An Efficient Single Sign-On Mechanism to Enhance Security by Using Hash Function

M.Shanmuga Priya
Assistant Professor, Computer Science Engineering, RVS Technical Campus, Coimbatore, India.

D.Rajapriya
Assistant Professor, Computer Science Engineering, RVS Technical Campus, Coimbatore, India.

V.Sathya Priya
Assistant Professor, Computer Science Engineering, RVS Technical Campus, Coimbatore, India.

Abstract – The security of Single sign-on (SSO) has been receiving a significant amount of attention in the field of distributed computer network, because SSO schemes are vulnerable to malicious attacks. A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. However, these schemes are not suitable for highly dynamic environments. Hence, this still calls for an efficient authentication scheme for distributed computer network. The aim of this project is implement the decentralized light weight authentication scheme called trust-extended authentication mechanism for distributed computer networks. It satisfies the following security requirements: anonymity, privacy, mutual authentication.

Index Terms – Authentication, distributed computer networks, information security, security analysis, single sign-on (SSO).

1. INTRODUCTION

With the widespread use of distributed computer networks, it has become common to allow users to access various network services offered by distributed service providers. Consequently, user authentication 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. After mutual authentication, a session key may be negotiated to keep the confidentiality of the data exchanged between a user and a service provider. In many scenarios, the anonymity of legal users must be protected as well. However, practice has shown that it is a big challenge to design efficient and secure authentication protocols with these security properties in complex computer network environments.

In 2000, Lee and Chang proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu pointed out that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. Meanwhile, Yang *et al.* identified a weakness in the Wu–Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti pointed out that Yang *et al.*'s scheme suffers from Deniable of Service (DoS) attacks and presented a new scheme. In 2009, Hsu and Chuang showed that the schemes of both Yang *et al.* and

Mangipudi–Katti were insecure under identity disclosure attack and proposed an RSA-based user identification scheme to overcome this weakness. Recently, authentication and privacy have been attracted a lot of attentions in RFID systems industrial networks, as well as general computer networks.

On the other side, it is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period(say one day), 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. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., *unforgeability*, *credential privacy*, and *soundness*. Unforgeability 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. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Formal security definitions of unforgeability and credential privacy were given in. A similar concept, called the generalized digital certificate (GDC), was proposed in to provide user authentication and key agreement in wireless networks, in which a user, who holds a digital signature of his/her GDC issued by an authority, can authenticate him/herself to a verifier by proving the knowledge of the signature without revealing it.

2. RELATED WORK

In [1], the author describes 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 multilevel 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 field bus security system validates the approach.

In [2], the author describes User identification is an important access control mechanism for client–server networking architectures. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time-synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, we propose a secure single sign-on mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks.

In [3], the author describes By exploiting a smart card, this paper presents a robust and efficient password-authenticated key agreement scheme. This paper strengthens the security of the scheme by addressing untraceability property such that any third party over the communication channel cannot tell whether or not he has seen the same (unknown) smart card twice through the authentication sessions. The proposed remedy also prevents a kind of denial of service attack found in the original scheme. High performance and other good functionalities are preserved.

In [4], the author describes Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, users' passwords are prone to be stolen and compromised under different threats and vulnerabilities. Firstly, users often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she will exploit it to gain access to more websites. Second, typing passwords into untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, keyloggers and malware. In this paper, we design a user authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. OPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms.

In [5], the author describes User authentication and key agreement is an important security primitive for creating a securely distributed information system. Additionally, user authentication and key agreement is very useful for providing identity privacy to users. In this paper, we propose a robust and efficient user authentication and key agreement scheme using smart cards. The main merits include the following: 1) the computation and communication cost is very low; 2) there is no need for any password or verification table in the server; 3) a user can freely choose and change his own password; 4) it is a nonce-based scheme that does not have a serious time-synchronization problem; 5) servers and users can authenticate each other; 6) the server can revoke a lost card and issue a new card for a user without changing his identity; 7) the privacy of users can be protected; 8) it generates a session key agreed upon by the user and the server; and 9) it can prevent the offline dictionary attack even if the secret information stored in a smart card is compromised.

