January 21, 2004
FOR IMMEDIATE RELEASE

**SECURITY EXPERTS URGE U.S TO ABANDON INTERNET VOTING PLAN**

*Online System Could Easily Allow Vote Tampering, Computer Scientists Say*

A federally funded online absentee voting system scheduled to debut in less than two weeks has security vulnerabilities that could jeopardize voter privacy and allow votes to be altered, according to a report prepared by four prominent researchers invited to analyze the system. All experts in cyber-security, they say the risks associated with Internet voting cannot be eliminated and urge that the system be shut down.

The report's authors are computer scientists David Wagner, Avi Rubin and David Jefferson from the University of California, Berkeley; The Johns Hopkins University and the Lawrence Livermore National Laboratory, respectively, and Barbara Simons, a computer scientist and leading technology policy consultant. They are members of the Security Peer Review Group, an advisory group formed by the Federal Voting Assistance Program to evaluate the system.

Administrators of this program, part of the U.S. Department of Defense, were charged with finding an easier way for U.S. military personnel and overseas civilians to vote in their home districts. Currently, these voters must rely on absentee paper ballots. But obtaining and returning paper ballots from a distant location can be a frustrating process that sometimes depends on slow or unreliable foreign postal services.

As an alternative, the federal program funded the creation of an Internet-based voting system called the Secure Electronic Registration and Voting Experiment, or SERVE. The system is slated to be used in 50 counties in seven states during this year's primary and general elections, handling up to 100,000 votes. The first tryout is scheduled Feb. 3 for South Carolina's presidential primary. The eventual goal is to provide voting services to all eligible overseas citizens, plus military personnel and their dependents, a population estimated at 6 million.

While acknowledging the difficulties facing such absentee voters, the authors of the security analysis conclude that Internet voting presents far too many opportunities for hackers or even terrorists to interfere with fair and accurate voting, potentially in ways impossible to detect. Such tampering could alter election results, particularly in close contests.

"Because the danger of successful large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear," the report states.

The authors of the report state that there is no way to plug the security vulnerabilities inherent in the SERVE online voting design.

"The flaws are unsolvable because they are fundamental to the architecture of the Internet," says Wagner, assistant professor of computer science at UC Berkeley. "Using a voting system based upon the Internet poses a serious and unacceptable risk for election fraud. It is simply not secure enough for something as serious as the election of a government official."

The researchers also believe that if no mishaps occur or are detected during this year's trial runs with the online voting system, federal or state governments might swiftly expand its use.

"The danger is that this system will work fine in a low-stakes setting like these first trial runs," says Rubin, technical director of the Information Security Institute at Johns Hopkins and an associate professor of computer science. "That will likely be used as an argument for expanding the system for even wider use. But that's like saying you don't ever need to wear a seat belt because you drove to work without crashing the car this morning."

The Internet voting plan, along with the growing use of touchscreen equipment not linked to the Internet, is part of a nationwide move toward greater use of computers, provoked in part by the problems associated with paper ballots during the 2000 presidential election. But the authors of the SERVE analysis conclude that opportunities for tampering are being overlooked in the rush to embrace new election technology.

"The SERVE system has all of the problems that electronic touchscreen voting systems have: secret software, no protection against insider fraud and lack of voter verifiability," says Jefferson. "But it also has a host of additional security vulnerabilities associated with the PC and the Internet, including denial-of-service attacks, automated vote buying and selling, spoofing attacks and virus attacks."

As currently implemented, certain members of the U.S. Armed Forces, the Merchant Marines, the Public Health Service and the National Oceanic and Atmospheric Administration, as well as U.S. citizens living abroad, are eligible to vote using SERVE. Such voters can go to the SERVE Web site using a Windows-based computer connected to the Internet and cast their ballots.

After studying the prototype system, however, the four researchers said it would be too easy for a hacker, located anywhere in the world, to disrupt an election or influence its outcome by employing any of several common types of cyber-attacks:

- A denial-of-service attack, which would delay or prevent a voter from casting a ballot through the SERVE Web site.

• A “Man in the Middle” or “spoofing” attack, in which a hacker would insert a phony Web page between the voter and the authentic server to prevent the vote from being counted or to alter the voter’s choice. What is particularly problematic, the authors say, is that victims of “spoofing” may never know that their votes were not counted.

• Use of a virus or other malicious software on the voter’s computer to allow an outside party to monitor or modify a voter’s choices. The malicious software might then erase itself and never be detected.

“Voting in a national election will be conducted using proprietary software, insecure clients and an insecure network,” says Simons, a former IBM Research Staff Member and a past president of the Association for Computing Machinery. “Congress and the Department of Defense should understand that providing soldiers with an insecure system on which to vote is not doing them any favors.”

The full security analysis of the SERVE system can be viewed online at http://www.servesecurityreport.org.

For detailed information about the SERVE system, including a list of participating states and counties, go to http://www.serveusa.gov/public/aca.aspx.

###

**NOTE:**

To arrange interviews with David Wagner, contact Sarah Yang at UC Berkeley’s Media Relations office at (510) 643-7741. Broadcast media who wish to interview Wagner should contact Julie Huang at UC Berkeley at (510) 642-6051.

To arrange print or broadcast interviews with Avi Rubin, contact Phil Sneiderman at The Johns Hopkins University news office at (443) 287-9960, or send e-mail to rubin@jhu.edu

Barbara Simons can be reached at (650) 328-8730 or simons@acm.org.

To contact David Jefferson, e-mail d_jefferson@yahoo.com.

###