System (In)Security

Richard A. Kemmerer

Computer Security Group

Department of Computer Science

University of California, Santa Barbara

http://seclab.cs.ucsb.edu

UCSB

UCSB Security Laboratory Mission

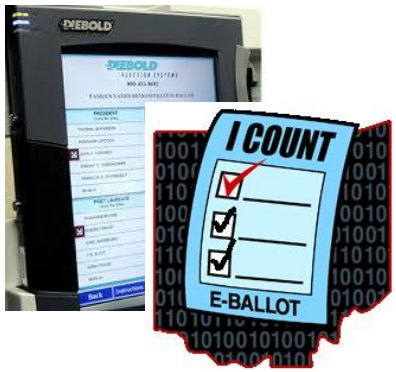
The focus of our work is systems and network security. We seek to create solutions that solve important security problems affecting a large number of users. The goal is to build security systems, deploy them in real-world environments, and perform experiments to characterize and explain their behavior.

UCSB Security Laboratory
Recent Areas of Research

Vulnerability Analysis

Malware Analysis
and Detection

Network Security /
Cyber-Situation Awareness



eVoting Security

Security in Social Networks

Cybercrime

First A Simple Test

Count the number of times the white shirt team passes the basketball

Lesson Learned

Beware of Gorillas invading your system while you are counting basketball passes

Know what to pay attention to

Electronic Voting: Are Your Votes Really Counted?

Richard A. Kemmerer

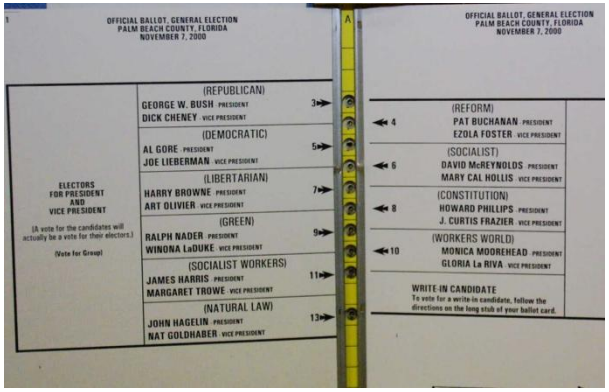
Computer Security Group
Computer Science Department
University of California
Santa Barbara, CA 93106, USA
http://www.cs.ucsb.edu/~kemm

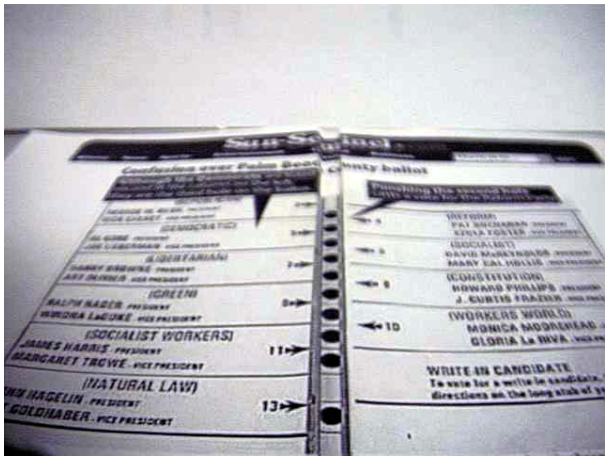
“Those who cast the votes decide nothing. Those who count the votes decide everything.”

- Joseph Stalin

Florida Hanging Chad (2000)

- Decisive race for the 2000 US presidential election
- Given to Bush by a margin of only 537 votes
- Plagued by several irregularities and problems, some of which have been attributed to the use of old and inadequate voting technology





Minnesota Senatorial Race (2008)

- Senatorial Race November 2008
- 7,000 ambiguous ballots challenged
- Result not decided until June 2009
- Race decided by 225 votes
- There are 4,131 precincts in Minnesota

Help America Vote Act (2002)

- Establishes an Election Assistance Commission
- Promulgates minimum election administration standards. For example, it establishes that:
  - Voters must be notified of errors and be able to review and change ballot before vote is cast
  - Vendors may adopt Voluntary Voting System Guidelines
- Provides funds to help all states and territory meet the new requirements ($4 billion)
- Central goal: to replace punch-card and lever voting systems with new, more modern systems

California on VVPAT (2005)

- Voter Verifiable Paper Audit Trail (VVPAT) is a method to assure voters that their votes have been recorded as intended [Mercuri00]
- A Secretary of State's directive makes it mandatory in California by 2005 [Shelley03]
- A state bill extends the deadline until 2006 [SB1438]

