ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

SECURE COMMUNICATION BASED ON AUTHENTICATION TECHNIQUES USING NIDS

Mr. P. Thangavel*, Dr. A. SenthilKumar
* Research scholar in Computer Science, Bharathiar University, Coimbatore
Assistant Professor in Computer Science, Tamil University, Thanjavur

DOI: 10.5281/zenodo.199473

KEYWORDS: Authentication; Denial of service; RSA;Network Intrusion Detection System.

ABSTRACT

Network Security is a unique, efficient and beneficial part in the management of network. Mostly many organizations around the world spend millions of revenue in every year for the safety and provide security regarding valuable corporate form of data's and information. 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. This paper gives a description ofthe available approaches for a network intrusion detection system (NIDS) in both software and hardware implementation.

INTRODUCTION

Network Intrusion detection system can be described as the process of identifying and taking necessary actions against malicious activities targeted to network and computing resources. A network intrusion detection system should continuously monitor the traffic crossing the network and compare with a previously known set of malicious activities or look for statistical deviation of the system under surveillance from its normal behavior. Aim of network security is to protect the device from unauthorized and potentially harmful activities such as denial of service attacks, port scans or attempt to crack into computers by monitoring network traffic. Network connected devices are very often susceptible to exploitation. The Intrusion detection system (abbreviated as IDS) placed in the network should be able to sense the unusual activity and alert the administrators. A set of well-defined rules eg. Snort and Bro are used to identify network events that are other than expected.

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 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.

Recently a financial transaction value which leads to the carrying Internet which uses WiBro networks is activated for the government, the security company and the bank, financial institution etc. There must be a inevitably which will be analyzing the security vulnerability due to which the financial transactions which leads WiBro carrying Internet and it prepares in financial accident. The security vulnerability of mobile stock trading from WiBro, it must analyze forensic fundamental data that must created and the stability and a security characteristic measure of financial transactions from the carrying Internet can be approach later on.
While developing a secure network, the following need to be considered -

1. Access – Only authorized users are allowed to communicate to and from a particular network.

2. 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.
3. 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
4. Integrity – This ensures that the message has not been changed during transmission.

DATA SECURITY AND AUTHENTICATION

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.

Table-1 Different Types Of Attacks On Network/Data

Attacks types	**Description**
Weak password recovery	Websites permit hackers to find a way to illegally obtain, modify or recover another user's password.
Brute force attacks	By trial and error, hackers can guess username, password, debit cards numbers, etc. This technique is highly popular
Insufficient authentication	Some websites don‟t authenticate much so hackers attack sensitive content
Shoulder surfing attacks	Hackers directly observe user while typing passwords or by some hidden cameras.

AUTHENTICATION TECHNIQUES

Following are the primary authentication techniques used in the public network these days:

A. ***Password and pin based:***

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.

Fig.1 shows working of password based authentication technique. The user first enters a name and password. It is required that the Client application binds itself to the Directory Server with a distinguished Name. The client uses the name entered by user to retrieve domain name. Next the client sends these credentials to the Directory Server. The server then verifies the password sent by the client by comparing it against the password stored in database. If it matches, the server accepts the credentials for authenticating the user identity. Then the server allows client so authorized to access the resources.

ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

In password-based authentication techniques, password policies are a set of rules that also have major roles in deciding how to administer password in the systems. There are multiple policies supported by directory servers. „Default" and „Specialized" are the two of them. The default password policy is part of the configuration for the instance, once modified, it cannot be replicated.

B. One Time Password (OTP) token

Using an OTP token as a second factor is accomplished by providing users with a hardware device that generates a constantly-changing second password that must be entered into the online banking Web site in addition to the normal password. OTP tokens require the user to carry the token with them to login to the bank Web site. If a customer has multiple banks that require OTP tokens, then the user must carry multiple tokens unless the banks integrate their systems to accept a single token.

C. E-mail or SMS one-time password (OTP)

Using e-mail or SMS OTP as a second factor is accomplished by sending a second one-time use password to a registered e-mail address or cell phone. The user must then input that second one-time password in addition to their normal password to authenticate to the online bank. This method is generally considered too cumbersome for everyday logins because there is a time lag before users get the OTP they need to login but is often used for the initial enrollment before providing another form of authentication.

