See: Harri Hursti work on this here. Thanks to Black Box Voting for permission to use.

Replaceable Media on Optical Scan

Harri Hursti with Eric Lazarus

Taxonomy

Modification of basic functionality by replacing unprotected executable on replaceable media

Method

Generally, memory cards are thought of as containing data, including primarily the ballot definition data files (files that allow the OpScan to read the ballots) and, secondarily, the vote totals.

However, can memorycards also contain executable program which is started by firmware. Due programming programming langages cababilities, modified programs can falsify reports produced, hide pre-set counters, etc. Due capabilities of the interpreter are not know, what are the extends to use this exploit for trojan horses and other software and not be fully understood.

At least one major vendor has replaceable media (specifically, its memory cards) carrying software. This easily modified software is responsible for printing out the vote totals. It prints the "zero" tally report at the start of polling, and vote totals after the polls close. However, it is not template or macro script, instead it is modified BASIC language variant, making pool of programmers able to write these programs very large

> *The perpetrator must (a) acquire access to the PCOS memory cards, or (b) be able to change files on the central tabulator before election definitions are loaded into memory cards or (c) connect the PCOS machine to telephone line for remote reprogramming of the card. There is no password or other methods preventing change of the card or remote reprogramming. Any of these methods (among others) can be used to replace the software responsible for report generation on them or replace the cards with new cards with modified software on them. Method a also enables pre-election manipulation of the vote counters, injection of extra data to be transmited to central tablulator Election Night and conceal this with modified pogramming.*
>
> *To avoid detection, the perpetrator must prevent or subvert any hand counting or replace the paper ballots with forged ballots.*

Applicability

This attack applies to Optical Scan systems where software resides on the memory cards or other forms of removable or rewritable media.

Given the confidentiality of voting technology in the US, it is not possible for us to know exactly how many vendors keep their “print drivers” or "report generators" (the software which tells the printer how to tally ballots) or other executable software on replaceable media. However, we are certain (via testing performed by Harri Hursti) that at least one major vendor has its report generation program on replaceable memory cards. Memory cards are not vetted by the Independent Testing Authorities before being used.

Resource Requirements

Perpetrator(s) will need some programming background and (1) access to the cards, (2) the ability to inject files directly or indirectly to central tabulator before election definitions (i.e., the "defined ballot" for the election) are copied to cards (tampering with the central tabulator might be done on-site, or via modem if locality using PCOS connects the central tabulator to a telephone line, or (3) reprogramming the memory card via modem if the PCOS is connected to the central tabulator via a telephone line.

Note: The central tabulator is most often employed to perform ballot definition (i.e., creating ballots for election), copying of ballot definitions to the memory cards (so that voter choice will be recorded accurately), as well as tabulation of voter choice. The central tabulator is a conventional PC with additional software added. Accordingly, it provides a convenient single point of attack from which one can modify all the printer drivers from all the PCOS scanners. If this machine were to be used to generate the list of the Automatic Routine Audit (ARA) random polling places to be hand-counted, the attackers could arrange to make sure that the attacked polling places were never audited. This would assist the perpetrator(s) in avoiding attack detection.

Potential Gain

The number of votes that could be stolen this way is only limited to the number that could plausibly be changed without raising suspicions due to differences with exit polling and other polling numbers, etc.

Likelihood of Detection

If no hand count is performed, detection is unlikely.

Countermeasures

- Automatic Routine Audit (ARA) were the polling places are not selected by the tally server but "out of a hat" from a list known to be complete.
- Avoiding interpreted programs (i.e. programs that are not "compiled" and therefore somewhat easier for attackers to read and/or modify.)
- Avoiding the use of software on replaceable media
- Avoiding the use of any software by making all programs into firmware (programs that are burned as read-only onto special memory chip) (see: Read Only Memory) and that is validated via a strong method (i.e., someone is authorized to periodically pull the memory chip to ensure that it has not been tampered with) as in the gaming industry.

  Use or 3rd party equiment and software to compare memory cards with known-to-be-good reference image. It is important to know that due the central tabulator can be infected, central tabulator itself can not verify authenticacy of the card.

Attack Economics

One person with programming experience and access to central tabulator and/or the PCOS units.

Variations on attack theme

Attacks where a marked ballot can change the tally total.

Conclusions

Automatic Routine Audit (ARA) is critical.

The ITA system appears to have failed to warn the potential buyers, the public at large and computer security experts that the architecture of this system left open a “backdoor” vulnerability.

Citations

- Original report

Retrospective

This "backdoor" to installing software means that the software inspected by the ITA is not even necessarily the software that will run on Election Day. In certain makes and models the Logic & Accurancy test software is completely separated from Election Day under all circumstances, rendering L&A test results always meaningless.

The fact that vendors have created a system which allows users to replace software via memory cards suggests that they are extremely concerned with creating a flexible, adaptable system. Unfortunately, this flexibility opens up risks we need to be aware of and to mitigate.

Comments:

From JohnKelsey - 2005-09-19 2:58 PM

It seems like the obvious countermeasures here involve not allowing executables to be tampered with. Any kind of open-ended evaluation ought to catch this, and any decent security standards should say that you're not allowed to leave executable code someplace where it can be accessed by the attacker without some kind of cryptographic protection.