ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

A Study on Distributed Architecture for Web Applications

[1] Vikas Reddy. S [2] Dr. Chandrashekara. S.N
[1] Assistant Professor [2] Professor & Head
[1][2]Dept.of CS&E, S J C Institute of Technology, Chickballapur

Abstract: **-- 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. In distributed system environment it is very important to provide service at any time, any where to the customers, this requires proper time management of all computing and networking resources, resource allocation on time and their proper utilization. In distributed environment security is primary concern. 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 . Security vulnerabilities dormant in a distributed system can be intentionally exploited or inadvertently triggered. The threats of exploitation or triggering are only potential, and materialize as an attack or an accident. Vulnerabilities exists in hardware, networks, operating systems, database systems, and applications. New ones are being discovered every day. 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.**

***Keywords*:-- Security, Web application, Architecture, Analysis of distributed Systems**

I. INTRODUCTION

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. [5]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.

Distributed system is an application that communicates with multiple dispersed hardware and software in order to coordinate the actions of multiple processes running on different autonomous computers over a communication network, so that all components hardware and software cooperate together to perform a set of related tasks targeted towards a common objective. Most people consider a distributed system and a network of computers to be the same. But these two terms mean two different but related things. [1] A computer network is an interconnected set of autonomous computers that communicated with each other. A user using a computer network understands that he uses different resources lying on different computers as a computer network does not hide the existence of multiple computers. But a distributed system on the other hand provides the feeling that the user is working on a single homogenous more powerful computer with more resources.

Applications

Rout ing Algor i thms ,Wi r e l e s s Sensor Networks,World Wide Web,Aircraft Control Systems,Industrial Control Systems,Distributed Rendering in Computer Graphics

II. RELATED WORKS

[1]Implementation of Security in Distributed Systems in this paper author describes about the comparative study of distributed systems, the security issues associated with those systems and their solutions.The main focus is on the Distributed Storage Systems and Distributed Databases.

In Distributed Storage Systems main objective is to protect the data in case of disk failure by redundant storage.There are four types of distributed storage systems Server Attached Redundant Array of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

Independent Disks (RAID), centralized RAID, Network Attached Storage (NAS) and Storage Area Network (SAN).NAS and SAN have slight differences in techniques adopted for transferring data between devices.SAN has better performance compared NAS.

This paper proposes threat model named CIAA threat model. This model addresses all the security issues namely, Confidentiality, Integrity, Availability and Authentication. In arriving at this model, authors have organized the threats on a distributed storage system under each category of the CIAA pillars of security and provided techniques that can be used to circumvent the threats.

Mutually Cooperative Recovery (MCR) mechanism enables the system to recover data in situations of multiple node failures. The transmission scheme and design a linear network coding scheme based on (n, k) strong- MDS code proposed help recover systems from failure with relative ease.

Distributed Database System is a collection of independent database systems distributed across multiple computers that collaboratively store data in such a manner that a user can access data from anywhere as if it has been stored locally irrespective of where the data is actually stored. When data is distributed across multiple networks or information is transferred via public networks, it becomes vulnerable to attacks by mischievous elements.

In traditional security model, all the data stored in database and the users who access that data belong to the same security level. A multilevel secure database system assigns security level to each transaction and data. Clearance level of a transaction is represented by security level assigned to it and the classification level of data is given by the classification level. A multilevel secure database management system (MLS/DBMS) restricts database operations based on the
security levels.

[2]Security & Distributed Systems in this author talks about security risks, benefits, objectives and mechanisms of distributed systems.

Security Risks Of Distributed Systems

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. Another risk is that unprotected systems may be used as an entry point into other inadequately protected but sensitive systems.

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. Distribution not only introduces additional risks t o c omp u t e r s y s t ems b u t a l s o a d d s complications to dealing with the risks. Communication may introduce significant time lag into the system in respect of security related information.

Security Benefits Of Distributed Systems Unauthorized 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.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.

Security Objectives

a]Confidentiality—Maintaining confidentiality of information held within systems or communicated between them. This typically means the prevention of unauthorized access to stored data files and the prevention of eavesdropping on messages in transmission.

b]Integrity—Maintaining the integrity of data held within systems or communicated between systems. This prevents loss or modification of the information.

c]Availability—Maintaining the availability of informa t ion he l d wi thi n sys t ems 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.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

d]Authentication—Authenticating the identity of communicating partners and authenticating the origin and integrity of data which is communicated between them.

Security Mechanisms

a]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, terrorist attacks and accidental or malicious damage by users and technicians.

