Asian Journal of Information Technology 7 (2): 64-68, 2008
ISSN: 1682-3915

Threat Analysis for P-LeaSel, a Multicast Group Communication Model

[1]S. Mary Vennila and [2]V. Sankaranarayanan
[1]Department of Computer Science, College of Presidency, India
[2]Anna University, Chennai, India

Abstract: Security threats in multicast group communication are inevitable, which makes threat modeling for any protocol, a must-do job. Threat modeling involves assessing the threats and vulnerabilities of a system and providing necessary mitigation measures. This study studies the response of the P-LeaSel 'p' LEAder SELection Multicast group communication model in accordance with the STRIDE threat standard. The study also compares the efficiency of P-LeaSel in response to threats with and without mitigation for multicast group communication.

Key words: Threat analysis, multicast group, communication, P-Lea Sel

INTRODUCTION

Multicast is an internetwork service for group communication, using the multicast address. Though, it thus reduces sender transmission overhead, the problem of scalability arises when multicast data need to be securely transmitted (Hardjono *et al*., 2000). The data can be secured by encrypting it with the group key, shared among all the group members. But, whenever the group members join or leave during the course of a multicast session, group re-keying must be done, to preserve the forward and backward confidentiality (Stallings, 1995). When there are frequent member changes, this also gives rise to scalability problem. LeaSel is a scalable, secured de-centralized group model (Elijah and Rhymend, 2002, 2003a, b; Elijah, 2004). The top ranking member of the group will be designated as leader and will be authorized to perform key generation and distribution. The Deputy Controller (DC) alone knows the leader and it is hidden from all other members of the subgroup, including the leader himself. The P-LeaSel (Mary *et al*., 2006) model, instead of a single leader, selects 'p' leaders with top remarks. This ensures a greater security and increased availability.

MULTICAST SECURITY THREATS

Since, multicast group addresses are public, any host interested in receiving multicast data can do so by just becoming the member of the group. Since the scope of the multicast session is large, the threats can be magnified. Typical network data travel through many network channels, before reaching all the corresponding group members. This increases eavesdropping opportunities to possible adversaries. These kinds of security attacks where adversaries try to gain access to the data without really disrupting the secure multicast protocol are called Passive Attacks.

Uncontrolled group access allows any host in the global network to send multicast data to a multicast group, which may cause congestion (Pe-Wah, 2003; Daniel, 2006; Ballardie and Crowcroft, 1995). This presents an opportunity to mount a denial of service attack against the group. Any host in the Internet may pose as another host that is a member of the group. It can send data, receive data, or acquire access to the secret keys, posing a legitimate member of the group. Such an attack is called masquerading. Further, an adversary can intercept data by eavesdropping or other means and replay it at a later time. This is called replay attack. Masquerading and Replay Attacks call for the receivers to be able to determine the source of multicast data. All these attacks are termed as Active attacks as they disrupt the multicast protocol.

STRIDE THREAT MODEL

In computer security, a threat model is a description of set of security aspects, that is, when looking at a piece of software (or any computer system) one can define a threat model defining a set of possible attacks to consider (Threat Modeling, 2004; Threat Analysis and Modeling, 2006; The STRIDE Threat model, 2005). It is often useful to define many separate threat models for one computer system, this way one has groups of more narrow set of possible attacks to focus on. Having a threat model, the

Corresponding Author: S. Mary Vennila, Department of Computer Science, College of Presidency, India

security personnel can assess the probability, the potential harm, the priority etc. of attacks and from this point on try to minimize or eradicate the threats. More recently, threat modeling has become an integral part of Microsoft's SDL (Security Development Lifecycle) process.

When you are considering threats, it is useful to ask questions such as these: How can an attacker change the authentication data? What is the impact if an attacker can read the user profile data? The threats can be categorized and modeled with the help of these pointed questions. One such threat model is STRIDE, derived from an acronym for the following 6 threat categories.

Spoofing is a process in which a member assumes the identity of an authenticated member and claims his rights. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database and the alteration of data as it flows between two computers over an open network, such as the Internet.

Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise-for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations.

Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it-for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

Denials of Service (DoS) attacks deny service to valid users-for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

Elevation of privilege. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself.

P-LEASEL MULTICAST MODEL

The architecture, as per 'P-LeaSel' is presented in Fig. 1.

