User authentication in securing communication using Digital Certificate and public key infrastructure

Usman Abubakar Idris¹, Jamilu Awwalu², Buhari kamíl³,

¹Faculty of Computing and Applied Science, Baze University Abuja, Nigeria

Abstract — Security threats are becoming more issues of concern for e-commerce, financial institution to cloud computing and network application. These papers introduce an application of user authentication which combine Digital Certificate (DC) and Public Key Infrastructure (PKI), including securing electronic transaction and data flow control. The main purpose of this paper is to solve the problems of transferring data across the network, such as phishing, eavesdropping, snooping, sniffing, modification and masquerading. Keywords — digital certificate, Public key infrastructure (PKI), authentication.

I. INTRODUCTION

Information Technology has become a component of our daily livelihood and imagine living without not technology services. Bank could not process internet or network payment, governments can transform their services to E-Government such as transparent revenue generation and tax collection, or even electronic voting systems. There have been tremendous efforts with the assistance of technology and the internet that has turn world to a global village, if we much use technology, we have to ensure their safety. This paper focus on secure transaction for user authentications using digital certificate, certificate key stores, certificate revocation lists, Socket Secure Layer (SSL), and public key infrastructure in securing internet transactions. There are software tools that allows users to understand these aspects of data security.

Digital certificates offer a process and steps to authenticate and secure internet transactions on open and closed networks. Digital certificates are used in securing emails, internet and mobile banking transaction, smart card authentication, file transfers and signing of digital software files. [1] Digital certificate operate the way E-passport works. Passport are issued by countries to their citizen while digital certificate are issued by certificate authorities. The passport provides the way to verify your identity as the real owner and gain entry to your destination. Likewise Digital certificates provide similar identification within the electronic world. The role of the certificate authority is to validate the certificate holder’s identity and to “sign” the certificate in order that it cannot be tampered with. Once a certificate authority has signed a certificate, the holder will pass their certificate to others, websites and network resources to prove their identity and establish encrypted, confidential communications. [2] Public Key Infrastructure or PKI technology is part of Digital Certificates described as virtual ID cards.

II. HOW IS DIGITAL CERTIFICATES ARE CREATED

A company have to register to purchase software and hardware from Certification Authority to setup and issue the certificates. The company have to develop a directory to provide data about the certificate holders and verification structure and security policies from the Certification Authority. The security policy is to identify who receives the identification card and those policies are applied to individuals using a certificate. However identification of individual is done by the Certification Authority, also how software and hardware components are integrated and managed, and how the certificates are manage over their period of time.

Types of Digital Certificates

There are four (4) different classification of digital certificates and each serves different purposes and functions. Also they operate in web browsers:

- Authority or Root Certificates: The authority certificate make it the root of a certification hierarchy, like Thawte. These certificates don't need to be signed by another 3rd party Certificate Authority —they are self-signed by the CA that created them. Once a certificate is self-signed, it shows the name of the institution that authorize it.
- Institutional Authority Certificates: These certificates are also called Campus Certificates. They are signed by a 3rd party Certificate Authority to verifying the authenticity of a campus certification. Campuses then use their “authority” to issue client certificates for faculty, staff, and students. [9]
- Client Certificates: These are called end-User certificates, identity certificates, or personal certificates. [9]
- Web Server Certificates: These certificates are meant for secure communications over internet, for instance making online purchase using credit / debit cards and prevent credit card theft and keeping your account information secure. They’re referred to as server-side certificates after obtaining Socket secure layer for your online purchase on the internet.

III.RELATED WORKED

User authentication have two key principal service institution that secure communications over the internet. Research is ongoing in these two areas.

A. Public Key Cryptography

The technology behind Public Key Cryptography was developed by Diffie and Hellman in 1976[9]. The Public Key Infrastructure (PKI) system is made of two pair of Keys mainly the Public Key and the Private Key. Both Public and Private Keys are similar and unique, there corresponding algorithms between the Public Key and the Private Key generated method that was irreversible and the Private Key could not be figured out from the Public Key practically (Security). Public key encryption generates keys that encrypt plaintext file into blocks of 64 bytes (as a 1024-bit key is generated) and this will undergo the process whereby a secret message needs to be sent from the public domain for the user to decrypt it. [11]

The principles of public key cryptography are illustrated below.

![Image](http://www.ijcttjournal.org)

**Figure 1:** Bob send an email to Alice by encrypting the email using Alice's public key. Only Alice have access decrypt the email even if other users receive it.

Bob have to make sure Alice receive the email, the email not been altered, modify or tempted and authenticate that Alice is the actual recipient. For Bob to sent an email to Alice, it has to create a hash algorithm as a plain text message and to cypher this hash function using non-public key. Bob needs to send his private encrypted hash and public encrypted message to Alice.

After both private and public hash algorithm is received, then Alice will rewrite the message of his personal key and regenerate the hash message. Alice will be able to add and rewrite the encrypted hash message of Bob's public key then compare the 2 hash values therefore authenticating that Bob sent the message and confirming the integrity and confidentiality of the message.

Authentication is only performed when a session is established and unstable executed task. However, authentication must be performed rapidly so that the user does not experience any undue latency. In fact in the BITW system described below authentication was not implemented and secure session keys were hard wired so as to minimise the software development. [9]

Advantages:

- Privacy policy and data confidentiality (eavesdropping) and data Integrity problems
- Public key Authorization - only key holders can participate
- One time password - only one key to generate
- Encrypting and decrypting for fast, efficient algorithms

Disadvantages:

- Problem Key distribution of the secret key to Alice and Bill.
- It’s no longer a secret, If everyone knows the Key. [11]

Public-key cryptography and connected standards underlie the protection options of the many products like signed and encrypted email, single sign-on, and Secure Sockets Layer (SSL) communications.

