International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

MULTI-FACTOR AUTHENTICATION TECHNIQUES USING BIBA ONE-TIME SIGNATURE

C. Divya* & K. Ramamoorthy**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Network Security issues are now becoming important as society is moving to digital information age. Data security is the utmost critical component in ensuring safe transmission of information through the internet. It comprises authorization of access to information in a network, controlled by the network administrator. The task of Network security not only requires ensuring the security of end systems but of the entire network. Authentication is one of the primary and most commonly ways of ascertaining and ensuring security in the network. In this paper, an attempt has been made to analyze the various authentication techniques such as Knowledge-based, Token-based and Biometric-based etc. Furthermore, we consider multi-factor authentications by choosing a combination of above techniques and try to compare them. We introduce the BiBa signature scheme, a new signatureconstruction that uses one-way functions without trapdoors. BiBa features a low verification overhead and a relatively small signature size. In comparison to other one-way function based signature schemes, BiBa has smaller signatures and is at least twice as fast to verify (which probably makesit one of the fastest signature scheme to date for verification).One of the main challenges of securing broadcast communicationis source authentication, which allows all receiversto verify the origin of the data. An ideal broadcast authenticationprotocol should be efficient for the sender andthe receiver, have a small communication overhead, allowthe receiver to authenticate each individual packet, provideperfect robustness to packet loss, scale to large numbers ofreceivers, and provide instant authentication (no bufferingof data at the sender or receiver side). We gratefullyacknowledge funding support for this research.Permission to make digital or hard copies of all or part of this work forpersonal or classroom use is granted without fee provided that copies arenot made or distributed for profit or commercial advantage and that copiesbear this notice and the full citation on the first page.

Key Words: Broadcast Authentication, Source Authentication for Multicast, One-Time Signature & Signature Based On a One-Way Function without Trapdoor

Introduction:

In this digital era more and more people becoming active on the Internet for their personal and professional, because of this internet is growing rapidly. But, along with the evolution of Networking and Internet, several threats such as Denial-of-Service (DOS) attacks and Trojan Horses have also risen drastically. So the task of securing the Internet or even the Local Area Networks is now at the forefront of computer network related issues. Being on public network, serious security threats can be posed to an individual's personal information and also to the resources of companies and government. Providing confidentiality, maintaining integrity and assuring the availability of correct information are the primary objectives. These threats are primarily present due to the ignorance shown by the users, weak technology and poor design of the network. Sometimes there are many network services that are enabled by

default in a personal computer or a router. Out of which many services may not be necessary and may be used by an attacker for information gathering. So it is better to disable these unwanted services to protect them from hackers and crackers More importantly, not only need to be concerned regarding the security at each end of the network rather the focus should be on securing the entire network.
While developing a secure network, the following need to be considered:

- ✓ Access – Only authorized users are allowed to communicate to and from a particular network.
- ✓ Authentication – This ensures that the users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.
- ✓ Confidentiality – Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.
- ✓ Integrity – This ensures that the message has not been changed during transmission.

For the past 25 years researchers have created and refineddigital signature schemes using one-way functions withouttrapdoors. These signaturesschemes are efficient for signature generation and verification, but the signatures are too large for many applications. We propose the BiBa signature, a new approach for signaturesbased on one-way functions without trapdoor. Thesignature size of our scheme is much smaller than most previoussignatures based on one-way functions; and the verification is also more efficient. However, our public keys arelarger than most previous systems, and the time to generatesignatures is also higher.Our new signature scheme immediately yields importantnew applications. In particular, we extend the BiBa signature scheme to design a newprotocol for authenticatingbroadcasts, such as streaming information broadcast overthe Internet. Many applications need to authenticate broadcastdata, i.e. verify the data origin. The main challengesto design an efficient broadcast authentication protocol is:

- ✓ Efficient generation and verification. The generationand verification overhead for the authentication informationshould is small. It is important that the verification overhead is small, since a large number of receiversneed to verify the authentication information, and some receivers might have restricted computationpower.
- ✓ Real-time/instant authentication. Manyapplicationssuch as stock quote broadcasts require real-time dataauthentication. Hence, neither the sender nor the receivershould buffer data messages before sending orverification.
- ✓ Individual message authentication. The receiver canauthenticate each individual message it receives.
- ✓ Robustness to packet loss. Internet broadcasts can encounterhigh packet loss. In many broadcast applications, lost packets are not retransmitted. Hence theauthentication protocol should tolerate high levels ofpacket loss.
- ✓ Scalability. Broadcast applications have a potentiallylarge number of receivers. The authentication informationshould be independent of the number of receivers.
- ✓ Small size of authentication information. Since thereceiver authenticates individual messages instantly, each message carries authentication information, hencea viable scheme should have a low communication overhead.

Literature Survey:

Overview:

1. "Network Security Analysis Based on Authentication Techniques":

Anupriya Shrivastava, M A Rizvi:

In this authentication technique, privacy and confidentiality can be maintained up to some extent. Users memorize there passwords and hence we can term these as Knowledge-based techniques. Passwords can be single words, numeric, phrases, any combination of these or personal identification number. But problem with this technique is that memorized passwords can be easily guessed or randomly searched by the hackers. Virtual Private Networks such as Point-to-Point Tunneling Protocol (PPTP) make use of both clear-text protocols such as Password Authentication Protocol (PAP) and MD5-based protocols like Challenge Handshake Protocol (CHAP). As it is clear, MD5 should be preferred due to sniffing attacks. Plain passwords must be avoided as far as possible. They should be used only with SSL certificates.

