To
Dr. Nasim Zaidi, Chief Election Commissioner, New Delhi

24 April 2017

Re: EVM Challenge

Dear Dr. Zaidi,

We are a group of well-wishers trained in engineering and the sciences. We understand that the EVM challenge has been initiated by the Election Commission as a response to allegations that the recent elections were rigged. From a technical perspective, such allegations are best addressed by auditing VVPAT records where they exist. The EC could, however, use this challenge as an opportunity to increase electoral process transparency. Additionally, independent of the outcome of the challenge, the EC should check the outcome of each election by creating, maintaining and auditing VVPAT records.

The issue of EVM security is not a political one, but a technical one. From a technical perspective, to understand what kind of tampering is possible, actions that might be performed by an insider in the process, or a criminal, should be allowed during the challenge. In the event that the EC prevents some type of access, (it disallowed physical tampering in 2009) it should explain why an insider or a criminal would not have that kind of access.

Additionally, we believe the following are necessary to fully understand EVM security strengths and weaknesses:

1. Individuals should be allowed to choose their instruments and to physically tamper with an EVM.
2. They should be provided design documents and test descriptions and results, as well as information about the security procedures in place, for each generation of EVM currently in use.
3. The results obtained by each team examining the EVMs should be made public.
4. Longer term testing by a team with in-depth expertise in computer security and voting system security should be performed, and its results be similarly made public, in the manner of the Top-To-Bottom-Review ordered by the Secretary of State of California, USA, in 2007.
5. A team of experts should be tasked with preparing recommendations to address each important security vulnerability discovered during the challenge and the longer term testing; their report and the decisions of the EC regarding timeline for addressing each issue should be made public. The process should be open, and comments from external experts should be solicited.

The EC should note that it is virtually impossible, whatever the qualification of the individual examining the EVM, to determine with certainty that EVMs are tamper-proof. Electronic devices can be designed to detect when they are being tested, and it is practically impossible to test for every possible configuration and scenario. Hence, if the EVM challenge does not detect a problem, this does not mean that election outcomes are guaranteed to be secure in the future; regular VVPAT audits can help address this issue.

Our Position on EVM Security

As engineers and scientists, we know that an electronic device, such as the EVM, is not transparent to the human voter. As such, the human voter does not know whether his or her vote was recorded or counted correctly. Further, our experience and education indicates to us that machine errors and human error in the processes of design, testing and deployment can result in an incorrect output.

Electronic devices cannot be guaranteed to be immune from tampering when there is a large number of insiders with access and non-insiders with mal-intent, attempting to subvert the deviceÕs functioning. These include everyone who may have access to the EVM over the cycle of design, manufacture, testing, storage, maintenance, calibration and deployment.

The Indian EVM is interesting from a design perspective because it is a single-purpose device, unlike most other voting machines developed elsewhere, and its functionality is achieved through a combination of hardware and firmware. The prescribed process for its use does not require wireless communication and it is not fitted with hardware to enable such communication. Thus, it is not immediately vulnerable to exactly the same attacks that work on other voting machines. However, the design by itself is not sufficient to protect the EVM from tampering or error. A general class of vulnerabilities is common to both the Western machines and the EVM. These vulnerabilities arise because of the difficulty of determining exactly what a given electronic machine will do in every scenario, and because those with physical access can change and probe aspects of the hardware or software (for example, they can fit the machine with a wireless receiver, swap out a ROM, or determine the key used to provide cryptographic security).

While the EC has announced several times that it believes that the EVM is tamper-proof because of certain design aspects, there has been no release of any detailed information about these design features. As a result, there is no clarity regarding EVM security.

The EVM Challenge, beginning on 1 May 2017, should be treated as a means through which voters and the public in the worldÕs largest democracy may understand the security strengths and weaknesses of their voting technology. It would be a waste of time and energy if the EVM Challenge is executed as a superficial exercise without full access and transparency. Our recommendations for enabling transparency in the process are listed in the main body of this letter.

Independent of the outcome of the EVM Challenge, the EC should enable the creation of VVPAT records, ensure their secure storage separate from the EVMs, and conduct regular VVPAT audits for each election. It is heartening to note that funding for VVPAT capabilities was recently approved by the Cabinet after persistent requests from the EC. The creation of the VVPAT records is not sufficient, however; the records for each election should be audited. Audits involve the examination of a randomly-chosen subset of the VVPAT records and are, generally, much more efficient than a full hand count.

The EC has a well-deserved excellent reputation worldwide. It successfully carries out elections in a very challenging environment: with a large number of voters over diverse geography, climate, literacy and culture, making extraordinary efforts to be inclusive of all voters. We hope that the EC will keep up the positive momentum and conduct a genuinely open and substantial EVM Challenge so that voters may understand better the capabilities and limitations of their voting technology. This can only enhance the trustworthiness of our elections and the vibrant nature of Indian democracy.

Signatories

Note that affiliations below are included for identification purposes only and do not reflect the view of the signatoriesÕ employers or collaborators.

