

NESSIE

Project Number	IST-1999-12324
Project Title	NESSIE
Deliverable Type	Report
Security Class	Public
Deliverable Number	D10
Title of Deliverable	Description of Methodology for Security Evaluation

Nature of the Deliverable

Document Reference NES/DOC/RHU/WP3/D10/3

Contractual Date of Delivery Y1 M12

Actual Date of Delivery Y2 M1

Editor Sean Murphy

Abstract

In this deliverable, we briefly outline the methodology used to assess the security of cryptographic primitives to the NESSIE project.

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.

1 Introduction

This report is the deliverable D10 of the NESSIE project. The report describes the broad methodology used to evaluate the security and suitability of the submitted primitives. The NESSIE project has attempted to define a methodology to compare in a fair and acceptable way the submitted primitives. It may evolve according to technical advances, remarks of the NESSIE members, Industry Board or cryptographic experts, and with problems encountered.

2 General Security Evaluation Issues

The NESSIE call for primitives gave the following detailed security evaluation criteria.

1. An attack should be at least as difficult as the generic attacks against the type of primitive (exhaustive search, birthday attack etc.).
2. Primitives will be evaluated against the security claims of the submitter. An attack requiring lower computing resources than claimed would usually disqualify the submission.
3. Primitives will be evaluated within the stated environment. Thus, consideration of vulnerability to side channel attacks (e.g., timing attacks, power analysis) may be appropriate.

We now discuss some of the issues that are central to the security evaluation and that are generally applicable. Issues that are specific to individual types of primitive are discussed in the next section.

2.1 Resistance to Cryptanalysis

Clearly, any submission should be resistant at the relevant security level to cryptanalytic attacks. Indeed, in the NESSIE call for submissions (reproduced above), it is stressed that failure to be resistant to such an attack would usually disqualify a submission. However, when assessing the relevance of a cryptanalytic attack, other factors such as the volume and type of data required to mount the attack will be considered.

2.2 Design Philosophy and Transparency

An important consideration when assessing the security of a cryptographic primitive is the design philosophy and transparency of the design of that primitive. It is easier to have confidence in the assessment of the security of a primitive if the design is clear and straightforward, and is based on well-understood mathematical and cryptographic principles. This is particularly relevant when making relative comparisons between primitives (see below).

2.3 Strength of Modified Primitives

One common technique used to assess the strength of a primitive is to assess a modified primitive, for example by changing or removing a component or reducing the number of rounds. Conclusions about the original primitive based on an assessment of the modified primitives have to be carefully considered as the inference may or may not be straightforward.

2.4 Relative Security

When assessing primitives designed to operate to the same security level in similar environments, it is natural to wish to compare their security. However, care has to be taken when making such comparisons. One measure that has been suggested is the *security margin*, but there is no general consensus about its definition or use. Furthermore, whilst the NESSIE project tries to ensure that each submitted primitive receives equivalent cryptanalysis, it is the case that some designs are easier to analyse than others (as discussed above).

2.5 Cryptographic Environment

In certain cryptographic environments, a cryptographic primitive may have been designed to possess intrinsic security advantages or disadvantages. An example would be a primitive that is resistant to power or timing attacks when implemented on a smart card. Such properties would be considered when assessing the security of a primitive.

2.6 Statistical Testing

The NESSIE project is carrying out statistical testing of submitted primitives (where relevant). The purpose of this statistical testing is to highlight anomalies in the operation of the primitive that may indicate cryptographic weakness and require further investigation.

3 Specific Security Evaluation Issues

In this section, we consider security evaluation issues that are specific to the different types of primitive. We give some generic attacks on types of primitive that will be considered by the NESSIE security evaluation. For convenience, we have placed the different types of primitive into four groups: block ciphers, message authentication codes (MACs) and hash functions, stream ciphers, and asymmetric cryptography. Clearly some comments about a category may have relevance to other categories. However, there may be other particular ways in which certain primitives may be vulnerable to attack, and individual cryptanalytic techniques specific to individual primitives may be developed to assist in assessing an individual primitive's security.

3.1 Block ciphers, Hash Functions and MACs

The NESSIE call for primitives specified the following security levels.

Block Ciphers

High: Key length of at least 256 bits. Block length at least 128 bits.

Normal: Key length of at least 128 bits. Block length at least 128 bits.

Normal-Legacy: Key length of at least 128 bits. Block length 64 bits.

Message Authentication Codes (MACs)

High: Key length of at least 256 bits.

Normal: Key length of at least 128 bits.

Hash Functions

High: Output length of at least 256 bits.

Normal: Output length of at least 128 bits.

Hash functions should be preimage resistant and second preimage resistant.

The applicability of the techniques of differential cryptanalysis, linear cryptanalysis, birthday attack and related key attacks (and their variants) on the submitted primitives, and the existence of weak key classes are amongst the factors considered by NESSIE in making security evaluations on this category of primitive.

3.2 Stream ciphers

The NESSIE call for primitives specified the following security levels.

Stream Ciphers

High: Key length of at least 256 bits. Internal memory of at least 256 bits.

Normal: Key length of at least 128 bits. Internal memory of at least 128 bits.

The applicability of the techniques of correlation analysis and re-keying (key initialisation) attacks (and their variants) on the submitted primitives and the existence of weak key classes are amongst the factors considered by NESSIE in making security evaluations on this category of primitive.

3.3 Asymmetric Primitives

The NESSIE call for primitives specified that the security parameters should be chosen such that the most efficient attack on the primitive requires a computational effort of the order of 2^{80} 3-DES encryptions. Furthermore, for asymmetric identification schemes, the probability of impersonation should be smaller than 2^{-32} .

Asymmetric cryptographic primitives are based on mathematical problems that are believed to be “difficult” to solve. Indeed, for some of the submitted primitives there is a proof of equivalence between finding cryptographic information and solving the difficult problem. Furthermore, some of the submitted primitives are based on similar difficult problems. The examination of the assumptions (including their practicality) underlying the asymmetric primitives forms a factor in the NESSIE security evaluation. However, the time and resources required to solve the difficult problem using current techniques is also a factor considered by the NESSIE security evaluation.

4 Development of a Security Evaluation

This document describing the NESSIE security methodology has given a list of important issues that are considered in making a security evaluation of a submitted primitive. Clearly, this list is not complete.

Cryptographic primitives with completely inadequate security can often be identified. However, for the remaining cryptographic primitives, the situation is nothing like as clear-cut. There is neither an automatic method of assessing the security of such a primitive nor a general consensus on the relative importance of different security criteria. The few previous initiatives that have undertaken a similar task to the NESSIE project, such as AES, have been more limited in scope and have reached a subjective judgement by experts on the security of such primitives. The NESSIE project will produce a security judgement for the submitted primitives based on the issues discussed in this report.