Indian J.Sci.Res. 17(2): 13 - 18, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A SURVEY ON CERTIFICATION SCHEMES TO STRENGTHEN THE -NETWORK SECURITY

[1]DrN Ramesh Babu, [2]DrPradosh Chandra Patnaik, [3]DrA VinayBabu
[1]Dept. of CSE, ASTRA, Chndrayangutta, Hyderabad
[2]Department of CSE, ASTRA, Chndrayangutta, Hyderabad
[3]Rtd. Professor of CSE & Principal, JNTU, Hyderabad.

Abstract
In the current scenario putting the various data into the network and the internet for communication or sharing the information over internet influencing high risk security in various ways. To deploy all types of secured platform in the networks, a Secure Network Design Architecture is needed. Among the various security domains, Network Security is of a major concern. The dynamic fluctuations in the behavior of Networks, yields a wide range of attacks those open doors for the bogus users to exploit the resources, illegitimately. Certification is the possible first-line of defense in any Networks for one entity to confirm its communicator to be legal. This Survey explains the various Certification Schemes that are being practiced. The methodologies of the certification schemes are discussed, their success and failures are studied and the various attacks that break them are traced.

Keywords—Network Security, Certification, Types ofCertification, Security Attacks.

I.Introduction

As the technologies are flourishing in the current era, there is a great desire among this generation people to learn and to master these technologies. Especially the technologies in the field of computing is growing exponentially because a large number of researchers and graduates are working in and developing this field. The major tool that has ignited the surge of this knowledge hunt is the Internet. Not just in the field of computing, but this Internet has its part in every fields that are existing. This communication and the money transactions makes security the major requirement. All who use internet for communication, money transaction and for many other services are in need of Privacy, Confidentiality and Availability. These criteria can be achieved only when the permissions are given to the users, to access the resources or to use the applications, by verifying their identity that is previously registered with the server. As the usage of internet communication and transactions are increasing one side, on the other side the threats are also increasing considerably. In the view of diagnosing these threats and attacks, we ended up in finding out five different Security Domains. They are Network Security, Device Security, Data Security, Application Security and Security Assurance.[1,2]

Effective Network Security can be achieved and maintained, only if the Network Architecture that is enforced is efficient enough to handle the dynamic fluctuations in the Networks. Because the intruders or the attackers always look for a connection between two systems that is idle, not needed and a feeble security filters. Over a considerable period of time many researchers working in Network Security domain and have come out with many and various results which has bettered the security issues.[3] The research has also given us the insight into various possible attacks that can interrupt the communication over the Internet. Denial-of-Service Attack, Identity Spoofing, Man-in-the-Middle Attack, Eavesdropping, Data Modification, Password-Based Attacks, Sniffer Attack, Replay Attack are some of the well-known Network Attacks. All these attacks are directed in finding a weak link in the firewalls, routers and switches. The attackers use these loop holes in the network devices to gain the access to the networks and perform their malicious transactions or communications. Many techniques have been proved to be improving and enhancing the security step by step.

Overview of Certification Schemes and Techniques

The basic security concepts include Confidentiality, Integrity, Certification, Authorization, Availability and Non Repudiation. One of the most important and traditional way of identifying the right user, in the Internet communications, is the use of Certification Techniques. Certification is a technique that is used to confirm whether the source of the request or access to a particular application or data is legitimate or bogus. There are various certification schemes that are being used in the current information technology scenario. Some of them are listed as Password-Based Certification, Certificate Based Certification, Identity-Based Certification, SSL-Based Certification, Biometric-Based Certification etc. There are various researches being done in all the above Certification schemes and much advancementare proposed, proving

[1]Corresponding Author

each methods to be secure and successful. This survey explains the various methodologies that are being used by the Certification Techniques and a comparative study of their efficiency in security.

Certification is one of the major techniques that is carried out to enhance the security of the Networks. Thecertification alone does not fulfill or accomplish the entire Network Security. But the various certification schemes that are followed, adds to the security. In this survey the six certification techniques discussed are Password-Based Certification, Certificate-Based Certification, Identity-Based Certification SSL-Based Certification, Biometric-Based Certificationand Multi-Factor Certification. One of the oldest and the most widely used certification scheme is the Password-Based certification. In this password-based certification the client authenticates itself to the server by providing the secret password that is known only to the client and which is registered with the server during the first phase of the communication called the Registration. This password based certification is the simplest way of authenticating a client with the server to which it is communicating. Thiscertification technique is light and it doesn't carry any overhead while being performed. Explaining the simple concept of certification, it can be said that the client has a unique username and a password associated with thatusername. This username and the password are registered and stored in the database of the server in a table. Once the client tries to authenticate itself to the server it provides its username and the password to the serverthrough any user interface or the web applications provided by the server itself.

