A Review of the SESAME Development

Per Kaijser

SIEMENS AG
D-81730 Munich, Germany
per.kaijser@mchp.siemens.de

Abstract. The development of the SESAME (Secure European System for Applications in a Multi-vendor Environment) security concept started approximately a decade ago. The flexibility and scalability properties, the focus on simple administration and the modular structure are some of the reasons why this architecture has formed the basis for several security products. This paper attempts to make a short summary of the SESAME development from its infancy to TrustedWeb, the latest solution particularly adapted for the administration and protection of Web-resources in large intra- and extranet environments.

1 Introduction/Background

During the decade of the 1980's most IT vendors were engaged in OSI (Open Systems Interconnections) standardization. Most of this took place in ISO TC97 (now ISO/IEC JTC1) and CCITT (now ITU-T). In the area of IT security, ISO had specified the OSI security architecture [1], which main result was the terminology and short description of some security services and in which layer of the OSI layer model they could be implemented. Work on a set of security frameworks [2], which described the various IT security concepts in some detail, but still far from defining the protocols and data structures needed for secure interoperability, had also started and was not finalized until 1996. The most important of the earlier work was the Authentication Framework in the joint ISO-CCITT work on Directory, best known as X.509, where the public key certificates was introduced and specified [3, 4]. Work on security in the international standardization bodies progressed very slowly, partly due to the fact that some nations did not encourage such work. Some IT vendors then decided to turn to their own standardization body ECMA. Here work on security standardization started in 1986 and their first document, a technical report on a security architecture for open systems was published in 1988 [5]. It was followed in 1989 by an ECMA standard [6] that clearly identified the various security services and security related data elements that are needed in order to secure a distributed system.

At the same time, some European vendors and the European Commission decided to speed up this important and promising work. The result was that the in the summer of 1989 the project SESAME (Secure European System for Applications in a Multi-vendor Environment) was born with Bull, ICL and Siemens
as equal partners. The two main purposes of the project was to speed up the security standardization process and to make a prototype in order to verify that the concepts promoted in the standards were both secure and implementable.

In the decade that has passed since the project started, the Information Society and the Global Information Infrastructure has evolved from OSI to internet technologies. This technology is used in internet, intranet and extranet environments and it has been shown that the SESAME concepts are not limited to the OSI model but can equally well be applied to the internet environment.

This paper attempts to describe some of the phases, strategies, results and explorations of the SESAME project and the SESAME technology. A description of the project and some experiences from the development process are found in the next section. It also explains the reasons and strategies behind some of the architectural features.

The SESAME concepts have been well received not only in standardization and vendor communities but also by users and scientists (see e.g. [8, 9]). The impact the project has had on standardization, research and products is summarized in section 5. The final section is devoted to TrustedWeb, which is one particular way of making use of SESAME in an intranet or extranet environment and that has achieved much attention.

2 The SESAME Project

Bull, ICL and Siemens made a proposal that was accepted by the European Commission and from July 1989 the project SESAME was founded and partly funded through the RACE (Research and Development in Advanced Communications Technologies for Europe) program. Standardization was a major part of the project and all interoperability aspects were immediately fed into various standardization committees, in particular ECMA. The emphasis of the first phase was the development of an architecture that could support a variety of security policies and security mechanisms. Authentication and access control in an open distributed network was the main focus of the project. To develop an architecture for the distribution of access rights in a distributed environment that allows for delegation in a controlled manner was a challenge. Secure communications (data integrity and data confidentiality) and thus key distribution not only within a security domain but also between different security domains were also seen as necessary ingredients in the architecture. A security service for non-repudiation was also included in the scope of the project. The project not only had to describe these concepts, but the components also had to be implemented in pre-competitive modules that would serve as proofs of the workability of the concepts. The project was completed in 1995.

First, the conditions and requirements for the architecture needed to be established. The project here benefited from the fact that the participants came from different cultural environments. The security policy and requirements for IT security in France are not identical to those in UK, and none of them as in Germany. It was a rather time consuming process to fully understand these and