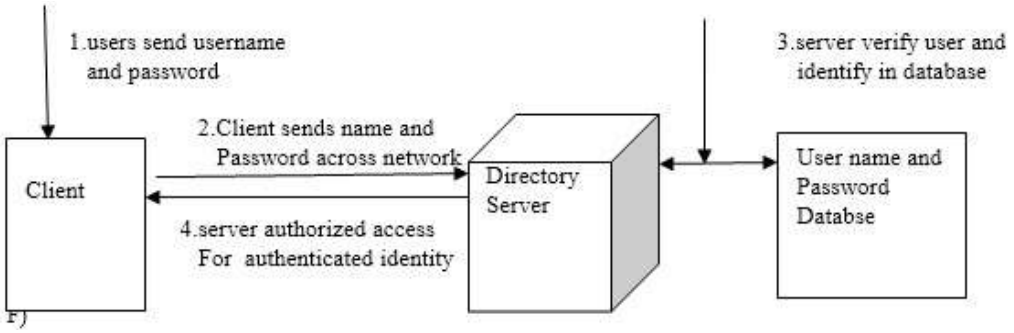

Fig. 1 Directory Server based authentication

D.The most common Authentication Methods used Today

As the news of network security breaches reaches more eyes and ears, thanks to high profile cases like the recent LinkedIn incident where millions of passwords were compromised, both consumers and regulatory agencies are putting increasing pressure on those in charge of enterprise security to step up their defenses.

Figure1.1 Biometrics

ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

The issue for network admin is that they are playing a continuous state of "catch-up," as newer exploits are developed by highly sophisticated cyber gangs in order to Keep their profitable fraud rings going as soon as earlier exploits are patched. Smart phones and tablets present an even greater challenge, as most of these devices lack the same malware defenses as their more robust cousins, desktops and laptops.

Transaction Authentication

Simply put, transaction authentication looks for logical flaws when comparing known data about a user with the details of the current transaction. For example, if a user that lives in the U.S. purchases several big ticket items while logged in from an IP address determined to be from a foreign country, this is cause for concern and would require extra verification steps to ensure the purchase is not fraudulent.

Biometrics

Biometrics literally means "measuring life," and refers to the use of known and recorded physical traits of a user to authenticate their identity, as no two individuals share the same exact physical traits. Common schemes include:

1. Voice recognition
2. Finger prints
3. Face scanning and recognition
4. Eye prints, such as retina and iris scans

Multi-Factor Authentication

MFA is really a blanket term that describes an authentication scheme that uses two or more independent sources to verify an identity, like:

1. Something **possessed**, as in a physical token or telephone
2. Something **known**, such as a password or mother's maiden name
3. Something **inherent**, like a biometric trait mentioned earlier

DENIAL OF SERVICE

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) the service or resource they expected.

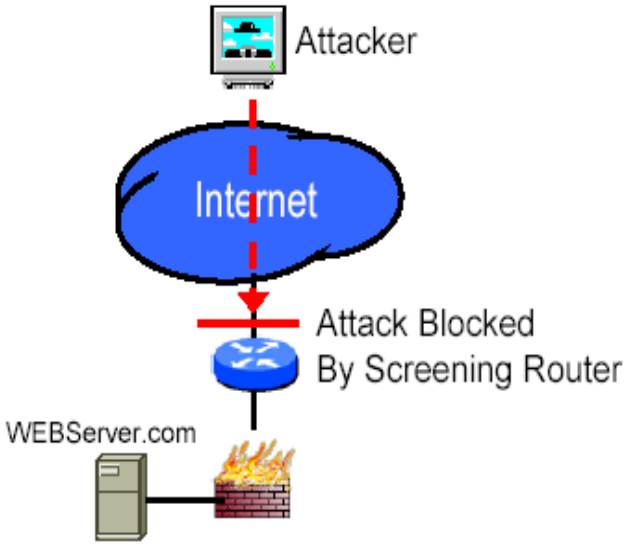

Figure 1-2: Screening Routers to prevent DOS attack

Victims of DoS attacks often target the web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the surf attack or ping of death.

The RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithms are one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation. Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for *p* and *q*, the resulting *n* will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining *d* without factoring *n* are equally as difficult.