Fig. 1: Password Based Certification

This simplest way of certification also suffers many attacks and intrusions. These malicious happeningsdegrade the advantages of this certification technique. Some of theattacks thatarepossiblecertification includes Phishing Attacks, Replay Attacks[1], Server Spoofing Attacks, Eaves Dropping Attacks,

Impersonation Attacks, Off-line Password Guessing Attacks [2], Denial –of-Service Attacks, Stolen-Verifier Attacks, Parallel Session Attacks, Insider Attacks [3] and Many Logged-In Users' Account. These attacks have drawn the attention of the researchers to develop new and promising protocols and techniques that would eradicate the flaws in the Password certification**.**

Lamport et al. [4] suggested an idea involving hash-based password certification scheme to mutually authenticate the client and the server. This scheme proved to be advantageous over eavesdropping and impersonation attacks. But this hash-based scheme failed to be immune to replay attacks. And the next great disadvantage is this that the hash computation in this technique is high. Peyravian and Zunic [5] delivered a new way of password certification and also password changing protocol using Collision Resistant one way hash function. This technique did not include encryption techniques.

The advantages of this proposal was, the proposal proved to be simple and straightforward, involving only one hash function. Even then this method suffers off-line password guessing attacks. Hwang and Yeh [6] worked on [5] and found that it is vulnerable to password guessing attack, eavesdropping attack and server spoofing attack. Then an improvement was made to it by adding Public Key Cryptosystem. Though this improvement achieves mutual certification, it suffers replay attacks [7]. Chang et al.

Certificate Based Certification

The Certificates are the most common form of trusted certification between the parties dispersed all over the world and communication through the World Wide Web15].A unique name and the corresponding public key are the parts of a Digital Certificate. The certificate might not look complex, but there's a great deal in this certificate generation because the certificates generated should be unique and unalterable. There are many issuers of this certificate. These issuersare called the Certificate Authorities (CA). The CAs are the trusted third parties who will sign the certificatesdigitally. The process of making and issuing this certificate is this that the document uses the digital signature to bind the public key with a unique identity of the document. The other

party that receives the certificate confirms that the public key belongs to a particular individual. There are certificates that are signed by certificate authorities and also the certificates that are self-signed. The public key infrastructure scheme uses the certificates signed by the CAs and the web of trust scheme uses the certificates that are self-signed or signed by other user. The various types of the certificates are Client SSL certificates, Server SSLcertificates, S/MIME certificates, Object-Signing certificates, CA certificates. A typical X.509 Digital Certificatewhich is widely used contains the followingfields. The Serial Number that uniquely identifies the Certificate, the subject that is the person or the entityidentified, the Signature Algorithm that is used to create the signature, the Signature which proves that the data or the document is originally from the issuer, the date of issuing and the date of expiry of the certificate that denotes the life of a certificate and it contains the public key and the algorithm used to hash the public key.

A large number of people provide their personal information and their banking details in their own personalaccounts of many social networking sites and banking sites respectively. So to have the details of the users safe and protected the network security has to be confirmed by the user. In password based certification the user provides his unique username and password to the server through a webpage. But this has resulted in a problem that the malicious users creates a web interface similar to that of the actual server and pretends to be the original. So the user provides their secret information through the false interface. And through this the attacker gets to know the secret details of the user. This attack is called “Phishing” [16]. This attack can be prevented by the usage of certificates to authenticate the user and the server mutually. The trusted third party, Certificate Authority (CA) [17] provides each certificates to the server and the client which is unique and unalterable. And every user trusts the server by the certificate that it holds and communicates with it confidently.

Comparing the passwords the certificates prove to be advantageous in some aspects. The password suffers a lot from the Brute Force attack which by trying all the possible random combinations try to figure out the actual combination. This sometimes consumes a lot of time, in case of strong password, but still it is breakable. But in this case the certificates are non-breakable towards the Brute Force Attack. When compared to the SSH publickeys, the public keys doesn’t know the identity of the user. The server should already have the names of the user registered with their corresponding public keys. But in certificates there is no need for this pre-registration, because the certificates have theseinformation integrated to it. Some fields where this certificates find its major advantages are Communication Security, Online Banking and E-Commerce.