System catalogs like, pg-authid‟ are used to store password for each user in database where we issue commands like CREATE, CREATE USER and ALTER ROLE to manage passwords. For example, CREATE USER jacks WITH PASSWORD info. If no password has been set up for a user, the stored password will be NULL and password authentication will always fail for that user.

Data Security is a challenging issue in the field of data communications. For securing information from hackers and crackers, authentication is the major phase in network security. It is a concept to protect network and data transmission over wired as well as wireless networks. Authentication is one of the primary techniques of ensuring that the person who is transmitting the information is whom he says he is. It is thus the process of determining the actual identity of users, systems or any other entity in network. To verify someone's identity, password is mostly used. To authenticate user or machines, different techniques can be used to perform authentication between user and machine or machine and another machine too.

2. Comparing Passwords, Tokens, and Biometrics for User Authentication:

Lawrence O'Gorman Avaya Labs, Basking Ridge, NJ, USA:

We use the term password to include single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. There are many studies showing the vulnerabilities of password-based authentication schemes. The basic problem with passwords can be explained succinctly: a memorable password can often be guessed or searched by an attacker and a long, random, changing password is difficult to remember.

Security systems and methods are often described as strong or weak. When used in relative terms, the meanings are clear. A door with a lock offers stronger security than one with no lock. A credit card number alone offers "weak" defense against repudiation because a user can easily deny a credit card charge by claiming that his credit card number was stolen. However, a credit card number plus a signature has "strong" defense (meaning "stronger" defense than without a signature) because the user leaves evidence of his presence by his signature. It is more difficult to measure security in absolute terms. One way to measure absolute strength and weakness of security systems is as follows. A strong system is one in which the cost of attack is greater than the potential gain to the attacker. Conversely, a weak system is one where the cost of attack is less than the potential gain. Cost of attack should take into account not only money, but also time, potential for criminal punishment, etc.

3. Multicast Authentication in the Smart Grid with One-Time Signature:
Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE:

Different applications in the smart grid have different requirements on multi cast authentication in terms of computation, communication and storage complexity, as summarized in Table II. The bandwidth cost of authentication should be as small as possible in wide area protection, since phasor data messages are transmitted at a very high frequency. However, bandwidth is not a big concern for the other three applications. Also, the storage cost at the receiver side should be kept low when the receivers are home appliances or field devices with very limited storage. Since the delay requirement is stringent in wide area protection, operation and control and in-substation protection, the computation cost of authentication should be low for the devices with constrained computing resources. In demand-response, because the time requirement is less stringent the computation overhead at the receiver side is less important. Generally speaking, the computation burden on the control center is not a big concern, but it cannot be too high.

An adversary (such as a terrorist or a disgruntled employee) may launch cyber security attacks to the power grid by forging multicast messages. To do this, the adversary can eavesdrop the communication channel and intercept a signed message that the sender multicasts to receivers. From the information in the intercepted message, the adversary can forge a signature for her own message and then inject her own message into the communication channel, which will be multicast to the receivers. Note that the adversary can also compromise a receiver to get a valid signed message instead of eavesdropping the communication channel. With the forged message and signature, the adversary can cause great damage to the power grid. For example, when the receivers are the distribution feeders that supply consumers in a large area, the adversary can include a disconnect command in the injected message which will cause a large-area breakout. Thus, it is important to authenticate multicast messages so that the receiver can verify if the messages come from the claimed sender and have not been modified during the transmission.

4. A Method of Risk Assessment for Multi-Factor Authentication:
Jae-Jung Kim and Seng-Phil Hong:

Many different types of online services have become available with the development of the internet. However, because the internet does not enable direct interaction between users, there are no methods of physical authentication for users who access important resources. Thus authentication of lawful users of internet services is paramount. As hacking technologies have become more diversified and advanced, security and authentication have become unable to rely on ID and password-based authentication alone. Single-factor authentication using an ID and password has been found to be vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, dictionary attacks and shoulder surfing. In recent times, there has been an increase in multi-factor authentication methods based on human characteristics, such as fingerprint recognition.In addition, the number of government policies demandingmandatory multi-factor authentication is increasing. The process of user authentication method selection is as follows.

- ✓ Transaction types, risk levels, user authentication methods and additional security measures used in the concerned service are examined.
- ✓ Threats and vulnerabilities in user authentication are analyzed.

- ✓ Influences on various transactions are analyzed and risk assessment is performed to identify the frequency andseverity of such threats and vulnerabilities.
- ✓ A user authentication method is selected based on a suggested user authentication level system.
- ✓ After applying the user authentication, a test is performed to ensure that the risk has beeneliminated.

5. Secure Authentication on the Internet- GSEC Gold Certification:

Roger Meyer& Carlos Cid:

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. The most prevalent form is probably the authentication with a user name and a password. Unfortunately it is also one of the most insecure methods. There is an unlimited range of variations of how a user can be authenticated to a web application. Some of the most popular ones are going to be described in the following. Authentication methods can involve up to three factors:

- ✓ Knowledge: something the user knows (e.g. a PIN or a Password)
- ✓ Possession: something the user has (e.g. a Smart Card or a USB Token)
- ✓ Attribute: something the user is (e.g. biometric characteristics like a fingerprint or the pattern of the eye)

An outofband transmission uses a channel different from the one the user is using to initiate then transaction. This separate channel gives an additional layer of security, as a potential attacker has to intercept both channels. Usually, the outofband channel is used for a second authentication factor like a one-timepassword (OTP). Outofband transmissions can be an email, an SMS (Short Message Service) to a mobile phone, a call or a fax. For example, after the institution receives the transaction request, an SMS is sent back to the originating individual with the details of the transaction including a one-time password, which the user has to enter to confirm the transaction.

