E-Voting (in)Security

Praveen Mandava
Department of Computer Science
University of Auckland.
mcho061@ec.auckland.ac.nz

Abstract

This paper discusses a successfully implemented internet based voting system, CyberVote. A brief description of the CyberVote system is presented. The aim of this paper is analyse the security threats CyberVote has to face and measures adopted by this system to counter these attacks. Implementation details and a detailed description of every threat that is existent to every online voting system is beyond the scope of this article. Some of more general and relevant threats to CyberVote system have been considered. Wherever possible a comparison with other known security techniques is provided for better analysis.

2. Introduction to CyberVote:-

"CyberVote is an innovative cyber voting system developed for internet connected terminals and mobile phones. It is a research and development (RDT) program being funded by the European commission, with additional funding from the companies and partners undertaking the work". It is a part of the Information Society Technologies (IST) 1999 program for research, technology development and demonstration under the fifth framework program (5^{th} PCRD) [9]. This project is carried out by a consortium led by EADS Matra Systèmes & Information of France [1] and grouping together**:** British Telecommunications of the United Kingdom [2], Nokia Research Center of Finland [3],

K.U.Leuven Research & Development of Belgium [4], Technische Universiteit Eindhoven of the Netherlands [5], Freie Hansestadt Bremen of Germany [6], Mairie d'Issy-les-Moulineaux of France [7] and Kista Stadsdelsnämnd of Sweden [8].

CyberVote is an internet voting system that incorporates a highly secured and verifiable internet voting protocol which can be used in local, regional or national elections. This system has been mainly developed to influence and increase the convenience and participation of voters during the elections. CyberVote will allow the voters to cast their ballot through any internet connected PC or terminals, handheld devices such as palmtops and communication devices such as mobile phones. This facility will be helpful to all citizens but will particularly benefit those who are ill or disabled, elderly people, hospital patients, those who are traveling on the Election Day, expatriates, citizens away in foreign countries or even those who are too lazy to make it to the polling station.

It will rely upon an innovative voting protocol developed with in the project that uses off-the-shelf cryptographic tools in combination with advanced cryptographic tools that were specifically developed for this project. It is claimed that this will guarantee the authentication of the voter, privacy of their ballot when sending it over internet, integrity of the whole system and while vote counting and auditing process. In one sentence CyberVote online voting system is described as, “simple to use, accessible and affordable for all voters and candidates” [10].

3. Working of CyberVote:-

The initial step in organizing and conducting an election through internet using CyberVote involves configuration of one or several vote servers. The voting server architecture involves, Election Configuration Manager, Electoral Roll Manager, Tally Manager, Information Pages Database, Election Parameter Database, Electoral Roll Database, Ballots Database, Election Information Service, Voting Engine and Tally

Engine. A detailed description of these fundamental elements and the interfaces between is provided in [11, section 3.4].

A client needs to have a web browser and a CyberVote client software which can be pre-installed or can be downloaded. Using this client software a voter can get information or a graphical demonstration of the voting procedure and also could have pictures or other related information about the candidates. A simpler version of the same client software can be provided for the voters using mobile phones. All the voters first have to go through the mandatory process of registering with the registration server with the help of registration client pre-installed with the CyberVote client software where their credibility will be checked so as to allow only the eligible voters to vote.

“The CyberVote client has a Graphics User Interface (GUI), a socket connection module, voting protocols, cryptographic library, message coding, and interfaces to hardware token reader connected to the user’s hardware platform and to Public Key Infrastructure (PKI) server” [11]. The voting protocol module handles all the communication between the voting server and the client terminal, by creating voting and registration related requests. The standard mechanism used in transferring the requests and information between the server and the client is the web server/ web browser model using the HTTP or HTTPS protocols and the socket connection module handles these kinds of network connections. Secret key algorithms such as Secure Socket Layer (SSL) protocols [12][13] or Transport Layer Security (TLS) protocol [14] which is an internet standard of SSL protocol is used for a secured communication between the web browser and the web server [11].

