

E-Voting Security

From 1992 to 1996, Rob Harris managed to rig 34 slot machines in Nevada to pay out money to him and his accomplices on demand. The attack did not require direct access to the slot machines; Harris simply inserted code into a device that gaming control employees use to test if machines are functioning correctly. When the machines were tested, a program was copied into the slot machines. The program did not affect the machines' performance—that is, until a particular sequence of coins was inserted, activating a special mode that caused the machines to pay out winnings in unusually large amounts. This fraud went undetected until Harris became greedy. When he won a US\$100,000 jackpot, officials investigated, and he was ultimately tried and convicted.

DAVID L. DILL
Stanford University

AVIEL D. RUBIN
Johns Hopkins University

Rob Harris was an insider. He worked for the Gaming Control Board in the Electronic Services Division in Las Vegas. (For more details on this story, see www.reviewjournal.com/lvrj_home/1998/Jan-10-Sat-1998/news/6745681.html.) Insiders commit crimes not only in gambling, but in banking and many other endeavors where computers protect valuable assets. Crime is easier and more profitable for insiders, whether it involves computers or not. We know about the Harris case only because he was caught, but how many times have such crimes occurred without being detected? We'll never know.

Electoral system

Our electoral system protects our government's assets, which greatly exceed the cash in slot machines, yet electronic voting machines are developed and deployed with far less rigor and care for security than gambling machines. The companies that sell these machines and the election officials who buy them generally fail even to acknowledge the possibility of an insider attack, or consider it only to dismiss it out of hand. Worse, such attacks would likely be undetected in most electronic voting ma-

chines, because there is no independent way to check whether votes are recorded accurately.

From a computer security perspective, electronic voting is the worst of all possible worlds. The assets at risk are extremely valuable; the incentives for people who want to tamper with the results are extremely strong; and the level of sophistication that some attackers can bring to bear is extremely high. As if that were not enough, the system must discard information that would normally be considered critical for later audits: the relationship between voters and their votes.

Recent events have brought the security problems with electronic voting systems into the national spotlight. It began when the source code for Diebold's electronic voting machine leaked onto the Internet. A study by researchers at Johns Hopkins and Rice universities uncovered serious security flaws; follow-up studies sponsored by the states of Maryland and Ohio found similar problems.

Hundreds of computer scientists and thousands of others have urged that all voting equipment have a voter-verifiable audit trail, which is a permanent record of the vote that the voter can check for accuracy be-



fore leaving the polling place and that is saved for later recounting (see the endorsements of the Resolution on Electronic Voting at www.verifiedvoting.org). Partly in response to this, California's Secretary of State mandated that all electronic voting machines must provide a voter-verifiable paper trail by 2006. In addition, federal legislation is under consideration, and several US presidential candidates have proposed similar requirements.

While states are moving toward electronic voting, the US government is also deploying a service to allow US citizens abroad and all military personnel to vote over the Internet using Windows machines running ActiveX. The project, the Secure Electronic Registration and Voting Experiment (SERVE), will allow voters in 51 counties in seven

states to vote in the 2004 general election. The government anticipates that over 100,000 votes will be cast this way. Government officials invited a review of this project by a group of security experts, whose report warns of serious security vulnerabilities in the system. (The report will be available at <http://servesecurityreport.org> by the time you read this.)

E-voting special issue

This special issue comes at a time when electronic voting and voter verifiability are receiving constant media attention. The three articles in this issue collectively provide an overview of the issues, a description of the problem, and a potential solution. “Election Security: Perception and Reality,” David Evans and Nathanael Paul’s article, describes the challenges with respect to electronic voting, security, and human factors. The authors outline voting systems’ requirements and provide a summary of existing technologies. The article then describes interface issues and ways of increasing trust in voting systems.

Jonathan Bannet, David W. Price, Algis Rudys, Justin Singer, and Dan S. Wallach’s article, “Hack-a-Vote: Security Issues with Electronic Voting Systems,” demonstrates the feasibility of the insider threat. The authors describe the Hack-a-Vote system in which students squared off against each other in a competition. One side attempted to hide malicious code that would change an election’s outcome, and the other side was tasked with detecting that code. The article demonstrates the ease of an insider attack and just how difficult it is to detect malicious code.

David Chaum’s article, “Secret Ballot Receipts and Transparent Integrity: Better and Less-Costly Electronic Voting at Polling Places,” describes a radically different voting system with mathematically provable properties that let each voter verify that his or her vote is not only cast accurately, but is counted properly in the final vote totals. Voters are provided with receipts for their votes with the interesting property that only the voter can decode the receipt. This avoids the vote selling and coercion that are usually of concern with voting receipts. The system is based on an open platform and represents a novel addition to the current crop of voting technologies.

In the future, we hope to see better voting machines that reduce the trust required in the software component and provide voters with confidence. Several states, such as California and Nevada, have already declared that voter verifiability will be part of any machine they use. We hope this positive trend will continue. □

David L. Dill is a professor of computer science at Stanford University. His research interests include formal verification of system designs including software, hardware, and protocols, and more recently, electronic voting. He received a PhD in computer science from Carnegie Mellon University. He is also the founder

of verifiedvoting.org, an educational and advocacy group for accountability in election systems. Contact him at dill@cs.stanford.edu.

Aviel D. Rubin is an associate professor of computer science and Technical Director of the Information Security Institute at Johns Hopkins University. He is author of several books including Firewalls and Internet Security, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), White-Hat Security Arsenal (Addison Wesley, 2001), and Web Security Sourcebook (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is associate editor of ACM Transactions on Internet Technology and an advisory board member of Springer’s Information Security and Cryptography book series. Rubin serves on the board of directors of the Usenix Association and on the DARPA Information Science and Technology Study Group. Contact him at rubin@jhu.edu.

How to Contact Us

Writers

For detailed information on submitting articles, visit www.computer.org/security/author.htm.

Letters to the Editors

Send letters to Kathy Clark-Fisher, Lead Editor, kclark-fisher@computer.org. Please provide an email address or daytime phone number with your letter.

On the Web

Access www.computer.org/security/ for information.

Subscription Change of Address (IEEE/CS)

Send change-of-address requests for magazine subscriptions to address.change@ieee.org. Be sure to specify *IEEE Security & Privacy*.

Subscribe

Visit www.computer.org/subscribe/.

Missing or Damaged Copies

If you are missing an issue or you received a damaged copy, contact membership@computer.org.

Article Reprints

For price information or to order reprints, send email to security@computer.org or fax +1 714 821 4010.

Reprint Permission

To obtain permission to reprint an article, contact William Hagen, IEEE Copyrights and Trademarks Manager, at copyright@ieee.org.