

EVM SECURITY - MYTHS AND REALITY

By Sameer Jalnapurkar

“The people who cast the votes decide nothing. The people who count the votes decide everything.” – Joseph Stalin

The arrest of Hari Prasad, MD of Net India and EVM security researcher, has had the positive effect of re-igniting the debate about the trustworthiness of our EVMs. Since fair elections are at the heart of democracy, this is a matter that concerns us all. In this article, our goal is to elucidate the issues related to EVMs and their use. These issues can be grasped, given a little patience, even by the non-technical layman. If short of time, we would urge you to read at least the section on hardware Trojans.

Some basic facts: An EVM is a simple computer. The main chip that controls the EVM is an imported "microcontroller". The software is also stored on this chip. EVMs are assembled by the Public Sector Units ECIL (Hyderabad) and BEL (Bangalore).

EVM software: The following points are noteworthy as regards the software:

1. In each of the Public sector Units (PSUs), there is a software development group of 2 or 3 engineers, and a software testing group. Nobody outside these groups is allowed to access the source code.
2. After the software is developed at the PSUs, compiled code is sent abroad to the microcontroller manufacturer. The software is installed on the microcontroller at the premises of the foreign manufacturer. (see ref. [1])
3. After the microcontroller chips are shipped by the foreign manufacturer, the software cannot be read. Thus, it is impossible to verify the software on Indian soil. [2]

The danger in this process is clear: Could the small software group in each PSU be influenced or compromised? What if the foreign microcontroller manufacturer makes changes the software before installation on microcontrollers? In either scenario, the Indian people have no way of finding out, since the software cannot be verified.

Software Trojans: At this point one may object: Are not the microcontrollers and the EVMs tested at the PSUs, and by a "mock poll" exercise before each election? Yes, but this is only "functional testing" [1]. The software itself is not verified. Functional testing cannot detect "Trojans" hidden in the software. A possible scenario is that an EVM could be instructed to favour a particular candidate using special key combinations. For example, to instruct the EVM to favour candidate number N , the procedure could be to press key numbers 14 and 16 simultaneously, followed by key number N .

Since the candidates in a constituencies are allotted key numbers in alphabetical order by

name, activation of a Trojan in favour of a particular candidate could be done any time after the names of the candidates become known. There are ways for such a Trojan to evade the mock poll test, even if activation is done beforehand [3]. The Trojan could also be activated during the poll (perhaps even by someone accessing the EVM as an ordinary voter), or after the polling is over, at any time up to the time of display of the result.

Randomization: EVMs are normally stored at the District Headquarters. Before use in a poll, they are first supposed to be randomly allotted to constituencies within the district. Then, inside each constituency, the allotment to polling booths is also supposed to be random. It is often claimed by the EC that these randomizations provide another layer of security. It is true that to activate a Trojan in advance, one would have to know to what constituency the machine was going. Thus, Trojan activation could not happen before the first level of randomization, in which EVMs are allotted to constituencies. It must be noted, however, that in general elections, a district corresponds roughly to one parliamentary constituency. In that case, the first level of randomization becomes vacuous, so Trojan activation could be carried out before it. The second level of randomization does not appear to play any useful role. Even in the case of state assembly elections, wherein there are multiple constituencies per district, the randomization itself could very well be rigged. The EC's procedures appear to provide ample opportunities for this - each individual state Chief Election Officer is supposed to develop his own randomization software [4]. Finally, we reiterate that Trojans could very well be activated during or after polling, which would defeat all randomizations.

The record of votes: EVMs are supposed to record each vote (and in fact, each key-press) with a time-stamp, the list of which can be printed out. EVM proponents often claim that this provides verifiability to EVMs. However, a Trojan that changes the election result will certainly change these records. It is not possible to verify whether a particular voter's vote was recorded correctly, unless the precise time at which the voter voted is independently recorded, using a clock synchronized with the internal clock of the EVM. Even if this is done, in case of any discrepancy, it would not be clear whether the voter is lying, or whether the EVM was rigged, or whether there was a problem with the clock synchronization.

