



# Vulnerabilities and Critical Security Issues with Diebold TSx Voting Machines

Cathy Reed

June 13, 2006



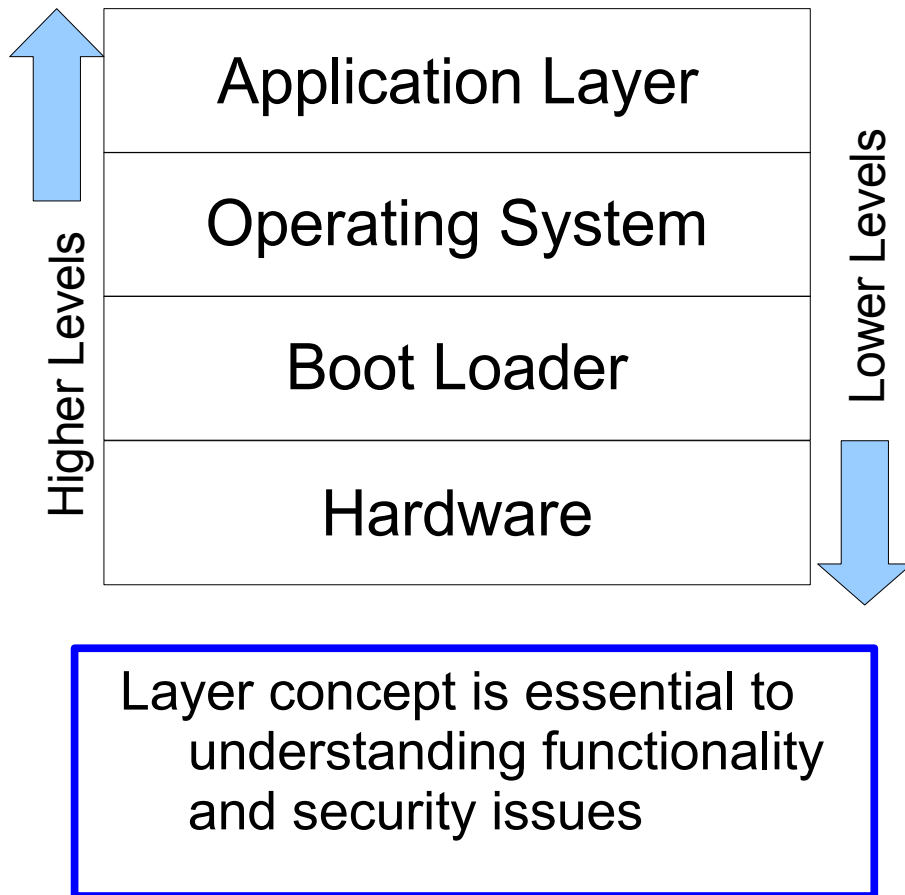
# Objectives



- Briefly discuss the nature of security issues discovered in Diebold TSx voting machines by Harri Hursti
  - This article addresses weaknesses to intentional tampering
  - Two Versions were published
    - One restricted because critical security vulnerabilities were specifically detailed
    - One available to the Open Public (addressed in this brief)
- Discuss directives to counties from Secretary of State
- Discuss recertification request and denial
- Key Facts related to likely Diebold injunction



# Architecture



- Diebold TSx voting machines can be depicted in a four level architecture
- “Back Doors” exist in all layers with very little security
  - Security cannot guard against deliberate attacks
  - One or all layers can be compromised
- Compromised layer can guard against clean-up by other layers
  - Other layers can conceal the contaminated layer



# Hardware (Lowest Layer)



- Motherboard has an interface to reprogram the boot loader which enables an auxiliary system to take over
  - Can be used to deliver malicious code
  - Software-based security cannot protect against this type of attack
- Cases secured with ordinary phillips-head screws such that anti-tamper seals remain intact
  - Unrestricted access to PCMCIA slots and SD/MMC slot
  - Motherboard has jumpers to enable otherwise disabled software features
- Hidden button in the casing is accessible to any voter
- “Feature” triggered by memory card erases flash memory
- A modem is also implemented on the motherboard with sets of “piggybacks” underneath the modem connection (reason unknown)



# Boot Loader



- Standard software development involves debugging tools that are removed in the finished product, before the software goes into production
  - Bootloader still retains debugging tools creating security holes
- Vulnerabilities in the boot loader allow the Windows CE Operating System to be replaced with a contaminated version
- Bootloader is “Network Aware” allowing an attacker to gain access through standard laptop (PCMCIA) cards, removable media and a network interface
- When booted, the bootloader looks for a particular filename on the PCMCIA card, and process based on the fact that the filename was correct – no failsafe mechanism
- If the boot loader is compromised, it cannot be used as a recovery path to a “clean system”



# Operating System



- Uses “Windows CE” OS similar to PDAs
  - Does not have security features of Windows XP
- Files can be replaced or modified by simply gaining access to the “Windows Explorer” application
  - A hostile attacker can alter system functionality, add new software and hidden processes to the system
- Contaminated Operating System can be loaded by the boot loaded
  - Network, Removable Storage and PCMCIA cards can be used



# Application Layer



- Unauthorized modifications to the Operating System and/or program libraries can alter application behavior without changing the application
- Application-layer macro had unpredictable results
  - Two identical machines exhibited different but reproducible behaviors
  - In one case, the macro skipped to “Page 4 of 3” in a three page ballot



# Additional Concerns



- These attacks can be permanent and survive through many election cycles
- “Delayed reaction” attack possible that lays dormant until an election years later
- Contamination can happen at any point of the lifespan of the voting machine and remain active and undetected
- When the memory card is full, the system will delete files from the card to free up memory, including election files.
- Deibold stated that 31 machines delivered machines were identical in both hardware and software
  - Available memory varied from 10% free to 62% free



# Conclusion



- There is a genuine reason for concern with Diebold TSx voting machines



# Directives to Counties from the Secretary of State



- In May 2006 with primary elections approaching, PA Secretary of State Pedro Cortez issued urgent directives to the county regarding potential security risks
- Michael Shamos of Carnegie Mellon University, examiner for electronic voting systems for PA said “it is the most severe security flaw ever discovered in a voting system”
- Diebold issued a warning that it had found a “theoretical” security vulnerability that could potentially allow unauthorized software to be loaded onto the system
- The New York Time article “New Fears of Security Risks in Electronic Voting Systems” published May 12, 2006 further identified these issues



# Recertification Request and Denial



- Request to re-examine the electronic voting system used in Lehigh County pursuant to 25 P.S. Sec 3031(a) of the election code
- Secretary of State Pedro Cortez denied the request for re-examination
- Please refer to handout for further details



# Key Facts

- H Hursti demonstrated vote totals could be changed in Deibold Optical Scanners
  - Secretary Cortez referenced Hursti Optical Scan Hacking Test as the key reason to deny the Deibold Optical scanner for use in Pennsylvania
- Since that time, H Hursti has demonstrated vulnerabilities to the Diebold TSx
- We believe the Diebold TSx should be decertified immediately