David D'Lima
Education: B. Tech. (IIT-Bombay); M. S. (North Carolina State University);
Position: Vice President, Integrated Platforms and Solutions
Wipro, Bengaluru

Shripad Dharmadhikary
Education: B. Tech. (IIT-Bombay)
Position: Policy Researcher
Manthan Adhyayan Kendra, Pune

Gautam Doshi
Education: B. Tech. (IIT-Bombay); M. Eng. (University of California, Berkeley);
Position: Senior Principal Engineer
Intel Co., Bengaluru

Bopana Ganapathy
Education: Ph. D. (University of Kentucky)
Position: VP Engineering & Site Leader
CA Technologies, Bengaluru

Manjusha Madabushi
Education: B. Tech. (IIT-Bombay); M. S. (Northwestern University);
Position: Co-founder
Talentica Software, Pune

A M Nagabhushan
Education: M. Tech. (IIT-Bombay);
Position: Professor
Ramaiah Institute of Technology (MSRIT), Bengaluru

Narendra Nande
Education: B. E. (Amravati University); M. E. (Shivaji University);
Position: Senior Director, Software Engineering
Eximius Design Inc., Bengaluru

Nitin Shimpi
Education: B. Tech. (IIT-Bombay); M. S. (Marquette University)
Position: Co-founder
Talentica Software, Pune

Soumitra Sen
Education: B. E. (Jadavpur University); M. Eng. (IISc.); PGSM-MBA (IIM, Bangalore)
Position: VP & Head of Engineering, Cloud Managed Security
Paladion, Bengaluru

K V Subrahmanyam
Education: B. Tech. (IIT Bombay); Ph. D. (TIFR Mumbai)
Position: Professor
Chennai Mathematical Institute

Sanjay Tambwekar
Education: B. Tech. (IIT-Bombay); M. S. (North Carolina State University);
Position: CTO
Qwikcilver Solutions, Bengaluru

Vibha Apte-Gaitonde
Education: B. Tech. (IIT-Bombay); M. S. (Oregon Health and Science University);
Position: TPM, Technical Infrastructure Deployment Engineering
Google, Mountain View

Hanmant P. Belgal
Education: B. Tech. (IIT-Bombay); M. S. (North Carolina State University);
Position: Principal Engineer
Intel Co., Sacramento

Rema Hariharan
Education: B. Tech. (IIT-Bombay); M. S. (Virginia Polytechnic Institute and State University); Ph. D. (University of North Carolina, Chapel Hill);
Position: Senior Principal Data Scientist
eBay, Austin

Milind Kandlikar
Education: B. Tech (IIT-Bombay); Ph. D. (Carnegie Mellon University);
Position: Professor, Liu Institute for Global Issues and Institute for Resources, Environment and Sustainability
University of British Columbia

Manisha Kher
Education: B. Tech. (IIT-Bombay); M. S. (Syracuse University);
Position: Senior Principal Software Engineer
New York Genome Center

Nasir Memon
Education: B. Eng. and M. S. (BITS-Pilani); Ph. D. (University of Nebraska);
Position: Professor, Computer Science and Engineering,
New York University (Brooklyn)

Varun Nagaraj
Education: B. Tech. (IIT-Bombay); M. S. (North Carolina State University); MBA (Boston University);
Position: President and CEO
Sierra Monitor Corporation, Milpitas

Bhagirath Narahari
Education: B. Tech (BITS-Pilani); M. S and Ph. D. (University of Pennsylvania);
Position: Professor, Computer Science
The George Washington University, Washington, DC

Gurumurthy Ramachandran
Education: B. Tech. (IIT-Bombay); M. S. (Virginia Polytechnic Institute and State University); Ph. D. (University of North Carolina, Chapel Hill);
Position: Professor, Environmental Health and Engineering,
Johns Hopkins University, Baltimore

Pankaj Rohatgi
Education: B. Tech (IIT-Delhi); Ph. D. (Cornell University);

Position: Fellow, Security Technology
Rambus Cryptography Research Division, San Francisco Bay Area

Sanjay Sarma
Education: B. Tech (IIT-Kanpur); M. E. (Carnegie Mellon University); Ph. D. (University of California, Berkeley)
Position: Professor, Mechanical Engineering
Massachusetts Institute of Technology (MIT), Boston

Amitabh Shah
Education: M. Sc. (IIT-Kanpur); M. S. and Ph. D. (Cornell University);
Position: Strategic Business Development Consultant to software companies
San Francisco Bay Area

Anil M. Shende
Education: M.Sc. (BITS-Pilani); M. S and Ph. D. (State University on New York at Buffalo);
Position: Professor of Computer Science
Roanoke College

Gitanjali Swamy
Education: B. Tech (IIT-Kanpur); Ph. D. (University of California, Berkeley); MBA (Harvard);
Position: Director of Special Projects, Private Capital Research Institute at Harvard Business School

Poorvi L. Vora
Education: B. Tech. (IIT-Bombay); M. S. (Cornell); M. S. and Ph. D. (North Carolina State University);
Position: Professor, Computer Science
The George Washington University, Washington, DC

Arun Yethiraj
Education: B. Tech. (IIT-Bombay); M. S. (Louisiana State University); Ph. D. (North Carolina State University);
Position: Meloche-Bascom Professor of Chemistry
University of Wisconsin at Madison