It is sometimes claimed (for example, in [5]), that any Trojan activation could be detected from the record of all key-presses. This claim is invalid, since a Trojan could very easily erase the key-presses that led to its activation.

Hardware Trojans: It is exceedingly important to note that even if the software is flawless, no software can be relied on to behave as expected if the hardware design itself is malicious. How justified is the fear of such "hardware Trojans"? The evidence is that the threat is very real. It is well worth reading with care the following excerpts from a study by John Markoff, published by the New York Times on Oct 27, 2009:

Current and former United States military and intelligence agency executives ... argue that the menace of so-called Trojan horses hidden in equipment

circuitry is among the most severe threats the nation faces in the event of a war in which communications and weaponry rely on computer technology.

As advanced systems like aircraft, missiles and radars have become dependent on their computing capabilities, the specter of subversion causing weapons to fail in times of crisis, or secretly corrupting crucial data, has come to haunt military planners. The problem has grown more severe as most American semiconductor manufacturing plants have moved offshore.

A recent White House review noted that there had been several “unambiguous, deliberate subversions” of computer hardware.

“These are not hypothetical threats,” the report’s author, Melissa Hathaway, said in an e-mail message. “We have witnessed countless intrusions that have allowed criminals to steal hundreds of millions of dollars and allowed nation-states and others to steal intellectual property and sensitive military information.”

Cyberwarfare analysts argue that while most computer security efforts have until now been focused on software, tampering with hardware circuitry may ultimately be an equally dangerous threat. That is because modern computer chips routinely comprise hundreds of millions, or even billions, of transistors. The increasing complexity means that subtle modifications in manufacturing or in the design of chips will be virtually impossible to detect.

“Compromised hardware is, almost literally, a time bomb, because the corruption occurs well before the attack,” Wesley K. Clark, a retired Army general, wrote in an article in Foreign Affairs magazine that warns of the risks the nation faces from insecure computer hardware.

“Maliciously tampered integrated circuits cannot be patched,” General Clark wrote. “They are the ultimate sleeper cell.”

Indeed, in cyberwarfare, the most ancient strategy is also the most modern.

Internet software programs known as Trojan horses have become a tool of choice for computer With hardware, the strategy is an even more subtle form of sabotage, building a chip with a hidden flaw or a means for adversaries to make it crash when wanted.

But as military planners have come to view cyberspace as an impending battlefield, American intelligence agency experts said, all sides are arming themselves with the ability to create hardware Trojan horses and to hide them deep inside the circuitry of computer hardware and electronic devices to facilitate military attacks.

In the future, and possibly already hidden in existing weapons, clandestine additions to electronic circuitry could open secret back doors that would let the makers in when the users were depending on the technology to function. Hidden kill switches could be included to make it possible to disable computer-controlled military equipment from a distance. Such switches could be used by an adversary or as a safeguard if the technology fell into enemy hands.

A Trojan horse kill switch may already have been used. A 2007 Israeli Air Force attack on a suspected partly constructed Syrian nuclear reactor led to speculation about why the Syrian air defense system did not respond to the Israeli aircraft.

Separately, an American semiconductor industry executive said in an interview that he had direct knowledge of the operation and that the technology for disabling the radars was supplied by Americans to the Israeli electronic intelligence agency, Unit 8200.

The United States has used a variety of Trojan horses, according to various sources.

In 2004, Thomas C. Reed, an Air Force secretary in the Reagan administration, wrote that the United States had successfully inserted a software Trojan horse into computing equipment that the Soviet Union had bought from Canadian suppliers.

According to a former federal prosecutor, ... during the early '80s the Justice Department, with the assistance of an American intelligence agency, also modified the hardware of a Digital Equipment Corporation computer to ensure that the machine — being shipped through Canada to Russia — would work erratically and could be disabled remotely.

Former Pentagon officials said the United States had not yet adequately addressed the problem.

