SECURITY FLAWS IN INTERNET VOTING SYSTEM

Sandeep Mudana

Computer Science Department

University of Auckland

Email: smud022@ec.auckland.ac.nz

Abstract

With the rapid growth in computer networks and internet, internet voting system can be a viable alternative for conducting an election and such a voting system must provide the same level of security as ordinary paper based elections. This paper discusses the various security threats for an online internet voting system and describes the most common threat in the communication medium, i.e. Denial of Service Attacks and its effects on the online voting system and describing few measures taken to prevent these attacks. However this paper does not propose a new online voting system. The paper also aims to provide a comparative overview of different authors based on the security measures taken to prevent the denial of service attacks.

Introduction

Internet Voting System is defined as a voting system, where we can cast our vote over Internet and send the vote to the concern election authority or officer safely. Internet voting is intended as a service to the electorate, so that the voters might have more convenience to cast their vote. They can vote from any where in the world by any computer connected to the Internet. The implementation of this internet voting system requires various technical solutions to ensure accurate voter authentication, secrecy of the ballot and security. As a voting method, any voting system (internet voting system or electronic voting system) needs confidence, without security there is no confidence. When designing any security architecture of any internet voting system, they should consider the insecurity of the communication medium. There are many security threats that are concerned with the internet for many commercial transactions like online payments, but still the advantages outweigh disadvantages for various business activities. And still there are been many research going on whether internet voting is safety or not, particularly in large organisation like any government elections in any country, most of the research organisations are still uncertain whether a secure internet voting system is suitable for a large organisation or not, because if something goes wrong in the internet voting system, then it would effect the decision of the entire country. And as the internet is open to the world, there are chances of various kinds of threats. In this paper I would introduce different kinds of threats to an internet voting system and as we know that the most common and important threat in internet is denial of service attack, so I would explain what denial of service attack is, types of attacks in denial of service and then explain how SERVE [1] or any internet voting system is effected by that and what are the feasible solutions or methods to avoid the attacks. [1, 2]

Requirements for Internet Voting System

According to [2] the basic requirements for the internet voting system are:

1. Authorization and authentication

Authorization is like only eligible or legal person can vote. For most of the government elections they require a minimum age of 18 years old to cast their vote. It can be done by the trusted authority and this process can be done before the elections.

Authentication is the process where the validation of the vote is checked at the time of casting the vote.

2. Mobility

This is one of the important factors in internet voting system; voter should be able to cast his vote from any where in the world, as long they have the required resources with them like internet, PC, etc. For this process authorization, authentication and some security features need to be implemented.

3. Flexibility

“Voters should be able to use different types of devices like desktop, laptop, mobile phones and different networks like Ethernet, wireless and dial-up connections”. [2]

4. Countability

This process is again dependent on authentication and authorisation. If these processes are implemented then Countability accepts, and this is nothing but to see that only the valid votes are counted.

5. Anonymity

“There should be no link between a particular vote and the person who cast the vote. In mandatory voting systems, the fact that the voter has cast a vote should also be recorded”. [2]

According to SERVE [1] the four main threats in internet voting system: [1]

1. Viruses or Malicious Software

There is a threat of introducing any malicious software onto the internet voting server before or on the Election Day by any communication link or email and also if huge number of PCs (personal computers) connected to the internet voting server, then any PC which is infected with virus, there might be more number of chances to spread the viruses to the voting server. The insecurity of the browser setup or operating system at the user end may easily lead to install the malicious software and which may change the confidentiality and integrity of the vote or even the vote may be changed without the knowledge of the voter before it is transmitted to the voting server. [1]

2. Hacking

If the links of the voting system is changed or hacked then the voter may face difficulty in casting his vote, which may change the confidentiality and integrity of the vote. [1]

3. Domain name service (DNS) attack

"Attacks against the Domain name service could route traffic to an attacker instead of to the legitimate vote service". [1]

4. Denial of service attacks (DOS)

This is a threat when the voter tries to cast his vote online and if the hacker overloads the election web server then that may lead to prevent the voter by not casting his vote. This type of attack is known as denial of service attack. According to the report of the SERVE [1] this is one of the serious attacks. [1]

What Denial of service attack is?

It is a resource-depleting attack on a network or on the internet such that the network would no longer be able to serve legitimate users.

If a user is under denial of service attack then his system may become unreachable due to the depletion of the resources of the system, thus the user could loose the control of his system. The denial of service attack can be directed at an operating system or at the network A proper planned denial of service attack is difficult to detect and may cause severe problem to the internet and as well as to the user. [4]

Denial of service attacks can happen by trying to flood the network with huge amount of traffic. The network will unable to know whether it's a legitimate traffic or malicious traffic during the attack. [4]

Distributed Denial of service attacks (DDOS)

"Distributed denial of service attacks are, thus, two stage attacks, the first stage being penetration of a large number of machines and the second stage the direct attack on the target". [4]

Distributed denial of service attacks are also hard to defend because the traffic is generated on huge number of systems and targeted to a specific system. These attacks are now very common and are primarily used for consuming up the bandwidth resources of the server.

"Distributed denial of service problems are expected to only become more severe and serious in the future. For instance, they could be used in cyber warfare to disable strategic business, government, public utility, and even military sites. They can also be used by cyber gangsters to blackmail companies that rely on internet connectivity for their revenues". [5]

Types of denial of service attacks

Denial of service attacks are basically divided into three different types [6]

1. Denial of service attack via bandwidth consumption

In this type of attack basically all the available bandwidth is consumed and no bandwidth remains for legitimate user. Basically a network might be flooded by UDP or ICMP ECHO packets to try and consume all available bandwidth.

