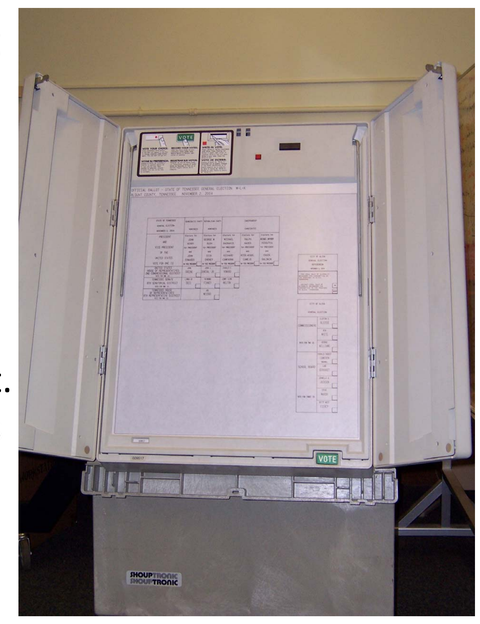
Dissecting a Voting Machine

Computer Science & Engineering Department

LEHIGH UNIVERSITY

Semih Demirbag • Advisor: Prof. Daniel P. Lopresti

About The Project & Machine

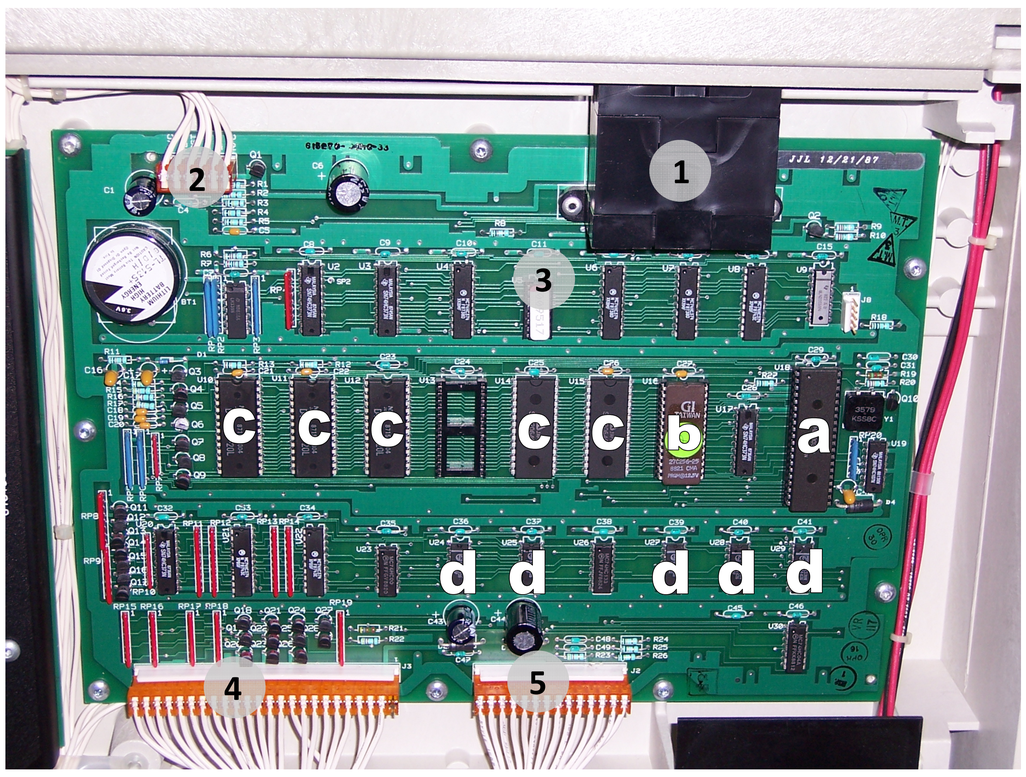


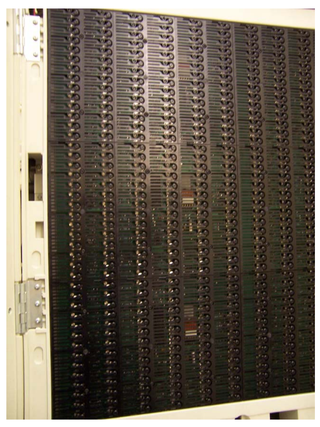
Danaher 1242 was first developed in 1983, and has been in use ever since. A full face, direct-recording electronic voting system, that is still used in several counties of Pennsylvania, including Bucks County. 1242 has a matrix of push-buttons, which are hidden behind the ballot sheet. Machine has a digital copy of this ballot in its memory, and it is programmed for the correct button-ballot configuration before an election. When elections are opened, machine stores the votes in its internal memory and a memory cartridge. Cartridges are collected at the end of the election day, and their contents are read by election officers.

1242 has many recorded problems during previous elections, where votes have been lost, and results were left in doubt. The aim of this project is to find out the internal design of this machine, and deduce if machine is susceptible to attacks software-wise, or, if it is possible to *hack* this machine.

Machine used in this project was manufactured in 1987, and acquired by Lehigh University for research. It was dismantled in order to access its micro controller, and determine its properties.

Components





The push button array behind ballot face

Under the back panel: officer's control panel (left), micro – controller (top-right) and power supply controller (bottom-right)

a  **Micro Processor**
(Hitachi HD6303RP)

b  **EPROM**
(27C256-25; 28 pin, 256K)

c  **Static RAM**
(ND4464C-20L,8192 bytes)
(SRM2064C-15, 8192 bytes)

d  **Demultiplexer**
(Phillips 74HC138N 3-to-8 line)

Other notable components are:

1. Memory cartridge port
2. Printer connection
3. Machine identifying EPROM
4. Connections to front button array and control panel.
5. Connections to power supply controller

Findings

- Access to machine's internal components are complicated but not difficult: memory card is accessible through a read-door. To reach the controllers and CPU, first the front panel that holds the paper ballot must be removed, in order to expose screws that hold the back panel, which are removable by readily available tools.
