Security Analysis of a Single Sign-On Mechanism using Elliptic Curve Cryptography in Distributed Computer Networks

R. Arunkumar[1] Mrs. J. VijiPriya[2]
[1]M. E. (Final Year) [2]M. E. ,M.Sc.(Ph.D), Assistant Professor
[1,2] RatnaVel Subramaniam College of Engineering & Technology.

Abstract--- Single sign-on (shortly called as SSO) is an authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. In our proposed work we use Elliptic Curve Cryptography (shortly ECC) for high efficiency with smaller key sizes useful for security arguments that has limited power .In the proposed system using ECC the cryptographic operations will be performed with fewer processor cycles and operation can be performed much faster and providing well-organized security arguments in distributed computer network.

Keywords: - Authentication, distributed computer networks, information security, security analysis, single sign-on (Shortly called as SSO).

I. INTRODUCTION

Distributed computer networks, has become common to allow users to access various network services offered by distributed service providers. Consequently, user authentication (also called user identification), plays a crucial role in distributed computer networks to verify if a user is legal and can therefore be granted access to the services requested. To avoid bogus servers, users usually need to authenticate service providers. Each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. An SSO scheme should meet at least three basic security requirements, i.e., enforceability, credential privacy, and soundness. Enforceability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. In the broadest sense, a network is any interconnected group of people or things capable of sharing meaningful information with one another. In a technology context, network is usually short for "computer network" or "data network" and implies that computers are the things sharing the meaningful information. At a conceptual level, all data networks consist of nodes, which refers to any computer or digital device using the network and links, the physical connections (either wired or wireless) that carry messages between nodes.

II. OVERVIEW OF SCHEME

Single sign-on (Shortly called as SSO) is an authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. In our proposed work use Elliptic Curve Cryptography (Shortly called as ECC) for high efficiency with smaller key sizes useful for security arguments that have limited power .In the proposed system using ECC the cryptographic operations will be performed with fewer processor cycles and operation can be performed much faster and providing well-organized security arguments in distributed computer network.

Networks also vary considerably in terms of the roles and responsibilities of the computers on that network and the relationships that tie those machines together. A computer totally disconnected from other devices is typically referred to as a standalone machine.

When several computers are interconnected, but no computer occupies a privileged position, the network is usually referred to as a peer-to-peer network. In this type of network, every computer can communicate with all the other machines on the network, but in general each one stores its own files and runs its own applications. With a client-server network, one or more servers will perform critical functions on behalf of the other machines (the clients) on the network. These functions might include user authentication, data storage, and the running of large, shared, resource-intensive applications such as databases and client relationship management (Shortly called as CRM) software. Typically, both peer-to-peer and client-server networks rely on a shared Internet connection for access to external resources of these basic network structures.

III. USER AUTHENTICATION

User Authentication is the process of individual identity conformation, to ensure that an individual is really who he claims to be. Probably the earliest user authentication mechanism was based on passwords. This concept was first proposed by Lamport in 1981 and remains the most common mechanism for user authentication for computer system and networks.

While such protocols have been widely used, a number of problems have appeared, for example a poor selection of passwords the shortcoming of capture by Trojan and reuse of passwords.

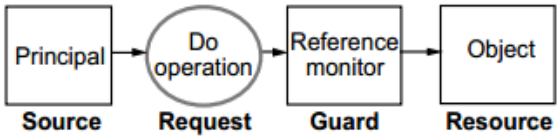

Fig. 1. The access control model.

Fig. 1: Access Control Model Requests to perform operations on objects.

A. A Reference Monitor

A guard for each object that examines each request for the object and decides whether to grant it. Objects Resources such as files, devices, or processes. The reference monitor bases its decision on the principal making the request, the operation in the request, and an access rule that controls which principals may perform that operation on the object. To do its work the monitor needs a trustworthy way to know both the source of the request and the access rule. Obtaining the source of the request is called 'authentication'; interpreting the access rule is called 'authorization'. Thus authentication answers the question ''who said this?'', and authorization answers the question ''who is trusted to access this?''. Usually the access rule is attached to the object; such a rule is called an access control list or ACL. For each operation the ACL specifies a set of authorized principals, and the monitor grants a request if its principal is trusted at least as much as some principal that is authorized to do the operation in the request. With the increasing usage of network services, a user may need to maintain more and more ID/ password pairs for accessing different distributed service providers.

B. Password Synchronization Vs Single Sign-On

	Password Synchronization	Single Sign-on
Process	Simply changes all applications to the same password. User continues to login to each of those applications separately, but uses same password.	Use single username and password to sign in to one site, the client authentication of other site done by specific server
Login times	Several times depends on the application required	Once for every domain

Table 1 Password Synchronization Vs Single Sign-On

This imposes a burden on users and service providers as well as the communication overhead of computer networks. To tackle this problem, a single sign-on (shortly called as SSO) mechanism has been introduced so that after obtaining a credential from a trusted authority, each legal user can use this single credential to authenticate itself and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements: completeness, soundness and credential privacy. Completeness of authentication requires that

- Both sides accept each other if they have matched the conversation
- The probability that one side accepts the other one who actually has not engaged in the matching conversation in negligible. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers.

IV. PROBLEM CHARACTERIZATION

Data networks are important to all contemporary organizations because they provide faster, easier access to any message or data that can be represented and stored in digital format. For example, when your colleagues and predecessors research an issue relevant to your organization and share their data and conclusions with you in a data format your computer recognizes, you can copy key information from their report into your own, saving yourself significant amounts of time If the colleague whose work you're relying on works in the same cubicle as you and they remember where they've stored the relevant report, a network may not offer significant advantages since you can turn to him or he and ask for the file on a CD or USB flash drive. However, in many organizations, large distances separate co-workers, and data sharing becomes a significant logistical problem in the absence of a network.

In addition to data sharing, computer networks also enable resource sharing, an important consideration in all budget-conscious charities and organizations. Rather than buying one printer for every employee and replacing them when they wear out, an organization with a network can buy a single printer, connect it to the network, and configure it in such a way that every computer user in the organization can print to it. The initial cost of a networked printer is usually more than the cost of a single desktop printer, but when considering costs on a per-user basis, the average cost of the networked printer is often much less than the cost of buying a printer for every employee.

A. System Architecture

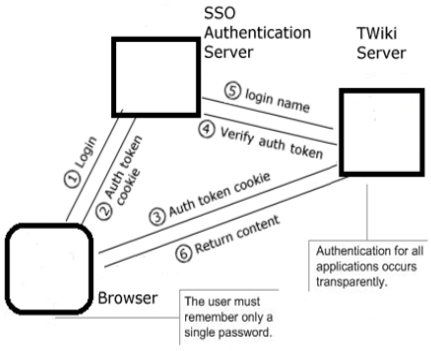

Fig. 2: System Architecture

While some networked devices such as printers, scanners, and fax machines have predetermined, specialized functions, you can also network and share generic, unspecialized computing power in the form of servers. Servers are large, powerful computers that can handle resource-intensive tasks more efficiently than desktop computers. As with the networked printer, the initial outlay for a server is more than that for a desktop computer, but across the organization, it's often cheaper to run the server-based version of a program since individual users won't need expensive, high-performance desktop and laptop

computers. Servers can also deploy software to other networked machines at a lower cost.

Individual computers provide opportunities for tremendous productivity gains, but they become many times more powerful when they're connected to one another in data networks that give them the ability to share data and processing resources.

With a network, five colleagues can read and edit an evolving document from their own computer with minimal effort and coordination. Without a network, these colleagues have to share time on the same computer or work out a process for exchanging removable storage media (for example, floppy diskette, or USB drive). In a similar fashion, networks let us all realize economies of scale by running resource-hungry applications on high-power hardware.

V. INDEPENDENT

The main objective of this paper is to provide security using elliptic curve cryptography in distributed computer network. To achieve soundness and credential privacy.

Security of ECC

- To protect a 128 bit AES key it would take a:
- RSA Key Size: 3072 bits
- ECC Key Size: 256 bits

NIST Guidelines for Public Key Sizes for AES			
ECC Key Size (Bits)	**RSA Key Size (Bits)**	**Key Size Ratio**	**AES Key Size (Bits)**
163	1024	1:6	
256	3072	1:12	128
384	7680	1:20	192
512	15360	1:30	256

Table 2 NIST Guidelines for Public Key Sizes for AES

In this paper work we proposed ECC to overcome the security problem of the existing advanced change lee scheme. Improved SSO scheme fails to meet credential privacy; it implies that Ateniese's RSA-VES fails to satisfy signature hiding. Elliptical curve cryptography is a method of encoding data files so that only specific individuals can decode them. ECC is based on the mathematics of elliptic curves and uses the location of points on an elliptic curve to encrypt and decrypt information. ECC affords efficient implementation of wireless security features, such as secure electronic mail and Web browsing. Soundness and signature hiding are the two core security Properties to guarantee the fairness of digital signature exchange using VES.

V. PROPOSED IMPROVEMENT

To overcome the flaws in the Chang-Lee scheme we now propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realizing fair exchange of RSA signatures. VES comprises three parties: a trusted party and two users say Alice and Bob. The basic idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses interactive zero-knowledge (Shortly NZK) to convince Bob that she has signed the message and the trusted party can recover the signature from the cipher text. After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

VI. CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (shortly SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, we explained why Hsu and Chuang's scheme is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy.

VII. FUTURE WORK

It is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work a preliminary formal model addressing the soundness of SSO has been proposed. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

- The mathematic background of ECC is more complex than other cryptographic systems Geometry, abstract algebra, and number theory.
- ECC provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman)

Mobile systems Systems required high security level (such as 256 bit AES).

REFERENCES

[1] W. Diffie and M. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory, 22:644-654,1976.
[2] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203–209,1987.
[3] V. Miller. Use of elliptic curves in cryptography. Advances in Cryptology—CRYPTO '85(LNCS 218) [483], 417–426, 1986.
[4] G. Faltings (July 1995): The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles. Notices of the AMS 42 (7): 743–746. ISSN 0002-9920. July 1995.

