Simulation for Security Provision, Attack Assessment and Profiling for Distributed Simulation

Richard N. Zobel
Department of Computer Science
University of Manchester
Oxford Road
Manchester M13 9PL, U.K.
rzobel@cs.man.ac.uk

KEYWORDS

Distributed Simulation, Security Provision, Encryption, Attacks, Forensics and Profiling.

ABSTRACT

Security provision for protection when employing simulators over the Internet, becomes daily more important for protection of data and operations. This paper identifies the two major activities of registration and message (data) passing. Encryption and decryption are discussed along the issues associated with authentication, digital signatures and certificates, and the need for a Certification Authority.

Much, but not all, of the interest for simulationists is associated with distributed simulation, mentioned here under the heading of Distributed Interactive Simulation (DIS), under which the secure federate architecture is discussed. For non-military applications simpler, lower cost solutions are sought.

However, the situation is complex and the use of secure transmission has only recently been considered necessary. Some situations of the provision of secure simulation services for civil applications have been done by the author's group. This is being extended to look at the operation of distributed simulation using security services whilst under attack. The use of agents for collecting forensic data after attacks to enable profiling of attackers has also been simulated. All of this has lead to the consideration for the design of a generic simulator to support these activities.

INTRODUCTION

Security for distributed systems, for transaction processing, for e-business, for e-commerce, for home computing, etc. has become a major activity, a major necessity, and a major concern. In many ways we have been naive in our realisation of the consequences of ignoring the necessity of providing adequate security for even the lowest levels of computing activity. After all, who would try to attack or destroy the files of those charitable organisations, which are concerned with provision of services for those who are needy and disadvantaged? It seems that there are no depths to which a few are prepared to descend for "fun". In the following sections of this paper, the author addresses a number of aspects of security, which can be applied to minimising attacks on computer systems and thus allows users to pursue their legitimate and laudable aims. Of necessity, the view has to be limited in a rapidly expanding field, to a restricted discussion of only some aspects, particularly of those within the experience of the author. However, it is the author's view that simulation can play substantial role in developing and establishing security provision in the current relatively unregulated Internet scenario. What follows is an exposition of the current visible state, subject to security service and confidentiality restrictions, of the art of the provision of secure use of the Internet and web-based applications.

It appears that there are two essential aspects of secure operation of networked computer systems. The first is provision of secure access to services and the second is secure operation of those services, especially in relation to message passing and transaction processing. Simulation has two roles to play here. The first is to verify security service

Proceedings 14th European Simulation Symposium
A. Verbraeck, W. Krug, eds. (c) SCS Europe BVBA, 2002

provision for distributed simulation systems, an area of growing importance both within and outside of the military industry. The second is to verify the operation and level of security provision for a wide variety of civil, industrial and commercial networked computer based systems and activities.

SECURE ACCESS TO SERVICES

The registration process illustrated in Figure 1 shows three tiers of operation. The upper tier provides a Graphical User Interface (GUI) for login and registration (and exit from registration) to a service activity. The login may be conventional or more complex. However, registration requires additional personal information. Further facilities include recovery from forgotten password, which again involves significant additional personal information, and the provision for system viewers who may observe but not interact or affect the system operation in any way, subject to registration permissions.

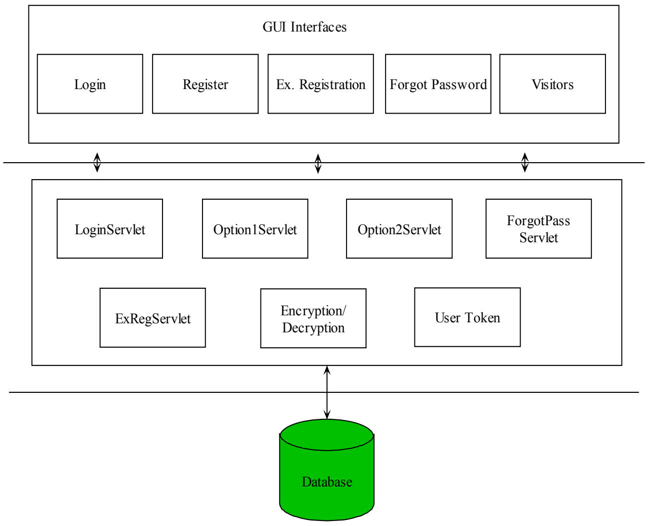

Fig. 1 The Registration Process

The second tier shows Java servlets for each of the GUI functions of the upper tier. In particular, we find here the encryption and decryption facilities and user tokens required for access to the security database. Higher level permissions are, of course, required for any changes to the database to be made, along with access to passwords and other sensitive information.