This is an adopted version of LeaSel (Leader Selection) architecture, already proposed and proved for both wired and wireless environment (Elijah and Rhymend, 2002, 2003; Elijah, 2003, 2004).

The Leader selection is where P-LeaSel differs from LeaSel. Instead of a single leader, the DC selects a set of 'p' leaders. At a given time, only one of them acts as the leader and the leader is alternated for every transaction. Thus, the 'p'-Leaders share the Key Management workload among them. Moreover, attacking this sub group becomes more difficult, as it involves attacking all the 'p' leaders, instead of one. Thus, the group key generation and distribution is not performed by any dedicated controller but instead by the 'p' leaders of the group and it is completely hidden from the group members (Marry *et al*., 2006). Thus the model achieves high scalability with secure key generation and distribution.

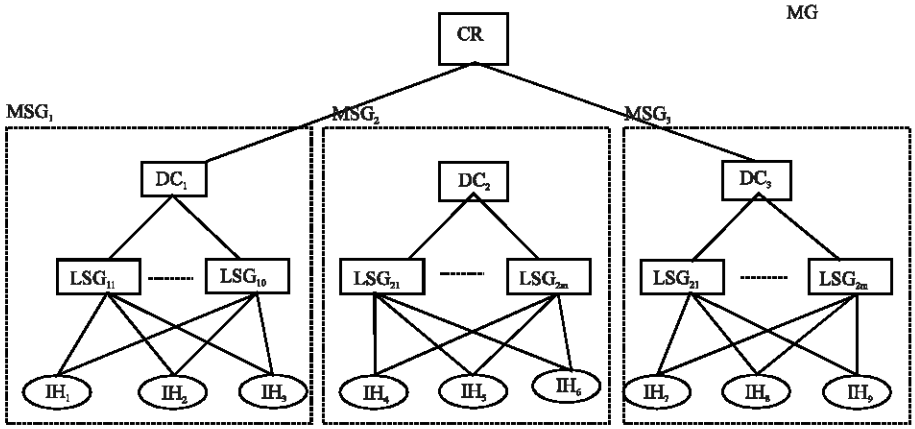

Fig. 1: P-LeaSel multicast model

Table 1: STRIDE threat table for P-LeaSel

Threat	A non leader announces himself as a leader	A non-sender modifies the message	A sender denies its connection with the message	Encrypted information is disclosed and exposed or the identity of the leader exposed	A service request not getting satisfied	A member claiming more rights than what he deserves
Threat type	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Target	Sub-group	Sub-group	DC	Sub-group	DC and controller	Sub-group
Mitigation measure	A certificate is generated and signed by the DC and sent along with the message to the Leader. A non-leader cannot resign, although can generate duplicate certificate and so cannot spoof	The signature is a hashed function of the message. So, modifying the message results in hash mismatch.	Every sender signs the message before it is sent, i.e., the message is encrypted using the private key of the sender. Thus the problem is eliminated.	The private keys of the members and the subgroup key take care of the problem of information disclosure.	The use of signed certificates by the DC avoids this threat.	Not a threat specific to P-LeaSel (using modified re-key procedure)

THREAT ANALYSIS OF P-LEASEL

STRIDE includes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege threats. STRIDE threat model has been applied to P-LeaSel and the reactive mitigation measures have been summarized in Table 1. The threat table categorizes the threats, based STRIDE Threat type and their targets and mentions the mitigation measures.

The Denial of Service is a common threat existing in all kinds of network applications. The mitigation measure for this threat does not require any modifications in P-LeaSel and any existing counter-measure for the threat can be incorporated to strengthen the system. The STRIDE threat model's introduction into P-LeaSel, imposes some modifications on the Re-keying and Member Join mechanisms of the P-LeaSel. The proposed modifications are highlighted below.

MITIGATION MODELING

The mitigation measures for the threats mentioned in the Threat Table needs some modifications to be done in the P-LeaSel model.

Modified P-LeaSel re-keying: Re-keying is the process which is carried out whenever a member leaves or joins a group. This process is done to preserve forward and backward confidentiality, preventing past and future members from misusing the subgroup key to receive or send multicast group messages. The Re-Keying process of P-LeaSel gets a modification in order to prevent Elevation of Privilege threat. The modified dialogue is shown below.