Existing System:

Overview & System Architecture:

Obviously, the network and the computer system of any institution is more and more threatened by the increased appearance of hackers, intruders, viruses, worms, and other malicious code. On the other hand, the complexity of the network due to different protocols and applications even in a medium sized institution like the UL continuously increases. Moreover, the popularity of wireless networks adds many new security problems. Therefore, practical system and network security should not be considered an all-or-nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. The research unit wants to examine how the security requirements for a very heterogeneous network, based on cable and wireless communication links, linking computers running the Microsoft Windows, Linux, and the Mac OS operating system, can be fulfilled "as good as possible" without limiting the freedom of the users more than necessary.

This general research problem has a strong relationship to the other subjects in the research group, since it combines cryptographic algorithms and results from Information Security Management. Especially, topics like Public Key Infrastructure (PKI), user authentication, and identity management play an important role in system and network security. But there are also other important technical and managerial aspects. Important technical aspects include the optimal usage of intrusion detection systems and intrusion prevention / reaction with firewalls, or a flexible and reactive

audit management to keep the ''window of vulnerability'' as short as possible. One technical research objective is a security enhancement for known insecure network protocols, e.g. the anonymity of low latency communication.

More exactly, this problem deals with non-observability (i.e., how to provide a way for one person to communicate with another person without allowing an observer to know it). Reliable non-observable communications will have a wide range of applications, from banking to free-speech and privacy issues. Practical schemes for this problem exist for high-latency communications (like e-mail), but for very-low latency communications (like VoIP) these ideas cannot be applied directly. Another technical research topic focuses on privacy and anonymity in network communication, e.g. how to enhance the privacy of the Domain Name Service (DNS) protocol. New approaches for certifying the correctness of program executions in hostile environments will be studied.

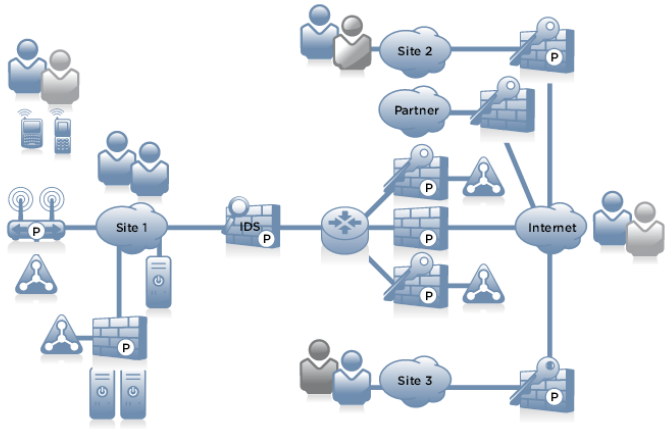


Figure 1: Existing system architecture with different networks

Besides these technical aspects, there is also a managerial aspect of network and system security, which is equally important. A security policy is a generic document that among others outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the institution security environment. A security policy goes far beyond the simple idea of "keep the bad guys out". It's a very complex document, meant to govern data access, web-browsing habits, use of passwords or more advanced access methods, and more. It specifies these rules for individuals or groups of individuals throughout the institution. A security policy should keep the malicious users out and also exert control over "potential risky" users within an organization. The group wants to examine in more detail, how the conflicting perspectives of network security and user-friendliness can be combined for the network at the UL. The definition of a security policy for an educational institution like the UL obviously has to consider the specific environment given at UL, especially the existence of three campuses with three already existing IT systems. The transformation of an existing network system with basic security to an optimally secured, flexible, and heterogeneous network at UL can be seen as a prototype application, where theoretical cryptographic and mathematical research is combined with practical steps for achieving best possible practical system and network security. Of course, analysis of the security requirements for the development of the IT system at UL in future (e.g., the introduction of information systems for various administrative tasks, or even Enterprise Resource Planning (ERP) tools) will also be an aspect of our research activity.

Disadvantages of Existing System:

- ✓ It is unsecure and no privacy, which means anyone can able access and modify the data.
- ✓ Leakage of privacy information due to WBAN'S unique characteristics, such as open medium channel, signal noise, mobile terminals, flexible infrastructure, and so on.
- ✓ Insecure Data's and it takes too long time for authentication with expensive infrastructure.
- ✓ Problem here is that the data records should have keywords associated with them to enable the search.
- ✓ Existing graphical password schemes where a password can be found within affixed number of trials.
- ✓ Analyses on Captcha security were mostly case by case or used an appropriate process. No theoretic security model has been established yet.

Proposed System:

Overview of the Proposed System:

In this digital era more and more people becoming active on the Internet for their personal and professional, because of this internet is growing rapidly. But, along with the evolution of Networking and Internet, several threats such as Denial-of-Service (DOS) attacks and Trojan Horses have also risen drastically. So the task of securing the Internet or even the Local Area Networks is now at the forefront of computer network related issues. Being on public network, serious security threats can be posed to an individual's personal information and also to the resources of companies and government. Providing confidentiality, maintaining integrity and assuring the availability of correct information are the primary objectives. These threats are primarily present due to the ignorance shown by the users, weak technology and poor design of the network. Sometimes there are many network services that are enabled by default in a personal computer or a router. Out of which many services may not be necessary and may be used by an attacker for information gathering. So it is better to disable these unwanted services to protect them from hackers and crackers More importantly, not only need to be concerned regarding the security at each end of the network rather the focus should be on securing the entire network.While developing a secure network, the following need to be considered:

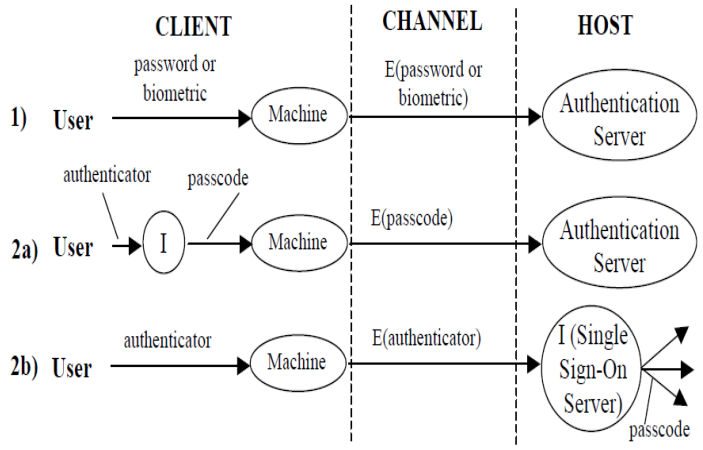


Figure 2: The overview of the proposed system with different authentication techniques

- ✓ Access – Only authorized users are allowed to communicate to and from a particular network.
- ✓ Authentication – This ensures that the users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.
- ✓ Confidentiality – Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.
- ✓ Integrity – This ensures that the message has not been changed during transmission.

What is Authentication?

The term authentication describes the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is part of cost online applications. Before a user can access its email account, its online banking account or its favorite online shopping account, it has to identify and authenticate itself to the application. The most common form of authentication is done through the use of passwords. Before describing the process of the authentication, we explain some terms. In this context, AAA is often used. AAA stands for Authentication, Authorization and Accounting. It is important to know the differences between those terms:

Authentication: the confirmation that a user is who it is claiming to be.

Authorization: the process to determine whether the user has the authority to issue certain commands.

Accounting: measuring the resources a user consumes during access.

Identification: Identification is the process that enables recognition of a user described to an automated data processing system. The login process consists of the following steps. To be recognized by an application, the user has to identify itself. Identification is achieved through the presentation of its credentials. The next step – authentication – essentially verifies a user's claimed identity. Once authenticated, the authorization defines what a user can see and do in the application. The accounting process is keeping track of user actions during allsteps.

Authentication	Types
Proof-of-Knowledge (Something you know?)	Passwords, PIN, Mom's Name, Phone# , etc
Proof-of-Possession (Something you have?)	Smartcards, Tokens, Driver's license, PKI certificates
Proof-of-Characteristics (Something you are?) -physiologically or behaviorally	Fingerprints, Hand geometry, Facial image, Iris, Retina, DNA, voice, signature patterns

Table 1: The need for secure Authentication

Internet usage and online applications are experiencing spectacular growth. Worldwide, there are over a billion Internet users at present. A big reason for the success of the Internet is the simplicity and that you can access the applications from anywhere. This growth in popularity has not gone unnoticed by the criminal element – the simplicity of the HTTP protocol makes it easy to steal and spoof identity. The business liability associated with protecting online information has increased significantly and this is an issue that must be addressed. Online fraud has become a

major source of revenue for criminals all over the globe. This has made detecting andpreventing these activities a top priority for every major company.

Main Objectives and Mechanisms:

Main Objectives:

- ✓ Long passphrase without as much user input.
- ✓ Help defeat casual attacks: (a) Need all factors to access via your UI & (b) Otherwise, need to brute-force.
- ✓ Understand what's going on in the market of multi-factor authentication.
- ✓ Look at solutions from a risk view, which problems are we actually solving/ trying to solve?
- ✓ To develop a multiple factor authentication system images. (Biometrics + Conventional + recognizable)
- ✓ To avoid the hardware dependency for OTS.
- ✓ To avoid attacks like shoulder surfing, guessing, key loggers.

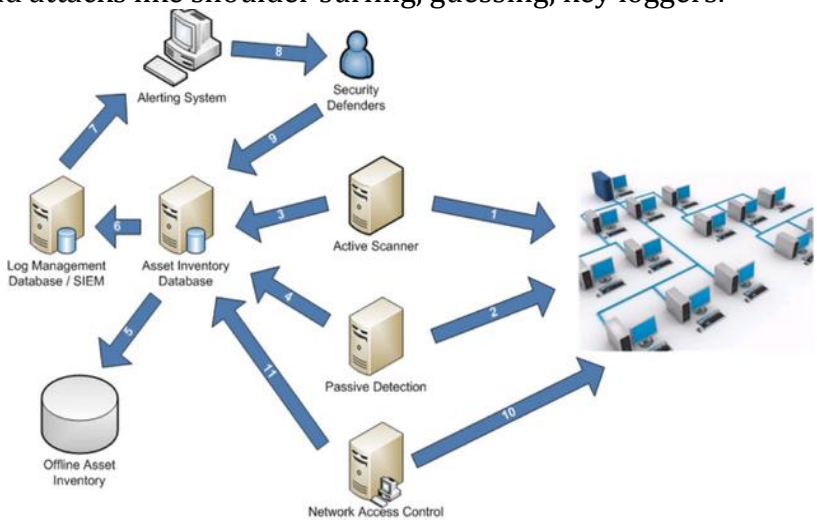


Figure 3: Network security principles when data forwarding

One-Time Signature:

- ✓ One time public and private keysEach key pair allows for signing (andverifying) of only one message.
- ✓ Verification time is usually very less.
- ✓ Good for broadcast environments, where quick source authentication is ofutmost importance. e.g Wireless networks.