The lowest tier comprises the security database and its access mechanisms.

MESSAGE PASSING

The principle activity of the systems requiring security protection is that of message passing, with the message including data, when appropriate. The principle protection provided here is that of encryption and decryption, so that those who have illegal access to the message also have significant difficulty in decoding the message and accessing the data. However, authentication procedures are also necessary for some applications.

Encryption and Decryption

As the millennia have passed the algorithms for encryption and decryption have necessarily become more sophisticated. Each new generation of cypher had to provide an ever greater lower probability of discovery. During the Second World War, the first calculating machines were developed to attempt to discover the encryption algorithm. History shows that they were successful. These machines gave rise to the first computers. In succession, these computers became ever more powerful and more capable of code breaking.
Now we find that code breaking is relatively easy for all but the most complex algorithms. This has lead to a mathematical approach to finding ever more difficult algorithms for encryption and decryption. Currently, the trapdoor function approach is successful. These involves a mathematical function for which it is easy to encode with a public key, but very difficult to decode without a second private key, known only to the recipient.

Current systems are employed in mobile phones, but because of processor speed and memory limitations, provide only limited security. Other systems, particularly in the finance sector, make full use of public key encryption. The commonly used RSA system provides a better level of security, but the use of elliptic curve cryptography provides a better speed - security level product and is increasingly being considered.

Digital Signatures and Non-Repudiation

Digital signatures are the equivalent to hand written or machine printed signatures. However, they can be much more secure and can be much more useful. In particular, they can provide protection against non-repudiation and guarantees for the integrity and authenticity of data [trustedweb, 2001, tda, 2001].

A digital signature is derived from both the signer and the data, which is being signed, thus binding the signer to the data in a manner that it is unlikely to generate the same signature with a different signer. The process of signing is illustrated in figure 2 below.

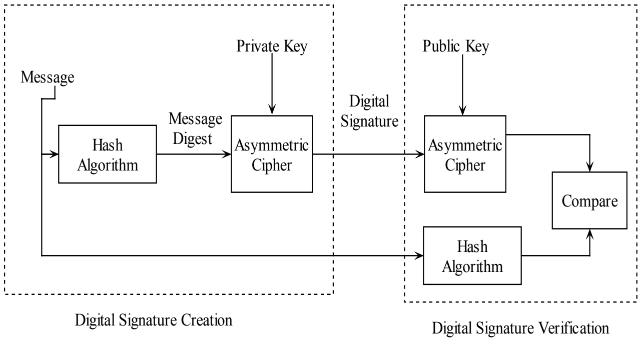

Fig. 2 Digital Signature Creation and Verification

The data is first processed by a hash algorithm to produce a message digest. This is encrypted using the private key of the signer and transmitted to the recipient along with the message. The recipient uses his public key to decypher the digital signature, which is then compared with the hashed message. If these are the same, then the recipient can be sure that the sender was genuine and the sender cannot repudiate the fact that he signed the message.

Authentication

The above process therefore helps to combat repudiation that is denial of involvement in the transaction. However, it does not guarantee that a public key does in fact belong to the individual or corporate entity claimed. This proof is generated through the use of digital certificates [trustedweb].

Digital Certificates

A digital certificate is a short document, which lists a name and other identifying information with a public key. A certification authority (CA) then signs the document with its own private key as described above. A certificate includes a version number, serial number, the CA name and person or entity the certificate identifies, validity period, public key, CA signature, and algorithm to be used [ece, 2001].

The are three types of digital certificate: an Identity Certificate (e.g. X.509) contains a public key combined with enough information to identify the key holder; an Accreditation Certificate identifies the key holder as member of a specified group, e.g. a Doctor; and an Authorization and Permission Certificate, used for delegation of authority.

Certification Authority

A Certification Authority is an organisation, which acts as the agent of trust in a Public Key Infrastructure (PKI) and is responsible for the software used to perform the CA's functions. These functions are: verification of users identities; issuing users with keys; certification of users public keys; publishing users certificates; and issuing of certificate revocation lists.

Clearly the users must have full trust of the PKI and the CA. If the system is seen to be reliable and secure it will be used with confidence. However, if the PKI or the CA or both are compromised, this trust will rapidly disappear.

DISTRIBUTED INTERACTIVE SIMULATION

Well documented, this activity commenced with the military training simulators, which were and are interconnected over networks for exercise training and management. Initially using the DIS (Distributed Interactive Simulation) methodology, the current technology employs the High Level Architecture (HLA) for synthetic environment management. The security is catered for by a specific module in the Run-Time Infrastructure (RTI). The software architecture is illustrated in figure 3.

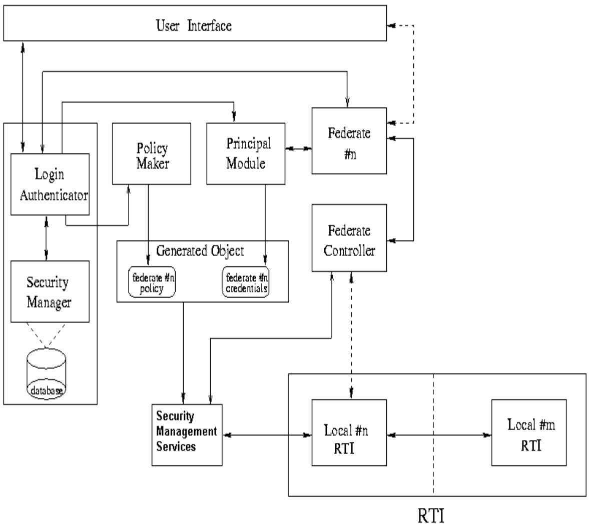

Fig. 3 Implementation of the Secure Federate Architecture

ASPECTS OF SECURITY FOR SIMULATION

More recently, this and other architectures have been proposed and developed for non-military applications. These require a cheaper and more robust architecture to overcome the problems of public network systems, necessarily employed for cost reasons.

Thus, implementations of registration and message passing systems with significant security features are necessary for applications where private, business and commercial secrecy and confidentiality must be maintained.

There are a number of authentication protocols proposed and in use, which can be employed in practical systems. These have been extensively studied and reasoned about. An excellent report on this important topic provides a good grounding [Burrows et al, 1990].

SIMULATION OF SECURITY ASPECTS

Provision of security systems for networked simulations is an important issue, and needs to address not only the provision and level of protection, but also the anticipated modes of attack and provide for protection against a wide variety of attack types.

This is a major task and yet, although such provision is necessary, it needs to be provided at a reasonable cost in terms of both money and processing time for real-time simulations.

Network Attacks

It is important to understand the nature of the types of attack currently employed on the Internet and World Wide Web. Attacks fall into three main categories. These are disclosure of data, such as credit card or banking details and private lists of email addresses, etc.; corruption or destruction of data, mainly caused by viral attack; and denial of service attacks, of which the distributed denial of service (DDoS) strain is most serious.

Tracing, Forensics and Profiling

Work at Manchester [Iwu et al, 2001c, 2002] describes a methodology using agents for the collection of data relating to attacks, with a view to undertaking trace-back and forensic analysis in order to profile the attacker(s) and subsequent conviction of offenders.

A simulator for the study of such an agent-based approach has been developed and is currently being evaluated, using private network and PVN techniques. Figure 4 illustrates the model for defensive simulation.