Certification

- Federal qualification process calls for machines to be tested by Independent Testing Authorities (ITAs)
- ITAs assess reliability, security and accuracy of machines
- Issues with certification process [Wagner06]:
  - ITAs are paid by vendors
  - Process lacks transparency (e.g., reports are proprietary, test failures are not publicly disclosed)
  - Testing is superficial, especially for security properties
  - Testing requirements are confusing

Brief History of Security Analyses

- Bev Harris discovers the CVS repository of Diebold's software (on a public FTP server) and identifies ways to bypass passwords and manipulate election results [Harris03]
- Johns Hopkins and Rice team concludes that Diebold's AccuVote-TS lacked "even the most minimal security standards" [Kohno03]
- Team identifies multiple vulnerabilities in SERVE, a proposed Internet voting system for US Military [Jefferson04]

Brief History of Security Analyses

- Princeton team obtains “from a private party” a Diebold’s AccuVote-TS voting machine (hardware and software), and shows how to develop a virus [Feldman06]
- Harri Hursti shows various methods to tamper with votes on Diebold machines for the HBO documentary “Hacking Democracy” [HBO06]
- Andrew Appel buys 5 used Sequoia’s AVC Advantage machines on an auction website ($82) and starts examining them [Appel07]

California Top-To-Bottom Review

- Review of electronic voting systems ordered by California Secretary of State (SoS) Deborah Bowen in summer 2007
- “Are our voting systems secure, accurate, reliable and accessible?”
- Investigates equipment by Diebold, Hart, Sequoia
- For each analyzed system, establishes the following teams:
  - Document review
  - Source code review
  - “Red” team

Top-To-Bottom Review

- SoS appointed teams (mostly) from UC campuses (Berkeley, Davis, Santa Barbara), led by D. Wagner and M. Bishop
- UCSB Computer Security Group was red team for the Sequoia system
- We were able to bypass both the physical and software security protections and completely compromise the voting process
- Sequoia system was decertified for use in California

Red Teaming

- Scope of work: try to compromise the accuracy, security, and integrity of the voting systems
  - "cause incorrect recording, tabulation, tallying or reporting of votes"
  - "alter critical election data such as election definition or system audit data"
- Testing environment: do not make assumptions about compensating controls or procedural mitigation measures
- Level of access: all information available to the SoS (machines, source code, documents) was available

Top-To-Bottom Review

- All testing permitted only in the secured room at the SoS office in Sacramento containing the “cage”

Ohio
EVEREST Project

- EVEREST: Evaluation & Validation of Election-Related Equipment, Standards & Testing
- Ordered by Ohio Secretary of State Jennifer Brunner in fall 2007
- Investigates equipment by Election Systems and Software (ES&S), Hart InterCivic, and Premier Election Solutions (formerly Diebold)
- Analysis similar to that for California
- Had election equipment at our home institutions

EVEREST Project

- Teams from Penn State, UPenn, WebWise Security, Inc, led by Patrick McDaniel
- WebWise Security was red team for the ES&S system
- We were able to bypass both the physical and software security protections and completely compromise the voting process
- ES&S system was recommended to be decertified for use in Ohio

