Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Different Security Issues and Attacks in Distributed System A-Review

[1] Manoj Kumar , [2] Nikhil Agrawal
[1,2] MTECH (Computer Technology and Application) ,Second Semester Students
National Institute Of Technical Teacher's Training and Research, Bhopal, India

Abstract —Now a days so many people are connected to the internet to access the different resources of their use and different companies are using distributed environment to provide their services to the customers. All these activities affect the economy of the country or world. So there is a need of more secure distributed environment in which all transaction and operations can be complete successfully in a secure way. In distributed System environment it is very important to provide service at any time ,any where to the customers, this require proper time management of all computing and networking resources, resource allocation on time and their proper utilization. In distributed environment security is primary concern. In this paper an analysis of different security issues related to data, physical security, network security , possible distributed system attacks, has been made.

Keywords: Distributed System, Information security , network security, physical security, firewall , Kerberos

I. Introduction

In the present scenario distributed system is widely used across the world by different companies to connect their various branches located at different geographical location. Distributed system coordinate the use of physically distributed computer. As stated by Andrew S. Tanenbaum ," Distributed system need radically different software than centralized system do". Security is vital for distributed and collaborative applications such as video-conferencing, clustering and replication applications, which operate in dynamic network environment and communicate over secure network i.e. Internet [1]. Some important concern that user faces when he/she use the distributed system is " security authentication, integrity ,confidentiality and authorization" . User should interact with resources in a transparent, open, scalable way. Openness in distributed system means each subsystem is continually open to interact with other system like client or server. Scalability in distributed system means system can be easily altered to accommodate change in the number of user, resources and other computing entities affected by it. Scalability may be either load scalability, geographic scalability and administrative scalability. Researchers now concentrate on distributed network security. As the use of distributed system is increasing day by day with the same rate threats of network attacks are also increasing. So better security techniques are required to implement in distributed system environment.

II. Classification Of Security Issues In Distributed System

The paper focused on the three issues for which security in distributed system should be maintain.

(1) Security of Information.
(2) Physical security in distributed system.
(3) Security of network and authentication policy.

III. Methodology Used For Security Issues

In this section there is discussion of security methodology and their management for information, physical and network security and authentication

A. Security of Information

Information which is maintained in the database is very important for the company . It is essential for any organization to store the data for future purpose and retrieve it or manipulate it for later use..There are three main constraints which should be properly maintain on the information

1) Integrity - Integrity of information means that information should be complete and accurate it should not be modified without permission of it's legitimate user.

2) Confidentiality - Confidentiality of information means information should not be access or used by unauthorized user. It should be secure.

3) Availability- Availability of information means that whatever information is needed by the legitimate user/system at any time should be available to that user/system.

When the private network of any company is connected to Internet or distributed system then chances of attack on the internal network, information and many application which use this information may run on different machine either may be desktop or mobile devices are increased. Intrusion detection system should be installed on these machine or devices

for security. Design of storage device also affect distributed system services The storage device design should have the features that data should be available to client in different geographical location quickly and personal and private detail should be controlled. [2]Now a days to maintain the security of data two main techniques are used in distributed system these are replication and secret sharing. The architecture based on the design data store is implemented by a set of number of server, Client make read and write operations with subset of servers. This can be assume as a public key infrastructure each client and server has a private key for which the public key is known. All the channel are secure against eavesdropping and replay attack. At each receiver ,requests are authorized using access control list, which are updated securely time to time by a system administrator , using separate service.

B. Physical Security in Distributed System

All the elements of a distributed system should be physically protected. Some [3]Internal control procedures are necessary for all hardware and software deployed in distributed, and less secure, environments. The level of security surrounding any hardware and software should depend on the sensitivity of the data that can be accessed, the significance of applications processed, the cost of the equipment, and the availability of backup equipment. Because of their portability and location in distributed environments, personal computers (PCs) often are prime targets for theft and misuse. The location of PCs and the sensitivity of the data and systems they access determine the extent of physical security required. In these cases, some companies, institutions should consider securing PCs to workstations, locking *or* removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts. Employees also should have only the access to PCs and data they need to perform their job. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls. Physical security of networks as well as PCs also includes power protection, physical locks, and secure work areas enforced by security guards. Physical access to the network components (files, applications, communications, etc.) should be limited to those who require access to perform their jobs. Network workstations or PCs should be password protected and monitored for workstation activity. All of these activities affect the services provided by the distributed system. In a distributed network frequencies emission also an important factor by which physical security can be controlled ,these frequencies emissions are either intentional and unintentional. Intentional emissions are those broadcast, for instance, by a wireless network. Unintentional emissions are the normally occurring radiation from monitors, keyboards, disk drives, and other devices. Shielding is a primary control over emissions. The goal of shielding is to confine a signal to a defined area. An example of shielding is the use of foil-backed wallboard and window treatments. Once a signal is confined to a defined area, additional controls can be implemented in that area to further minimize the risk that the signal will be intercepted or changed.

