione Ugo Bordoni

2 United States National Institute of Science and Technology: Advanced Encryption Standard

The open workshops organized by the project will provide visibility across the cryptographic and information security research community as a whole, as has the contribution to the AES process.

4. Standardisation

Most partners are already strongly involved with the standardisation of cryptographic primitives in different bodies (ISO, ISO/IEC, IEEE, and IETF). The different options for standardisation will be explored during the first half of the project and standardisation strategies will be developed. The appropriate standards bodies will be informed about the ongoing project status. During Year 3, steps will be taken to set up the processes to introduce the recommended primitives into the selected standardisation bodies. This can be achieved by producing descriptions of the finalists, in the format required by a specific body. Special care will have to be taken that the status (finalist versus recommend) does not create confusion.

A final element of the dissemination processes is the publication of results in scientific and industrial publications. This includes conferences such as Eurocrypt, Fast Software Encryption, Crypto, and Asiacrypt, journals such as the Journal of Cryptology, Cryptologia, and Dr. Dobbs's, and also an edited volume (for example, in the Springer-Verlag Lecture Notes in Computer Science).

5. Exploitation

Siemens AG

Some of the most commonly used cryptographic algorithms of today are no longer "state of the art", such as e.g. the block cipher DES and the hash function MD5. For DES, the block size of 64 bits and the key length of 56 bits are too small; and for MD5, the output length of 128 bits does not offer enough protection against attacks.

One of NESSIE's main aims is to provide cryptographic primitives that are "state of the art", which will be of great interest to all Siemens business units where security plays an important role.

Block ciphers to be submitted to NESSIE, e.g., must have a block length of at least 128 bits (except for legacy block ciphers) and a key length of at least 128 bits; and collision-resistant hash functions, e.g., must have an output length of at least 256 bits.

5.1 Exploitation of Primitives

a) Exploitation of security primitives selected by NESSIE

A broad range of Siemens products, from phone cards and car immobilisers to email encryption systems, require security primitives. The correct choice of the primitives used is essential for the security of the products. Here the rich portfolio of algorithms which NESSIE plans to recommend will be very useful. Moreover, instead of having to evaluate the strength of the algorithms considered, it will be possible to rely on the results of the NESSIE security analysis.

The Siemens unit which offers security products is ICM CD IS. It is not known which products will be in the definition phase in the year 2002 and later, when the NESSIE recommendations will be available, but the product lines where the NESSIE recommendations can be applied are the following:

- Encryption Devices

- Software Security Products Online
- Software Security Products Offline
- PC Security and Smartcards
- Built-In-Security
- Basic Encryption Components

ICM CD IS wants to add the security algorithms recommended by NESSIE to its cryptographic software library ACRYL, which is part of the product line “Basic Encryption Components”. Thus, the NESSIE algorithms will be available for the other product lines of ICM CD IS and, since ACRYL is also used outside ICM CD IS, for the whole company.

Another part of Siemens which has declared great interest in the NESSIE results is the smart card unit of Infineon Technologies (formerly Siemens Semiconductors). Infineon CC delivers 40% of the smart card chips of the world market. It wants to be comprehensively informed about NESSIE in order to be able to identify submissions suitable for its future smart cards as soon as possible.

Siemens VT (Transportation Systems) uses cryptography to achieve railway safety. This approach to safety is quite new, and the selection of suitable cryptographic algorithms is controversial. Railway operators, authorities which approve railway equipment, and the manufacturer of the equipment have to agree. VT welcomed the Siemens participation in NESSIE because they hope that the NESSIE results will be both efficient and generally accepted.

SBS FS (Siemens Business Services, Financial Services) develops software for home banking, where security of course plays an important role. Digital signature algorithms are particularly important in this context. Hopefully, NESSIE will provide some digital signature algorithms based on elliptic curves, which are faster and need less memory than those based on RSA.

Siemens ICN needs security for multimedia applications. Since there are strict performance constraints for these applications, efficient NESSIE primitives will be very useful, in particular fast MACs.

For other Siemens business segments, where security or safety is not a central point, requests for cryptographic primitives are not foreseeable on longer terms. However, experience shows that such requests keep turning up. For many of these requests, the NESSIE results may be the answer. The availability of the NESSIE algorithms in ACRYL will make it very comfortable for the Siemens units to use them.

b) Exploitation of security weaknesses found by NESSIE

Negative results can also be very important for consulting about security primitives. If NESSIE finds weaknesses of security primitives, warnings can be issued in consulting. If NESSIE finds weaknesses of cryptographic algorithms used in Siemens products, the early information will enable Siemens to minimise the damage. Obviously, it is completely unforeseeable whether NESSIE will detect such weaknesses.

