Free essay on network security

Law, Security

Abstract

Security in computing systems is an important requirement of present day technology as connectivity and data-sharing is increasing day by day. One of the best solutions to increase security is to work on operating system security mechanisms. Operating system security can be achieved through the use of mandatory security policy and trusted path allowing the safe access to users' data with the help of proper authentication and cryptographic techniques. Mandatory security policy and the use of trusted path could also help in reducing or eliminating the activity of malicious software or users. Some of the widely accepted security solutions such as mobile code security efforts, firewalls, the Kerberos network authentication system, and network security protocols, are clearly showing that secure operating systems are important in providing security in connected environments. In this paper, different aspects of network security and their protection mechanisms have been addressed.

In the article, " The inevitability of failure: The flawed assumption of security in modern computing environments" by Loscocco et al., (1998), it has been noted that security in computing systems is an important requirement of present day technology as there is a significant rise in connectivity as well as data sharing. This connectivity is present almost everywhere. Especially, with the rise of World Wide Web, almost every business requires some level of advanced security.

In order to provide security, it is important to work on operating system security mechanisms. It has been reported that distinction between data and code is vanishing resulting in the introduction of malicious code in an

application that can be installed in a system without knowledge of the user. So, a secure operating system can help in providing security against such threats.

In providing an operating system security, mandatory security policy has to be utilized. This policy can be divided into different kinds such as an access control policy specifying the access of objects under the control of operating system; an authentication usage policy specifying the authentication mechanisms, and a cryptographic usage policy specifying the cryptographic mechanisms to protect the data. Although mandatory security policy is unable to completely remove the problem of high bandwidth covert channels, it is still helpful in improving security by enhancing the required sophistication of the system. It can protect the user against unintentional execution of untrustworthy software.

Another strategy that can be used in providing security is the use of " Trusted path" that can only be used by the trusted software and cannot be imitated by other programs. This trusted path can help the user in getting protection from malicious software, which can obtain important information of the user and perform functions on behalf of the user. Moreover, trusted path mechanism can also help in addition of other trusted applications. It is important for operating systems to provide their own protected path mechanisms as it would not only be easy to use but it would also be more efficient.

The access control mechanism can be affected by malicious software, if proper policy is not followed. This malicious software could affect the security or policy's rules, thereby making it possible to access the user's

data without any consent. So, it is important to use trusted path mechanism in the operating system for complete control of the user over access of any program. Moreover, mandatory security mechanisms in the operating system can help in ensuring proper access to protected objects.

Mandatory security policy and trusted path features are also helpful in controlling the affect of malicious applications on cryptographic algorithms. With the help of mandatory security mechanisms, it could be ensured that the application invoking the cryptographic token is undisturbed in the presence of malicious software or users. On the other hand, protected path mechanism can help in ensuring that malicious software would not be able to change the cryptographic token or algorithm. Another problem with cryptographic token is its misuse by an unauthorized application. This unauthorized application can operate on behalf of other users or it may also result in misuse on behalf of the authorized user. Mandatory security and protect path features can also help in protecting from the misuse of cryptographic token.

Secure operating systems are essential to increase the security of computing systems. This is clear from the fact that some widely accepted security solutions such as mobile code security efforts, firewalls, the Kerberos network authentication system, and network security protocols depend on the characteristics of secure operating system.

In case of mobile code security efforts, researchers are working on the addition of more security measures to decrease the problem of hostile mobile code gaining unauthorized access to the user’s data. This problem is not only limited to the applets downloaded from the internet but also include

the applications actively installed by the user. In this case, Java applications are most important to consider. So, continuous work is underway to enhance security features to Java with the help of expanded access control model, or more control over access of some class libraries. An important approach to “ securing” mobile code is the use of digital signature in applets that can limit the use to trusted sources. Although native ActiveX is completely based on digital signatures, it has one problem of all-or-none proposition, i. e. native ActiveX control is not constrained to a limited security domain. In this case, mandatory security mechanisms can help in restricting the browser to a limited security domain.

Kerberos is a network authentication service that has been used for the provision of security for the World Wide Web. It is used along with other systems that rely on Kerberos. It is a physically secure service but it can be used only by the Kerberos authentication servers. This service has been designed for an environment, where the client workstations and the network are considered as untrustworthy.

IPSEC and SSL are network security protocols that are used to provide authentication, confidentiality, and integrity services. The IPSEC works on the secure retrieval of information, and SSL works on the level of transport protocol and the application protocol. However, mandatory security mechanisms are essential in both IPSEC and SSL implementation as both of these require not only secure channels but also secure end points.

A network firewall is required to develop a trust boundary between two different networks. Modern firewall architectures are based on the use of bastion hosts, which are used to provide minimal and required services.

However, flaws in proxy servers could result in penetration. So, mandatory security mechanisms are required to protect proxy servers. Moreover, mandatory security mechanisms can help in providing protection against malicious insiders that could affect the work of firewalls.

Issues motivated by the article have been addressed in a sufficient detail. After addressing the different important points, it has been noted in the article that total system security can only be achieved by the use of a proper balance of security systems. In a well balanced security system, different security mechanisms work with each other, thereby reducing the vulnerability of the system. For example, in a covert channel, auditing and detection mechanisms can work together to decrease the chances of exploitation. Authors have concluded that in order to achieve, a well balanced secure system, it is important to work on secure operating systems.

In one of the references, it has been noted that mobile code technologies such as Java and ActiveX usually require a single type of security policy. This security policy can help in improving portability and performance of the system. Authors of this paper are of opinion that combining elements of security checks can give the best solution to security of systems (Wallach, Balfanz, Dean, & Felten, 1997).

In another paper about Kerberos, researchers have noted that although Kerberos has been adopted by many organizations, it has its own limitations and weaknesses. These limitations and weaknesses are probably due to the specifics of the MIT environment. Researchers have also provided some recommendations for changes in Kerberos system. These changes included

chances in basic login protocol, enhanced authentication through Kerberos server, strong checksums, and relation to protocol extension to basic authentication (Bellovin, & Merritt, 1990). Moreover, it is important for the system to work in different environments that could be different from MIT environment.

In another article, experts have reported that assurance has to be increased to enhance the degree of trust on a system. It has been reported that the addition of security enforcement mechanisms and Trusted Computing Base (TCB) could protect the systems in higher-risk environments (Latham, 1986).

References

Bellovin, S. M., & Merritt, M. (1990). Limitations of the Kerberos authentication system. ACM SIGCOMM Computer Communication Review, 20(5), 119-132.

Latham, D. C. (1986). Department of Defense trusted computer system evaluation criteria. Department of Defense.

Loscocco, P. A., Smalley, S. D., Muckelbauer, P. A., Taylor, R. C., Turner, S. J., & Farrell, J. F. (1998). The inevitability of failure: The flawed assumption of security in modern computing environments. Paper presented at the Proceedings of the 21st National Information Systems Security Conference.

Wallach, D. S., Balfanz, D., Dean, D., & Felten, E. W. (1997). Extensible security architectures for Java (Vol. 31): ACM.