C. Security of Network and Authentication Policy

Technical security of network in distributed system is main area of focus in security of distributed environment. It basically involve how we make secures the network from network related attacks and how we handle the authentication mechanism.

The paper basically focused on firewall technique for security of network and *Kerberos* for authentication.

1) Firewall to Protect Network

Firewall is a system that is the sole point of connection between the internal network and protect it from the outside network. Basically firewall protect a network from unauthorized traffic by filtering out the unwanted traffic coming into or going from the secure network. There are certain decision rules in firewall technology on the basis of these rule firewall filter the data packet. These rules are based on predefined security policies. Routers also present a useful choke point for all of the traffic entering or leaving a network. In some cases attacker may hide the actual address of the data packet and make the address like the packet belong to internal network destination send to internal network - that is, packets that claim to be coming from internal machines but that are actually coming in from the outside - because such packets are usually part of address-spoofing attacks.[4] In such attacks, an attacker is pretending to be coming from an internal machine. So in such cases Decision-making of this kind can be done only in a filtering router at the perimeter of your network. Only a filtering router in that location which is the boundary between "inside" and "outside" network is able to recognize such a packet, by looking at the source address and whether the packet came from internal network connection or the external network connection.

The above figure shows that interior router which work as firewall identify the packet which is actually send by attacker and reject the data packet which actually coming from attacker. [5]The Methodology used in firewall is that it divide the whole network into three zone – internal network, demilitarized zone (DMZ) and the out side network. Here DMZ play an important role the DMZ is used to handle the services such as DNS and email server that need to access from outside.DMZ can be accessible by both internal network and outside network but host in DMZ network can not access the internal network , in this way internal network is secure. *Optimization techniques which make it's working more efficient. The general framework suggested in [6], for rule based firewall optimization. In framework, it captures the semantics of ACL (Access Control List) in terms whether each packet is accepted or rejected. To accomplish this, it divides packet space into independent partitions to correctly consider the changed set of packets matched by rules as the packets are processed within an ACL. Additionally, it compared to existing approaches. In this way, this model is able to find the optimal rule for reordering. Thus, it can also be used to compare and evaluate other optimization approaches and recognize their practical benefits and limitations. Authors in [6], focuses on the optimality of rule orders generated by the optimization rather than running time of the optimization algorithms because its direct impact on firewall performance and running time optimization does not affect firewall performance and one-time offline process. The process used for firewall optimization provides an algorithm, which given an ACL and a traffic profile, produces the*

optimal reordered rules. It is based on a novel rule-based partitioning of the packet space and reduction to integer programming. It formally establishes the correctness of the algorithm. It uses a semantic formalization of firewalls and its equivalence. An equivalence argument connecting this formalization with the reduction to integer programming..It provides an evaluation framework for rule based firewall optimization techniques. It is specially used to empirically evaluate two representative heuristic algorithms. New one additional introduced production firewall configuration, which is effective for understanding the tradeoffs of firewall optimization techniques.