Yi et al. proposed an optimized protocol for mobile networks with security and certification based on certificates. This method enjoys the advantages of simpler algebraic computation and a lesser storage area. In this method [YOL protocol], the mutual certification and the key distribution between the mobile user and the base station is easy. But the certificates suffer replay attacks, in here. Another method using the timestamp is proposed to prevent the replay attack, but proved to be a failure [18-19]. Then again an improvementto the YOL protocol is proposed [20]. This protocol ensures the certification and privacy on mobile communications. This prevents the replay or forging attack. MagyariAttilla et al. proposed a new certificate based single sign-on mechanism. In this middleware a new feature is added, which is the XPCOM components, a service that can be used on any platform that supports Mozilla Firefox.

[8] proposed a symmetric key cryptosystem that would strengthen the password certification, but the issue was the burden that the symmetric key cryptosystem causes on the client side. Zhu et al. [9] suggested an advanced scheme by using public key encryption/ decryption. This also involved time stamp and salting techniques. A hardware called Trusted Platform Model [TMP] was used which stores the salt file in client’s hard disk. Irrespective of the advantagesthe TPM it suffers serious clock synchronization problem. Recent trends have given us the Smart Card-based certificationschemes [10] in remote login. The advantage of this system is that the client and server can be authenticated by using a small memorable password and also without maintaining a password-verifier table. But this also is vulnerableto offline password guessing attacks [11], DoS attacks [12] and Replay attacks [13]. Hafizul and Biswas [14] proposed an Elliptical Curve Cryptography based password certification. The advantages that this techniques holds is that it prevents replay attacks, password guessing attacks, impersonation attacks, DoS attacks, many logged-in users’ attack, server spoofing attack, perfect forward secrecy and insider attack.

Identity Based Certification

The security issues in the cloud computing has pulled the attention of the researchers in recent times. When analyzing the security issues, they found Identity-Based Cryptography (IBC), a variant of the public key cryptosystem. In this method, the unique identifier that represents the user is the public key of that particular user. And it can be used without any certification check. This type if identity based certification best suits the Cloud Computing scenario, because the entities are greatly flexible in the security infrastructure and also they are certificate free. Another advantage over the

traditional PKI is this that IBC is light and the keys are used flexible and easy management of keys than by the PKI. Hongwei Li et al. proposed a Hierarchical Architecture for Cloud Computing with the characters like light weight and small key size. This system used Identity Based Encryption and Identity BasedSignature for cloud computing which resulted in a protocol called Certification Protocol for Cloud Computing (APCC). When compared to SLL Certification Protocol, APCC is efficient and light weight and certificate free. Another great advantage is its Scalability which suits it best for the cloud computing. Some application problems like the problem of identity based encrypted e-mail is solved by the framework proposed for constructing identity based and broadcast encryption systems, by Boneh et al. [21]. In the grid systems to improve the user side performance, Mao et al.[22] proposed an identity based non-interactive certification framework.

Fig 2: Smart Card Based Certification

One of the major identity based certification scheme is the Smart Card based certification. Smart cards are typically a small, handy plastic cards in which a small memory or a microprocessor is embedded. This memory contains a value or information that are used by the smart cards when the cards are inserted in to a card reader. There are a lot of fields in which the smart cards are in use likehealthcare, banking, entertainment, transportation and many other. The smart cards improve the convenience and the security of the transactions. In the smart card based systems, the data are maintained highly secured because the secret information are neither stored in a system nor is copied in any disk. So the chance ofcopying the secret data is less and eradicated almost. Also the secret is always carried with the user and no chance of misusing is available. This system protects the user from a range of security threats including careless storage of passwords and many other. Also the cost spent on managing the passwords and resetting them is very high. And the smartcard systems prove to be advantageous than these. The smart cards are also used in remote login. In the Smart card based certification scheme by using password, proposed by Shiuh-Jeng Wang [23], the password verification tables are not used. Because it uses the public key system's signature property. This method proved to be secure in point of factoring the large number and in the discrete logarithmic problem.

The smartcard based security mechanisms have two types of technology. Contact card technology and Contactlesscard technology. Some of the security issues in the contactless cards are Eavesdropping, Interruption ofOperations, Denial of Service, Covert Transactions, Communication Links and Dual Modes.