In [6], the author describes The EPCglobal Network is an emerging global information architecture for supporting Radio-Frequency Identification (RFID) in supply chains. Discovery services for the EPCglobal Network are distributed services that serve the following pivotal lookup function: Given an identifier for a real-world object, e.g., an Electronic Product Code (EPC) stored on an RFID tag, they return a list of Internet addresses of services that offer additional information about the object. Since a client's information interests in the EPCglobal Network can be used to create inventory lists and profiles of his physical surroundings, as well as be used for business intelligence on the flow of goods in corporate applications, protecting client privacy becomes crucial. In particular, privacy mechanisms should by design be integrated into discovery services where the client's information interests could be analyzed by many potential adversaries. This paper introduces SHARDIS, a privacy-enhanced discovery service for RFID information based on the peer-to-peer paradigm. The idea is to enhance confidentiality of the client's query against profiling by cryptographically hashing the search EPC and by splitting and distributing the service addresses of interest. Furthermore, a probabilistic analysis of the privacy benefits of SHARDIS is presented. SHARDIS was implemented using the global research platform Planet Lab. Several performance experiments show its practical feasibility for many application areas.

In [7], the author describes The significance of radio frequency identification (RFID) security is increasing explosively, leading to a research trend. The current most severe RFID security issues are privacy and authentication security. The

renewable identity (ID) approach with a central database is the current dominating approach to achieve user privacy and authentication security. Although, the approach will cause more problems that renewable ID will increase RFID tag cost and will enable denial of service (DoS) attacks while the central database will reduce system mobility. To solve the dilemma, a new protocol with two original approaches, which are the label sharing approach to protect customer and the removable central database approach to enhance system mobility is proposed in this paper. The security properties of the new scheme are verified by using Colored Petri Net (CPN) and algebra proofs.

In [8], the author describes Although awareness is constantly rising, that industrial computer networks (in a very broad sense) can be exposed to serious cyber threats, many people still think that the same countermeasures, developed to protect general-purpose computer networks, can be effectively adopted also in those situations where a physical system is managed/controlled through some distributed Information and Communication Technology (ICT) infrastructure. Unfortunately, this is not the case, as several examples of successful attacks carried out in the last decade, and more frequently in the very recent past, have dramatically shown. Experts in this area know very well that often the peculiarities of industrial networks prevent the adoption of classical approaches to their security and, in particular, of those popular solutions that are mainly based on a detect and patch philosophy. This paper is a contribution, from the security point of view, to the assessment of the current situation of a wide class of industrial distributed computing systems. In particular, the analysis presented in this paper takes into account the process of ensuring a satisfactory degree of security for a distributed industrial system, with respect to some key elements such as the system characteristics, the current state of the art of standardization and the adoption of suitable controls (countermeasures) that can help in lowering the security risks below a predefined, acceptable threshold.

In [9], the author describes In today's globalized business world, outsourcing, joint ventures, mobile and cross-border collaborations have led to work environments distributed across multiple organizational and geographical boundaries. The new requirements of portability, configurability and interoperability of distributed device networks put forward new challenges and security risks to the system's design and implementation. This paper addresses the collaborative control issues of distributed device networks under open and dynamic environments. The security challenges of authenticity, integrity, confidentiality, and execution safety are considered as primary design constraints. By adopting policy-based network security technologies and XML processing technologies, two new modules of Secure Device Control Gateway and Security Agent are introduced into regular distributed device control networks to provide security and safety enhancing.

In [10], the author describes Public-key digital certificate has been widely used in public-key infrastructure (PKI) to provide user public key authentication. However, the public-key digital certificate itself cannot be used as a security factor to authenticate user. In this paper, we propose *the concept of generalized digital certificate (GDC)* that can be used to provide user authentication and key agreement. A GDC contains user's public information, such as the information of user's digital driver's license, the information of a digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority(CA). However, the GDC does not contain any user's public key. Since the user does not have any private and public key pair, key management in using GDC is much simpler than using public-key digital certificate. The digital signature of the GDC is used as a secret token of each user that will never be revealed to any verifier. Instead, the owner proves to the verifier that he has the knowledge of the signature by responding to the verifier's challenge. Based on this concept, we propose both discrete logarithm (DL)-based and integer factoring (IF)-based protocols that can achieve user authentication and secret key establishment.

