Did Your Vote Count?

November 17, 2008

If you're in California, you can thank UC Santa Barbara's Computer Security Group for helping ensure it did. If you live in another state with electronic voting systems...

Every vote counts? or does it? When a presidential election rolls around, that question suddenly takes center stage. Now, thanks to the Computer Security Group (CSG) in the Computer Science Department at UC Santa Barbara, we know a lot more about the security and vulnerabilities of electronic voting machines, and specifically about how and where those machines could be breached by hackers and the votes erased or results altered.

The Bad News is...

... they found electronic voting systems wide open to abuse and identified numerous opportunities to infiltrate and compromise the voting process.

They exposed vulnerabilities when voting machines are prepped and tested at county offices, while they're stored unprotected at precincts before elections, and even during the few minutes someone is in the voting booth.

The Good News is...

At least in California, the state has acted on the group?s findings to safeguard the
integrity of the vote by decertifying most of the machines, recertifying some after procedural modification for restricted use, and relying more heavily on traditional paper ballots.

?I think (Secretary of State for California) Debra Bowen has done a good job of securing things here in California,? said Professor Richard Kemmerer, head of the security group.

Ms. Bowen invited the group to Sacramento last year to assess the Sequoia voting machines. At the same time, experts from UC Berkeley and UC Davis were reviewing other leading brands, Diebold (now Premier Election Solutions) and Hart InterCivic.

While California has mothballed or modified many of its suspect machines, some states using similar equipment have taken no action. ?Those states are still very vulnerable,? Kemmerer said.

Currently, seven states rely completely on direct touch-screen electronic voting. And according to Bev Harris, founder of Black Box Voting, a nonprofit watchdog group based in Renton, Wa., about 99 percent of all votes are now cast electronically or electronically scanned.

Convinced that voting machines and optical scanners are equally vulnerable, Harris favors paper ballots and full public scrutiny of the counting process. She further argues that, since many precincts have modest numbers of votes which can be easily counted by hand, it makes little sense to use computers for the process.

Kemmerer has been working in the field of computer security for more than 30 years. When he joined the UCSB faculty in 1979, he estimates there were fewer than 10 universities with computer security groups, and maybe only half those were active.

The reason was simple: for many years, computer security just was not considered an issue. Kemmerer recalls someone he talked to in 1983 asking why he needed a password for his computer, saying there was nothing in there he minded anyone else seeing.

Twenty-five years later, most people use passwords to protect their computers, knowing they contain a labyrinth of financial and personal information that they definitely do not want to share.

Still, says Kemmerer, it took a couple of major global events before everyone woke up to the importance of security and the potential havoc that could be created by people
hacking into computer systems.

The first was Y2K. When the global clock ticked over from 1999 to 2000, a lot of people were expecting systems failures triggered by the so-called ?millennium bug?, a failure of computers to recognize the year ?00? after decades of double-digit numbers.

?I think the real value of all this was that people began to realize that computers control everything we do,? said Kemmerer, ticking off things like water and power supplies, nuclear reactors and rail networks.

The second event was the terrorist attacks of September 2001 which Kemmerer says raised the specter of assaults on nations through their computer networks; this, in turn, increased the importance of intrusion detection and cyber defense.

?I think the real value of all this was that people began to realize that computers control everything we do,? said Kemmerer, ticking off things like water and power supplies, nuclear reactors and rail networks.

Since 9/11, much more funding has become available for studying computer security, reliability, privacy and intrusion detection. ?So, after 30 years, I no longer have to explain why we need to be looking at this,? he said.

According to Kemmerer, technology now exists to stage all manner of malicious attacks, from targeting a pacemaker inside someone?s chest to launching massive ?denial of service? attacks that can cripple a corporate giant on the other side of the world.

Ironically, the tools to become a cyber thief or online hacker are readily available online. ?You can go online and shop for attack tools to do this,? said assistant professor Christopher Kruegel. ?You barely need any technical knowledge.?

Kruegel, who joined the faculty and the Computer Security Group a year ago, paints a grim picture of the cyber landscape in which the threat from criminals in places like Eastern Europe, Russia and China is becoming more serious but less visible.

Because we hear less these days about ?worms? and other highly contagious Internet viruses, Kruegel thinks people have been lulled into a false sense of security. ?But it?s not getting better, it?s getting worse,? he says. ?It?s just not so obvious.?

For many years, this research unit within UCSB?s Department of Computer Science was known as the Reliable Software Group?it was only about 18 months ago that the
name was changed to the Computer Security Group, a more accurate reflection of its core focus.

A decade ago the group was looking at Web browsers and experimenting with its own versions of spyware, the little software package you may unknowingly take home after visiting a site and which then tracks your every cyber move.

In the late ?90s, CSG set up spoof attacks showing it could penetrate online bank accounts, obtain customer names, account and PIN numbers, and even (theoretically) transfer money around. It then told the banks so they could plug the holes.

The Federal government?s focus fell on electronic voting in the wake of the Florida presidential election shambles eight years ago, when the world watched election officials trying to interpret votes by intently studying hanging chads.

After a series of hotly-contested recounts left candidates George Bush and Al Gore only a whisker apart, the electoral bickering was finally silenced by a Supreme Court decision enabling Florida to certify the vote in Bush?s favor.

