International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 50-53
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

COMPUTER SYSTEMS SECURITY AND SUPPORT FOR INTERNET VOTING SYSTEM

Dr. Vinod Kumar
Assistant Professor
Department of CSE
Dev Samaj College for Women
Ferozepur City

Shivam Kumra
Assistant Professor
Department of CSE
Dev Samaj College for Women
Ferozepur City

Jagdish Kaur
Assistant Professor
Department of CSE
DAV College for women
Ferozepur City

ABSTRACT - India is a democratic country in the world. Democracy is defined as a government of the people, by the people and for the peoples. In Indian democracy people have the right to select their representatives using votes. Voters have to present personally at the voting booth to cast their vote under the supervision of authorized election commission members. For a variety of reasons voters may not be able to cast vote remotely. In this paper we propose a solution through internet voting. This is efficient, time saving, secure, helpful for youth awareness and physically disabled peoples. In this paper first we describe the best security methods for the security of information at network level, operating system level and physical securities for internet voting.

KEYWORDS - RSA, Honey algorithm, Internet voting, Firewall, Biometric

I. INTRODUCTION

As democracies across the world are facing challenges related to accessibility, scalability and security and cost of voting system. With the growing use of internet, internet voting is the best alternate solution to the problem. We introduce the different security schemes in order to secure internet voting system. We proposed new security techniques to secure the voting system.

II. NETWORK SECURITY

In past years, computer was primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of peoples are using networks for banking, shopping, and filing their tax returns, the Indian democracy is not escaped from this. As democracies across the globe are fighting challenges related to paper voting system. With the spread of internet coverage in the country and smartphones are the alternatives to this problem. The paper focuses on an alternate secure voting system using internet through computers or smartphones. Voting through machines is the main problem occurs when data transfer on internet. The requirements of information security within an organisation have undergone two major changes in the last several decades to prevent and monitor unauthorized access misuse, modification or denial of computer network. The security of information felt to be valuable to an organization was provided primarily by physical and administrative means .With the advancement in technology, an automated tools for protecting files and other information stored on the computer system is required. The technicalities of implementing internet voting system are a result of attempt to reconcile the use of internet voting with emerging and existing standards to which electronic elections should adhere. These standards include the need for secure online voter authentication, protection of secrecy of vote, appropriate transparency mechanisms. in this paper we will discuss security methods at different levels.

III. NETWORK SECURITY THREATS

Masquerade: When one entity behaves like another. We can say masquerade attack happened when one person obtain the right of authentication code of (authorized user) like userid and password to get extra rights.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 50-53
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

Modification of data: This means the attack on message to alter some position of message or delay the message by attacker.

Denial of service: This attack take place when the availability to a resource is blocked or another form can be the disruption of an entire network.

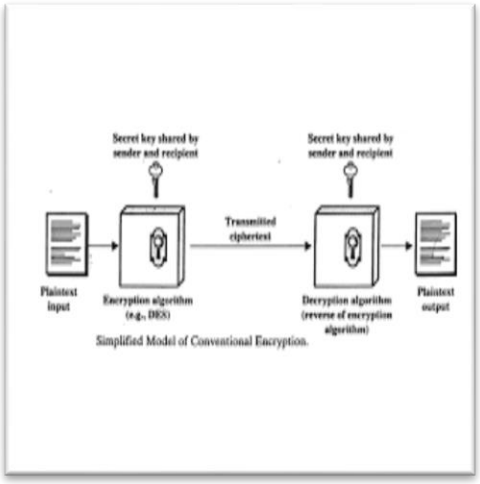
IV. NETWORK SECURITY MECHANISM

Transposition Ciphers

Transposition Ciphers method change the positions of letters to reorder them. A character in First position may appear in ninth position and character in seventh position may appear in third position. This method uses a key for mapping the locations of letters. The key should not contain the repeated letters.

