IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 11-13

E-Authentication Security Mode by Using Token System

Neha Sharma (PhD. Research Scholar)

Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

ABSTRACT

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge issues when this process involves the remote authentication of individual people over an open network, for the purpose of electronic government and commerce [1]. The strategy in this document assumes the authentication and transaction take place across an open network such as the Internet. In cases where the authentication and transaction take place over a controlled network, agencies may take these security controls into account as part of their risk assessment.

Keywords: Electronic, Authentication, Token, Security, password, Information, System

INTRODUCTION:

In accordance with e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet, however in some cases access to the network may be limited and access control decisions may take this into account [2].

E- Authentication begins with registration. An applicant applies to a Registration Authority (RA) to become a subscriber of a Credential Service Provider (CSP) and, as a subscriber, is issued or registers a secret, called a Token, and a credential that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

The subscriber's name may either be a verified name or a pseudonym. A verified name is associated with the identity of a real person and before an applicant can receive credentials or register a token associated with a verified name, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called identity proofing, and is performed by an RA that registers subscribers with the CSP. At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym [3]. This information assists relying parties that is parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4.

In this guidance, the party to be authenticated is called a claimant and the party verifying that identity is called a verifier. When a claimant successfully demonstrates possession and control of a token in an on-line authentication to a verifier through an authentication protocol, the verifier can verify that the clamant is the subscriber. The verifier passes on an assertion about the identity of the subscriber to the relying party. That assertion includes identity information about a subscriber, such as the subscriber name, an identifier assigned at registration, or other subscriber attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application). Where the verifier is also the relying party, the assertion may be implicit. In addition, the subscriber's identifying information may be incorporated in credentials (e.g., public key certificates) made available by the claimant [4]. The relying party can use the authenticated information provided by the verifier/CSP to make access control or authorization decisions.

Subscribers with RAs and CSPs

In the conceptual e-authentication model, a claimant in an authentication protocol is a subscriber to some CSP. At some point, an applicant registers with an RA, which verifies the identity of the applicant, typically through the presentation of paper credentials and by records in databases. This process is called identity proofing. The RA, in turn, vouches for the identity of the applicant (and possibly other verified attributes) to a CSP. The applicant then becomes a subscriber of the CSP.

Corresponding author: Neha Sharma

The CSP establishes a mechanism to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber. The CSP registers or gives the subscriber a token to be used in an authentication protocol and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful verified attribute [5]. The subscriber may be given electronic credentials to go with the token at the time of registration, or credentials may be generated later as needed. Subscribers have a duty to maintain control of their tokens and comply with the responsibilities to the CSP. The CSP maintains registration records for each subscriber to allow recovery of registration records.

There is always a relationship between the RA and CSP. In the simplest and perhaps the most common case, the RA/CSP is separate functions of the same entity [5]. However, an RA might be part of a company or organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have relationships with different CSPs as well.

Tokens used for Authentication

Tokens generically are something the claimant possesses and controls that may be used to authenticate the claimant's identity. In e-authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for e-authentication is a secret and the token must be protected [6]. The token may, for example, be a cryptographic key, that is protected by encrypting it under a password. An impostor must steal the encrypted key and learn the password to use the token.

Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

• Something you know (for example, a password)

• Something you have (for example, an ID badge or a cryptographic key)

• Something you are (for example, a voice print or other biometric)

Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key [7]. Such a device is considered to effectively provide two factor authentications, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key.

The secrets are often based on either public key pairs (asymmetric keys) or shared secrets. A public key and a related private key comprise a public key pair. The private key is used by the claimant as a token. A verifier, knowing the claimant's public key through some credential (typically a public key certificate), can use an authentication protocol to verify the claimant's identity, by proving that the claimant has control of the associated private key token [8].

Tokens that provide a higher level of assurance incorporate two or more factors. The four kinds of tokens are:

Hard Token

A hardware device that contains a protected cryptographic key. Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall:

- Require the entry of a password or a biometric to activate the authentication key;
- Not be able to export authentication keys;
- Be FIPS 140-2 validated:
- Overall validation at Level 2 or higher,
- Physical security at Level 3 or higher.