Auditing and Tallying the votes is the last phase of internet voting system, CyberVote. This tabulation phase determines the count of votes that are valid and correctly received by the end of the voting phase and logs all other security problems that have occurred in the earlier phases. The tallier client software is responsible for making the final election results available in the web pages for the voters [11].

For a detailed implementation and technical reports on the CyberVote project is provided in [14] and [15].

4. Security Issues Concerning CyberVote :-

Every online or internet based system should satisfy a set of basic security requirements as described by Dr. Guido Schryen in [17] and other security issues that are specific for internet voting systems as described in [18]. “CyberVote implements high security measures not only in the steps in which the voters authenticate themselves and cast their votes, but also in the steps in which the votes are tallied and the election result is published and verified”. The designers and proponents of CyberVote system claim that this innovative internet voting protocol uses advanced cryptographic techniques to ensure integrity, secrecy of vote in ballot, uniqueness, privacy and authentication of the voters. CyberVote relies on Public Key Infrastructure for its operation. Individual votes are encrypted using a public key encryption algorithm called Homomorphic El-Gamal encryption scheme which uses randomly generated numbers [18].

According to the report on security analysis of CyberVote [18], they have divided the threats to their system into threats at the communication part, threats at the client side, threats at the server side and other general threats that are common to both the server and the client. In the following section I will try to analyze the security threats to CyberVote system and the measures they have consider to eliminate or mitigate them. These threats have been classified and presented in the same manner as in the security analysis report on CyberVote [18].

4.1. Communication Threats

Communication threats are those threats that arise from the network which carries out the communication between the server and the client (network in this sense refers to internet).

4.1.1 Denial of Service (DoS) Attacks :-

“Attacks where the legitimate users are prevented from using the system by malicious activities is termed as Denial of Service” [19]. In an internet voting environment a hacker could mount Denial of Service attack by overloading the election web server and preventing the voters from using the internet voting service. Basically there are two forms that these kinds of attacks can take. One of the possibilities can be that an adversary can swamp the network connection of the voting web server with junk data that clogs up the network and prevents the legitimate traffic getting through. The other variant can be that he can overload the web server’s computational resources with useless tasks that keep it busy and makes unable to attend the requests from the voters.

The defense mechanism adopted in CyberVote system against Denial of Service attacks is the implementation of secured routing protocols. CyberVote adopts a more common method of blocking these kinds of attacks by setting up a filter, or a sniffer on the network (e.g. Egress/ingress filters). “These filters can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed to block messages containing that pattern, protecting the Web servers from having their lines tied up”[18]. Other than this is no specialized or advanced prevention technique has been implemented in CyberVote.

Chun-Kan Fung and M.C. Lee in [20] discuss about Client puzzle based authentication and key establishment protocol, which can effectively resist Denial of Service attacks. This protocol generates puzzles of predetermined difficulty and sends to every client who requests a connection. The client has to commit its resources to solve the puzzle before expensive computational resources and memory allocations are committed by the server. This procedure will serve as a deterrent to the attacks that might exhaust server resources

[20]. This protocol can be implemented directly or in combination with the existing protocols to any internet voting to prevent or mitigate the effects of Denial of Service attacks.

4.1.2 Eavesdropping and Masquerading :-

A hacker may intercept and read the data traveling through internet, this is he can eavesdrop on the network and “Masquerading is sending or receiving messages using another entity’s identity” [18]. Attacker can pose as a voting server, present false ballot and client software and any voter who fails to check the certificate validity will be compromising his privacy and credentials details to the attacker. Another serious threat is the attack on the Domain Name Service (DNS), in which all the traffic to a legitimate voting server can be routed to a false web server set up by an adversary. In man-in-middle attacks, the adversary interposes between the voting server and the client terminal and simulates the communication the between them which can disenfranchise voters. The possibility of such threats is further worsened when the voter uses a public terminal to cast his vote like a terminal in library or a cyber café. The cyber café operator himself can take control of the terminal and act as man-in-middle [18] [19].