Re-keying dialogue

DC -> L : (K_GQ || (CERT)E_{PrD})E_{UL}
L -> M_{SG} : (SK' || (CERT)E_{PrD})E_{SK}

The Deputy Controller (DC) sends the Re-keying request concatenated with the signed Certificate (CERT)E_{PrD}, to the Leader (L) of the subgroup. The certificate is provided by the DC as the proof of authenticity of the Leader. This combo message is encrypted with the Leader's public key (E_{UL}), so that only the Leader can decrypt it back and understands the request. Thus Information Disclosure threat has been mitigated by the usage of keys. Once reading the "K_GQ", the Key Generate Request, the Leader generates a new subgroup key SK'. Then the new key SK' is concatenated with the signed certificate sent by the DC to the leader. This combo message is encrypted using the old subgroup key SK and sent to all the other subgroup members denoted by M_{SG}.

The signed certificate is sent along with the new key to ensure for the members that DC only initiated the re-keying process. This also prevents any non-leader re-keying the subgroup, by generating a new subgroup key without the knowledge of the DC and sending it to the members, since signature is an encryption with the Private key of the DC.

Thus Elevation of Privilege is completely eradicated using the modified Re-Keying process of P-LeaSel.

Modified P-LeaSel member join: Whenever a new member joins, Re-keying needs to be done, as already pointed out. But the Member join operation faces the Repudiation Threat. A member may send a join request to a multicast group and deny his connection with the request. This results in unnecessary Re-keying and multicast traffic. To prevent this, P-LeaSel Member Join dialogue is modified as follows:

Member Join Dialogue

M -> DC : ((JREQ)E_{PrM})E_{UD}
DC-> L : (K_GQ || (CERT)E_{PrD})E_{UL}

$L \rightarrow M_{SG}$: (SK' || (CERT)E_{PrD}) E_{SK}
$L \rightarrow M$: (SK')E_{UM}

The joining member sends the Join Request to the Deputy Controller signed with his private key (JREQ)E_{PrM}. The signed request is sent, encrypted with the public key of the DC, EUD. The signature on the request serves to identify the sender. This eliminates Repudiation Threat, since the member cannot deny his connection with the request, because he has signed it. Then the Re-keying process as seen in previous section is carried out. The leader then sends the new subgroup key to the joining member using the Member's (M) public key.

IMPLEMENTATION USING NS-2

The STRIDE model was incorporated into P-LeaSel with the above mentioned modifications and was implemented using ns 2.26.The behavioral changes of the P-LeaSel model, with the mitigation measures applied, was analyzed in terms of security. The implementation was carried out for the essential three threat categories on the P-LeaSel model and the security improvements are plotted. Simulation results were traced for up to 2000 nodes for all the threats with and without the mitigation measures applied and the sample graphs are given in Fig. 2-4.

Leader spoofing is an important threat in P-LeaSel, because a leader is one who is involved in the key generation and distribution process.

If a leader is spoofed, the key generation and distribution process gets some malicious treatment. The mitigation measure, as already pointed out is the use of certificates, signed by the Deputy Controller. Figure 3 shows the number of successful spoof attempts with the effect of number of nodes, with and without the mitigation measure applied. The effect of mitigation is around 2%.

Information Disclosure, in our context is the exposure of the identity of the leader of a group. Regarding Information Disclosure, it is evident from the graph that nearly 5% of the leaders' identities are exposed when the number of nodes is 250. When the number of nodes scales to 2000 nodes, this reduces to about less than 1%, with the mitigation measure applied.

Regarding the Denial of Service, P-LeaSel with mitigation stands above. The ratio of successful hack attempts, which is around 0.08 for 250 nodes declines to nearly 0.04 as number of nodes reaches 2000.