OTS is a promising solution for multicast authentication in the network, since it can provide instantaneous authentication without message buffering delay and it can tolerate the compromise of one receiving nodes. OTS is conceptually similar to PKC-based signatures in that the sender uses a private key to sign a message and the receiver uses a public key to verify the signature. However, OTS is much moreefficient in computation since it is built upon one-way functions without trapdoors. OTS was proposed independently by Lamport and by Rabin and then improved by several works. In these schemes the signature size can be hundreds and even thousands of bytes, which is too large. Recently, Perrig proposed the BiBa signature, which reduces the signature size to 130 bytes. The disadvantage of BiBa is that it requires a long time to sign a message. To reduce the signing cost, Reyzin and Reyzin proposed the HORS signature. HORS only needs one hash computation to sign a message, making it the fastest OTS in signature generation. HORS also improves the signature verification cost and its signature size is similar to that of BiBa. Due to its efficiency, HORS has been used

in several works to authenticate time-critical multicast messages. However, HORS has some weaknesses when applied to the network. First, in applications where the receivers are resource constrained, the public key size of HORS is too large, which means a high storage overhead at the receiver side. Though some recent work improves the public key size of HORS, the scheme cannot be applied to one-way chain based authentication protocols and thus the distribution of the public key becomes an issue. Second, the signature size of HORS is too large for the wide area protection application. In a typical setting, one HORS signature has 130 bytes, but a phasor data frame may only have 48 bytes based on the IEEE C37.118 standard.

Applications of One-Time Signatures:

- ✓ Regular signature schemes
- ✓ On-line/Off-line signature schemes
- ✓ Forward-secure signature schemes
- ✓ Multicast packet authentication
- ✓ BiBa Broadcast authentication scheme

Advantages of the Proposed System:

- ✓ Cyber adversaries frequently attempt to steal legitimate user or administrative credentials when they compromise a network. These credentials allow them to easily propagate on a network and conduct malicious activities without installing additional exploits, thereby reducing the likelihood of detection and making it easier for less sophisticated adversaries.
- ✓ The user has to prove they have physical access to a second factor that either they have (passport, physical token or card) or are (fingerprints, facial recognition), or
- ✓ The credentials the cyber adversary obtains expire, ensuring that even if the cyber adversary compromises those credentials; they can't be used to enable future access or intrusion activity.
- ✓ You're 100% certain you can identify everyone connecting to your site. You correctly reject an attacker attempting to brute force their way in. Many types of MFA, such as an SMS contact, allow you an out-of-band way to communicate with the authentic user to let them know their account is under attack. There are many reasons you might want to do this, even if both you and the user know their account is safe: To allow them to contact authorities and attempt to identify the attacker, for example.
- ✓ Your system is 100% accurate today but may be compromised in the future. Reasons might include:
    - You make use of a crypto system that is strong enough to discourage all attackers now, but in a decade, technological advances have made it cheap enough to break the crypto that it's now worth attacking. MFA means the crypto system is no longer the only point of failure.
    - Perhaps when you say 100% accurate, you mean "This system is so hard to fool, that nobody would ever bother going to the expense of fooling it." (By creating a clone of your wife, for example.) This is an important distinction. If the value of information in your system increases dramatically at some point in the future, your security may now be inadequate, because the economics of breaking in have changed. MFA increases the expense further, improving your security from an economic standpoint.

- Your IT staff introduces a serious bug in a future version of the product; you're perfect system no longer works when that happens, but MFA could continue to work.

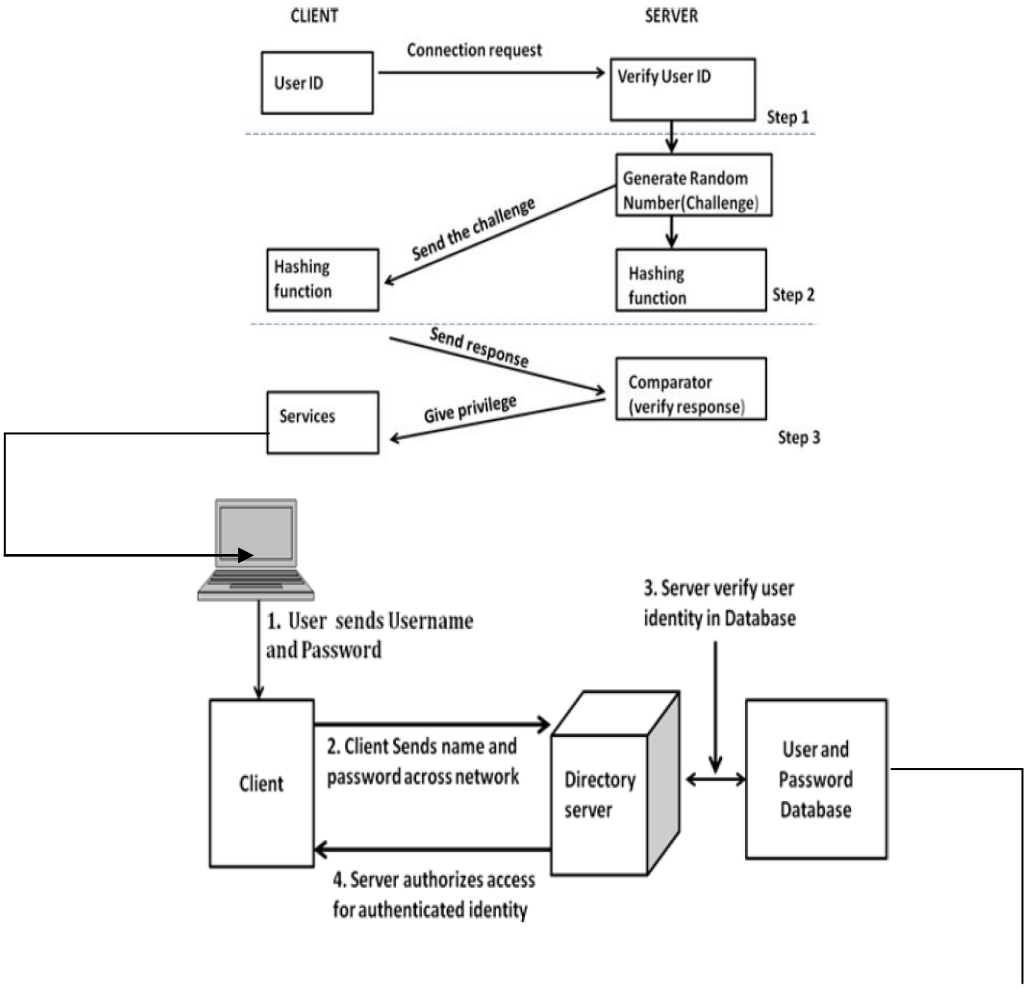
✓ Your system is 100% accurate in the sense that only the authentic user can access the account. However, the authentic user can be forced, under duress, to access their own account. MFA may provide a way out of this situation for the user. For example, if it requires a physical device which is time-locked or location-locked, and can't be accessed even under duress.

