

FOR IMMEDIATE RELEASE

Thursday, April 29, 2010

India's Electronic Voting Machines Proven Insecure

A collaborative study by a team of Indian and international experts has revealed that the electronic voting machines used in Indian elections are vulnerable to fraud. Even brief access to the machines, known in India as EVMs, could allow criminals to alter election results.

These research findings are at odds with claims made by the Election Commission of India, the country's highest election authority, which has maintained that weaknesses found in other electronic voting systems around the world do not apply to India's EVMs. Less than a year ago, it stated: "Today, the Commission once again completely reaffirms its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever." [1] As recently as two days ago, the Chief Election Commissioner described electronic voting machines as "perfect" and claimed that "till today, no individual could prove that the EVMs used by the EC can be tampered with." [2]

Almost the entire population of India votes on electronic voting machines. There are around 1.4 million of the machines in use, all of the controversial "Direct Recording Electronic" (DRE) variety. Such machines record the votes only 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. Paperless electronic voting systems have been criticized globally and more and more countries and US states are abandoning such systems altogether.

In a video released today, the researchers show two demonstration attacks against a real Indian EVM. One attack involves replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favor of a chosen candidate. These instructions can be sent wirelessly from a mobile phone. Another attack uses a pocket-sized device to change the votes stored in the EVM between the election and the public counting session (which in India can be weeks later).

This study was performed by researchers at NetIndia, (P)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.

The researchers were also surprised to find that the vote-counting software in the EVMs 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 US and Japan, this has led to a situation in which nobody in India knows for sure what software is in these machines or whether it counts votes accurately.

Hari Prasad is a computer engineer and managing director of NetIndia, a Hyderabad-based technology firm. Prasad organized the study and says the findings are the culmination of a seven month investigation. "Everywhere I looked there were more security problems. I am glad that with the presentation of this work, the debate over whether India's EVMs are secure is over. We need to look forward now. India deserves a transparent election process, which these machines simply cannot deliver."

Rop Gonggrijp, a security researcher from the Netherlands, also took part in the study. Says Gonggrijp: "Never mind what election officials say, this research once again shows that the longstanding scientific consensus holds true—DRE voting machines are fundamentally vulnerable. Such machines have already been abandoned in Ireland, the Netherlands, Germany, Florida and many other places. India should follow suit."

Gonggrijp continues: "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. How is the voter supposed to tell the difference?"

Professor J. Alex Halderman of the University of Michigan helped develop the new attacks along with his students. "Almost every component of this system could be attacked to manipulate election results," says Dr. Halderman. "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."

G.V.L. Narasimha Rao is a well known political analyst and author of the book titled "Democracy at Risk! Can we trust our EVMs?" Commenting on the results of the scientific study, he said, "*Today, the distrust among political leaders of all hues in voting machines is so high that most losers are wondering if they had been unfairly defeated in polls. It is about time India shunned paperless voting to make its election outcomes verifiable and auditable.*"

[1] ECI press release, August 8, 2009

[2] Interview with Navin B Chawla, Rediff.com India news, April 26, 2010