B.RSA Algorithm Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

ISSN 2349-4506
Impact Factor: 2.785
Global Journal of Engineering Science and Research Management

NETWORK INTRUSION DETECTION SYSTEM

Ever increasing demand of good quality communication relies heavily on Network Intrusion Detection System (NIDS). Intrusion detection for network security demands high performance. Network Intrusion detection system can be described as the process of identifying and taking necessary actions against malicious activities targeted to network and computing resources. A network intrusion detection system should continuously monitor the traffic crossing the network and compare with a previously known set of malicious activities or look for statistical deviation of the system under surveillance from its normal behavior. Aim of network security is to protect the device from unauthorized and potentially harmful activities such as denial of service attacks (forcing the targeted computers to reset or to consume its resources so that it is not able to provide the intended service), port scans or attempt to crack into computers by monitoring network traffic. Network connected devices are very often susceptible to exploitation. The Intrusion detection system (abbreviated as IDS) placed in the network should be able to sense the unusual activity and alert the administrators.

The goal of modern network traffic is to provide a high speed good quality communication keeping up with the demand of ever increasing data usage. Deep packet inspection with regular string matching is a very common method of network intrusion detection. Implementation of Signature based network Intrusion Detection System (NIDS) requires to match a predefined string or predefined pattern that is already identified as harmful to the network. As the IDS should inspect the data packets at the rate of data connection, a very high performance is required for the IDS string matching operation. Also the rule set gets regularly updated with the evolution of fresh attacks. Hence the hardware system used to implement NIDS should have the feature of dynamic reprogramming. Both of these features of high network traffic collection ability and dynamic reprogramming is supported by FPGA devices. Hence they are suitable candidates for hardware implementation of NIDS. But the high network traffic collection ability is not matched by the device frequency. Hence like multi core parallelization of microprocessors it is mandatory approach to implement parallelism in FPGA based NIDS traffic analysis.

The network intrusion detection system can be placed at a choke point such as the company's connection to a trunk line [1], or can be placed on each of the hosts that are being monitored to protect from intrusion. Intrusion, incident and attack are three terms that we often come across while discussing Intrusion Detection System.
A NIDS should have the following desirable features [4]:

- System should be fault tolerant and run with the minimal human supervision.
- The NIDS should not be susceptible to attacks from the intruder
- NIDS should not interfere with the normal operation of the system.
- It should be possible to reconfigure the NIDS over time with the changing rules and security policies of the network.
- NIDS should be portable to different architectures making it easy to deploy.
- NIDS should be general to detect different types of attacks and should have as less number of false positives as possible.

Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting.

The primary methods used by N-IDSs to report and block intrusions are:
Reconfiguring third-party devices (firewall or ACLs on routers):
Command sent by the N-IDS to a third-party device (like a packet filter or firewall) to immediately reconfigures itself so as to block an intrusion. This reconfiguration is made possible by sending data explaining the alert (in the packet header(s)).

ISSN 2349-4506
Impact Factor: 2.785
Global Journal of Engineering Science and Research Management