The Internet traffic passes information through various network device and computers, and can be intercepted by third parties such as:

- Eavesdropping: Information remains intact; however its privacy is compromised. For instance, somebody might gather MasterCard numbers, record a sensitive spoken communication, or intercept classified info.
- Tampering Information in transit is modified or replaced then sent to the recipient. As an example, somebody may alter an order for goods or change a person’s resume.
- Impersonation. Information passes to an individual who poses as the as the real owner. Impersonation can take two forms:
  - Spoofing. A person can assume to be someone else. For example, a person can assume to have the email address or a computer can falsely identify itself as a site called www.example.net.
  - Misrepresentation. A person or company can misrepresent itself. For example, a site called www.cyber.com can pose to be an on-line store when it really receives credit-card payments but never sends any goods.
Public-key cryptography provides protection through:

- Encryption and decryption allow two communicating parties to disguise information they send to each other. The sender encrypts and scrambles information and the receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is feasible to an intruder.
- Data which has been detected allows the receiver of information to verify that it has not been modified in transit. Any modification or substitute data are detected.
- Authentication allows the recipient of the data to determine its source by confirming the source identity.
- Nonrepudiation prevents the source of data from claiming at a later date that the information was never sent. [12]

B. Digital Certificate

The digital certificate, as a passport when communicating, is issued by a third party, the Certification Authority (CA), and usually used to identify and verify the end entity. [8] Asymmetric key pairs are used to sign and verify a plaintext file. For this purpose, a hash of the plaintext file is created using MD5. This hash is then encrypted via RSA using the private key to generate a digital signature. [11]

Using a Digital Signature to Validate Data Integrity as shown in figure 2 illustrates the way a digital signature can be used to validate the integrity of signed data.

Figure 2: Using a Digital Signature to Validate Data Integrity

Figure 2 shows two transfers to the recipient of some signed information: the first data and also the digital signature, that may be a unidirectional hash of the first information encrypted with the signer's personal key. To validate the integrity of the information, the receiving code initial uses the general public key to rewrite the hash. It then uses identical hashing formula that generated the first hash to get a replacement unidirectional hash of identical information. Finally, the receiving code compares the new hash against the first hash. If the 2 hashes match, the information has not modified since it had been signed. If they are doing not match, the information might be tampered with since it had been signed, or the signature might be created with a personal key that doesn't correspond to the general public key assigned by the signer.

If the 2 hashes match, the recipient may be sure that the general public key accustomed rewrite the digital signature corresponds to the non-public key accustomed produce the digital signature. Confirming the identity of the signer jointly needs how of confirming that the general public key belongs to a selected entity. A digital signature is comparable to a written signature. Once knowledge are signed, it's tough to deny doing thus later, presumptuous the non-public key has not been compromised. This quality of digital signatures provides a high degree of non-repudiation; digital signatures build it tough for the signer to deny having signed the info. In some things, a digital signature is as wrongfully binding as a written signature. [12]

IV. EFFECTS OF PUBLIC KEY CRYPTOGRAPHY

The following direct results may be expected from implementing a PKI solution:

- The flexibility to verify the identity of the opposite party over the network.
- The flexibility to verify the believability of knowledge (that it's not been falsified).

Despite these advantages, the speed of adoption continues to be quite low. A number of the explanations are needed for this operation and therefore the problem in understanding the technology, quantifying the profit fits, and creating the desired investment selections (it is troublesome to inspire adoption of the technology).

However, from a unique perspective, the following secondary advantages can even be achieved:

- The intentions of the party manufacturing the knowledge may be verified.
- The security of the info may be bonded (falsification may be detected) over long periods.

With the previous, responsibility for the content of messages or digital info on the network will be clearly established through language, that addresses the requirement to assign social responsibility (for governments, money establishments, industry, politicians, doctors, architects, etc.) or responsibility in trade or for creating specific statements (auctions, social networking services, etc.) and additionally to preventing unauthorized activity, PKI has the additional advantage of elucidative responsibility during this approach. In fact, some financial establishments have really begun the observe of language transmitted info (email preventing falsification at any later date. the requirement for digital language, and corresponding timestamp technology, is predicted to extend as conversion
progresses and therefore the quantity of digital information that has to be safely maintained and keep over longer periods of your time will increase. The language of documents and logs is one potential technique of providing the proof needed to implement internal controls supported by the Japanese version of SOX legislation.

Finally, if the safety and security of services offered can be demonstrated by having each element in the network (users, servers, nodes, terminals, mobile phones, information appliances, etc.) certified, this should be a factor in attracting users to these services.

V. DISCUSSION

Advantages of using public key cryptography reduces the struggles in key management as a result of one key trying to take the place of other symmetrical keys. Advancement in digital certificates permit the use of distributed and manage public keys. Digital certificates don’t seem to be self-managing. The design of digital certificates requires wide circulation, therefore the management of those certificates should address the distributed nature of digital certificates. Digital certificates need an infrastructure to manage the certificates keys within the context planning to be used. Public key infrastructure (PKI) is separable from digital certificates. PKI is liaises for issuing certificates, making distribution of those certificates through a path, and validatory certificates. PKI is liable for the underlying work that supports digital certificates and allows them to produce the capabilities that serves.

VI. CONCLUSIONS

For a digital certificate to be managed, it’s to be structured in an obvious and reliable means in order that the knowledge in the certificates are often simply retrieved and understood. For instance, passports follow structure permitting people to simply perceive the knowledge in a way that they never have seen before as long as digital certificates area unit are standardized, they will be scanned and understood not withstanding who issued the certificate.

REFERENCES