02.11.2010

This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.

Analysis of an Electronic Voting System

TADAYOSHI KOHNO | ADAM STUBBLEFIELD | DAN S. WALLACH

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. We conclude that this voting system is unsuitable for use in a general election. Any paperless electronic voting system might suffer similar flaws, despite any certification it could have otherwise received. We suggest that the best solutions are voting systems having a voter-verifiable audit trail, where a computerized voting system might print a paper ballot that can be read and verified by the voter.

Dept. of Computer Science and Engineering, University of California at San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA. E-mail: tkohno@cs.ucsd.edu. URL: http://www-cse.ucsd.edu/users/tkohno. Most of this work was performed while visiting the Johns Hopkins University Information Security Institute. Supported by a National Defense Science and Engineering Graduate Fellowship.

Information Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. E-mail: astubble@cs.jhu.edu. URL: http://spar.isi.jhu.edu/.astubble.

IInformation Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. E-mail: rubin@cs.jhu.edu. URL: http://www.avirubin.com.