Outline

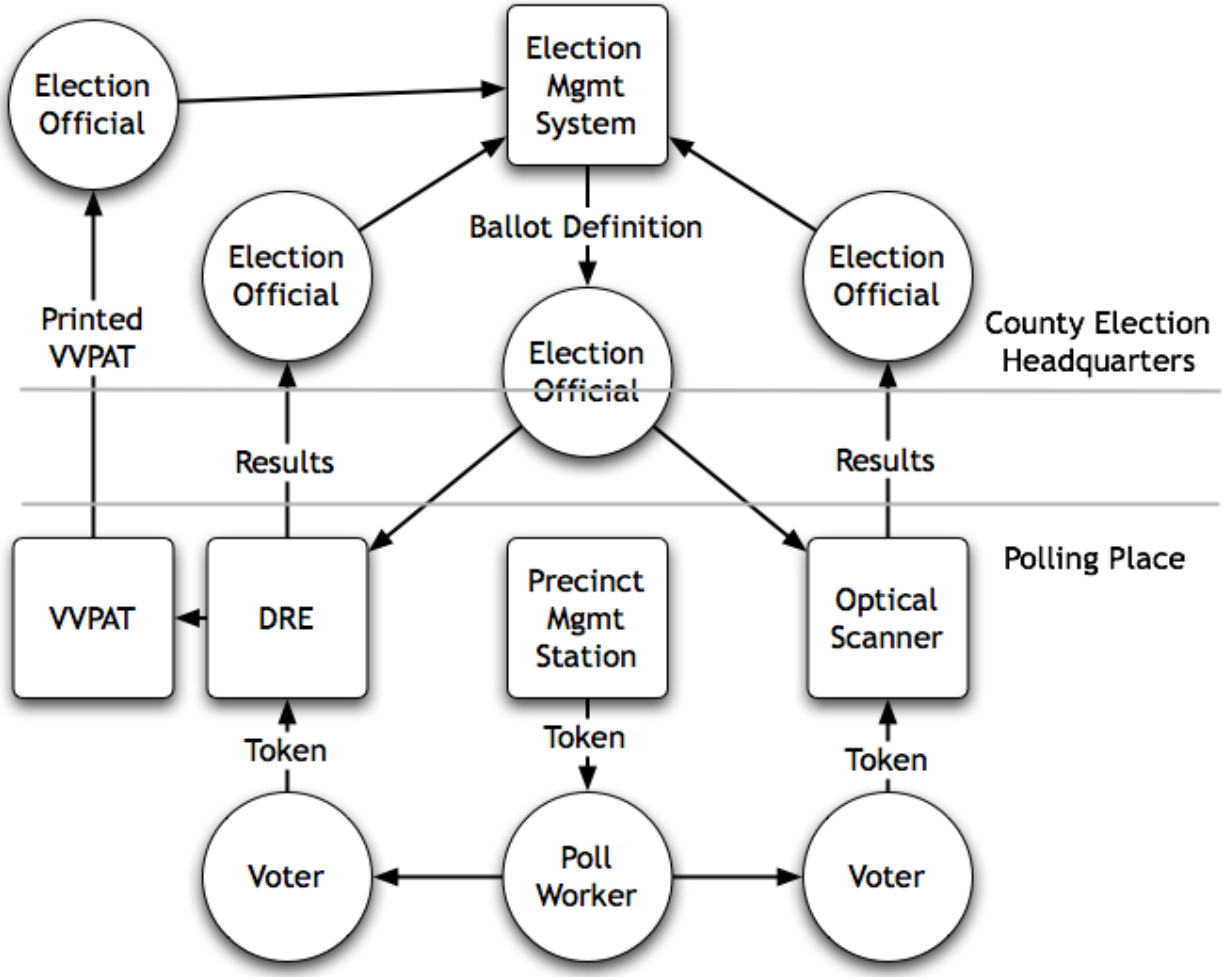
- Background
  - History and previous security studies
  - California Top-To-Bottom Review (TTBR)
  - Ohio EVEREST Project
- Electronic voting
  - Generic electronic voting system overview
  - Sequoia system
- Sequoia red teaming
  - Threat model
  - Findings
  - Attacks
  - Lessons learned

Electronic Voting System Overview

Components

- At the polling place:
  - Precinct Management Station
  - Direct Recording Electronic (DRE) voting machines with VVPAT printers
  - Paper ballot optical scanners
- At the election headquarters in the county:
  - Election Management System (EMS)
  - High-speed paper ballot optical scanners
- Data Transport Devices (DTD)

Reference Model: Components



Voting Process Phases

- Pre-voting
  - Ballot definition are generated and recorded on media for distribution
  - Voting machines are prepared and distributed
  - Valid voter logbooks are created
  - Logic and Accuracy Testing (LAT) of DRE and scanners
- Voting
  - Voters arrive at polling place, sign into logbook, are given token, cast their votes
- Post-voting

Sequoia System

WinEDS

- Is a Windows-based program for entering, editing, collecting, and reporting election information
- Implements an access control system based on user accounts and roles (separated from the Windows accounting)
- Can be used in networked settings with multiple WinEDS systems accessing a single database (based on Microsoft SQL Server)

HAAT

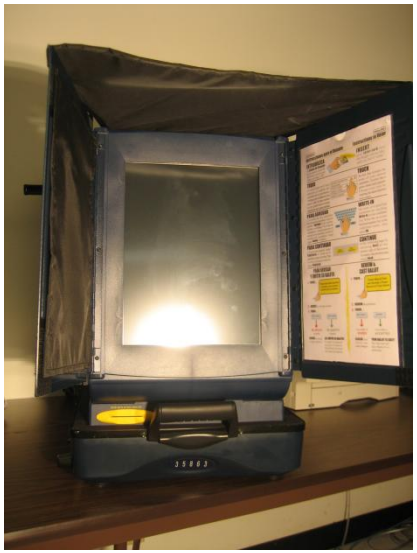
- Hybrid Activator, Accumulator and Transmitter
- Used to activate voter cards used by the Edge DRE
- Has the capability of consolidating votes and transmitting precinct tally to election headquarter over a cellular network (not used in California)
- Uses a removable Flash card for its memory

Card Activator

- Used to activate voter cards used by the Edge DRE
- Has the capability of consolidating results cartridges and transmitting results over a modem (not used in California)
- Written in C, runs on DOS, on a 486

AVC Edge

- Is a Touchscreen-DRE system with an attached VVPAT printer
- Consists of special purpose computer including its proprietary software and hardware
- Implemented by 124K lines of C code