✓ This one is probably the most generally applicable: Access is about both authentication and authorization, and an authentic user who is authorized to use the system today may get fired, and no longer be authorized to use the system tomorrow. MFA can provide a double-check that their account is deactivated correctly. For example, if they must turn in their keys, including their code-generating device used for MFA, deactivating their account becomes a secondary concern.

✓ The value provided by these benefits varies based on the value of the information you're trying to protect, what type of MFA you're using, what type of primary authentication you're using, and so on, but the bottom line is that someone may find these compelling reasons to use MFA even in a "perfect" system.

System Architecture:

Internal Section:



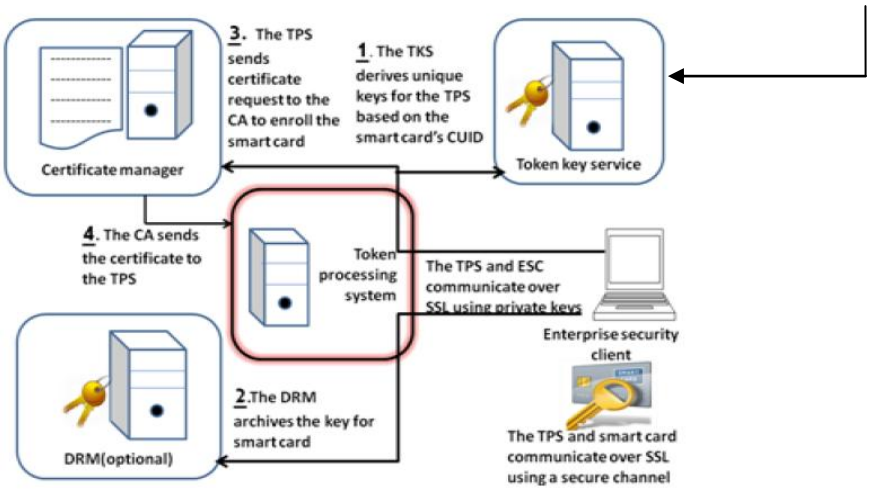


Figure 4: Combined authentication techniques with Biba one-time signatures

Experimental Results:

