Hack-a-vote: Students learn how vulnerable electronic voting really is

October 7 2008

This week undergraduate and graduate students in an advanced computer security course at Rice University in Houston are learning hands-on just how easy it is to wreak havoc on computer software used in today's voting machines.

As part of his advanced computer science class, Rice University Associate Professor and Director of Rice's Computer Security Lab Dan Wallach tests his students in a unique real-life experiment: They are instructed to do their very best to rig a voting machine in the classroom.

Here's how the experiment works:

Wallach splits his class into teams. In phase one, the teams pretend to be unscrupulous programmers at a voting machine company. Their task: Make subtle changes to the machines' software -- changes that will alter the election's outcome but that cannot be detected by election officials.

In the second phase of the experiment, the teams are told to play the part of the election's software regulators. Their task is to certify the code submitted by another team in the first phase of the class.

"What we've found is that it's very easy to insert subtle changes to the voting machine," Wallach said. "If someone has access and wants to do damage, it's very straightforward to do it."

The good news, according to Wallach, is "when looking for these

changes, our students will often, but not always, find the hacks."

"While this is a great classroom exercise, it does show how vulnerable certain electronic voting systems are," Wallach said. "If someone had access to machines and had the knowledge these students do, they surely could rig votes."

Even though students were often able to find the other team's hacked software bugs, Wallach said that in real life it would probably be too late.

"In the real world, voting machines' software is much larger and more complex than the Hack-a-Vote machine we use in class," he said. "We have little reason to believe that the certification and testing process used on genuine voting machines would be able to catch the kind of malice that our students do in class. If this happened in the real world, real votes could be compromised and nobody would know."

Wallach hopes that by making students aware of this problem, they will be motivated to advocate changes in America's voting system to ensure the integrity of everyone's vote.

In 2006, electronic voting machines accounted for 41 percent of the tallied U.S. votes. Fifty percent were cast on paper, and 9 percent "other," including New York's lever machines.

Source: Rice University