Transport Layer Security (TLS) and its predecessor Secure Socket Layer (SSL) are standard protocols for security by establishing a secure channel between the communication entities. Any sensitive data being sent are sent through the secure channel. This SSL based certification is performed mostly by using certificates. The SSL certificate has a key pair and a subject. This pair of keys work together to form a secure channel and the subject describes the identity of the website owner or the certificate owner. The main thing in this SSL certificate certification is this that the trusted CA should sign it digitally. There are self-signed certificates also available. So anyone can create a certificate. So the browsers were designed to accept the certificates that are signed only by the trusted CAs. The SSL secure channel is laid by SSL handshake. This is invisible to the user. In this handshake mechanism the client requests the server's certificate and the server sends its certificate to the client and it verifies the certificate and client verification is optional in many case. Once the server is verified to be the right one, the client and the server exchange their cipher specifications. The type of key used, the encryption method used and the way of communication that are going to be followed in that session is mutually exchanged between the client and the server in this exchange. So they have laid a secure channel. These certificates, though beneficial, have some short comings. The certificate authority can be a fraudulent one and if so, the whole scenario will be open to attacks. Also getting a digital signature from the CA is costly. And the processing overhead also is high. The password based SSL is proposed by Michel Abdalla et al. that avoids the need of a certificate authority. We use passwords during the handshake and exchange the secret details securely. They don't just exchange the common secret key directly. They derive the secret key for encryption through the exchanged information. The following are the steps involved in the SSL handshake:

Biometric Based Certification

Whenever new security ideas are proposed, sooner they also become susceptible to attacks. Also the researchers, on the other side are not tired in finding out new techniques to provide a strong security. This resulted in a new technology called the Biometrics. Biometrics is the technology in which the biological trait of a user is extracted and is used to verify the identity if the user. Some of the often used biometric traits are Fingerprints, Iris Pattern, DNA Strand, Voice Pattern and Keystroke Pattern. Biometric falls under the Physiological-Based or Behavior-Based certification techniques [25]. The physiological traits includes stable human characteristics like fingerprint, shape and geometry of face, fingers, hands and ears, pattern of veins, iris, teeth and DNA samples. The behavioral trait includes the rate of moving, voice, key-stroke and signature dynamics. The biometrics finds its application in many fields. Forensic Applications, Government Applications, Commercial Applications categorizes the biometric applications. An application involved in criminal investigations comes under Forensic Applications. Government applications include passport verification, border and immigration control, voter registration and e-Government. Commercial applications like network logins, e-Commerce, ATMs, Mobile Phones and many more.These biometrics are mainly used in certification techniques because they are always with the user and it is unforgettable and cannot be lost. Biometricsare also vulnerable to many attacks. Some of the possible attacks are Client Attack, Host Attack, Eavesdropping, Theft and Copying, Replay Attack, Trojan Horse Attack, Denial of Service Attack and Non-Repudiation Attack [26]. Client attack can be prevented by using large entropy and by providing limited attempts. Host attack can be prevented by the Capture device certification. Eavesdropping, Theft and Copying can be prevented by Copy-detection in the capture devices and Capture device certification. Capture device certification via challenge-response protocol is helpful in preventing Replay attack.

All the security mechanisms have some or the other breaches in their working. So a new way sprung forth from the researchers. This included the Multi-Factor Certification. In this technique, two or more security factors are combined to bring forth an enhancement in security. Goumin Yang, Duncan S. Yong [27] proposed a multifactor certification using passwords and smart cards. They analyzed the security requirements and developed a generic construction framework for smart-card-based password certification. D.Pugazhenthi [28] proposed a new technique that adds to the multi-factor certification. Use of multi-biometric security for the cloud computing is suggested. Multiple biometric fingerprints are extracted from the user during enrollment and then the templates are stored in the cloud provider's end. And also the fingerprint templates and the images provided every time are encrypted for the enhanced security.

CONCLUSION

This review includes various certification schemes and their application methodology. It explains various advancements made in those certification schemes and their success in providing security to the user. It also lists out the possible attacks on these schemes of certification. The methods that are proposed to protect the system from the attacks are also discussed.

REFERENCES

[1] GaganDua, NitinGautham, Dharmendar Sharma, Ankit Arora, "Replay Attack Prevention in Kerberos Certification Protocol Using Triple Password" International Journal of Computer Networks & Communication (IJCNC) vol. 5, pp. 59-70, March 2013.