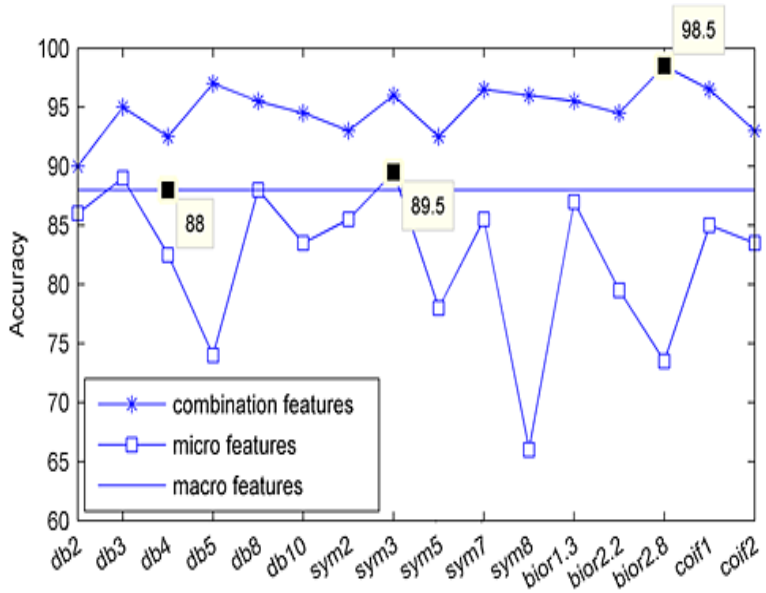


Figure 5: Result of an accuracy of the data

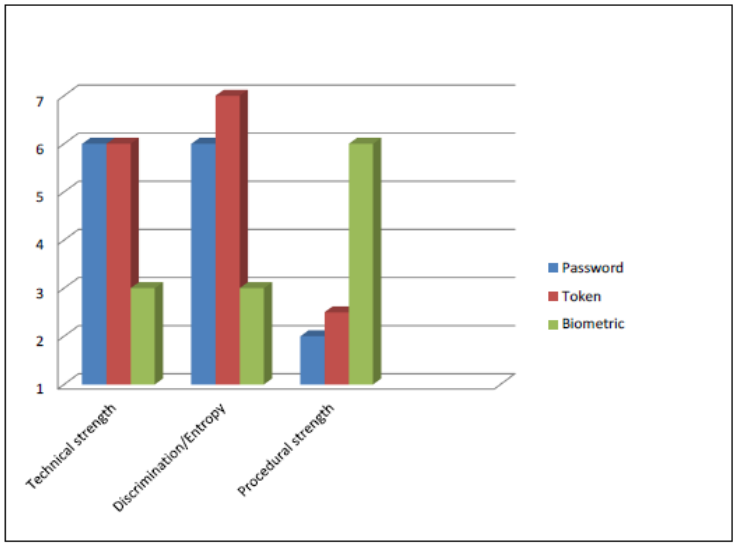


Figure 6: Result about the strengths of multi-factor authentication techniques

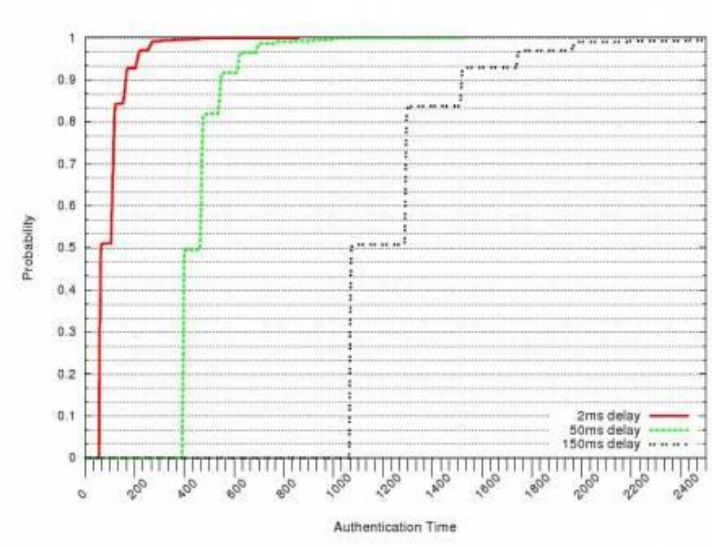


Figure 7: Results of feasibility of the data

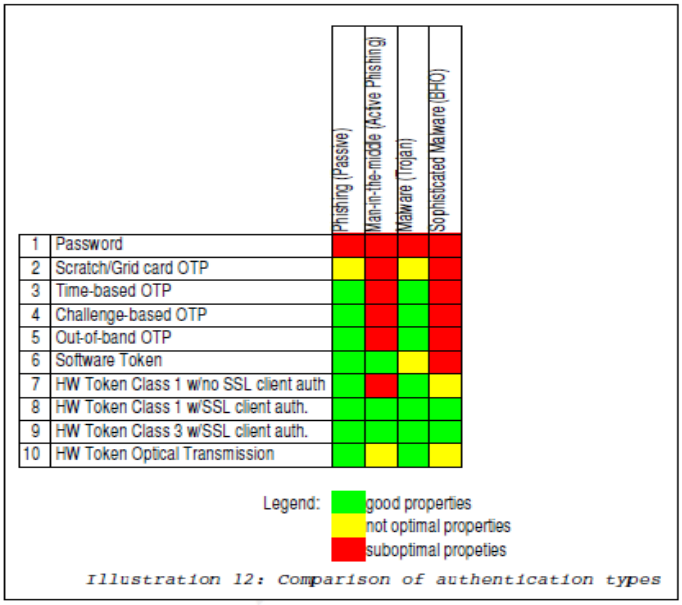


Figure 8: Results of authentication types

Functions of System Design:

Network security, each authenticator result must be satisfied. As a Boolean AND operation is performed for each factors authentication results, so all must be affirmative. Two factor authentications in ATM cards are the card itself and its password. So even if the card was lost or stolen, we can ensure that the safety is maintained until hacker's don't know cards password. This example of token plus password are mostly implemented today. Other combinations of token and biometric ID are also considered as secure techniques if it's difficult for user to remember passwords, but they require costly machines. But the combinations of biometric and passwords implementation are not so common because biometric usually includes sake for convenience. For comparing the above three authentications, we consider three important factors shown in the Graph 1 and finally calculate the composite of all those factors to determine the Binding strength which becomes the single point of comparison. But, the model that we use to find out this value makes use of individual weaknesses rather than individual strengths where weakness = 1/strength. As a result, we get the following equation:

Binding Weakness = Discriminatory Weakness + Procedural Weakness + Technical Weakness

Having setup the above equation, we determine the individual strengths as per the following parameters:

Discrimination Strength: For passwords, number of attempts in a defined time period. In case of tokens, we consider their distinct number. Whereas, for Biometrics, we need to find out the number of different attempts feasible.

Technical Strength: For all the three authentication mechanisms, security evaluation process is carried out.

Procedural Strength: This is hard to determine as it may depend on many environmental factors such as site security and staff discipline. But, still we use a specific set of parameters to gauge the value such as length, randomness and frequency of change in the case of Passwords; physical security and user discipline in the case of Tokens and for Biometrics, inherent strength is sufficient.