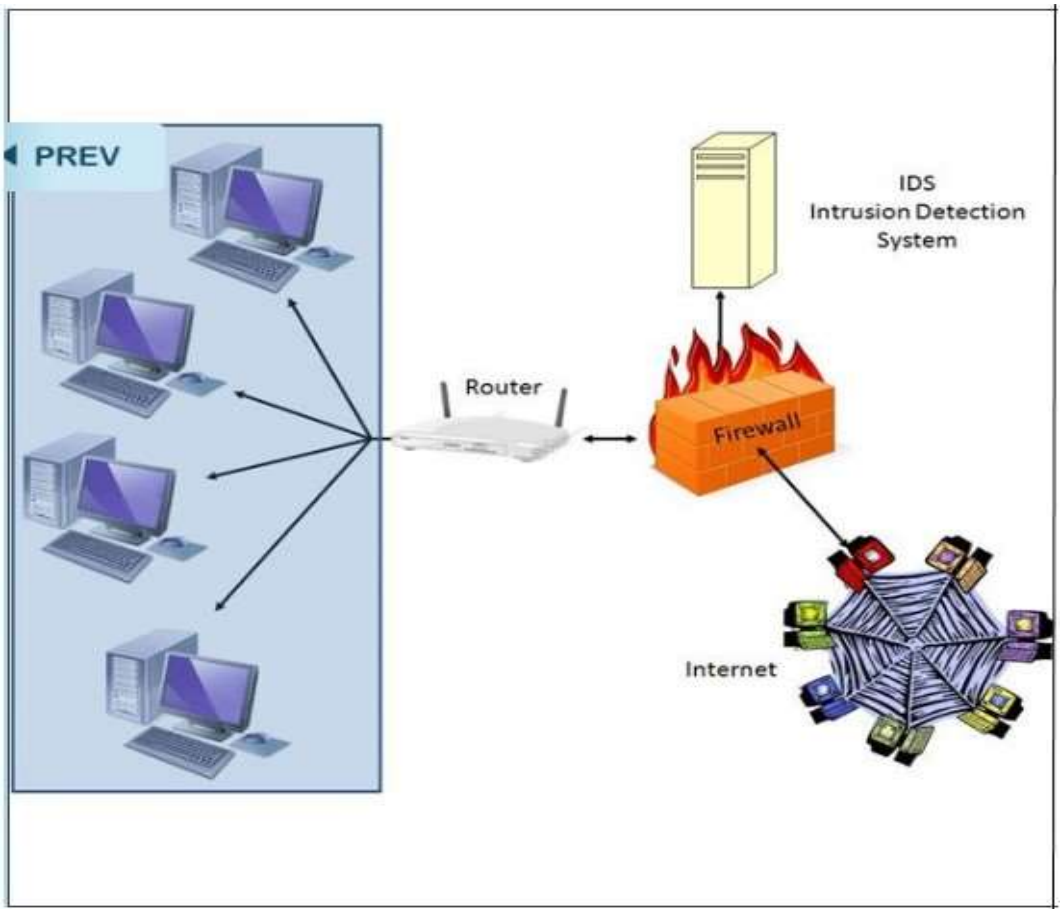

Fig 1.3 Network Intrusion Detection System

- **Sending an SNMP trap to a third-party hypervisor**:
  Sending an alert (and details on the data involved) in the form of an SNMP datagram to a third-party console like HP Open View, Tivoli, Cabletron Spectrum, etc.
- **Sending an email to one or more users**:
  Sending an email to one or more inboxes to report a serious intrusion.
- **Logging the attack**:
  Saving the details of the alert in a central database, including such information as the timestamp, IP address of the intruder, IP address of the target, the protocol used, and the payload).
- **Saving suspicious packets**:
  Saving all raw network packets captured, and/or only the packets which triggered an alert.
- **Opening an application**:
  Launching an outside program to perform a specific action (such as sending an SMS text message, or playing a sound to indicate an alert)
- **Sending a "*Reset Kill*"**:
  Constructing a TCP FIN packet to force a connection to end (only valid for intrusion techniques that use the TCP transport protocol).
- **Visual notification of an alert**:
  Displaying an alert on one or more management console(s).

TECHNOLOGY SOLUTIONS

As in the past years, technology is continually advancing and that the criminal element will adopt new technology as it comes along. With a growing number of personal data devices and other sophisticated technology, criminals are becoming more able to conceal their actions. Protecting the nation's critical digital infrastructure requires a comprehensive view of security that combines physical, digital and procedural components. These components are necessary and unique to each individual environment and must not impact normal daily activities, while providing the level of cyber security necessary to guard against the many known and unknown threats in cyberspace. Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. Cybercrime can affect service providers, banks, individuals and law enforcement authorities. A compromise on one network can allow an intruder either direct access to a partner's private data or indirect access by allowing a back door into the partner's network. Further threats to cyber security include (1) misconfiguration of computer systems; (2) poor user and administrator education; (3) poor software design; (4) network and system design issues; (5) substandard operational procedures; (6) use of insecure protocols; (7) weak passwords; (8) and finally, lack of awareness and in difference.

A large number of companies still do not have in place an information security policy. Awareness is fundamental as without it, market forces will not drive improvement. If the client is not demanding security with the supplied service, then IT suppliers will not be encouraged to supply it. By putting in place a security policy, businesses promote best practice in relation to the use of their systems and access to their information. Security breaches are often caused by poorly implemented internal processes, and a lack of staff awareness or lax control. Businesses need to implement their own cybercrime crackdown and install up-to-date bug patches. Tools are available to prevent unwelcome intrusion, secure e-commerce infrastructure and protect communications between businesses and third parties. The most common technologies employed are: firewalls, physical security systems, encryption of critical data in transit and storage, manual patch management and filtering and virus scanning.