CyberVote uses authentication services to protect against masquerading. It uses Secure Socket Layer (SSL) protocol and Transport Layer Security (TLS) protocol that arranges a secure session between the server and the client. “SSL operates a handshake procedure to authenticate and exchange keys for the session. Public key encryption is used to generate a master secret between client and server, which in turn is used to generate session keys. In addition to exchange of keys, SSL allows negotiation of a cipher algorithm for the session” [18]. This kind of server certification can successfully avoid any man-in-middle attacks.

In order to prevent attacks on Domain Name Service (DNS) and spoofing of the voting server, Domain Name Server Security (DNSSEC) is used which provides Cryptographic authentication of DNS information. The designers and proponents of CyberVote system

claim the CyberVote protocols themselves use advanced cryptographic techniques to ensure the confidentiality of the voting process and the usage of SSL/TLS is just a additional layer of security measure [18].

But a different scenario of the above arguments was presented in [19]. The authors here claim that it is not possible to avoid such threats with the current internet environment. Even the usage of encrypted information exchange between the communicating parties does not help in preventing these threats. However, it is claimed that CyberVote system is more robust and tolerant to these kinds of attacks.

4.2. Client Threats

This section deals with the threats originating from the client side and the influence they have on the integrity and security of the entire voting system. Nature of these threats and the measures CyberVote system implements to prevent such threats is analyzed in the following section.

“Regardless of the kind of secure communication channel and voter authentication, a malicious code in a voting client can actually change the voter’s vote without the voter or anyone else noticing”. The fraud committed by such malicious code will be hard to detect or it might never be detected at all as they erase themselves after doing the necessary damage. Moreover such code can corrupt the data before the information is encrypted or authenticated. Following are some of the related threats that can arise from the client side of the voting system.

Trojan horses, Viruses and Worms

“If such a program were to be widely distributed and then triggered on or about Election Day, any voters could be disenfranchised or have their votes modified. Attacks do not

have to be confined to individual or random voters, but can be targeted on a particular demographic group" [18].

Accessing Screen or Keyboard

The attacker can steal sensitive data like authentication information or the voter's choice while casting the vote by logging the keystrokes, reading the mouse movements and clicks or even by taking snapshots of the screens [18].

Use of Remote Controlled Software

Use of such software can be a great threat to the secrecy and integrity of the ballot. With the help of such software an adversary can monitor the voter's actions and can even modify the ballot without the voter's knowledge [18].

CyberVote system implements a method of secure user interface which can be applied to CyberVote client software. In this method, the client will record voter specified display parameters and stores itself in a secured place. When a malicious code tries to pose itself as client module, then the user can identify the difference in display settings and take necessary action. CyberVote client also provides operating system security by configuring the operating system parameters such as process and access control to certain devices and thus provides memory protection and limited access to screen and keyboard. By protecting the memory it can prevent malicious code from executing and by limiting the access to keyboard and screen, it makes sure that no other application is reading the keystrokes and mouse movements other than CyberVote client software. CyberVote officials urge the voters to have virus scanners and personnel firewalls installed with all the updates in their systems [18].

"Perhaps the greatest challenge with Internet voting arises from the fact that, in contrast to conventional elections, electoral authorities no longer have control over all the equipment used by voters" [19]. Authors of the SERVE [19] report argue that, hackers and other adversaries can gain access to a large number of computers and the officials would be powerless to protect the integrity of the election. They believe that when the

voter uses others or a public terminal, there can be a remote spying or subversion software installed. Backdoors placed in software installed on the voters PC can monitor the user's actions and can subvert the voting process. Use of virus scanners and firewalls will be of little help as new viruses and Trojan horses are created very rapidly and they can only be detected and removed only after some time. Target based attacks can also be initiated on a small or large scale, than can disrupt the election process. "Even though such large scale attacks are detectable, there may be little one could do beyond invalidating the entire election, hardly a desirable outcome" [19].