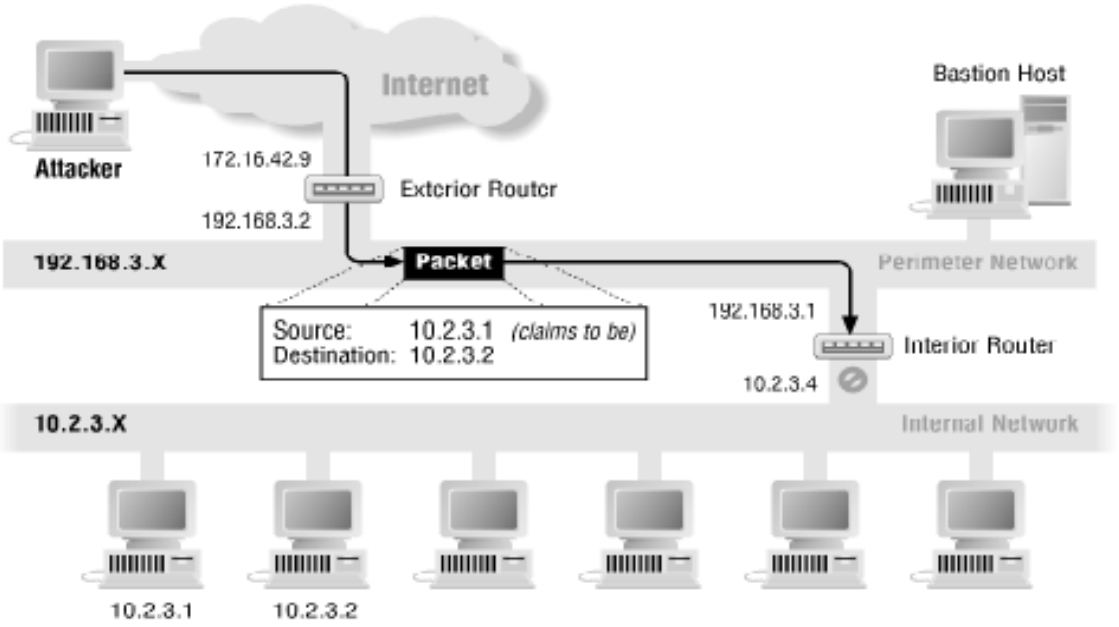


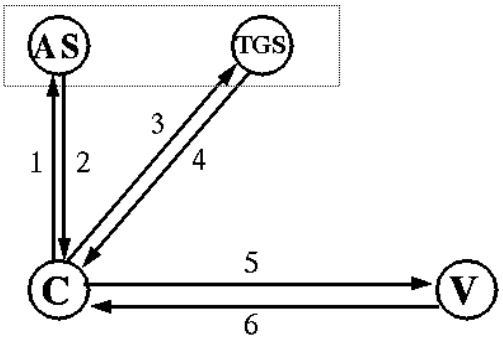
Figure 1 : Source Address Forgery

2) Kerberos for Authentication in Distributed System.

Due to increasing use if internet and technology enabled business activities , may organization use encryption technique to protect sensitive information transmitted over the internet and other networks . in the area of online application and client server computing where communication is TCP/IP Based there Kerberos protocol is used. Kerberos is an authentication system which is used in distributed system. It is adopted by many enterprises , organizations , universities . [7]Kerberos use cryptography concept. Kerberos provides evidence of a principal's identity to protect against the identity related attacks . In the working of Kerberos principal is main actor a principal is generally either a user or a particular service on home machine. A principal consists of the three-tuple: <primaryname, instance, realm >.If the principal is a user — a genuine person — the primary name is the login identifier which may be any email id or user name which is unique to each user and the instance is either null or represents particular attributes of the user that is root. If the principal is not a user it is a service of the system , then service name is used as the primary name and the machine name is used as the instance i.e. rlogin.myhost. The realm is used to distinguish among different authentication domains.

Kerberos principals may obtain tickets for services from a special server known as the ticket granting server, or TGS. A ticket contains assorted information identifying the principal, encrypted in the private key of the service.Here are some notation used in this technique {Tc,s }Ks = {s, c, addr, timestamp, lifetime, {Kc,s }c client principal, s server principal, tgs ticket-granting server,Kx private key of 'x',Kc,s session key for 'c' and 's',{in f o}Kx info encrypted in key Kx. {Tc,s }Ks Encrypted ticket for 'c' to use 's'.{Ac }Kc,s Encrypted authenticator for 'c' to use 's' addr client's IP address.Since only Kerberos and the service share the private key Ks, the ticket is known to be authentic.The ticket contains a new private session key, Kc,s , known to the client as well; this key may beused to encrypt transactions during the session. To guard against replay attacks, all ticketspresented are accompanied by an authenticator: {Ac }Kc,s = {c, addr, timestamp}Kc,s [7]This is a brief string encrypted in the session key and containing a timestamp; if the time does not match the current time within the (predetermined) clock skew limits, the request is assumed to be fraudulent. For services where the client needs bidirectional authentication, the server can reply with {timestamp + 1} Kc, s This demonstrates that the server was able to read timestamp from the authenticator, and hence that it knew Kc,s; that in turn is only available in the ticket, which is encrypted in the server's private key.

Tickets are obtained from the TGS by sending a requests, {Tc,tgs }Ktgs , {Ac }Kc,tgs .In other words, an ordinary ticket/authenticator pair is used; the ticket is known as the ticket granting ticket. The TGS responds with a ticket for server s and a copy of Kc,s, all encrypted with a private key shared by the TGS and the principal: {{Tc,s }K s ,Kc, s }Kc,tgs. The session key Kc,s is a newly-chosen random key. The key Kc,tgs and the ticket-granting ticket itself, are obtained at session-start time. The client sends a message to Kerberos with a principal name; Kerberos responds with{Kc,tgs ,{Tc, tgs }Kegs }Kc The client key Kc is derived from a non-invertible transform of the user's typed password. Thus, all privileges depend ultimately on this one key. Note that servers must possess private keys of their own, in order to decrypt tickets. These keys are stored in a secure location on the server's machine.