3. ARCHITECTURE DIAGRAM

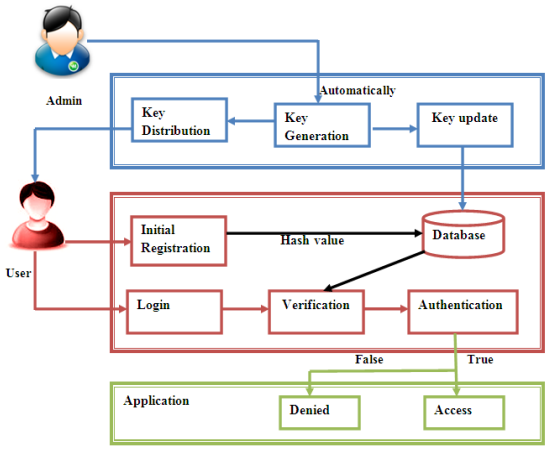

Fig 1 Architecture diagram of an efficient single sign on mechanism to enhance security

The above architecture diagram (Fig 1.) explains that implementation of single sign on mechanism to enhance security.

A. Security Requirement Module

In the security requirement module, user can enter the Initial registration for login process. After completion of Initial registration process, the user information is stored into the database as a Hash value. The Hash function value can't retrieve by the attackers. LE only needs to hold a secure key set that is stored in the security hardware and it does not need to store any authentication information of the user. When the key

lifetime is going to end, the key set generation scheme. We can see that the new PSK The key generation scheme has a one-way feature of the hash function.

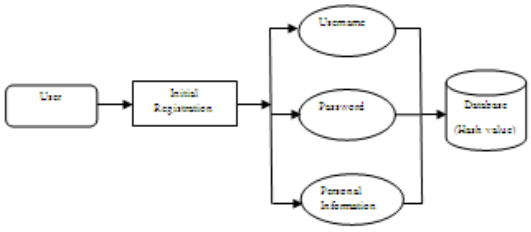

Figure 3.1 Security Requirement Module

B. Verification Information Module

In the Verification Information can be done in the login phase of the user. After successful login process, the verification can be done. The hash value retrieve from the database, compare with the original value if it is correct means enter into the system, otherwise user login process is terminated. The login procedure is the first checkpoint. The OBU will detect an error event immediately if the user has malicious intentions. When a user wants to access the service, he/she inputs IDi and PWi to the OBUi If the information is correct, the OBUi performs the general authentication procedure.

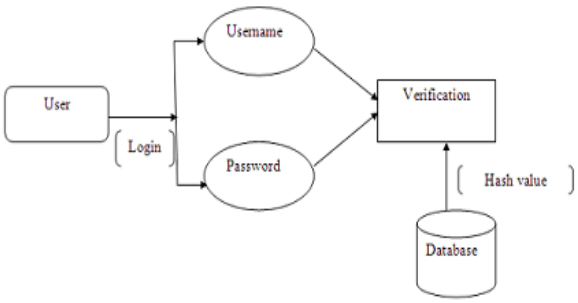

Figure 3.2 Verification Information Module

C. Trust-Extended Authentication Module

In the Trust-Extended Authentication Module, the new algorithm can be implemented for SSO scheme called as TEAM. The mutual authentication can be provided and also reliability of the system can be increased. The performance of the system can be increased by using the simple hash function and XOR operation in the system. The hash function and XOR operation will take low computation cost. The results can be generated quickly. The trust-extended mechanism based on the concept of transitive trust relationships to improve the performance of the authentication procedure. The state of a mistrustful OBU becomes trustful and then obtains an authorized parameter (i.e., PSK) when the OBU is authenticated successfully. The steps of the general authentication and the trust extended authentication procedures are the same.

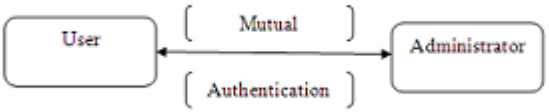

Figure 3.3 Trust Extended Authentication Module

D. Key Update Procedure

In the key update procedure, the lifetime of the key can be end means, the updation can be performed. The user of the system can use the key at a valid time. If the user want to extend the application access process means the key updation can be performed. The key generation is the automatic process, the admin can be distribute the key to user, and update the key to the database of the system. For the authentication purpose, the old key verification can be performed in the key verification process. The key update procedure is performed when the key lifetime of the TV will terminate. The key update procedure is triggered when the key lifetime is below the predefined threshold.