- CPU and memory modules are old, but information on them still exists. Model and instruction set is available for the CPU, as well as freely available programs for disassembly. ERPOM resides on a socket and not soldered, so it can be removed. Details, such as pin configurations, on the memory module is available. There exists universal programmers that can read and write to this particular chip.
- Manufacturer's description states that ballot data, which is the configuration of push buttons that correspond to a specific candidate on the paper ballot, is stored on a memory cartridge that wasn't available with the machine. Cartridge contains information about the state of all push buttons, active or inactive. Cartridge contains an EPROM and two EEROMs. Cartridge contains a write-protection fuse, which disables writing to EPROM when it is blown, suggesting that the chips are soldered to the memory module. When a vote is cast, electronic results are stored at six locations: three chips on the cartridge, and three static RAM chips. Vote data on these chips are compared, and in any mismatch machine stops taking more votes.
- Election officer's manual requires cartridges to be collected at the end of the election session, and brought to a data center where technicians check the cartridges, and gather the individual election results on cartridges using a cartridge reader/programmer interfaced to a laptop. According to the Danaher manual, machines can be set to be a *precinct totalizer*, reading all the cartridges and summing up the votes.

Analysis & Example

Danaher is a machine that is built for one specific task, elections, hence it features numerous security features. Hacking the machine requires expertise, time, access and resources. For testing, a Danaher can be acquired through a government surplus sale, which is how Lehigh acquired this machine. Back panel can be removed in 15 minutes. Information on CPU and memory still exists, available on Internet. Several ROM programmers apparently can read and write to the EPROM that is used on this machine, which are also available through suppliers. Since machine does not have any serial ports or any other means of external access to controller, reprogramming must be done and implemented before the election, which requires access to machine. However, with these elements in place, it is manageable to intervene with machine's programming. One possible scenario a *secret knock*; machine will expect a trigger, such as one of the unused buttons at the front panel. During the election, when the trigger is pushed, machine will record any later vote same as the one that was placed during the trigger.