"A simple bandwidth consumption attack can exploit the throughput limits of servers or network equipment by focusing on high packet rates – sending large numbers of small packets. High packet rate attacks typically overwhelm network equipment before the traffic reaches the limit of available bandwidth". [6]

"In practise, denial of service is often accomplished by high packet rates, nor by sheer traffic volume". [6]

2. Denial of service attack via protocol attack

These attacks are almost directly target the host machines and these are overcome by the patches in the operating system. Examples of protocol attacks.

- "SYN flood is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections". [6]

- In Smurf attack the attacker sends an ECHO request message directed to broadcast addresses. When the request is received by other systems in the network, all the systems in the network will reply to the ECHO message to the target system and as the number of request received from all the systems in the network are high and as it is difficult to manage by the amount of buffer allocated to the target system. [6]

3. Denial of service attack via logical attack

"Logical attacks exploit vulnerabilities in network software, such as web server, or the underlying TCP/IP stack". [6] Examples of logical attacks are [6]

- Teardrop
- Land crafts
- Ping of death
- Naptha

How Denial of Service attack affects internet voting system

According to the SERVE [1] report, “denial of service attack are serious risk for SERVE” [1]. The author says that it can affect the internet voting system in two different ways of denial of service attacks, in the first attack an hacker may able to change the network connection of the targeted web server with junk data that clogs the network and prevents the user or voter by accessing the web server and casting his vote. [1] A real time example in our daily life for this kind of attack is an email address we get more than 100,s of junk mails which are not relevant to us, and we waste most of the space in the mail box, by this we miss the required or wanted mails as they bounced because the inbox is filled with the unnecessary junk mails.

In the same way the hacker could overload the election web server with irrelevant data and prevent the electorate to cast his vote. “On the internet, denial of service attacks are often much more devastating, because internet denial of service attacks can be automated with a computer, and because suck attacks can often be mounted untraceably over the internet. [1]

In the second attack the hacker may put irrelevant resources with useless task on the election web server so that the server is busy; as if the server is busy it may unable to respond to the legitimate voters. This type of attack may mostly done on the last day of the election, as most of the electorate may plan to cast their vote on the last day, so if this kind of attack is done on the last day then most of the voters may fail to cast their vote.

Feasible Measures for denial of service attack

According to Cyber vote [3] some of the security measures that can be taken to avoid the denial of service attack [3]

“As a measure of precaution, routers have to be upgraded with the implementation of secure routing protocols. One of the more common methods of blocking a “denial of

service" attack is to set up a filter, or "sniffer," on a network before a stream of information reaches a site's web server. The filter 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 patter, protecting the web server from having their lines tied up". [3]

According to [7] some of the security measures can be taken to avoid denial of service attack.

- Filtering all the packets in the network which are entering and leaving the networks can prevent attacks from the neighbouring networks. "This measure requires installing ingress and egress packet filters on all routers". [7]

- Upgrade the host computers with the latest security patches and techniques, for example in case of the SYN flood attack. Increase the size of the connection queue, decrease the time-out waiting for the three-way handshake and employ vendor software patches to detect and circumvent the problem, these can be done to protect the host computers can take to guard themselves from the denial of service attack. [7]

- Disabling the IP broadcast, the host computers will not used as amplifiers in ICMP Flood and Smurf attacks. To prevent this attack all the neighbouring networks need to be disable IP broadcast. [7]

- Unused network services should be disabled to prevent tampering and attacks. [7]

- Monitoring the traffic patterns on the network can know when the system is under attack, and can protect itself by the attack. [7]

Conclusion:

In this paper we discussed about the internet voting system and its security threats, concentrating more on a particular threat namely, denial of service attacks on the internet. The other variants of these kinds of attacks and few possible counter measures that can be implemented in order to reduce the denial of service attacks.

In accordance with the arguments presented in the report [3] it can be derived that there is no realistic prevention technique to avoid denial of service attacks. There exist few precautionary measures which reduces the possibility of such attacks. According to the authors of [7] they argue that there is no complete solution in preventing the denial of service attacks, only few measures can be taken to avoid and defend to these attacks.

From the above articles and arguments produced by the authors of these articles I conclude that there are no complete defensive techniques existing for the resisting denial of service attacks. But only they are some precautionary measures which can be taken to avoid and defend the denial of service attacks. Hence I conclude that without the complete prevention of these attacks it's not a good idea to implement online internet voting system for any organisation like any country's government elections, as the total outcome of the election depends on the securing functions of the online voting system.

References

1. **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.

2. **Internet voting: concerns and solutions**
Chuan-Kun Wu; Sankaranarayana, R.;
Cyber Worlds, 2002. Proceedings. First International Symposium on, 6-8 Nov.2002
Pages: 261 - 266

3. **CyberVote consortium. D6V1, Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting, January 28, 2002. Vol.1.**
http://www.eucybervote.org/TUE-WP2-D6V1v1.0.pdf

4. **Protecting the Internet from distributed denial-of-service attacks: a proposal**
Crocker, S.D.;
Proceedings of the IEEE, Volume: 92, Issue: 9, Sept. 2004
Pages: 1375 - 1381

5. **Results of the Distributed-Systems Intruder Tools Workshop**
CERT Coordination Center and other
http://www.cert.org/reports/dsit_workshop-final.html
http://www.cert.org/reports/dsit_workshop.pdf , Nov 1999.

6. **Managing the Threat of Denial-of-Service Attacks v10.0**
Allen House holder, Art Manion, Linda pesante, George M. Weaver, CERT/CC
CERT Coordination Centre in collaboration with Rob Thomas
October 2001
www.cert.org/archive/pdf/Managing_DoS.pdf

7. **Defeating distributed denial of service attacks,**
Xianju Geng; Whinston, A.B.;
IT Professional , Volume: 2 , Issue: 4 , July-Aug. 2000
Pages:36 - 42