“The more we looked at this problem the more concerned we were,” said Linton Wells II, formerly the principal deputy assistant defense secretary for networks and information integration. “Frankly, we have no systematic process for addressing these problems.” [6]

Making matters worse is the fact that detecting hardware Trojans in a complex integrate circuit, which can have tens of thousands or even millions of transistors and interconnections, is virtually impossible. Indeed, the view of the US military is:

“Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits.” [7]

The present situation is that we have no way to verify, on Indian soil, the software installed at the premises of the foreign microcontroller manufacturer. But it is important to keep in mind that even verifying the software would not assure safety. A hardware Trojan is practically undetectable, and may well cause our system to behave in ways quite different from what we expect.

So what would it take for an election system to be acceptable? No nation can rightfully call itself a democracy if its election system is based merely on trust. What is needed is transparency and verifiability, not just for select technical experts, but also for the candidates and ordinary citizens. It was this fundamental principle that led the German Supreme Court to completely ban the use of EVMs. Even if the absence of software or hardware Trojans could be guaranteed (which is not possible), there would still be a need for a paper record of the votes.

There have been proposals for the EVM to print votes on a roll of paper than stays inside the machine, and can be viewed through a window. However that is still quite unsafe, because of the dangers of pre-printed rolls and excess vote-printing. Also, the reliability of the printer is an issue.

Another possibility is for the EVM to print out a receipt (like an ATM), which can be verified by the voter and put by him into a ballot box. This is acceptable, but again, the printer could be problematic.

A third possibility is to use a machine to either stamp or punch votes on ballot papers, which could then be counted either by hand or by machine. This is also acceptable, but the chain of custody of the ballots is of utmost importance – **the voter must be given the ballot paper, must verify it, and then put it by hand in a ballot box that is continuously under observation, and physically separate from any machine.**

It should be remembered that the traditional way of paper ballots and hand counting, used without a hitch recently in Telangana, is also quite good. Fraud can occur in the traditional system, but the scale is limited, and it is also much easier to detect. As a general rule, the more technically complex a system, the more opportunities there are for dishonest insiders to perpetrate large scale, undetectable frauds.

It would be naïve to take for granted that all election administrators will always have the best interests of democracy at heart. In fact, one former Chief Election Commissioner was, as per a judicial commission report, a person who had “rendered himself unfit to hold any public office which demands an attitude of fair play and consideration for others.” [8] The moral is that the price of freedom is eternal vigilance.

Coming up on October 4 is an all-party meeting called by the Election Commission, to discuss, amongst other issues, the trustworthiness of EVMs. It is hoped that citizens will take an informed stand, and make their voices heard. Our democracy can survive only through your active involvement.

The author can be contacted at evm.security@gmail.com

Notes and References:

[1] Press Release issued by the Election Commission, available at <http://www.pib.nic.in/release/release.asp?relid=51718> .

[2] Interview of Dr PV Indiresan, Technical Advisor to the Election Commission. This interview can be seen at <http://www.youtube.com/watch?v=ZICOj1dEIDY> (from time 3 min 30 sec to 4 min 20 sec).

[3] One possibility is to specify, during activation, when the Trojan is to become effective. This would rely on the EVM's internal clock. The time specified can be after the mock poll is expected to be over. The other possibility is for the Trojan code to be written so as to be come effective only after a sufficiently large number of votes, where the threshold is more than the number of votes that could be cast in a mock poll test.

[4] EC Checklist for CEOs - http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/CEO_checklist.pdf , page 18.

[5] Indiresan Committee report on EVMs, <http://www.scribd.com/doc/6794194/Expert-Committee-Report-on-EVM>

[6] Old Trick Threatens the Newest Weapons, <http://www.nytimes.com/2009/10/27/science/27trojan.html>

[7] Defense Science Board Task Force, "High performance microchip supply" Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Feb. 2005.

[8] "Chawla should step down", The Pioneer, Feb 10, 2009.
<http://www.dailypioneer.com/155464/Chawla-should-step-down.html>