Tripple DES

This algorithm replaced the DES (Data Encryption standard).This algorithm applies the data encryption standard block cipher three times to each data block. The key size is 168,112 or 56 bits. The block size is 64 bits and performs 48 rounds. Tripple DES is a better solution for financial services and other industries.



Simplified Model of Conventional Encryption.

RSA Public key cryptography

While there may be many algorithms and keys that have this property, the RSA algorithm (named after its founders, Ron Rivest, Adi Shamir, and Leonard Adleman) has become almost synonymous with public key cryptography. In order to choose the public and private keys, one must do the following: Choose two large prime numbers, p and q. The larger the values, the more difficult it is to break RSA but the longer it takes to perform the encoding and decoding. Compute n = pq and z = (p-1)(q-1).Choose a number, e, less than n, which has no common factors (other than 1) with z. (In this case, e and z are said to be relatively prime). The letter 'e' is used since this value will be used in encryption. Find a number, d, such that ed -1 is exactly divisible (i.e., with no remainder) by z. The letter ’d’ issued because this value will be used in decryption. Put another way, given e, we choose d such that the integer remainder when ed is divided by z is 1. (The integer remainder when an integer x is divided by the integer n, is denoted x mod n).The public key that Bob makes available to the world is the pair of numbers (n,e); his private key is the pair of numbers (n,d).key distribution: For symmetric key cryptography , the trusted intermediary is called a Key Distribution Center (KDC), which is a single, trusted network entity with whom one has established a shared secret key. We will see that one can use the KDC to obtain the shared keys needed to communicate securely with all other network entities. For public key cryptography, the trusted intermediary is called a Certification Authority (CA). A certification authority certifies that a public key belongs to a particular entity (a person or a network entity). For a certified public key, if one can safely trust the CA that the certified the key, then one can be sure about to whom the public key belongs. Once a public key is certified, then it can be distributed from just about anywhere, including a public key server, a personal Web page or a diskette.

Blowfish

This algorithm is highly recommended for e-commerce platforms to manage secure payments to password management tools. This is more flexible encryption method. Blowfish is symmetric cipher that split message into 64 blocks and encrypt them individually.

Twofish

Twofish is fastest method to encrypt the data. it is used in both hardware and software environment.

Honey Encryption

It is a new method that will deter hackers by serving up fake data in response to every incorrect guess of password. If the attacker does eventually guess correctly, the real data should be lost amongst the

crowd of spoof data. For example if an attacker used software to make 10,000 attempts to decrypt the credit card number, they would get 10,000 different fake credit card numbers.

V. OPERATING SYSTEM LEVEL SECURITY

Operating system security refers to protect the system resources like cpu, memory, disk, data and software programs form auditing, destruction by any unwanted program or event by unauthorized entity.

VI. THREATS TO OPERATING SYSTEM

Worms

The named worms because this program crawls from computer to computer through network and email. Worms exploit the operating system by spreading itself.

Viruses

Viruses are program that infect other program by adding their own codes to gain its control when these infected files opened.

Spyware

Spyware is software that used to get the information about a person or organization without their knowledge. This is like tracking software.

Trozen

Trozen are that program which performs an unauthorized action on our computer like delete information on drive, make system hang, steal the information etc. They are spread by hackers.

Rootkits

Rootkits are mask providing programs that keep away from anti virus's software to detect them. Rootkits can modify the operating system on computer and its basic functions.

VII. SECURITY MECHANISM

Antivirus software

Antivirus software protects our computer from viruses, malware, spyware, worms and trozen easily. There are various antivirus softwares available in market. These software protect our computer from viruses, updating virus definitions, block viruses, prevent infections from viruses, worms. Some of best anti viruses are :Ad-Aware anti viruses+, Microsoft security, Herd protect, Vircleaner, Bitdefender Anti viruses free, Roboscan, Clamwin, Comodo Anti viruses, Vipre rescue, escan Anti viruses Toolkit etc.