It is quite clear from the arguments presented in this article that the defenses provided by CyberVote system against the threats arising from the client side of the system are not quite sufficient and effective. It can be deduced that, CyberVote is prone to attacks from the client side and such attacks could results in voter disenfranchisement, loss of privacy of the voters, vote buying, selling and switching even to the extent of reversing the outcome of that election.

4.3. Server side Threats

Denial of Service by Overloading the Server

Denial of Service can be achieved by consuming the network resources of the server or by consuming the disk space or CPU resources of the server. Another possibility that could result in server unavailability is destroying or altering the configuration information of the server. A detailed explanation of Denial of Service has been presented earlier in this report.

Unauthorized Access to Servers

An attacker could launch such an attack by gaining certain access privileges like passwords of the legitimate users of the server. “Some of the ways attackers use are sniffing, replay attack, password file stealing, observation, social engineering” [18].

Loss of Data due to Benign Failures

These kinds of attacks could lead to crashing of the voting server or disruption in network connectivity.

CyberVote system adheres to a more rigorous approach in detecting and preventing the Denial of Service attacks to the server. A firewall is implemented which not only routes the traffic to the voting server but also filters both inbound and outbound traffic and prevents any entry of the illegitimate user from launching Denial of Service attacks. This system also implements other measures such as cookies, rate limiting, disabling any unused or unneeded network services, redundant and fault tolerant network configurations. The use of cookies in CyberVote system prevents attacks that arise from IP spoofing as receiving any invalid cookie indicates that the IP address specified in that cookie is a fake one and the server rejects those kinds of messages and terminates the connection with that client and resets all the data structures that it has previously allocated for that connection. Rate limiting mechanism implemented in CyberVote system limits the bandwidth or the number of packets of a particular class that can enter the network. CyberVote system places replicated servers and duplicate lines at different sites so as to prevent loss of data in case of an attack or a server crash. Cryptographic techniques such as use of smartcards for secure login procedures for talliers and administrators are employed while accessing different servers [18].

These security enhancements adopted by the CyberVote system to defend the voting server against all possible attacks seem to make it one most secured voting server. Although firewalls and other implemented defense mechanism maybe stronger than the

regular ones, but still their abilities are limited. In addition they themselves could be a single failure point or bottleneck. “If defensive measures are triggered under a Denial of Service attacks that disperses offensive packets without obvious traits, the defensive methods will usually initiate enormous defensive sessions for all kinds of attacks, and then overwhelm themselves by propagating controlling messages, complicated computations, or immense raw data”[23]. Hence the CyberVote system can not guarantee its integrity during an attack that is higher in magnitude.

5. Conclusion

In this paper I have discussed an actually implemented internet based voting system, CyberVote. Implementation and the working of the system were also briefly described. The security features implemented by CyberVote system have been analyzed and I have also attempted to compare and contrast them with few existing known techniques. All the security details about CyberVote system discussed in this paper are taken from the public deliverables reports available at [16]. The actual system was tested with more than 1000 voters on 3 trial elections conducted in France, Germany and Sweden. The system demonstrated a very high level of security (90%) and voter satisfaction [10]. But judging the system based on few trails involving a very few individuals can not measure actual efficiency and the vulnerabilities or the attacks an internet based voting system such as CyberVote can come under.

“Because there are many different kinds of attacks that could be conducted against any internet based voting systems, it is essentially impossible to protect against all of them. While any particular attack taken in isolation might have a mitigation strategy, the cost of the defense could be high and would be added to the cost of defending against all the other attacks that have been anticipated. Worse yet, defenses created to inhibit one kind of attack may amplify the risks of another. And of course an attack that has not been anticipated remains a serious risk” [19]. There has not been any attempt to breach the security of CyberVote system does not mean that there was no attack at all. Many attacks

can be cleverly disguised hence they go undetected. With the help of the arguments provided it can be concluded that it is too early to implement CyberVote system on a large scale.

