Remote User Authentication Schemes: A Review

Narendra Singh Panwar*, Dr. Manmohan Singh Rauthan#, Dr. Amit Agarwal$

*Department of Computer Science & Engineering, Uttarakhand Technical University, #Department of Computer Science & Engineering, HNB Garhwal University, $
Department of Computer Science & Engineering, University of Petroleum &Energy Studies, Dehradun,

Abstract: To secure the resources or information from illegitimate users various kinds of authentication schemes have been designed and developed. Some of these schemes are vulnerable to a variety of attacks. In last decade authentication schemes based on smart card has been proposed to withstand the possible attacks on verification table. Smart card provides a convenient storage and processing capability to the users. It is widely used for a range of applications such as remote user authentication, ID verification and access control. The present study gives recent developments in the area of smart card based authentication schemes and their comparative analysis. It also presents security requirements to the design and development of best authentication scheme. We have taken various authentication schemes as sample for efficiency comparisons and provide comparison results based on various operation used in respective schemes. This paper identified various security requirements which are must require in strong and efficient authentication schemes: Authentication schemes built on presented security requirements can be applied for online health care system, telecare system, Medicare system etc. for patient health care data privacy.

Keywords: remote user, authentication, security, smartcard.

I. Introduction

Remote user authentication (RUA) is a technique to securely authenticate remote users over insecure network. Authentication schemes are used before the user make use of the remote services through computer networks. A remote server is used to verify legitimacy of the users prior to access the resources from remote server. The RUA schemes are one of the critical security primitives due to the Internet's openness and lack of security concern in the Internet activities. In a networked system, when a user legitimate user requests a remote server's service, he/she must pass a user authentication process. Through this user authentication process, the server can determine either the user can make use of the provided services or not. When a user uses a service in a remote server, then the communication between the user and the server must be kept secret. They must use a session key for protecting their communications. Smart Cards are extraordinarily useful as crypto devices. A primary reason for this is that they have the quite unique ability of being capable of generating and protecting a private signing key which can never leave the card. In this paper we have carried out a comprehensive survey on some of the distinguished smart card based remote user authentication schemes.

A remote user authentication scheme with a password table was proposed and claimed that the proposed scheme is secure even though an malicious attacker has intercepted the message between a user and a remote server[1][2]. In a network environment, a remote server provide services to all the legitimate remote users. During the last decade several user authentication schemes developed with smart cards have been proposed[3-10][38-39]. Further it has been claimed that to avoid the risk of exposing the information in the secret password file of a system to illegitimate users, one should store the scrambled values f(PW) in the file for every password PW, where f is a “one-way” function, i.e. a function that is easy to evaluate but very hard to invert[11]. It has the advantage that the password files need.

A remote user authentication scheme based on ElGamal’s cryptosystem was proposed[12]. It was claimed that the scheme does not maintain any verification table and it is secure against replay attack. However, it is vulnerable to impersonation attack[13]. Further improvement were given by[14]which was also cryptanalyzed[15]. An enhanced authentication scheme was proposed to withstand impersonation attack in which login request variables are computed from $S_M$ instead of ID[16]. Additional improvement was proposed in which $S_M$ is computed instead of ID, its login request contents are $(S_M || C_{in}, C_1, C_2, T_1)$, where $C_{in} = C_3(S_M)$. An ID based scheme using RSA cryptosystem has been proposed[17]. However, it exhibit impersonation attack[13]. Further improvement has been proposed[14] which has all the merits of the previous scheme with an added trait of mutual authentication. It has been found that the scheme does not resist impersonation attack[18]. In 2004, Das et al.[19]proposed a dynamic ID-based remote user authentication scheme to prevent the risk of
Remote User Authentication Schemes: A Review

ID-theft and to resist against the impersonation attack. Das et al. scheme was cryptanalyzed and it is demonstrated that an attacker can login onto the remote server with his chosen random password[16].

