A Security Analysis of the **S**ecure **E**lectronic **R**egistration and **V**oting **E**xperiment (**SERVE**)

January 21, 2004

A web manuscript

By,

Dr. David Jefferson, d.jefferson@yahoo.com
Dr. Aviel D. Rubin, rubin@jhu.edu
Dr. Barbara Simons, simons@acm.org
Dr. David Wagner, daw@cs.berkeley.edu

Available at : http://servesecurityreport.org/

presented by : Mandava Praveen.

Summary

- This report is a review and critique of computer and communication security issues in the SERVE voting system, an internet-based voting system being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program).

- This report identifies potential vulnerabilities the SERVE system might have to various kinds of cyber-attacks, and tries to evaluate the degree of risk they represent to the confidentiality and the integrity of an election process.

What is serve?

- To participate, an eligible voter first must enroll in the SERVE program, which can be done completely electronically by presenting suitable citizenship or ID documents. This information is stored on the central web server and is later updated in the database.

- After enrollment, the voter will be able to register to vote, and then to vote from any internet-connected PC.

- When someone casts his vote, the completed ballot is stored on the SERVE central server, and later downloaded by the local election official for later canvass.

Significant threats to the security of SERVE

- Lack of Control of the Voting Environment

  → when a voter uses someone else's computer and

  → when the voter's own computer contains malicious software.

- Spoofing and Man in the Middle Attacks

  → Control the client machine

  → Control the local network

  → Control an upstream network

  → Spoof the voting server

  → Attack the Domain Name Server (DNS).

Significant threats to the security of SERVE (contd.)

- Denial of Service Attacks
  - » Ability to swamp the network connection of a targeted web server with junk data that clogs up the network and prevents legitimate traffic from getting through.
  - » The ability to overload the web server’s computational resources with useless tasks that keep it busy and eventually makes it unable to respond to connections from legitimate users.

→ Distributed Denial of Service (DDoS) attack.

→ Last-Day Denial of Service attacks.

Appreciative Comment

- Provides detailed description of the vulnerabilities of SERVE, and analyzes the significant threats to the security of the SERVE, taking into consideration earlier FVAP voting systems over the internet.

Critical Comments

- Short on technical details.
- Some of the threats described in this article like spoofing, vote buying, insider attacks, viral attacks on voter’s PC or in an extreme case spying on large set of users distributed over a large geographical area are not realistic.

Critical Comments (contd.)

- Pictures SERVE as entirely defenseless even against minor attacks, where as these kind of vulnerabilities were found in earlier online voting systems and the designers and developers of the SERVE system were well aware of it and might have offered resistance to these attacks to a certain degree.

Question

- Without compromising the confidentiality and integrity of an election process is it possible to construct an online voting system (such as SERVE) and implement it on a large scale with the current architecture of the internet and the PC hardware and software?