Since that debacle, companies like Sequoia, Election Systems & Software (ES&S), Diebold and Hart have begun offering hardware and software that they claim will accurately and securely record democracy in action.

However, Kemmerer and his team, who also completed a study of the ES&S system for the Ohio Secretary of State, strongly disagree. ?These companies all saw a market,? he said. ?In the process they made a lot of assumptions that were never tested?until now.? Associate professor Giovanni Vigna, co-leader of the eight-member testing team, says it?s obvious that systems have been built up piecemeal and lack a clear overall design. ?Anyone who has taken two classes of computer science could do better,? he said.
teams battle through a qualifying round just to grab one of eight spots in the final.

Vigna, who teaches a class on hacking, said DefCon is a hardcore event attracting challengers from areas like the military and security companies, some of whom won’t even give their names.

The DefCon competition is based on a Capture-the-Flag scenario: each team is given the same computer to defend and to use in attacking their opponents’ systems. Teams score points by hacking into the opponents’ systems, indentifying their weaknesses, attacking those flaws, blocking attacks on their own systems, and repairing damage inflicted on their systems by others’ attacks.

In 2002 Vigna started something similar just for universities. Now billed as the world’s largest university-based hacking competition, the International Capture the Flag event takes place at UCSB during a single day each December. Last year it drew 36 teams, comprising about 450 students, from universities in the United States, Europe, India, South America, Australia and Russia.

Each team in the competition has an Internet server providing virtual services, such as banking, car rental, or retail sales. The web pages have all been seeded with vulnerabilities which the teams have to find and patch on their own servers while trying to compromise others. The university competition is simpler and briefer than DefCon, said Vigna. It’s also an educational experience. Help is available to the competing teams, and the students gain knowledge through the competition.

**Relevant links:**

DEFCON Hacking Convention and Competition:  
[defcon.org](http://defcon.org) [2]

Vigna, whose areas of research include Web security and intrusion detection, criticized the abysmal quality of the software and elementary mistakes found in many components of the patchwork systems.

UCSB’s computer security experts uncovered vulnerability and exposure to risk
throughout the election process, and documented their findings in two short videos that have so far logged nearly 80,000 viewings on YouTube. The group’s work and their videos have been covered by the New York Times, Forbes, and multiple national technology and political blogs.

Critics have suggested that what CSG was able to achieve with unlimited laboratory access to machines and plenty of time, could not possibly be duplicated in a real election. The team’s video and reports, however, show how quickly they were able to corrupt the memory card and, with it, the voting machine; indeed, they demonstrated a whole series of equally fast attacks and related problems.

Their demonstrations included showing how quickly equipment security seals can be bypassed, even inside the voting booth—a voting machine results cartridge is switched in under 18 seconds, and various other machine components can be accessed by removing a few housing screws.

Malicious software, capable of deleting votes or switching them between candidates, can be introduced as easily as planting a USB flash drive or by accessing a memory card.

The group also demonstrated a Trojan virus which was programmed to conceal itself by behaving normally when the system was routinely tested, then corrupting results during voting; such a virus can also be programmed to delete itself after the election, leaving no trace it was ever there.

Finally, the group showed that vote-flipping software could be programmed to spread through the system-like a virus, meaning a single criminal intrusion at one machine could eventually infect many others.

The significance of all this is not lost on Vigna, especially after the razor-thin margin in the 2000 presidential race. “We already know which are the critical, swing states,” he says, suggesting the corruption of relatively few precincts could well determine a state or national election outcome.

“I’m appalled there are still states allowing electronic voting with no paper trail,” says Vigna, an Italian who is astonished that this country lets its precious democracy hang by such a slender thread.

He sees two solutions: One is to create an entirely new system with built-in, ongoing security checks; the other is to implement continuous security evaluations of existing systems, using independent, fulltime, paid monitors.

Vigna believes one way to safeguard the voting process is to fill out paper ballots and count them through optical scanners. Although these are also vulnerable, he says they are simpler and easier to secure than voting machines.

“With paper ballots you have a paper trail and can have a recount if necessary. If everything else goes down you can still vote, but if the machines fail you can’t vote.”

Voters can feel grateful to UCSB’s Computer Security Group for helping protect their franchise. In turn, Secretary of State Bowen earns one vote—of thanks—from Vigna.
She had the guts to take our recommendations to heart and find the least painful way to trade off what we’re using right now with the security issues we raised.

Relevant links:

- Computer Security Group [3]
- California Secretary of State’s Top-to-Bottom Review [5]

Latest Issues

Tag Cloud

ocean biomedical inventions optics electrical engineering recruiting photonics organic solids Amazon organic semiconductors CAMP biomolecular regenerative medicine internet materials coenzyme Q10 nuclear spin memories undergraduate research nanotubes eye Computer Science virus Luann Becker social networking Four Eyes Lab energy pancreas environment physics hydrogen John Bowers brain semiconductors quantum computing disease data centers proteins biodiversity Brad McRae solar energy bacteria SIMS MEMS CNSI thermoelectric

Source URL: http://convergence.ucsb.edu/article/does-your-vote-count

Links: