
Cuyahoga County Ohio Possibly Exposed Election System to Computer Virus

(November 02, 2006) - Contributed by Steven Hertzberg, Election Science Institute

The memory cards that will be used to store votes on Election Day in Cuyahoga County, Ohio were stuck into ordinary laptop computers in September, possibly exposing the county's election system to a virus infection. This serious security lapse was caught on video through the efforts of Cleveland resident Adele Eisner and Cleveland-area filmmaker Jeffrey Kirkby, who has graciously made his raw footage available on the Internet for personal viewing here.

Just one month ago a Princeton evoting study showed that the memory cards used in Diebold touchscreen voting systems could carry computer viruses that would infect voting machines and steal votes on the infected machines.

"Diebold has repeatedly stated that this type of security breach is virtually impossible due to security practices employed by the vendor and election officials," said Edward Felten, Professor of Computer Science and Public Affairs at Princeton University. "Anyone who watches the video can now see for themselves that a virus could penetrate the election system via tasks performed by election staff."

The new video shows a group of election workers sitting at tables, each with a laptop computer. An official explains that these laptops were gathered from around the office, and some are the personal laptops of election workers. Each worker has a laptop and a stack of memory cards, and is inserting the memory cards one by one into the laptop. Cuyahoga County officials claim that every one of the county's memory cards gets this treatment, in order to archive vote records from the May 2006 primary election onto CD-ROMs.

Ordinary laptops are of course vulnerable to computer viruses and other malicious software. Given the number of ordinary laptops in the room, it is reasonably likely that at least one is infected with spyware, a virus, or other malware. This puts at risk the memory cards, and the votes they will record from next week's election.

Given the vulnerability of touch screen voting systems, election procedures must be stringent and consistently followed. Safe procedures call for memory cards to be inserted only into computers that are carefully secured and never connected to the Internet. Using ordinary laptop computers, borrowed from offices and homes, to process memory cards is dangerous. The video shows that this practice is not the isolated act of a few election workers, but an official plan put in place by election officials.

"Not only does this video demonstrate how potential security threats can be realized, this is yet another illustration of how election officials are forced to develop their own processes and procedures in order to operate their new election systems," said Steven Hertzberg, Project Director at Election Science Institute. "Often we find that critical procedures and essential tools were not developed or deployed with this new election system, leaving election officials to fend for themselves. Diebold should have provided an archiving system as part of their delivery to jurisdictions, before this system went live nationally."

Voting machine vendors and election officials often argue that rigorous procedures can compensate for the technical weaknesses of voting machines. Some jurisdictions implement such procedures well, but many do not. Talking about procedural controls is easy. Putting them into practice is much harder.

"I first raised concerns to the Cuyahoga County Board of Election in mid-Summer, after Secretary of State Blackwell released an advisory about transferring electronic election data to CD ROM. After I witnessed the transfer, I raised concerns a potential security breach to Cuyahoga Board of Elections Chairman Bennett and the rest of the board on October 2nd," said Adele Eisner. "Unfortunately, the board simply defended its dangerous practice."