AMOGHVARTA

ISSN : 2583-3189

A study of Security Risks of Network Distributed Systems

ORIGINAL ARTICLE

Author
Dipak Sharan
PhD, Research Scholar
Capital University,
Koderma, Jharkhand, INDIA

Abstract

Security in a distributed system poses unique challenges that need to be considered when designing and implementing systems. A compromised computer or network may not be the only location where data is at risk; other systems or segments may also become infected with malicious code. Because these types of threats can occur anywhere, even across distances in networks with few connections between them, new research has been produced to help determine how well distributed security architectures are actually performing. In the past, security was typically handled on an end-to-end basis. All the work involved in ensuring safety occurred "within" a single system and was controlled by one or two administrators. The rise of distributed systems has created a new ecosystem that brings with it unique challenges to security. Distributed systems are made up of multiple nodes working together to achieve a common goal, these nodes are usually called peers.

Key Words

Security benefits, Security framework, Architectural levels of security services, Security objectives.

Introduction

There are special factors of risk in distributed systems. Existing distributed systems offer significant opportunities for the introduction of insecure or malicious software. They also permit hacking and browsing. Even those distributed systems which are intended to support a low or medium risk area of business still have to be careful today not to leave themselves wholly unprotected. Vigilant management is required against attacks leading to denial of service. Even where these attacks do not compromise data integrity, they may be both inconvenient and expensive. The experience of people affected by the "Internet Worm" (Spafford, 1988) illustrates this. A deliberately created program propagated itself across several networks, especially in the India. Although it did not itself cause any damage, it reproduced itself continuously until it had absorbed all the resources of computers it had invaded and brought them to a halt. The cost of recovery was estimated at millions of Rupee. Other risks of this kind are described in (I.D.I.I 2020). Similar effects can be caused accidentally. In particular, the incorrect handling of error reports in electronic mail systems can cause "mail storms" which swamp the network. This can be caused if a message containing errors is broadcast to multiple sites If each receiver site reports the error back to the originator and separately triggers off a retry of the entire broadcast, the number of messages grows exponentially until the network halts. Another risk is that unprotected systems may be used as an entry point into other inadequately protected but sensitive systems. They used

unprotected systems as bases from which to probe systematically for security weaknesses in other more sensitive systems, with a surprisingly high degree of success. This resulted not only in the exposure of confidential information, but also in extra costs for several sites who only discovered that they had been penetrated when their bills for communication were unexpectedly high. There is a direct risk of exposure of confidential information in the uncontrolled, unprotected use of public networks between nodes of the system for information transfer. There are many opportunities for network staff to gain access to transmitted information but, in addition, any satellite or point-to point radio link may be intercepted with the appropriate equipment. If a secure network is required, encryption and access controls are essential. Distribution not only introduces additional risks to computer systems but also adds complications to dealing with the risks.

For example: communication may introduce significant time-lag into the system in respect of security-related information; this may make it difficult for the security management system to correlate information which, taken together, would indicate a security breach; splitting the system into different geographical, political, technical or administrative domains complicates the setting and management of a coherent security policy; it also adds to the difficulty of tracing security breaches which are initiated from a different domain.

Security Benefits of Distributed Systems

However, in addition to the down-side of introducing risks, there are compensating factors in distributed systems which can be used to enhance system security. Unauthorised access to corporate data can provide the intruder with valuable strategic information. The advantage of distribution in this case is that it allows sensitive data to be distributed throughout the system. Thus only by knowing the way in which it is distributed and accessing it at all locations can an intruder obtain complete information. The damage which can result when the processing capability of a system is disrupted can be very high, particularly when a high premium is placed on the ability to process information. Distribution can provide alternative locations from which to acquire processing resources. Accidental failures typically occur at one site at a time, and deliberate attempts to disrupt a service would require interference with a number of sites simultaneously. There may be a variety of security requirements within a distributed system. One advantage of distribution is that it does not constrain all components of a system to accept the same security regime. If the environment is partitioned into separate security domains, each domain can reflect a different aspect of the organisation's policy concerning security. Overall control is obtained either by negotiated security interaction policies between the managers of domains or by a hierarchical structuring of domains with one manager taking responsibility for coordinating the interactions of all.

Security Framework

The objectives of security within distributed systems can be defined at a number of different levels, from a high-level objective such as "to safeguard the organisation's assets" to a low level one such as "ensure that no dictionary words are used as passwords", with a hierarchy of objectives in between. Each level helps to achieve the objectives of a higher level. These objectives may be achieved by mechanisms at several different architectural levels within a distributed system. An example of this, mentioned below in section II.D.1, is the protection of data in transmission. This can be achieved by link protection, by end-to-end protection, or at an intermediate level. The combination of security objectives and the architectural levels at which they may be supported together form a framework in which to describe security. The International Standards Organisation (ISO) Open Systems Interconnection (OSI) Security Architecture (ISO, 7498-2) defines a set of security services based on generally agreed objectives and sets out the options for the architectural levels at which these may be provided.

Objectives

It is helpful to distinguish between the primary and secondary objectives of security. The primary objectives correspond to threats such as disclosure, corruption, loss, denial of service, impersonation, repudiation. The

secondary objectives lead to the specification of services to support the primary ones. There are three primary security objectives which apply to both stored data and messages in transit. They are:

Confidentiality: Maintaining confidentiality of information held within systems or communicated between them. This typically means the prevention of unauthorised access to stored data files and the prevention of eavesdropping on messages in transmission. However, in high-security applications there may also be a requirement for protection against revealing information which may be inferred solely from the fact that data is being transmitted and not from its contents. This information can be derived from traffic analysis, analysis of the source, destination and volume of communications. A classical case of traffic analysis is a military one in which preparation for troop movements could be revealed by the increased volume of communications between units.

Integrity: Maintaining the integrity of data held within systems or communicated between systems. This prevents loss or modification of the information due, for example, to unauthorised access, component failures or communication errors. In data communications, it may also be important to prevent the repetition of a message. For example, a message in an Electronic Funds Transfer system authorising the transfer of funds from one account to another must not be sent and acted on twice. Protection from this risk is known as prevention of replay. Integrity can be achieved in two different ways: either preventing the occurrence of failures at all, or detecting the occurrence and recovering from it. Prevention may be achieved by a number of means; by physical protection, by access control against unauthorised actions and by procedural measures to prevent mistakes. Detection and recovery require timely detection, combined with backup facilities which make it possible to start again from a situation of known integrity.

Availability: maintaining the availability of information held within systems or communicated between systems, ensuring that the services which provide access to data are available and that data is not lost. Threats to availability may exist at a number of levels. A data file is unavailable to its user if the computer which provides the service is physically destroyed by fire, or if the file has been irretrievably deleted, or if the communication between user and computer has failed. As with integrity, two different modes of protection are available: prevention; and detection and recovery using backup facilities. Two other primary security objectives apply specifically to communication between users and/or programs:

Authentication: authenticating the identity of communicating partners and authenticating the origin and integrity of data which is communicated between them. It is important for several purposes. Authenticating the identity of the originator of a message gives confidence, in electronic mail systems, that messages are genuine. It also provides a basis for audit and accounting. It is a requirement for access control systems based on the identity of users of the system. Authentication of message contents enables the detection of integrity failures in messages.

Non-repudiation: this is the prevention of a user wrongly denying having sent or having received a message. The first of these is known as proof of origin and the second as proof of delivery. Non-repudiation is important in any situation in which the interests of the sending and receiving parties may be in conflict. For example, in a stock transfer system it would be in the financial interest of the sender to repudiate a selling order if the value of the stock subsequently rises, and in the interest of the receiver to repudiate it if it falls. It is a key issue for contractual systems based on EDI (Electronic Data Interchange), for example, purchase and supply systems.

The secondary security objectives identified by the Security Architecture are as follows:

Access Control: Providing access control to services or their components to ensure that users can only access services, and perform data accesses, for which they are authorised. Access control is one means which is used to achieve Confidentiality, Integrity and Availability. It can be provided by physical and/or logical mechanisms. Unauthorised access to a personal computer may be prevented by a key lock disabling

5 the keyboard. Access to a shared system may be controlled by a logical access control system using access rules based on the authenticated identity of users.

Audit Trail: Providing an audit trail of activities in the system to enable user accountability. An audit trail provides evidence of who did what, and when. The important special case of audit of access control systems is discussed in section V.B.

Security Alarm: The detection of occurrences indicating an actual or potential security failure should raise an alarm and cause the system to operate in a fail-safe mode. Some security failures are not detected at the time, and cannot be reported on, like the failure of the access control system to detect an unauthorised access because of its own weakness. Other activities may be indicative of possible security failures, and need investigation; for example, a changed pattern of access by a user. The objective in this situation is to minimise, simultaneously, the risk of loss if there really is a security failure and the inconvenience to the user if there is a false alarm. The security objectives outlined above are interdependent, and should not be taken in isolation. Authentication is the basis for achieving many of the other objectives. Authenticated user identities are needed for identity-based Access Control, Non-Repudiation and Audit Trail, but password-based Authentication requires both Access Control to protect the password file and encryption-based Confidentiality for further protection if the Access Control fails. Access Control, besides requiring and supporting Authentication, is a basis for Confidentiality, Integrity and Availability. Audit Trails and Security Alarms both depend upon and support the other objectives.