Firewalls

A firewall is a hardware or software system which is used to prevent unauthorized access to or from network. Firewall prevent the entry of viruses and other pets into the network, to prevent confidential information from leaking out. Firewalls are designed to prevent unauthorized internet users from accessing private networks connected to internet. Firewalls are designed to filter the packets before passing the traffic and they decide which packets to be transmitted or not.

VIII. PHYSICAL SECURITY

Biometrics

Biometrics refers to the study of measurable biological characteristics in computer security. Biometrics is an authentication to check physical characteristics automatically. There are several biometrics schemes used for authentication like face (analysis based on facial characteristics), fingerprint (the analysis of fingerprints), voice (the analysis of tone, frequency of a person's voice)and hand geometry(the analysis of shape of hand).

Reduced the Trusted computing base

The ballot definition in voting comprises a state machine and a set of static bitmap. The software used in ballot system act as virtual system for this ballot program. It transition between states and send bitmaps to display devices based on voter's input e.g. touch screen. A ballot definition of this sort can be audited for correctness independently of the voting machine software. The voting machine should be examined by expert. There should be system in which module that must be trusted are forced to be small and clearly compartmentalized by dedicating separate computer to each. Each module on isolated CPU, memory be analyzed and audited independently without they collude using side channels.

IX. SECURED ELECTRONIC INTERNET VOTING SYSTEM

An electronic voting system is a system in which the election data is recorded, stored and processed as

digital information. Most countries believe that internet voting will occur within next decades. Internet voting can meet the voting needs of the physically challenged peoples or working professionals. There will be various small applications be proposed by several countries in near future. This will help the people to vote at any time, anywhere .Internet voting one can vote from an internet browser in one's personal computer or by email, electronic fax. A voted ballot sent through internet is paperless .This will be helpful for military and overseas voters where ballots are not received in time.

X. CHALLANGING AREAS FOR INTERNET VOTING SYSTEM

An internet voting system must be secure and transparent. An internet voting system must guarantee the integrity of election data. Keep the personal information of voters safe. Authentication of voters should be kept secret. No person gets to vote more than ones. Every person should be verified before casting internet vote.

XI. INTERNET VOTING SYSTEM TECHNIQUES

Cryptographic Techniques

In cryptography, encryption is the process of encoding the information related to election data that hackers cannot read it. The information is encrypted using encryption algorithms into an unreadable form cipher text. This is done with key. And adversary can see cipher text but should not be able to read it. Only authorized party can decode it. For secure internet voting system RSA public key cryptography, Tripple DES and Honey algorithms are suggested at network level.

Biometrics

The identification of biological characteristics can be done. In this, voter can be verified by his/her signature or voice.

Antivirus softwares

Antivirus software can be used to protect computer where election ballot or data stored from viruses, worms, rootkits etc.

Firewalls

Firewall can protect the system from unauthorized entity by blocking them not to enter in private network.

XII. CONCLUDING REMARKS

When technology carelessly applied to system, then it can create risks and challenges that will shake the public's confidence. However technology itself can offer solutions. We should take the advantage of current momentum. The opportunity exists now and we should not let it go. We have presented a security architecture at network level, operating system level and physically level that permit the avoidance of problems between voters and election system .The internet voting system can increase the voters attendance and make available to everyone to vote from anywhere in country especially for physically disabled.

XIII. REFERENCES

[1] Bandyopadhyay M., Baumik P (2010) "*Zone Based Ant Colony Routing In Mobile Ad-hoc Network*" Copyright Clearance Centre (CCC) 978-1-4244-5489-1/10(IEEE 2010).

[2] Chen G., Guo T., Wang W., Zhao T. (2006), "*An Improved Ant-Based Routing Protocol In Wireless Sensor Networks"*1-4244-0429-0-/06(IEEE 2006).

[3] D. Kim, J. Garcia and K. Obraczka, "Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate", IEEE Transactions on Mobile Computing. Vol 2, no 2, 2003, pp.161-173.

[4] Gabber E., Smith M. A. (2004) "*Trail Blazer: A Routing Algorithm Inspired By Ants"*, IEEE International Conference on Network Protocols (ICNP'04).