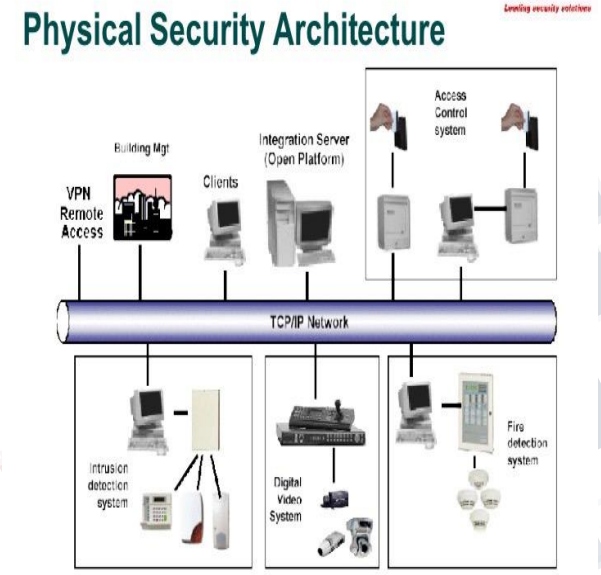


Fig 1:Physical Security Architecture

b]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 avoi d the pa s s ive e ave sdropping of electromagnetic radiation from visual display units, printers and processors. The modulated signals can be detected by nearby radio receivers and analyzed to reveal the data being displayed, printed or processed.

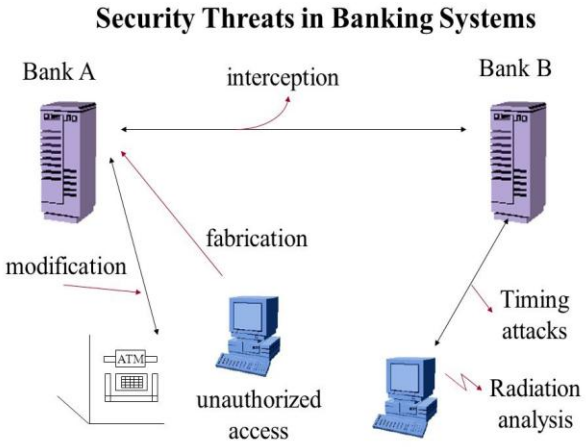


Fig 2:Electronic Security Mechanism

c]Authentication

1. Personal Authentication

The aim of personal authentication in computer systems is to verify the claimed identity of a human user.

2.Message Authentication

The aim of message authentication in computer and communication systems is to verify that the message comes from its claimed originator and that it has not been altered in transmission.

[3]Vulnerabilities and Threats in Distributed Sy s t ems t h i s p a p e r t a l k s a b o u t t h e vulnerabilities ,threats and mechanisms to reduce it.

Vulnerabilities:A vulnerability can be defined as a flaw or weakness in system security procedures, design, implementation, or internal controls. A vulnerability can be accidentally triggered or intentionally exploited, causing security breaches.

Modeling vulnerabilities includes analyzing their features, classifying them and building their taxonomies, and providing formalized models.

Threats:Threats against systems as entities that can intentionally exploit or inadvertently trigger specific system vulnerabilities to cause security breaches. An attack is an intentional exploitation of vulnerabilities, and an accident is an inadvertent triggering of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

vulnerabilities. Both materialize threats, changing them from potential to actual. Threats can be classified according to actions and consequences. Mechanism to Reduce Vulnerabilities and Threats Using Trust in Role-Based Access Control The t r adi t iona l , ident i ty-ba s e d approaches to access control are inadequate or even inapplicable to open computing, including Internet-based computing. In addition, the common user authorization approach of granting access privileges to users based solely on user's ownership of digital credentials, presented directly to the system, has its share of problems.

In the proposed model authors have incorporated comprehensive aspects of trust in social systems and computer science applications. One challenge was to select care fully all and only useful trust aspects needed for our system design in a way preventing adverse affects on the flexibility or performance. Authors developed algorithms for automating evaluation of trust, or inference of trust. They produce trust ratings for a user based on:

(a) Dynamic, continuously updated system's own view of user's behavior in interactions with the system.

(b) System's own evidence records.

(c) Evidence records obtained from "foreign" reputation servers.
(d) System security policies. The capability to use trust ratings for users was applied for enhancing the well known role based access control (RBAC) mechanism. Trust management is performed in this system by a trust enhanced role mapping (TERM) server, which interacts with RBAC and a reputation server in the process of user authorization.

[4] S e c u r i t y i s s u e s i n Di s t r i b u t e d Systems ,According to Andrew S. Tanenbaum, "Distributed systems need radically different software than centralized systems do." Modern computer systems provide service to multiple users and require the ability to identify the user making a request accurately. In traditional systems, the user's identity is verified by checking a password typed during login; the system records the identity and uses it to determine what operations may be performed.

The process of verifying the user's identity is called authentication. Password based authentication is not suitable for use on computer networks. Passwords sent across the network can be intercepted and subsequently used by eavesdroppers to impersonate the user. There are many different types of distributed computing systems and many challenges to overcome in successfully designing one. The main goal of a distributed computing system is to connect users and resources in a transparent, open, and scalable way.

The security to the network in distributed system is very important and the techniques that can be used are [5] using fire walls and Kerberos. 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. 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.