A user friendly authentication scheme using one way hash function was propose[20]. It was proved that the scheme is weak against impersonation attack and then further improvement was also proposed[21]. It was pointed out that the scheme is vulnerable to guessing attack, forgery attack; to overcome these weaknesses, an improved scheme was also proposed[22]. However, due to the symmetric structure of communicating messages, this scheme does not resist reflection attack and parallel session attack. In 2009, Id-based authentication with key agreement schemes for mobile devices communication on elliptic curve cryptosystem based on pairing free, certificate less were discussed to overcome various attacks.

In 2010, Lee et al.[23] have analyzed the security of the smart card based user authentication scheme proposed by Lee et al.[21]. Their security analysis showed that Lee et al.[21] scheme does not achieve its main security goal of the two-factor security. To demonstrate this, they have shown that the scheme is vulnerable to an off-line dictionary attack in which an attacker, who has obtained the secret values stored in the user’s smart card, can easily find out its password. Besides reporting the security problem, they showed what really is causing the problem and how to fix it and proposed the scheme which improves on Lee et al.[21] scheme. In 2011, Khan et al.[24] showed that Wang et al.[25] cannot provide user anonymity because of the transmission of ID and proposed an improved dynamic ID-based remote user authentication scheme, which can provide user anonymity, mutual authentication, and session key establishment, and resist against several attacks, such as stolen-verifier, insider, DOS, replay, and parallel session attacks. Further Jenq et al.[26] show that Lee et al.[23] scheme is still vulnerable to password guessing attack, server spoofing attack and masquerade attack. Author compare the scheme with Lee et al.[23] to prove that the computation cost, security and efficiency of the proposed scheme are well suitable for practical applications in a distributed system.

In 2015, efficient and secure authenticated key agreement protocol based on elliptic curve cryptosystem for user anonymity, for UMTS network, grid network has been discussed. Novel mutual authentication scheme for session initiation protocol based on elliptic curve cryptography implemented for controlling communication on the internet was proposed by [27]and [28].Recently S Hong[29] proposes the use of a Media Access Control (MAC) as a security tool in the beginning of authentication stage and claimed that it contributes to secure the group member authentication while the MAC spoofing problem is avoided and the secure user authentication can be assured as the MAC-based authentication is being used. User authentication scheme for IoT has been proposed by Rafida et al. [30]. It was claimed that low communication overhead is required by the proposed scheme because the size of the message for authentication between user and server is too short and fulfill the properties of Zero Knowledge proof, provides solutions against various threats in network. Table 1 shows the comparison of computational cost of various authentication schemes.

<table>
<thead>
<tr>
<th>Authentication Schemes</th>
<th>Registration phase</th>
<th>Login phase</th>
<th>Authentication phase</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User end</td>
<td>Server end</td>
<td>User end</td>
</tr>
<tr>
<td>[14]</td>
<td>-</td>
<td>1H ⊕</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[16]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[17]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[18]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[19]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[20]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[21]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[22]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
<tr>
<td>[23]</td>
<td>-</td>
<td>1H</td>
<td>1H + 3H</td>
</tr>
</tbody>
</table>

II. Conclusion

A handful of user authentication schemes using biometrics and smart card have been studied in this article. It has been analyzed that the authentication and security of the schemes have been enhanced with more and more research. For security purpose, the servers are also designed not to store the password and verification tables or the biometric records in it. In order to build a strong authentication system, both the user and the server should be involved in mutual authentication and should also be properly synchronized. An ideal biometric based smart card authentication scheme is also resistant to impersonation attack, replay attack, stolen smart card attacks, server spoofing attacks, insider attacks, password guessing attacks, man-in-the-middle attacks and denial of service attacks and should conform to the perfect forward secrecy.
Remote User Authentication Schemes: A Review

Notation used in Table 1: $\oplus$: Exclusive OR operation, H: Hash function, U: User’s end, S: Remote Server’s end.

References
[32]. Kumar M. Security Analysis of a Remote User Authentication Scheme with Smart Cards. 2005. -.

www.ijesi.org
Remote User Authentication Schemes: A Review


