UCSD Computer Security Expert: Touch-Screen Voting Machine Concerns Persist

October 29, 2004

Rex Graham

A computer security expert at the University of California, San Diego who has analyzed the software of one of the most popular touch-screen voting machines says election officials should regard any touch-screen machine that operates suspiciously on Tuesday as part of a "crime scene" to be investigated by computer forensics experts.

"Without specific expertise in computer forensics, election officials could inadvertently destroy critical indications of tampering or malfunction," said Yoshi Kohno, a computer security expert at UCSD who co-authored a 2004 paper in *IEEE Symposium on Security and Privacy* that found a variety of basic security flaws in an early version of the software in the Diebold AccuVote-TS machines. Kohno collaborated on the analysis of the Diebold software with Aviel D. Rubin, a computer science professor at Johns Hopkins University, Adam Stubblefield, a graduate student at Johns Hopkins; and Dan S. Wallach, a computer science professor at Rice University.

Kohno testified in July before the U.S. House of Representative's Committee on House Administration that the current generation of paperless electronic voting machines should not be used in an election. A study by Election Data Services Inc., of voting equipment used by election jurisdictions across the United States found that as many as 50 million registered voters are expected to cast ballots on electronic equipment during Tuesday's election.

Voting machine manufacturers have vowed to fix security problems discovered by Kohno and his colleagues, but Kohno said that since the software of most electronic voting machines is legally exempt from independent analysis, neither he nor election officials have a way to independently verify that touch-screen voting machines will perform on Tuesday as they should.

The Association for Computing Machinery (ACM), the world's oldest professional society of computer scientists, recently cited the security vulnerabilities that Kohno and his colleagues found in its recommendation that all electronic voting systems should generate a paper record to be inspected by voters to verify the accuracy of their ballot. Such a physical record of a ballot cast on a touch-screen machine, which only Nevada requires, would also serve as one type of independent check on the voting system. Peter G. Neumann, chair of the ACM Committee on Computers and Public Policy, wrote in the October 2004 special edition of *Communications of the ACM*, which was dedicated to problems with electronic voting machines, that the computer security community is deeply concerned with weaknesses in certification of voting machine software, the inability of testing to provide assurances that votes are counted correctly, the general secrecy of the evaluation process and vendor-commissioned evaluations, and the lack of any mechanism to perform independent recounts and audits of vote totals.

"Suppose each voting machine accidentally or maliciously records only a single vote for the wrong party on Tuesday; That could be enough to change the outcome of the election," said Kohno. "This is not just an idle concern. After all, after an election in Fairfax, VA, last year, election officials discovered that their electronic voting machines misrecorded a vote for one candidate one out of 100 times."

Washington state voting activist Bev Harris downloaded the Diebold AccuVote-TS software in 2002 after stumbling upon it by chance while she was surfing the Internet. The Diebold software "source code" that Harris downloaded is the only one that has undergone analysis by an independent group. Kohno testified in July that "spot-treating" security problems may raise the bar for a successful attack, but is no guarantee that other security flaws will be detected and fixed. "Unless all components of the revised system, including the software and revised procedures, are open to the public for public scrutiny and review, the public will have no reason to believe that the spot-treatment actually succeeded in addressing the security problems," Kohno testified.

The Diebold study indicated that it was theoretically possibility for somebody intent on adding votes for their candidate could change a few letters in hundreds of thousands of lines of software instructions to accomplish their goal.

The National Institute of Standards and Technology (NIST) has activated the National Software Reference Library as an "evidence room" housing digital signatures of voting machine software designed by Diebold, Sequoia Voting Systems, and other vendors. However, the data is limited in its usefulness because, as the NIST website states, "once software is installed on a voting machine, it is incapable of generating a digital signature."

"The NIST software library is a good first step in this effort to eventually verifying that voting machines have not been tampered with, but even improvements to this library won't identify other vulnerabilities," said Kohno. "We should keep in mind that many other kinds of attacks are possible."

Some problems that could seriously interfere with accurately registering voters' intent in the ballot box would go undetected even if a full forensic investigation is completed. For example, Kohno said that each touch-screen machine must be adjusted so that a fingertip pressed to a given candidate's name actually records a vote for that candidate. Touch-screen machines must be properly calibrated in the same way that personal digital assistants, which also have touch screens, must be calibrated. "The voting machine software could be uncompromised, but there have been problems with calibration, which could decrease the ability of voters to cast their votes the way they intend to," said Kohno. "Uncalibrated machines would behave like the infamous 'butterfly ballots' of 2000 where some Florida voters thought they were voting for one candidate when their votes were actually tallied for another."

Kohno said that any investigation of electronic voting machines after Tuesday's election - even by skilled computer forensic experts - may be inadequate. "Touch-screen voting machines are black boxes," said Kohno, "However, unlike the black box flight recorder of an airliner recovered after an accident, voting machines are sadly not designed to reveal whether the intent of each voter is accurately recorded on Election Day."

Media Contact: Rex Graham, UCSD Communications, (858) 822-3075