For distributed systems kerberos is better compared to other methods,So this paper proposes kerberos. Kerberos for Authentication in Distributed System Kerberos is an authentication system which is used in distributed system. It is adopted by many enterprises , organizations , universities .Kerberos use

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

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

Tool	Comments
mytoken.exe (Platform SDK)	Command prompt tool to display the content of a user's access token: This includes the user's rights and group memberships.
whoami.exe (Default Windows installation)	Command line tool to look at the content of the user's access token (use the /all switch).
klist (Resource Kit)	Command prompt tool to look at the local Kerberos ticket cache. Klist can also be used to purge tickets. Klist is a very simple but very important tool that you can use to find out how far the authentication got.
Kerbtray (Resource Kit)	GUI tool that displays the content of the local Kerberos ticket cache.
Netdiag (Support tools)	Netdiag helps isolate networking and connectivity problems by providing a series of tests to determine the state of your network client. One of the "NETDIAG" tests is the Kerberos test. To run the Kerberos test, type "netdiag /test:Kerberos" at the command prompt.
Replication monitor (replmon) (Support tools)	Using Replication monitor, an administrator can not only check the replication traffic but also the number of AS and TGS requests and the FSMO roles.
Network monitor (Server CD)	Network monitor does not come out of the box with a parser for the Kerberos protocol. However, a special Kerberos parser dll is available from Microsoft.
Setspn (Support Tools)	Tool allowing you to manage (view, reset, delete, add) service principal names (SPNs).

Table 1:Kerberos troubleshooting tools

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 us e d t o di s t ingui s h among di ff e r ent authentication domains. Kerberos principals may obtain tickets for services from a special server known as the ticket granting server, or TGS. A ticket contains

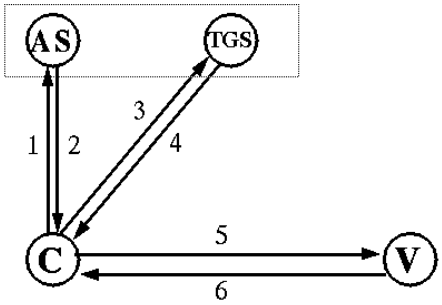
Sl No	Method	Advantages	Disadvatages
1	Kerberos	1.Prevents intrusion attacks 2.Permits interoperability with other Kerberos realms 3.Provides authentication across the Internet of Web	1.Requires continuous availability of central server 2.Needs own set of Kerberos keys
2	Firewall	1.Bloks Trojans 2.Stops Hackers 3.Monitors traffic	1.Internal Attack 2.Diminishes Performance 3.Costly 4.Legitimate User Restriction

Table2: Kerberos and Firewall comparison

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 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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016



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 3: Complete Kerberos Authentication Protocol

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.

CONCLUSION

A sophisticated distributed system is on par with nanotechnologies and artificial intelligence. It has the potential to distribute energy needs for processing.It provides mechanisms which captures data in real time and process it as needed .There are many reasons that make distributed systems is viable such as high availability, scalability, resistant to failure, etc.

In this paper the development of distributed systems is discussed in terms of what a distributed system is and the objectives of setting up a distributed system. From all the available distributed systems, the possible solutions are discussed where in the security of Kerberos depends critically on synchronized clocks. In essence, the Kerberos protocols involve mutual trust among four parties: the client, server, authentication server and time- server. If any one of these parties fails, then the security of the whole system is compromised. This paper also talks about the solution for the attacks, investigation of vulnerabilities and threats on distributed networks .By studying 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.The security issues and solutions proposed for different systems are summarized and compared with each other.

REFERENCES

[1] Mohamed Firdhous, Implementation of Security in Distributed Systems – A Comparative Study, International Journal of Computer Information Systems, Vol. 2, No. 2, 2011

[2] Jonathan D. Moffett Security & Distributed Systems

[3]Bharat Bhargava and Leszek Lilien, Vulnerabilities and Threats in Distributed Systems ,Springer-Verlag Berlin Heidelberg 2004

[4] Emir Accilien ,Security issues in Distributed Systems

[5] Manoj Kumar, Nikhil Agrawal, Analysis of Different Security Issues and Attacks in Distributed System, International Journal of Advanced Research in Computer

Science and Software Engineering,Volume 3, Issue 4, April 2013

[6] Andrew S Tanenbaum and Maarten van Steen, Distributed Systems: Principles and Paradigms, 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007.

[7]Zakaria Suliman Zubi, "On distributed database security aspects," in International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, 2009, pp. 231-235.

[8] B. Bhargava, "Vulnerabilities and Fraud in Computing Systems," Proc. Intl. Conf. IPSI, Sv. Stefan, Serbia and Montenegro, Oct. 2003.

[9] Ragib Hasan, Suvda Myagmar, Adam J Lee, and William Yurcik, "Toward a threat model for storage systems," in Proceedings of the 2005 ACM Workshop on Storage Security and Survivability (StorageSS '05), FairFax, VA, USA, 2005, pp. 94-102.

[10] N. Heintze and J.D. Tygar, "A Model for Secure Protocols and Their Compositions," IEEE Transactions on Software Engineering, Vol. 22, No. 1, 1996, pp. 16-30.