Next, we substitute these values into the above equation and determine the Binding Strength for each authentication mechanism.

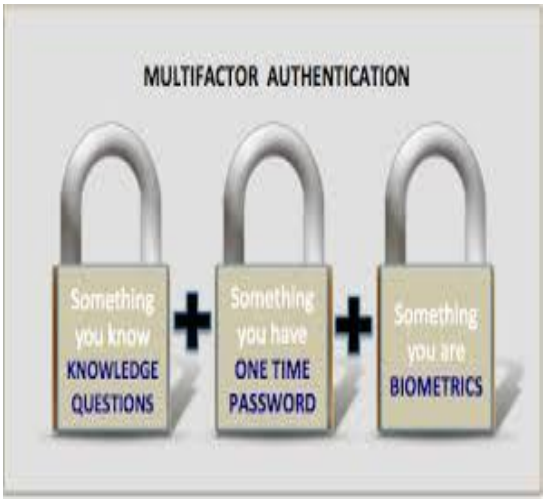


Figure 9: Design of Multi-factor authentication

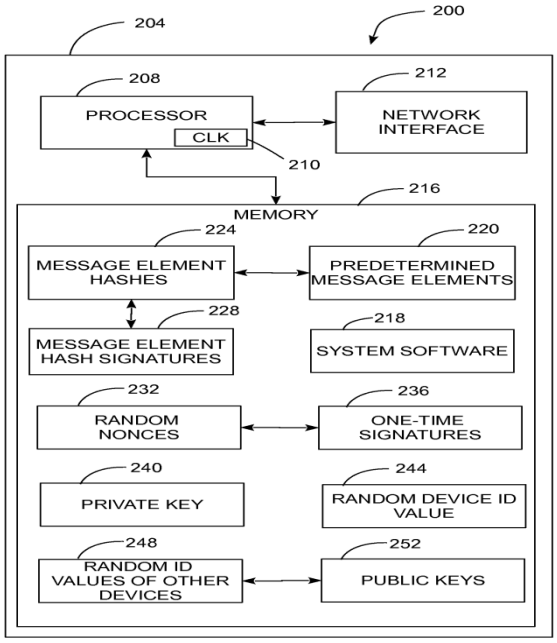


Figure 10: Design of One-Time Signatures

Future Enhancement:

Recyclingn Public keys that were authenticated but unusedcan be safely used in forthcoming time intervals. The onlyrestriction that must be taken into account is to avoidmemory exhaustion attack on the receiver. This is becausean adversary may intentionally break the communicationchannel betweenRandSwhich will determine the senderto further store public keys until its resources will exhaust.To avoid these maximum life-spans of the public keys canbe fixed.

It may be also tempting to recycle unused parts of thechains corresponding to the public keys. If the new tips areauthenticated this can be done but combining this with theprevious procedures results in an unsafe protocol. For exampleconsider thatSdecides to use an unused part of a publickey and authenticates it using the top level chain. Now anadversary that has intentionally broken the communicationbetweenSandRcan use the newly committed tips to forgea signature. Because of this, reusing parts of the public keysshould be avoided.

Conclusion:

Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. Password based technique is best if you have to remember a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember. Token based techniques provide added security against denial of service (DoS) attacks. In comparison to above two, techniques biometric cannot be easily stolen so it provides stronger protection. As signals, biometric can be easily copied by attackers so it should not be deployed in single factor mode. Furthermore we can choose a combination of above technique as discussed above. All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor also.

In this paper, we proposed an OTS scheme TSV to facilitatemulticast authentication in the smart grid. Compared withexisting schemes, TSV generates much smaller signature andhas much lower storage requirement. Thus, it is more appropriatefor smart gridapplications such as demand-response andwide area protection. The benefit is at the cost of increased computationsin signature generation and/or verification. However, TSV can flexibly allocate the computations between the sender and receiver. We formulated the optimal computation allocationproblem and proposed an effective and efficient heuristic algorithmto solve it. We evaluated TSV with implementations andcase studies.

References:

1. Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.
2. Lawrence O‟ Gorman, “Comparing Passwords, Tokens, and Biometrics for User Authentication”, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.
3. Jae-Jung Kim and Seng-Phil Hong, “A Method of Risk Assessment for Multi-Factor Authentication”, Journal of Information Processing Systems, Vol.7, No.1, March 2011.
4. Stamati Gkarafli, Anastasios A. Economides, “Comparing the Proof by Knowledge Authentication Techniques”, international Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2).
5. Roger Meyer, “Secure authentication on the internet” As the part of security reading room, SANS institute 2007.

6. Dale Vile, Freeform Dynamic, "User convenience versus system security", 2006.
7. D. L. Jobusch, A. E. Oldehoeft, "A survey of password mechanisms: Weaknesses and potential improvements," Computers and Security, Vol. 8, no. 8, 1989, pp. 675-689.
8. Chandrasekar, A., Rajasekar, V. R. and Vasudevan, V. "Improved authentication and key agreement protocol using elliptic curve cryptography". International Journal of Computer Science and Security, 3(4): 325-333, 2009.
9. Schneier, B. (2005). Two-factor authentication: too little, toolate. Communication s of the ACM. Volume 48 , Issue 4, 136.Schneier, B. (2005). The Failure of Two-Fa ctor Authentication.
10. Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time-valid one- time signature for time critical multicast data authentication," in Proc. IEEE INFOCOM, 2009, pp. 1233–1241.