India's electronic voting machines are vulnerable to attack (w/ Video)

April 29 2010

(PhysOrg.com) -- Electronic voting machines in India, the world's largest democracy, are vulnerable to fraud, according to a collaborative study involving a University of Michigan computer scientist.

Even brief access to the paperless machines could allow criminals to alter election results, the seven-month investigation reveals.

In a demonstration video available at IndiaEVM.org, the researchers show two attacks against an actual Indian electronic voting machine. One attack involves replacing a small part with a look-alike component that can be instructed to steal a percentage of the votes from a candidate. Another attack uses a pocket-sized device to change the votes stored in the machine between the election and the public counting session, which in India can be weeks later.

"Almost every component of this system could be attacked to manipulate election results," said J. Alex Halderman, a U-M assistant professor of computer science and engineering who, with his students, helped to develop the attacks to test the security of the system. "This proves, once again, that the paperless class of voting systems has intrinsic security problems. It is hard to envision systems like this being used responsibly in elections."

These research findings are at odds with claims made by the Election Commission of India, the country's highest election authority, the researchers say. The commission, which maintains that weaknesses found in other electronic voting systems around the world do not apply to India's, has called the Indian machines "fully tamper-proof."

Almost the entire population of India uses electronic voting machines to cast ballots. The approximately 1.4 million machines in use there are of the "Direct Recording Electronic" (DRE) variety. DREs record votes to internal memory and provide no paper records for later inspection or recount. With DREs, absolute trust is placed in the hardware and software of the voting machines, the researchers say. Paperless electronic voting systems have been criticized globally and many countries and U.S. states are abandoning such systems.

"Such machines have already been abandoned in Ireland, The Netherlands, Germany, Florida and many other places. India should follow suit," said Rop Gonggrijp, a security researcher from the Netherlands who took part in the study.

"Never mind what election officials say, this research once again shows that the longstanding scientific consensus holds true: DRE voting machines are fundamentally vulnerable. In order to have any transparency in elections, you need to have votes on paper. Computers can be programmed to count votes honestly, but since nobody can watch

them, they might just as easily be programmed to count dishonestly."

The researchers also noted that the vote-counting software in the electronic voting machines is programmed into so-called "mask programmed microcontrollers," which do not allow the software to be read out and verified. Because these chips are made in the United States and Japan, nobody in India knows for sure what software is in these machines or whether it counts votes accurately, the researchers say.

"Everywhere I looked there were more security problems," said Hari Prasad, a computer engineer with NetIndia, Ltd who organized the study. "India deserves a transparent election process, which these machines simply cannot deliver."

This study was performed by researchers at NetIndia, Ltd., in Hyderabad, the University of Michigan in the United States, and at a non-profit in the Netherlands that specializes in electronic voting related issues.

Provided by University of Michigan