However, technological tools are not enough to combat transporter cybercrime problems. For example, the computer virus dubbed the "*Love Bug"* had forced email servers to shut down in Europe and spread wildly in the US. The virus caused US$7 billion damage. Renal Ramones authored the Love Bug virus, but was not prosecuted for computer hacking because the Philippines did not have a law that dealt with computer crime at that time. The Philippines subsequently brought into force a new law covering electronic commerce and computer hacking, but it could not be applied retrospectively to the *Love Bug* case. The case illustrates the need to update current Legislations and to address cybercrime at an international level through a harmonized legal framework, such as a Convention or Treaty. As any action taken over the Internet is global, it also requires a global response.

FUTURE TRENDS

Over the past years there has been a rise in the use of existing forms of carrying out covert operations by means of information technology. These include ever greater use of encryption, money transfer facilitated by computer system and increasing fraud over the internet. With the retention by top information technology specialists by transnational crime groups and terrorists, we can expect to see new and innovative uses of information technology by these groups.

Of greatest concern to many governments and international financial systems is the possibility of serious intrusions into critical systems. These intrusions could include the introduction of viruses that would destroy critical data, the posting of harmful websites that cannot be brought down and even the full scale incapacitation of critical computer systems.

CONCLUSION

The growing dependence of industry and society on IT, and the growing threat of cybercrime, require that serious effort be devoted to IT security. Due to interdependence and interconnection beyond any one system's or organisation's boundaries and responsibilities, the usual parochial and short-term focus of IT security is no longer adequate. We must consider the possible impacts on or from, other systems (often in other organizations), whether caused by accidental hardware, software or operational faults, or - as analyzed in this paper - by malicious acts, including possibly by insiders.

REFERENCES

1. Lawrence O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.
2. Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No: 04.
3. [Online]Available: http://www.authenticationworld.com/Token-Authentication.
4. [Online]Available: http://www.authenticationworld.com/Authentication-Biometrics.
5. 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.
6. 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.
7. [Online]Available: http://www.duosecurity.com.
8. [Online]Available:http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication %20Technique.pdf.
9. Stamati Gkarafli, Anastasios A. Economides, "Comparing the Proof by Knowledge Authentication Techniques", international Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2).
10. Roger Meyer, "Secure authentication on the internet"As the part of security reading room, SANS institute 2007.
11. R. Dhamija, and A. Perrig,"Déjà Vu: "A User Study Using Images for Authentication", 9th USENIX Security Symposium, 2000.
12. R. Morris, K. Thompson, "Password security: A case history," Comm. ACM, Vol.22, no. 11, Nov. 1979, pp. 594-597.
13. B. L. Riddle, M. S. Miron, J. A. Semo, "Passwords in use in a university timesharing environment," Computers and Security, Vol. 8, no. 7, 1989, pp. 569-579.
14. S. M. Bellovin, M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," Proc. 1992 IEEE Computer Society Conference on Research in Security and Privacy, 1992, pp. 72-84.
15. Anupriya Shrivastava, M A Rizvi, "RESEARCH ARTICLE Network Security Analysis Based on Authentication Techniques ". A Monthly Journal of Computer Science and Information Technology .ISSN 2320–088X ,IJCSMC, Vol. 3, Issue. 6, June 2014, pg.11 – 18. A Monthly Journal of Computer Science and Information Technology.
16. Miss. Shwetambari G. Pundkar, Prof. Dr. G. R. Bamnote, "RESEARCH ARTICLE ANALYSIS OF FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY" .ISSN 2320–088X ,IJCSMC, Vol. 3, Issue. 4, April 2014, pg.841 – 846.
17. A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. no. 6,2004.
18. Akdeniz, Y. (2003). An Advocacy Handbook for the Non Governmental Organizations. Cyber-Rights and Cyber-Liberties
19. Bannisar, D. (2000). A Draft Commentary on the Council of Europe Cybercrime Convention. Retrieved 1 July,2005,http://www.privacyinternational.org/issues/cybercrime/coe/
20. Convention on Cybercrime is available at: http://conventions.coe.int/Treaty/en/
21. Crawford, S. (2004, December 19). Cybercrime Convention. Retrieved 1 July, 2005, from,http://scrawford.blogware.com/blog/_archives/2004/12/19/209645.html
22. www.crime-research.org_library_Terrorism_Cybercrime.
23. http://www.tweakandtrick.com/2012/06/most-common-authentication-methods-used.html
24. http://archive.securitypronews.com/2003/0925.html
25. http://ccm.net/contents/166-intrusion-detection-systems-ids
26. https://www.sans.org/security- esources/idfaq/what_is_id.php