[2] Cheng-Chi Lee, Chia-Hsin Liu, Min-Shiang Hwang, "Guessing Attacks on Strong-Password Certification Protocol" International Journal of Network Security, vol. 15, pp. 64-67, January 2013.

[3] E. Eugene Schultz, "A Framework for Understanding and Predicting Insider Attacks" Elsevier Science Ltd, October 2002. L. Lamport, "Password certification with insecure communication" Communications of the ACM, vol. 24, pp. 770–772, 1981

[5] Y.F. Chang, C.C. Chang, Y.L. Liu, "Password certification without the server public key" IEICE Transactions on Communications, E87-B pp. 3088–3091, 2004.

[6] L. Zhu, S. Yu, X. Zhang, "Improvement upon mutual password certification scheme" International seminar on business and information management, pp. 400–403, 2008.

[7] Y.L. Jia, A.M. Jhou, M.X. Gao, "A new mutual certification scheme based on nonce and smartcards" Computer Communications, vol. 31, pp. 2205–2209, 2008.

[8] X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan, "Cryptanalysis and improvement on two efficient remote user certification scheme using smart cards" Computer Standards and Interfaces, vol. 29, pp. 507–512, 2007.

[9] H.C. Hsiang, W.K. Shih, "Weaknesses and improvements of the Yoon–Ryu–Yoo remote user certification scheme

using smart cards" Computer Communications vol. 32, pp. 649– 652, 2009.

[10] T. Xiang, K.W. Wong, X. Liao, "Cryptanalysis of a password certification scheme over insecure networks" Journal of

Computer and System Sciences, vol. 74, pp. 657–661, 2008.

[11] SK Hafizul Islam, G,P, Biswas, "Design of Improved

Password Certification and Update Scheme Based on

Elliptic Curve Cryptography" Mathematical and Computer Modelling, vol. 57, pp. 2703-2717, 2013.

[12] SunExpert Magazine, June 1997.

[13] R. Gowtham, IlangoKrishnamurthi, "A Comprehensive and Efficacious Architecture for Detecting Phishing Webpages"

Computer and Security, vol. 40, pp. 23-37, 2014.

[14] Lidong Zhou, Fred B. Schneider, Robbert Van Renesse

"COCA: A Secure Distributed Online Certification Authority" ACM Transactions on Computer Systems, vol. 20, pp. 329-368, November 2002.

[15] M.S. Hwang, Y.L. Tang, C.C. Lee, "A new protocol using time-stamp for mobile network certification and security"

Technical Report (CYUT-IM-TR-2000-01), Department of Information Management, Chaoyang University of Technology, Taiwan, November 2001.

[16] D. S. Wong, "An optimized certification protocol for mobile network reconsidered," ACM Mobile Computing and

Communications Review, vol. 6, pp. 74–76, 2002.

[17] Cheng-Chi Lee, I-En Liao, Min-Shiang Hwang, "An Extended Certificate-Based Certification and Security

Protocol for Mobile Networks" ISSN 1392 – 124X Information Technology and Control, vol. 38, pp. 61-66, 2009.

[18] D. Boneh, "Generalized Identity Based and Broadcast Encryption Schemes" Lecture Notes of Computer Science (LNCS), vol. 5350, pp. 455-470, 2008.

[19] W. B. Mao, "An Identity-Based Non-interactive

Certification Framework for Computational Grids" http://www.hpl.hp.com/ techreports/2004/HPL-2004-96.pdf, 2004.

[20] Shiuh-Jeng Wang, Jin-Fu Chang, "Smart Card Based Secure

Password Certification Scheme" Computer and Security, vol. 15, pp. 231-237, 1996.

[21] Michel Abdalla, Emmanuel Bresson, Olivier Chevassut,

Bodo Moller, David Pointcheval, "Strong Password-Based Certification in TLS using the Three-Party Group Diffie-

Hellman Protocol" International Journal of Security and Networks, vol. 2, pp. 284-296, 2007.

[22] "Biometrics and Standards", December 2009

[23] Lawrence O. Gorman, "Comparing Passwords, Tokens and Biometrics for User Certification" Proceedings of the IEEE, vol. 91, pp. 2019-2040, December 2003.

[24] Guomin Yang, Duncan S. Wong, Huaxiong Wang, Xiaotie Deng, "Two-Factor Mutual Certification Based on Smart

Cards and Passwords" Journal of Compuer and System Sciences, vol. 74, pp. 1160-1172, 2008.