References

[1] EADS Matra Systèmes & Information of France
Available at : http://www.mdtvision.com.fr/infogen/societe/societe.html

[2] British Telecommunications of the United Kingdom
Available at : http://www.bt.com

[3] Nokia Research Centre of Finland
Available at : http://www.nokia.com

[4] K.U.Leuven Research & Development of Belgium
Available at : http://www.kuleuven.ac.be/kuleuven/

[5] Technische Universiteit Eindhoven of The Netherlands
Available at: http://www.tue.nl

[6] Freie Hansestadt Bremen of Germany
Available at : http://www.bremen.de/info/statistik

[7] Mairie d'Issy-les-Moulineaux of France
Available at : http://www.issy.com

[8] Kista Stadsdelsnämnd of Sweden
Availale at : http://www.kista.com

[10] Karl Schlichting et al., "CyberVote, Deliverable D22: 4th Evaluation Report", Version 1.0, European Commission Research Contract IST-1999-20338, 91 pp., 23 May 2003.
Available: http://www.eucybervote.org/HB-WP6-D22-v1.0.pdf, October 2004.

[11] Sylvie Brunessaux et al., "CyberVote, Deliverable D7: Report on mock-ups of architectures and overall system architecture", Version 2.0, European Commission Research Contract IST-1999-20338, 49 pp., 12 March 2002.
Available at: http://www.eucybervote.org/MSI-WP2-D7V2-V1.0.pdf

[12] **Analyzing Internet security protocols**
Yasinsac, A.; Childs, J.;
High Assurance Systems Engineering, 2001. Sixth IEEE International Symposium on , 22-24 Oct. 2001
Pages:149 – 159

[13] **Inside SSL: the secure sockets layer protocol**
Chou, W.;
IT Professional , Volume: 4 , Issue: 4 , July-Aug. 2002
Pages:47 – 52

[14] **Transport layer security: how much does it really cost?**
Apostolopoulos, G.; Peris, V.; Saha, D.;
INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE ,

Volume: 2 , 21-25 March 1999
Pages:717 - 725 vol.2

[16] "CyberVote Public Deliverables Reports"
European Commission Research Contract
Contract number: IST-1999-20338.
Available at: http://www.eucybervote.org/reports.html

[17] **Security aspects of internet voting**
Schryen, G.;
System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on , 5-8 Jan. 2004
Pages:116 – 124

[18] "CyberVote, Deliverable D6: Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting"
Version 1.0, European Commission Research Contract
IST-1999-20338, 55 pp., 28 January 2002.
Available at: http://www.eucybervote.org/TUE-WP2-D6V1v1.0.pdf

[19] **A Security Analysis of the Secure Electronic Registration and Voting \ Experiment (SERVE)**
D. Jefferson, A. Rubin, B. Simons, D. Wagner.;
Web manuscript, 21 Jan 2004.
Available: <http://servesecurityreport.org/>, February 2004.

[20] **A denial-of-service resistant public-key authentication and key establishment**

protocol

Chun-Kan Fung; Lee, M.C.;

Performance, Computing, and Communications Conference, 2002. 21st IEEE International , 3-5 April 2002

Pages:171 – 178

[21] **Requirements for a general framework for response to distributed denial-of-service**

Gresty, D.W.; Shi, Q.; Merabti, M.;

Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual , 10-14 Dec. 2001

Pages:422 – 429

[22] **Distributed denial of service attacks**

Lau, F.; Rubin, S.H.; Smith, M.H.; Trajkovic, L.;

Systems, Man, and Cybernetics, 2000 IEEE International Conference on , Volume: 3 8-11 Oct. 2000

Pages:2275 - 2280 vol.3

[23] **Analysis of denial-of-service attacks on denial-of-service defensive measures**

Wang, B.-T.; Schulzrinne, H.;

Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE , Volume: 3 1-5 Dec. 2003

Pages:1339 - 1343 vol.3