1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Figure 2: Complete Kerberos Authentication Protocol

IV. ATTACKS IN DISTRIBUTED SYSTEM

The paper focused on Distributed denial of services and Identity attacks that mostly occur in distributed system .

A. Distributed Denial of Services Attack

Denial of services is an attack in which the main purpose of attacker or hacker is to destroy the service of resources used by the legitimate user when this attack occur in distributed system then it is called distributed denial of services attack. [8]A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, and causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, a hacker begins by exploiting a vulnerability in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. Yahoo, Buy.com, RIAA and the United States Copyright Office are among the victims of DDoS attacks. DDoS attacks can also create more widespread disruption. In October 2010, for example, a massive DDoS attack took the entire country of Myanmar offline. A computer under the control of an intruder is known as a zombie .

B. DDoS Prevention

Many researchers are working for the solutions by which DDoS can be prevented. The paper focus on some exiting solutions and some suggested solution for DDoS. Some current effort to prevent DDoS are following-

1) ISP Filtering -Almost all ISPs have IP filters to try preventing various types of attacks. A lot of ISPs detect malicious packets with known signatures and/or bad TCP/UDP options. This also prevents few attack vectors[8]. Government can also help in case of such type of attacks , governments can enforce policies on some ISPs to block certain routes and/or subnets in case of attacks. But these efforts are very local even ISPs in the same country often do not share data about blacklisted IPs or malicious hosts.

2) Monitoring Teams -There are several teams that monitor internet activity and create a dynamic list of IPs with a metric for their threat level. Team Cymru, as an example, monitors specific Internet critical infrastructure, providing the results in this section. This permits the viewer to determine the scope and duration of Internet-effecting outages, and the localized effect of such outages. Many such monitoring projects use ICMP (ping), yet this isn't a great measure of performance. For this reason we also monitor connectivity to Internet critical infrastructure and between Team Cymru pods using both TCP and UDP. The monitoring focuses on DNS and BGP, the two most critical services.

3) *Hunting Tools* - There are several tools for hunting botnets that are not publicly available used by some law enforcement authorities. Microsoft has developed one of those tools recently. Although Microsoft is reluctant to give out details on its botnet buster -the company said that even revealing its name could give cyber criminals a clue on how to thwart it!- company executives[8].

Some other solution may be suggested to prevent the DDoS are Heterogeneity in Operating System and Cloud Computing .When There is only one operating system in the world that everybody uses. Now it's going to be very easy for the attackers to write one exploit that runs on every single machine on earth! On the contrary, if every single machine had its own operating system, then an attacker must write malware for every specific user. In this latter scenario, botnets would not exist for sure. It would require a gigantic amount of work. The point from this argument is that heterogeneity of platforms makes it statistically harder on the attacker to write a malware that spreads well. The problem is that most of the personal computers on earth run Microsoft software. Recently, servers also are migrating to Microsoft. This fact makes the decision pretty easy for the attacker when he is choosing the platform under which his agents are going to work.

[8]Cloud computing has been out there for while now. It is actually doing quite well. Amazon EC2 and Google clouds are getting pretty big and are used in numerous ways. Unfortunately, cloud computing is used for bad purposes also. Phishers are using cloud endpoints to provide their network with load balancing and survivability. Fast-flux enabled phishing sites using rapid DNS rotation across a large number of end points helps phishers evade most filters. With backup websites on the cloud and a good plan for the rotation, one could make use of multiple small servers across multiple cloud vendors and survive a strong DDoS attack.