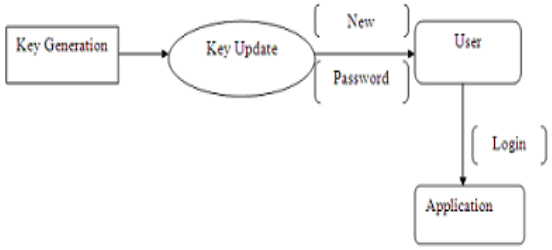

Figure 3.4 Key Update Module

E. Analysis Module

In this section, we will analyze the security of our proposed scheme. The system performance can be analyzed by the admin. The performance of the system can be monitored by the admin, generate the report for performance. It can be very high because of low computation cost and computational time of process is very low. The storage space of the content is less, because of the information can't be stored as is usual, it can be stored as a hash value. Even if an adversary intercepts a number of messages during a certain period, he cannot trace the user's physical position because the system's anonymity mechanism uses a dynamic identification process. Each vehicle needs to store the entire public key of users.

4. PERFORMANCE EVALUATION

When comparing the performance of the current single sign-on architecture to the proposed architecture, our experience is that the user does not suffer any substantial additional delays. In this section, compare the proposed and the existing schemes in terms of computational complexities and communication costs.

The following notation is used to facilitate the performance evaluation:

Tf: The time for performing a one-way hash function f

Tinv: The time for performing a modular inverse computation

Tmul: The time for performing a modular multiplication computation

Texp: The time for performing a modular exponentiation computation

KxK: the bit-length of x

Notice that the time complexities for performing the modular exponentiation, multiplication, and inverse operations are O(log3(N)), O(log2(N)), and O(log2(N)), respectively (Camenisch, 1998). Yet, the time complexity for performing the one-way hash function depends on what cryptographic primitive it employed. However, it will not influence the comparison since the numbers of executing the one-way hash function are the same for both schemes.

The comparisons between the proposed scheme and the existing scheme are stated in Table 1.

SECURITY PROPERTIES BETWEEN EXISTING AND PROPOSED

	Existing	Proposed
Mutual Authentication	✓	✓
Anonymity	✓	✓
Privacy	✓	✓
Against Denial of Service	✓	✓
Against Modification attack	x	✓
Against Replay attack	x	✓
Fast Error Detection	x	✓
Session Key agreement	✓	✓

Table 1 for Security properties

It can be seen that the proposed scheme is more efficient than the existing scheme in both the computational complexities and the communication costs.

5. COST AND FUNCTIONALITY CONSIDERATION

Low Communication and Computation Cost:

We suppose that p and n in the schemes are of 1024 bits to make the discrete logarithm and factoring problems infeasible. We suppose that the block size of secure asymmetric cryptosystems is 128 bits, and the output size of a secure one-way hash function is 128 bits.

Let EXP be the time of one exponential operation, $Hash$ be the time of one hashing operation. The major benefit of using hash function and XOR operation instead of Rivest–Shamir–Adleman (RSA) cryptosystems is the reduction of the communication cost and computation cost for low-resource devices.

6. CONCLUSION

To implement a decentralized light weight authentication scheme called TEAM to protect valid users in VANETs from malicious attacks. The amount of cryptographic calculation under TEAM was substantially less than in existing schemes because it only used an XOR operation and a hash function. Moreover, TEAM is based on the concept of transitive trust relationships to improve the performance of the authentication procedure.

REFERENCES

[1] 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.

[2] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Trans. Ind. Electron.*,vol.59,no. 1, pp. 629–637, Jan. 2012.

[3] 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.

[4] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks,"*IEEE Trans. Inf. Forensics Security*, vol.7, no. 2, pp. 651–663, Apr.2012.

[5] 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.

[6] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacy-enhanced discovery service for RFID-based product information," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp.707–718, Aug. 2012.

[7] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 689–696, Aug.2012.

[8] A.Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," *IEEE Trans. Ind. Inf.*, vol. PP, no. 99,2012, DOI 10.1109/TII/2012.2198666.

[9] Y. Xu, R. Song, L. Korba, L.Wang, W. Shen, and S. Y. T. Lang, "Distributed device networks with security constraints," *IEEE Trans. Ind.Inf.*, vol. 1, no. 4, pp. 217–225, Nov. 2005.

[10] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Trans.Wireless Commun.*, vol. 10, no. 7, pp. 2372–2379, Jul. 2011.