

# Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections Following Project EVEREST

K. Butler, W. Enck, H. Hursti, S.  
McLaughlin, P. Traynor, P. McDaniel  
USENIX EVT 2008


Presented by  
Siddharth Murali

$\pi$



$\pi$

## Introduction

- › Ohio's voting systems
    - Premier Elections Solutions
    - Hart InterCivic
    - Election Systems & Software
  - › Project EVEREST
    - Teams from academia and industry to assess risks with Ohio's current voting systems
  - › Penn State Team
    - Focused on Hart InterCivic and Premier systems
- 

## Hart InterCivic System

- › Typical election procedure in Ohio
  - Master key generation
  - Election database creation
  - Data is written to storage cards called MBBs
  - One MBB is used per JBC/eScan
  - SERVO software is used to reset memory of eScans
  - SERVO is also used to transfer shared key from eCM to JBC/eScan
  - Voters fill out paper ballots, enter them in the machine, which tallies the results
  - MBBs are retrieved and processed to create a election result database
  - Machines are backed up and firmware is verified

## Hart – Election Data Integrity

- › Single Shared key is used for an entire county
  - Easy to retrieve for an attacker with physical access
- › MBB Images
  - Data can be removed by copying
- › Bypassing passwords
  - Passwords are kept in a config file that is easily read
- › Third-party vulnerabilities
  - Uses functionality from old Windows OS

## Hart – Unsafe Functionality

- › Many testing features used in legitimate interfaces
- › eScan
  - Config file is available, can do things like allow duplicate ballots
- › JBC and eSlate
  - Can create fake button presses to vote any number of times
- › EMS
  - Can silently write the key to a debug file in plaintext
- › Ballot Now
  - Autovote menu allows attacker to generate and print pre-filled in ballots

## Hart – Malicious Insiders

- › Polling Place
  - Poll workers can collude with voters or monitor them to influence votes
- › eScan
  - Replaced memory card containing the executable, and booted into Linux
- › JBC
  - Voter codes can be rapidly generated during early voting
- › Election Headquarters
  - Tally software can be fooled into discounting votes, UI is configurable through Windows registry

## Hart - Auditing

- › Can alert an auditor about suspicious events or presence of malicious intent
- › EMS Audit Logs
  - Database storing logs can be attacked and logs modified, easy if you know passwords
- › Compromising the VVPAT record
  - Attacker who controls the printer interface can print anything to it
- › Open Interfaces on voting equipment
  - JBC and eScan have interfaces that allow erasing of votes and audit logs via commands through an Ethernet cable

## Premier Elections System

- › Election begins by defining ballot
- › GEMS server communicates over LAN with EMP, which encodes memory cards used at the polling places
- › EMP is a PC running Windows 2000 connected to an external drive bay
- › Election is opened by a precinct administrator who inserts a Supervisor card into the EMP
- › Voters receive a Voter card, insert it into the machine and vote
- › The voter then returns the voter card, and the supervisor closes the election by inserting his card
- › Memory cards are shipped to the election headquarters which communicate the results to GEMS server over LAN, which prints an official summary



## Premier – Vote Integrity and Privacy

- › Casting an unlimited number of ballots
  - Multiple voter cards can be used after exploiting vulnerabilities in AV-TSX
- › Exposing Voter choices
  - Audit log timestamps can indicate when a voter entered, and can approximate the voter's choice
- › Failure to address previous vulnerabilities
  - Large portions of EMP code was copied exactly from AV-TSX


## Premier – Malicious Insiders

- › State of Ohio required that additional third party software like McAfee, Verdasys Digital Guardian be used to protect GEMS
- › Protecting GEMS with Digital Guardian
  - Enforces 2 policies
  - 3 users created with unique access privileges
- › Circumventing Digital Guardian
  - Misconfiguration of Windows
  - Limitations of approach for policy specification
  - Can modify bootloader config and disable Digital Guardian


## Premier – Software Update Authentication

- › ExpressPoll
  - Attacker that can power cycle and insert new memory card can load and execute the file (like a bootloader) on the memory card
  - Source of files is never authenticated
- › VCE
  - No authentication of new software loaded
  - Can be used to create valid Voter Cards by just turning device off and pressing off button again to load new software
- › Digital Guardian
  - Adversary can replace a whitelisted application to gain its privileges

## Premier – Trustworthy Auditing

- › ExpressPoll
    - Audit logs can be modified/deleted by anyone in possession of the device
  - › Digital Guardian
    - Activity Logging is disabled by default
  - › EMP
    - Logs can be modified outside the application, or deleted without alarm
  - › AV-TSX VVPAT
    - Printer wires are easily exposed
    - Can easily insert chemicals to destroy information written to printer paper
- 

## Premier –Security Engineering Practices

- › Ineffective Application of Security Techniques
    - Same data key used throughout the county
    - Decryption key used in EMP derived from serial number
    - ExpressPoll provides no database protection
  - › Systemic Trust Assumptions
    - Same data key used by EMP and all AV-TSX devices
    - EMP can perform all AV-TSX operations and validate the results
    - EMP always trusts user to enter correct data, user cannot change the value if entered wrong
- 

$\pi$

## Discussion

- › Contributions/Limitations of the paper?
- › Do you think that these attacks have influenced elections?
- › Have there been any changes in these machines in the past 8 years?
- › Similar projects in other states?