Malicious Takeover of Voting Systems: Arbitrary Code Execution on Optical Scan Voting Terminals

Russell J. Jancewicz Aggelos Kiayias Laurent D. Michel
Alexander C. Russell Alexander A. Shvartsman

Center for Voting Technology Research and Computer Science & Engineering
University of Connecticut, Storrs, CT 06269, USA
russell.jancewicz@uconn.edu, {aggelos,ldm,acr,aas}@cse.uconn.edu

ABSTRACT

This work focuses on the AccuVote Optical Scan voting terminal (AV-OS) that is widely used in US elections. We present a new attack that can be delivered without opening the system enclosure, and without changing a single bit of the system's firmware. The attack is launched by inserting a maliciously programmed AV-OS memory card into the terminal. The card contains binary code that exploits careless runtime memory management in the system's firmware to transfer control to alternate routines stored in the memory card. Once the control is taken by the injected code, the voting system is forced to operate according to the wishes of the attacker. In particular, given that the attack results in the execution of the arbitrary code, an attacker can completely take over AV-OS operation and compromise the results of an election. It is also noteworthy that once a memory card is compromised it can be duplicated using the native function of the voting terminal. In some past elections it was observed that up to 6% of all memory cards were involved in card duplication. There exists a non-trivial possibility that the infection on one memory card can propagate virally to other cards in a given election. This development was performed without access to the source code of the AV-OS system and without access to any internal vendor documentation. We note that this work is performed solely with the purpose of security analysis of AV-OS.

SAC'13 March 18-22, 2013, Coimbra, Portugal.