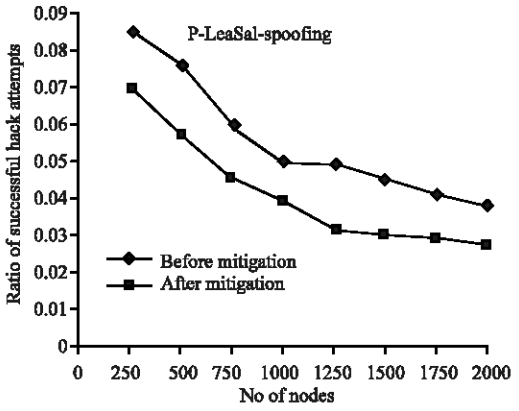

Fig. 2: Spoofing threat

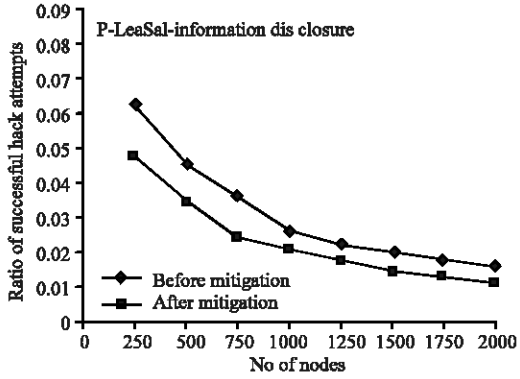

Fig. 3: Information disclosure threat

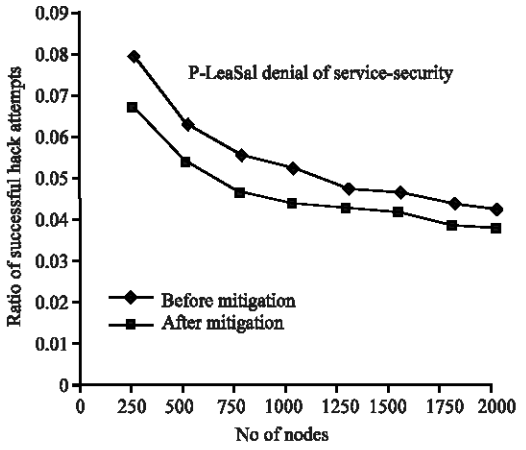

Fig. 4: Denial of service-threat

CONCLUSION

The P-LeaSel model, with all the necessary mitigation measures applied, becomes more effective in a highly scalable network. In general, external and internal threats

exist in any model and it is the internal threats which will be more difficult to secure against. But in P-LeaSel, even internal threats like Leader Spoofing, Information Disclosure etc, have been mitigated successfully. It can be very well seen that the effectiveness of P-LeaSel is sustained even in the presence of threats, both internal and external.

REFERENCES

Ballardie, T. and J. Crowcroft, 1995. Multicast-specific Security Threats and Counter-measures. In: Proc. Symposium on Network and Distributed system security. San Diego, California, pp: 2-16.

Daniel G., 2006. Assessing Software Security Using Threat Models, Bachelor Thesis, Dependable, Embedded Systems and Software Group, Department of Computer Science, Darmstadt University of Technology.

Elijah, B.R. and V. Rhymend Uthariaraj, 2002. LEASEL: An Efficient Key Management Model for Scalable Secure Multicast Sytem. In: Proceedings of ICORD, India.

Elijah, B.R., 2004. Design and Analysis of Secure Multicast Models for Wired and Mobile Networks, Phd Thesis submitted at Anna University, Tamil Nadu, India.

Elijah, B.R. and V. Rhymend Uthariaraj, 2003. Evaluation and Analysis of Computational Complexity for Secure Multicast Models, Springer Verlag, Lecture Notes in Computer Sci., 2668: 684- 694.

Elijah, R.B. and V. Rhymend Uthariaraj, 2003. FAULT Tolerant Analysis of Secure Multicast Models. In Proceedings of IEEE Int. Conf. ICICS-PCM, Singapore.

Hardjono, T., B. Cain and N. Doraswamy, 2000. A Framework for Group Key Management for Multicast Security, Ietf Internet Draft.

Mary, V.S., S. Srinivasan and T.C. Rangarajan *et al*., 2006. PLEASE- 'p' LEAder SElection for multicast Group Communication, IJCSNS Int. J. Comput. Sci. Network Security, 6: 11.

Pc-Wah Yau, 2003. A Threat Model for Mobile Ad'Hoc Networks, Mobile VCE Research Group, University of London, Egham, Surrey, TWZO OEX, UK.

Stallings, W., 1995. Network and Internetwork Security, Prentice Hall Inc, (active and passive attacks).

The STRIDE Threat Model, 2005. © Microsoft Corporation.

Threat Modeling, 2004. Frank Swiderski and Window Snyder, Microsoft Press, ISBM 0-7356-1991-3.

Threat Analysis and Modeling, 2006. v2.0, © Microsoft Corporation.