5.2 Exploitation of Methodologies

a) Exploitation of methodology and cryptanalytic approaches

Beyond the information about the cryptographic algorithms evaluated by NESSIE, Siemens also expects indirect results of the project.

The Center of Competence Security at Siemens Corporate Technology is the main place within Siemens where the strength of cryptographic primitives is evaluated; and the

experience from NESSIE should have a positive effect on these activities. The methodologies and cryptanalytic approaches learned from the other NESSIE partners will certainly be useful for other security evaluations.

Since such security evaluations are not planned a long time ahead, it is not possible to give concrete examples for which the NESSIE experience will be useful.

b) Exploitation of the toolbox for the evaluation of cryptographic algorithms

The Center of Competence Security at Siemens Corporate Technology already has a rich toolbox for the evaluation of cryptographic primitives, but NESSIE will produce a valuable extension. It is clear that an evaluation by tools can never be sufficient to be convinced of the strength of an algorithm, but negative results from tools can be a very efficient way to detect weaknesses of cryptographic primitives. The existing toolbox is being extensively used both for the development and for the evaluation of cryptographic algorithms, and the new tools will extend the scope of properties covered. Furthermore, the tools have been used for the evaluation of statistical properties of hardware random number generators. Some of the tools to be developed in the NESSIE project will also be useful for this.

Probably such an evaluation of random numbers will be the first exploitation of NESSIE results. The physical random number generator of new members of the Infineon CC families of SLE 66 and 88 cryptocontroller chips will undergo an extensive statistical analysis. The NESSIE tools suitable for such testing will be used for this, in addition to the tools already available, as soon as they will have been implemented.

The toolbox already existing at the Center of Competence Security at Siemens Corporate Technology mainly provides tests for stream ciphers and block ciphers. It already contains quite a variety of stream cipher tests, so that the new block cipher tests to be developed in NESSIE, e.g. for differential and linear cryptanalysis, will be particularly welcome.

5.3 Dissemination of the NESSIE results

One means of communication about NESSIE and its results will be the “Siemens Security Newsletter”, which is provided by the Center of Competence Security at Siemens Corporate Technology and distributed quarterly to more than 200 subscribers.

Since considerable consulting about security primitives is done at the Center of Competence Security at Siemens Corporate Technology, where the Siemens part of the NESSIE project is located, there will be very short paths of communication for the propagation of NESSIE recommendations within SIEMENS.

The Center of Competence Security at Siemens Corporate Technology presents, once a year, its current projects and results to the Siemens business units. This presentation will be a suitable frame for disseminating the NESSIE activities and results.

Siemens Corporate Technology has key account managers for all Siemens business units. Especially those for ICM, Infineon CC, VT, and SBS will be informed about the NESSIE results, in order to reach a broad distribution in their units.

But the Center of Competence Security at Siemens Corporate Technology will not only rely on the key account managers to make the NESSIE results known; we will also give special talks to the business units most interested, e.g. Infineon CC, which we have already done to inform them about the AES candidates.

The Center of Competence Security at Siemens Corporate Technology offers quarterly seminars about cryptography. These seminars will also be a good opportunity to inform about NESSIE.

The Center of Competence Security at Siemens Corporate Technology usually invites representatives from the industry once a year, e.g. representatives of banks and insurance companies, who are interested in new developments concerning security. These meetings will also be used to disseminate the NESSIE results.

Two experts in cryptography at the Center of Competence Security at Siemens Corporate Technology hold regular lectures on cryptography at universities in Munich; they will integrate the NESSIE results into their lectures as soon as they are available.

Siemens representatives play an active role in several security related standardisation bodies, e.g. ISO/IEC JTC-1/SC 27 (IT Security Techniques), ITU-T SG16, IETF, and ATM Forum (Security Working Group). They will have the task to support the cryptographic primitives suggested by NESSIE in these bodies.

Siemens Intranet pages provided by the Center of Competence Security at Siemens Corporate Technology will allow all interested parties within Siemens to follow the NESSIE activities and to be informed about the NESSIE results.

If the NESSIE activities lead to significant scientific results, these results will be submitted to major crypto conferences like Eurocrypt or Crypto.

So, Siemens will benefit in various ways from the NESSIE project, and a number of means will be used to assure a high visibility of NESSIE for the Siemens Units.