Soft Token

A cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token key shall be encrypted under a key derived from some activation data [9]. Typically, this activation data will be a password known only to the user, so a password is required to activate the token. For soft tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher, and may be either a hardware device or a software module. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

One-Time Password Device Token

A personal hardware device that generates "one time" passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by using an Approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password [10].

Password Token

A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings [11] however some systems use a number

of images that the subscriber memorizes and must identify when presented along with other similar images.

Token Threats processing

If an attacker can gain control of a token, they will be able to masquerade as the token's owner. Threats to tokens can be categorized into attacks on the three factors:

- Something may be stolen from the owner or cloned by the attacker. For example, an attacker who gains access to the owner's computer might copy a software token. A hardware token might be stolen or duplicated.
- Something you know may be disclosed to an attacker. The attacker might guess a password or PIN. Where the token is a shared secret, the attacker could gain access to the CSP or verifier and obtain the secret value [12]. An attacker may install malicious software (e.g., a keyboard logger) to capture this information. Finally, an attacker may determine the secret through off-line attacks on network traffic from an authentication attempt.
- Something you are may be replicated. An attacker may obtain a copy of the token owner's fingerprint and construct a replica.

There are several complementary strategies to mitigate these threats:

- **Multiple factors** raise the threshold for successful attacks. If an attacker needs to steal a cryptographic token and guess a password, the work factor may be too high.
- **Physical security mechanisms** may be employed to protect a stolen token from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- **Complex passwords** may reduce the likelihood of a successful guessing attack. By requiring use of long passwords that don't appear in common dictionaries, attackers may be forced to try every possible password.
- **System and Network security controls** may be employed to prevent an attacker from gaining access to a system or installing malicious software.

Conclusion

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. In accordance with e-authentication is the process of establishing confidence in user identities electronically presented to an information system.

REFERENCES:

1. Public Procurement Service (PPS), Bidder Identification and Fingerprint Registration Process, 2010, April.
2. OMB M-04-04, E-Authentication Guidance for Federal agencies, 2003, December, 16.
3. NIST, Special Publication 800-63, Electronic Authentication Guideline, 2006, April.
4. Ministry of Citizens' Services, Electronic Credential and Authentication Standard, 2010, April.
5. Bret Hartman, "From Identity Management to Authentication: Technology Evolution to Meet Cyber Threats", ITAA IdentEvent 2008.
6. Fidelity National Information Services, Multi -Factor Authentication Risk Assessment, 2006.
7. OWASP foundation, OWASP Testing Guide, 2008 v3.0, pp.140-143.
8. IETF RFC 4683, Internet X.509 Public Key Infrastructure Subject Identification Method (SIM), 2006.10.
9. Pinkas, B. & Sander, T. (2002) 'Securing Passwords Against Dictionary Attacks' *Proceedingsof the 9th ACM conference on Computer and communications security*. ACM, pp. 161-170.
10. Ray, P. P. (2012) 'Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices'. *Journal of Information Engineering and Applications*, 2 (2). pp1-11.
11. relbanks.com (2012) *Banks Around the World*. Available at: http://www.relbanks.com (Accessed: 02/4/2014).
12. Suo, X., Zhu, Y. & Owen, G. S. (2005) 'Graphical Passwords: A Survey', *Computer Security Applications Conference, 21st Annual*. 5-9 Dec. 2005. pp. 10 pp.-472.
13. Verizon (2013) *2013 Data Breach Investigations Report.* Verizon Enterprise Security Solutions.Availableat:http://www.verizonenterprise.com/resources/reports/rp_databreachinvestigations-report-2013_en_xg.pdf (Accessed: 02/04/2014).
14. Weir, C. S., Douglas, G., Richardson, T. & Jack, M. (2010) 'Usable Security: User Preferences for Authentication Methods in e-Banking and the Effects of Experience'. *Interacting with Computers*, 22 (3). pp 153-164.
15. Williamson, G. D. & Money–America's, G. (2006) 'Enhanced Authentication in online Banking'. *Journal of Economic Crime Management*, 4 (2).
16. Yampolskiy, R. V. (2007) 'User Authentication via Behavior Based Passwords', *Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island*. 4-4 May 2007. pp. 1-8.
17. Zhao, Z., Dong, Z. & Wang, Y. (2006) 'Security Analysis of a Password-based Authentication Protocol Proposed to IEEE 1363'. *Theoretical Computer Science*, 352 (1–3). pp 280-287