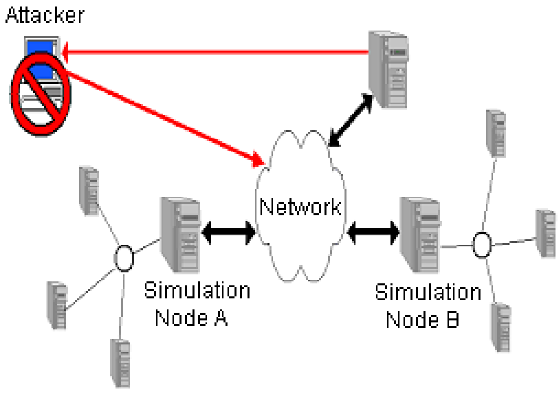

Fig. 4 A Defensive Simulation Model

A GENERIC SIMULATOR FOR SIMULATION SECURITY

This work has lead to a number of simulation exercises and studies. From this it emerges that there is a need for a generic simulator for studying a variety of aspects of security for use with distributed simulation in order to maximise the utility of such a tool for a variety of distributed simulation and communication system simulation applications.

One application which has looked at recently, is that of improving the security of mobile phones [Ahmed 2001]. A new application for linking remote dynamic system simulations to a local animator looks promising for distance learning and also for continuing professional development packages, and will need at least copyright protection.

CONCLUSIONS

Following a brief review of security issues and techniques, the author has considered the provision of security for distributed interactive simulation and synthetic environments for civil applications over the Internet. Such a provision has been implemented for the security module of the HLA RTI. It could also be modified for other related distributed simulation management systems.

The paper then goes on to consider where simulation might be used to assist with evaluating attacks and provision of protection against attack. Finally, the use of agents to gather forensic data about attacks, which have occurred for profiling the attacker, has been presented along with a simulator for study of the agent-based system.

Such diverse but related simulations have lead to the consideration of the design of a generic simulator to aid the development of security services for simulation.

REFERENCES AND BIBLIOGRAPHY

Ahmed F.Q., MSc thesis, Manchester University, U.K. Dec. 2001.

Burrows M., Abadi M and Needham R. A Logic of Authentication. SRC Research Report 39. UK

Cappellini V., Barni M., and Bartolini F. SIGNAL PROCESSING, Vol. 81, No. 6, June 2001. Elsevier, Amsterdam. ISSN 0165-1684. Special Section on Theoretic Aspects of Digital Watermarking.

ece. Digital Certificate http://www.ece.wpi.edu/infoeng/textbook/node216.html

Sarwar M. F. MSc thesis, Manchester University, U.K. Dec.. 2001.

tda. Digital Signatures and Certification Authorities http://www.tda.ecrc.ctc.com/kbase/doc/brief/digsig.htm

trustedweb. SSE Introduction to Security http://www.trustedweb.com/intro/CA.html

ABOUT THE AUTHOR

Richard N. Zobel became an Associate Member (AM) of IEE in 1965, a Member (M) of BCS in 1970 and a Chartered Engineer (C.Eng.) in 1990. Educated at Colfes Grammer School, London, U.K. 1950-57, he holds the degrees of B.Sc.(Eng.) 2.1 Hons. (Electrical Engineering), London University, London, U.K., 1962, and Ph.D. (Hybrid Computer Techniques), Manchester, 1970.

He has had experience in both industry and academia. 1962 - 1966 ENGINEER, SENIOR ENGINEER, Guided Weapons Systems, Sperry Gyroscope Co., 1966 - 1989 LECTURER IN COMPUTER SCIENCE, Manchester University. 1989 - SENIOR LECTURER IN COMPUTER SCIENCE, Manchester University, United Kingdom. He has over 100 scientific publications and has successfully supervised over 90 postgraduate students.

Dr. Zobel has been involved in digital signal processing, instrumentation and design environments, in simulation aspects of real-time embedded systems, the development of design and simulation environments for mixed application areas, and in distributed simulation in concurrent engineering. His recent research activities concern security aspects of distributed systems and in distance learning for CPD. He is now semi-retired but remains very active.

He is past UKSim Chairman, past EUROSIM Executive Board Member, and past Board Member of SCS in the USA and Europe.