US e-voting system cracked in less than 48 hours

Friday, 16 March 2012 10:26 -

Researchers at the University of Michigan have reported that it took them only a short time to break through the security functions of a pilot project for online voting in Washington, D.C. "Within 48 hours of the system going live, we had gained near complete control of the election server", the researchers wrote in a paperPDF that has now been released. "We successfully changed every vote and revealed almost every secret ballot." The hack was only discovered after about two business days – and most likely only because the intruders left a visible trail on purpose.

The security experts investigated common vulnerable points such as login fields, the virtual ballots' content and filenames, and session cookies – and found several exploitable weaknesses. Even the Linux kernel used in the project proved to have a well known vulnerability. They were also able to use the PDFs generated by the system to trick the encryption mechanism, while unsecured surveillance cameras provided additional insights into the infrastructure. While the open source nature of the code made their work somewhat easier, they believe that attackers would have been able to make quick headway even if the system had been proprietary.

More...