IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 146-149
www.iosrjournals.org

Security Analysis of a Single Sign-On Mechanism For Distributed Computer Networks

C. Ramakrishnan[1], S. Dhanabal[2],
[1]*II year M.E, Computer Science and Engineering,*
[2]*Assistant Professor, Department of CSE, PGP College of Engineering and Technology, Namakkal,*

Abstract: *Single sign on mechanisms allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. There are few practical and secure single sign on models, even though it is of great importance to current distributed application environments. Most of current application architectures require the user to memorize and utilize a different set of credentials (eg username/password or tokens) for each application he/she wants to access. However, this approach is inefficient and insecure with the exponential growth in the number of applications and services a user has to access both inside corporative environments and at the Internet. Single sign on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well organized security arguments. In this paper, however, it is shown that their scheme is actually insecure as it fails to meet security during communication, in order to provide a secure authentication digital signature with hash function is researched for future work.*

I. Introduction

A distributed computer system consists of multiple software components that are on multiple computers, but run as a single system. The computers that are in a distributed system can be physically close together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible configurations, such as mainframes, personal computers, workstations, minicomputers, and so on. The goal of distributed computing is to make such a network work as a single computer. Distributed systems offer many benefits over centralized systems, including the following:

Scalability
The system can easily be expanded by adding more machines as needed.

Redundancy

Several machines can provide the same services, so if one is unavailable, work does not stop. Additionally, because many smaller machines can be used, this redundancy does not need to be prohibitively expensive.Distributed computing systems can run on hardware that is provided by many vendors, and can use a variety of standards-based software components. Such systems are independent of the underlying software.

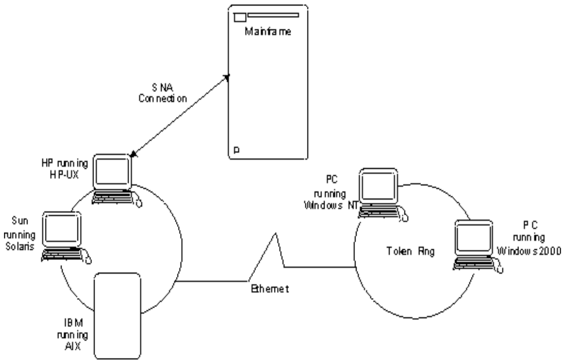

Fig1.open distributed system

Client – Server Model

A common way of organizing software to run on distributed systems is to separate functions into two parts: clients and servers. A client is a program that uses services that other programs provide. The programs that provide the services are called servers.

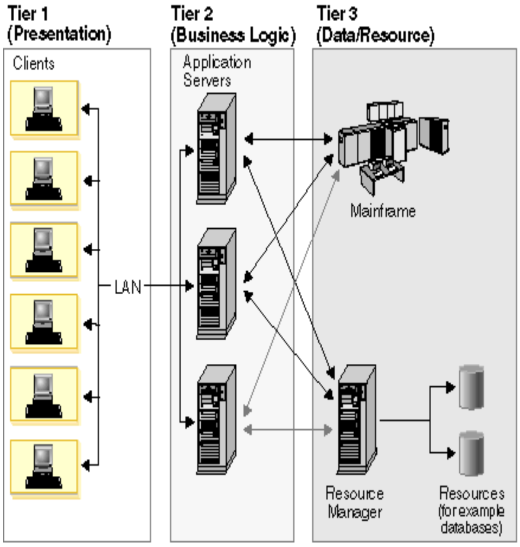

Fig1.2. three tier client / server architecture

II. Literature Survey

2.1Anonymity Enhancement on Robust and Efficient Password Authenticated Key Agreement Using Smart Cards

Our password-authenticated key agreement scheme using smart cards has been really efficient and effective. In terms of efficiency, besides the low communication costs, our solution builds on the efficient cryptographic primitives of secure hash function and symmetric cipher, which may be easily instantiated in and thus inherently viable for smart card environment. In terms of effectiveness, our solution not only preserves mutual authentication, key agreement, initiator anonymity, and the functionality of password updating but also can prevent initiator traceability, insider attack, offline password-guessing attack, and DoS attack.

2.2 Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards

We have proposed an efficient and robust user authentication and key agreement scheme that not only can satisfy all the merits of Fan et al.’s scheme but also can provide identity protection, session key agreement, and low communication and computation cost by using elliptic curve cryptosystems and can prevent the insider attack. Our proposed scheme is very useful in limited computation and communication resource environments to access remote information systems. In addition, our proposed scheme can withstand the offline dictionary attack even if the secret information stored in a smart card is compromised.

2.3 Formal Vulnerability Analysis of a Security System for Remote Fieldbus Access

As field bus networks are becoming accessible from the Internet, security mechanisms to grant access only to authorized users and to protect data are becoming essential. This paper proposes a formally-based approach to the analysis of such systems, both at the security protocols level, and at the system architecture level. This multi-level analysis allows the evaluation of the effects of an attack on the overall system, due to security problems that affect the underlying security protocols. A case study on a typical fieldbus security system validates the approach.

2.4 Review of Security Issues in Industrial Networks

While advanced techniques have been continuously developing for several years, to protect office and business networks from information technology-based attacks, the same has not happened for IACS, mainly because of their peculiarities and priorities in security requirements, that make them different from conventional computing systems. So, while sophistication in cyber attacks always improves, security management in IACS has remained more or less the same until recently. The interconnection of subsystems through public communication networks and the Internet, the introduction of wireless communication technologies, and the increasing adoption of general-purpose operating systems and s/w available off-the-shelf has then significantly contributed to increase the exposure of IACS to security threats.

2.5 Distributing Internet Services to the Network's Edge

In the context of industrial information technology, the Internet and World Wide Web increasingly are seen as a solution to the problem of providing "anywhere, anytime" services. In the classical view of an Internet-enabled IT infrastructure, services are requested and consumed by a user (e.g., a human requesting plant production data from his or her desktop) and data are provided by an origin server (e.g., a Web server located in a plant that can authenticate users, implement encryption, serve data, and source multimedia streams).

III. Dynamic id based encryption and hashing algorithm :

Steps for data authentication

Step1: sender encrypts message using receiver public key
Step2: when receiver receives message from sender, receiver request a private key from key server
Step3: the key server sends an investigating message to sender, for receiver authentication
Step4: after getting the verification message from sender, the key generator provides a private key to receiver for decryption any time.

Steps for node authentication

```
  Step 1: User u generates hash id using H(n) = PUB_KEY/ IDENTITY
  Step 2: Neighbors node also generates hash id in the same way
 Step 3:
{   If (hash_id (user) = hash_id(provider))
           Then node is authenticated  }
  Else{   Node is malicious node
         }
```

Modules description

Wireless network setting

This module is developed to node creation and more than 30-50 nodes placed particular distance. Wireless nodes placed intermediate area in a distributed network. Each node knows its location relative to the sink. The maximum dimension of node is set as x=4000 and y=4000. The size of the nodes is set as 35 and the ultimate time simulation is 10 ms.Thespeed of network nodes set as 10-15 m/s.

Registration phase

In this phase, upon receiving a register request from network nodes, SCPC – smart card producing center provides a fixed length unique id to all network nodes for identification process, SCPC generates an id using RSA signature algorithm which provides a necessary public key and signature to network nodes for its identification purpose. The network nodes communicate with other nodes using this generated id.

Data routing phase

The user and provider establish a communication through multi hop path through the shortest path, the path establishment or path discovery is done through CBR (credit based routing), in the identified path the data is routed from several users through SSO – single sign on mechanism of authenticated user.

Authentication phase

In this phase, RSA-VES is employed to authenticate a user, while a normal signature is used for service provider authentication. Consider an adversary node try to injectfalse packets to provider in order to confuse the provider about original data packets and also tries to receive the original data packets from user. The RSA – VES algorithm enhanced to authenticate the original packets, the private key is used by the provider to decrypt the original packets.

Malicious node detection and legitimate node identification phase

For the proposed malicious node detection process digital signature dynamic source configuration routing is enhanced, which states KEY SERVER tends to verify the authentication of provider. By this proposed technique any number of users, intermediate nodes and provider can verify each other through dynamic hash function technique. In hash function technique if user wants to verify the provider the USER U generates a hash id through hash function H(n)= PUB_KEY/IDENTITY, the public key and id of user U generates hash id. In the same way the PROVIDERS generate the hash id, if the user u hash id and provider hash id are same then the nodes are authenticated for data transmission and authentication.

Graph analysis

The simulated graphs evaluates the performance level of proposed system over existing system, the PDR , throughput enhancement factors evaluated through graphical analysis.

Advanced uses of AODV

- Because ofits reactive nature, AODV can handle highly dynamic behavior of VehicleAd-hocnetworks.
- Usedforboth unicastsandmulticasts using the'J'(Join multicastgroup) flagin thepackets.

Limitations/disadvantages of AODV

- Requirementonbroadcastmedium
- Itisvulnerabletomisuse:Themessagescanbemisusedforinsiderattacksincludingroutedisruption, route invasion, no deisolation, and resource consumption.
- AODV lacks support for high throughput routing metrics: AODV is designed to support the shortest hop count metric. This metric favors long, low-band width links over short, high-bandwidth links.
- High route discovery latency: AODV is a reactive routing protocol. This means thatAODVdoesnot discoveraroute untilaflowisinitiated. This route discoverylatency resultcanbehighinlarge-scalemeshnetworks.

DSDV - the destination sequenced distance vector protocol

DSDV is one of the most well known table-driven routing algorithms for MANETs. It is a distance vector protocol. In distance vector protocols, every node i maintains for each destination x a set of distances {dij(x)} for each node j that is a neighbor of i. Node i treats neighbor k as a next hop for a packet destined to x if dik(x) equals minj{dij(x)}.

Advantages Of DSDV

- DSDV protocol guarantees loop free paths.
- Count to infinity problem is reduced in DSDV. We can avoid extra traffic with incremental updates instead of full dump updates.
- Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

IV. Conclusion

We demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential. The second attack violates the soundness of authentication .we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy.It is shown that their scheme is actually insecure as it fails to meet security during communication, in order to provide a secure authentication digital signature with hash function is researched for future work.

References

[1]. X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800, Feb. 2010.

[2]. W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556, Jun. 2008.

[3]. M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 30–40, Feb. 2011.

[4]. A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol. PP, no. 99, 2012,DOI 0.1109/TII/2012.2198666.

[5]. A. C. Weaver and M. W. Condtry, "Distributing internet services to the network's edge," IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404–411, Jun. 2003.