Architectural Levels of Security Services

The ISO Security Architecture identifies the possible communication protocol layers of the Open Systems Interconnection Basic Reference Model at which each security service could be provided. A security service, such as confidentiality, can be applied to communication at different layers in the model but it is not sensible to apply the service at all of the layers. For instance, a user who is obtaining end-to-end confidentiality through encryption (see III.E) at the Presentation Layer, has no need of Data-link encryption as well (see figure 2). Further standards work will identify appropriate profiles of security services for particular applications.

Security Mechanisms

A number of different mechanisms are used to achieve security objectives. They include:

- Physical and electronic security of components of the system;
- Authentication mechanisms;
- Access control mechanisms;
- Communication security mechanisms.

They are described briefly here. Interested reader are referred to further reading for more detail.

Physical Security Mechanisms

Physical security mechanisms are used for protection of equipment and for access control outside the scope of logical access control or encryption. They are necessary for protection against risks such as fire, tempest, terrorist attacks and accidental or malicious damage by users and technicians. Physical security requires a variety of mechanisms: Preventive Security - strong construction, locks on doors, fire resistance and waterproofing; Detection and Deterrence - movement detectors and door switches linked to alarms, security lighting and closed circuit television; Recovery - the provision of a backup site, with alternative computing and communication arrangements. A basic level of physical security is always necessary even in the presence of logical access control and encryption. In some situations physical protection may be simpler and more secure than a logical solution; for example, by controlling physical access to terminals and personal computers and their data and by storing sensitive data on demountable media. Illustrates a situation in which

encryption needs to be supplemented by physical line protection if complete end-to-end protection is to be achieved. It is necessary because the encryption unit is not an integral part of a secure terminal.

Electronic Security Mechanisms

Electronic security mechanisms may be needed for protection against interference from static electricity and RF (Radio Frequency) interference, both of which can cause computer and communication equipment to malfunction. They are also required for Radiation Security to avoid the passive eavesdropping of electromagnetic radiation from visual display units, printers and processors. The modulated signals can be detected by nearby radio receivers and analysed to reveal the data being displayed, printed or processed. Preventive devices are commercially available, and there are also military standards of protection (so-called "Tempest" proofing).

Conclusion

A distributed system is composed of many independent units, each designed to run its own tasks without communicating with the rest of them except through messaging service. This means that a single point of failure can render a system completely incapable without any warning since there is no single point that can perform all necessary operations.

Attacks related to distributed systems are an area of active research. There were two main schools of thought, those who believed that network worms could be stopped by employing firewalls and those who did not.

A firewall might do nothing about worms and their ability to spread across various types of networks, especially wireless networks and the Internet. This was because although firewalls were able to stop intruders from gaining access through the firewall, they were unable to stop a worm from self-replicating.

References

1. Estivill Castro V. and Murray A.T. (1998), 'Spatial clustering for data mining with genetic algorithms,' in Proceedings of the International ICSC Symposium on Engineering of Intelligent Systems, pp. 317-323.
2. Fogel D.B. and Stayton L.C. (1994), 'On the effectiveness of crossover in simulated evolutionary optimization', Bio Systems, Vol.32, No.3, pp. 171-82.
3. Foody G.M. and Mathur A.. (2004), 'A relative evaluation of multiclass image classification by support vector machine'. IEEE Transactions on Geoscience Remote Sensing, Vol. 42, pp. 1335-1343.
4. Goldberg D. (1989), 'Genetic Algorithms in Search, Optimization and Machine Learning'. Reading, MA: Addison-Wesley.
5. Grabmeier and Rudolph A. (2002), 'Techniques of cluster algorithms in data mining', Data Mining and Knowledge Discovery, Vol. 6, pp. 303-360.
6. Guoqiang Peter Zhang (2000), 'Neural Networks for Classification: A Survey', IEEE Transactions on Systems, Man and Cybernetics—PartC: Applications and Reviews, Vol. 30, No. 4, pp 451-462.
7. Hall L.O., Ozyurt I.B. and Bezdek J.C. (1999), 'Clustering with a genetically optimized approach,' IEEE Transactions on Evolutionary Computation, Vol. 3, No.2, pp. 103-112.
8. Hertz J., Krogh A. and. Palmer R.G. (1991), 'Introduction to the Theory of Neural Computation', Addison-Wesley, New York, USA.
9. Huang C., Davis L.S. and Townshend J.R. G. (2002), 'An assessment of support vector machines for land cover classification'. *International Journal of Remote Sensing*, Vol.23, pp. 725-749.
10. Jain A.K. and Dubes R.C. (1989), 'Algorithms for Clustering Data', Englewood Cliffs, NJ: Prentice-Hall.

——==00==——