B. Identity Attack in Distributed System

[9]In structured P2P application used Key-Based Routing (KBR) to assign application components such as traffic indirection, storage servers or measurement servers to the live node in the network. An attacker can take control and maintain KBR messages as its own. Attacker, make use of KBR information, that each node only sees a small subset of the overlay members. It is known as Identity attack. Any spiteful peer on the path of a KBR message can respond to the source code and maintain, as it is request's destination. The undetected attacker takes a control of particular key and its related applications. Multiple attackers can jointly perform stronger attacks. That is, separate the node from the network and effectively perform the manual partitioning of the overlay. Nodes detect the identity attack through the generation and timely distribution of self-verifying, "Existence proofs". The overlay nodes periodically, sign and distribute these proofs on behalf of well-defined regions of the namespace they reside in . For each section, a small number of randomly selected proofs are stored and provide them on request through proof manager. Existence proofs are digitally signed certificates. In [9], Self-verifying evidence of an attack is the first mechanism, used to track down and mark attackers. It also allowing overlay peers to locate and avoid attacker's node in favor of more reliable alternative routes. Second mechanism is to track attackers via blacklist; it verifies the valid evidence of the interested third parties in the network. If it found, adds it to the blacklist. Each node on the blacklist has an associated counter, which is incremented each time a new alert is presented showing that node performed an attack. Third mechanism is evading attacker via malice-aware routing. In this technique, once attackers have been identified with blacklists, nodes can actively avoid them when routing KBR requests.

1) Securing P2P Network against Identity Attack

Structured P2P overlay can simplify data storage and management for a verity of large scale

Distributed applications. Thus, the usefulness of the infrastructure has been validated by study of real world use of structured overlay applications [9]. Still, these applications infrastructures are susceptible to numerous critical spiteful attacks. One of them is Identity attack, which allows the spiteful peer in the network to capture application request and assume the responsibility of any application component.

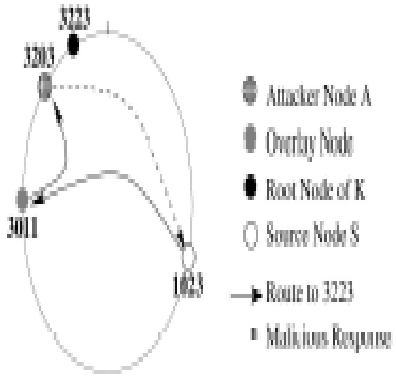


Figure 3: the Identity Attack. 1023 sends a message towards key 3222. Before the message reaches the root 3223, an attacker intercepts it and responds as the root.

V. CONCLUSION

In this paper different security aspect in like information security , physical security , technical security of networks are studied. All these securities should be properly implemented in distributed environment. In this paper the techniques to implement these securities has been discussed. In this paper two attack DDoS and Identity Attack are also discussed . These attack may occur in distributed system and also has been occurred in the past . In this paper solution for these attack have been discussed. However after studied all these making the distributed system more adaptive and dynamic is a typical task. Security of distributed system is more complex than stand alone system security and needed some more effort.

ACKNOWLEDGEMENT

We are grateful to Our Teachers from Department of Computer Engineering and Application at National Institute Of Technical Teacher's Training and Research , Bhopal , Madhya Pradesh (India) for motivating and providing guide to write the paper .

References

[1] *Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, John L. Schultz, Jonathan Stanton and Gene Tsudik, "Secure Group Communication Using Robust Contributory Key Agreement", IEEE Transactions On Parallel And Distributed Systems, Vol. 15, No. 5, pp. 468-480, May 2004.*

[2] *Subramanian Lakshmanan, Mustaque Ahamad, and H. Venkateswaran, "Responsive Security for Stored Data", IEEE Transactions On Parallel And Distributed Systems, Vol. 14,No. 9, pp. 818-828, September 2003.*

[3] *"Physical Security in Distributed IT Environments" [Online]. Available: http://www.ithandbook.ffiec.gov*

[4] *"Packet Filtering" , Chapter 6 [Online]. Available: http://www.diablotin.com/librarie/networking/firewall/ch06_01.htm*

[5] *Larry L. Peterson And BRUCE.S.DAVIE "Computer network " (2009 edition, page no 626 and 627)*

[6] *Ghassan Misherghi, Lihua Yuan, Zhendong Su, Chen-Nee Chuah and Hao Chen,"A general Framework for Benchmarking Firewall Optimization Techniques", IEEE Transactions On Network and Service Management, Vol. 5, No. 4, pp. 227-238, Dec 2008.*

[7] *Emir Accilien CMPT 585 001 "Security issues in Distributed Systems:Is Kerberos the Answer?" [Online].Available : http://www.pages.csam.montclair.edu*

[8] *Ahmed Saafan "Distributed Denial of Service Attacks: Explain nation, classification and suggested Solutions" (23 March 2009) [Online]. Available: http://www.exploit-db.com*

[9] *Krishna P.N. Puttaswamy, Haitao Zheng, and Ben Y. Zhao, "Securing Structured Overlays against Identity Attacks", IEEE Transactions On Parallel And Distributed Systems, Vol. 20, No. 10, pp. 1487-1498. October 2009.*