Optech Insight and Insight Plus

- Are precinct-based optical readers for “mark-sense ballots”
- Consists of a scanner which covers the ballot box
- Runs on a Z80 chip

Optech 400-C

- Is a high-capacity, high-speed optical scanner used to count “mark-sense” ballots and tabulate results
- Composed of an optical reader attached to a Windows PC protected by a large chassis with metal door and lock

Data Transmission Devices Cartridges

- Specially formatted PCMCIA memory cards
- Primarily used to load election definitions prepared by WinEDS used in AVC Edge and Card Activator
- Different kinds:
  - Results
  - Consolidation
  - Simulation
  - Firmware update

Data Transmission Devices
USB Flash Drive

- Generic USB flash drive
- Used to transfer election definition from WinEDS to HAAT

Data Transmission Devices Voter SmartCard

- Simple, memory-constrained devices
- Prepared by Card Activator or HAAT
- Used as hardware token to authenticate a voter on AVC Edge and authorize the voter to cast a single vote

Threat Model

Threat Model: Attacker's Goals

- Modify the vote counts
- Prevent voting
- Delegitimize the integrity of election process
- Delay the availability of results

Threat Model: Possible Attackers

- Outsiders
- Voters
- Poll workers
- Election officials
- Vendor employees

Findings

Findings: Data Integrity

- Much critical data resides on removable media that pass through several hands
- Safeguard mechanisms are largely ineffective or absent
- Attacker can alter
  - Results stored on results cartridges
  - Firmware of AVC Edge
  - Firmware of optical ballot scanners
  - Firmware of HAAT and card activator

Findings: Physical Security

- A variety of seals are used to prevent unauthorized access to hardware components of the system
- In many cases, seals can be easily bypassed by using simple techniques and tools
  - Bending hinges
  - Unscrewing screws
- All components are vulnerable to these attacks

Findings: Cryptography

- Cryptographic mechanisms are used extensively, but are ineffective
- Bad design and implementation errors:
  - Hardcoded keys
  - Obsolete algorithms (SHA-0, single DES in ECB mode)
  - Inadequate algorithms (16-bit CRC as MAC)
  - Implementation issues (algorithms implemented from scratch, SHA code ignores secret key parameter)

Findings: Access Control

- Complex access control configuration
  - Role maintenance dialog in WinEDS has 615 checkboxes
- Insecure architecture
  - Access control is enforced only in the client, not on the server
- Access control does not protect the right features
  - Updating the firmware on the Card Activator does not require a password
- Insecure default settings
  - If the password file is empty, the Card Activator proceeds without requiring any password

Findings: Software Engineering

- Complexity
  - 800K lines of code
  - 10 languages (4 assembly)
  - 6 interpreted languages
- Weak input validation
  - WinEDS does not sufficiently check data stored on USB sticks, results cartridges, and database
  - AVC Edge does not sufficiently check results cartridges

Attacks

Automatic Code Execution on WinEDS

- Vulnerability: WinEDS host operating system executes “autorun” files when removable media is inserted
- Requirements: attacker inserts a U3 USB drive in the host computer
- Effect: malicious code is executed on the system running WinEDS
- Attack scenario: the malicious code installs a trojan horse, which modifies election data (by accessing the database) and/or results cartridges

Arbitrary Code Execution on AVC Edge

- Vulnerability: integer overflow vulnerability in AVC Edge
- Requirements: attacker constructs a results cartridge with a malicious election definition
- Effect: when the election information is loaded on the Edge, the vulnerability is exploited and the attacker's payload is executed
- Attack scenario: the attack payload replaces the original firmware with a malicious version, obtaining complete control of the machine

Testing Mode Detection on AVC Edge

- Issue: a global variable is used to store the current execution mode
- Effect: an attacker can check the value of the variable to detect whether the machine is in Logic and Accuracy Test (LAT) mode
- Attack scenario: the modified AVC Edge behaves correctly in LAT mode and maliciously during the election

Forging Voter Cards

- Vulnerability: Voter Cards are DES-encrypted using a static key, are protected by a simple checksum value, contain the creation information
- Requirements: attacker obtains valid smart cards
- Effect: attacker can recover the static key, decrypt the voter card, arbitrarily modify it
- Attack scenario: attacker creates a new valid Voter Card with modified creation information, which allows the attacker to cast multiple votes

Putting it All Together: Sequoia Virus

- By leveraging the “Automatic Code Execution” vulnerability on WinEDS, an attacker is able to install a Trojan on the WinEDS system
- The Trojan modifies results cartridges created by WinEDS so that the “Arbitrary Code Execution” vulnerability on AVC Edge is exploited and a malicious firmware is installed on the AVC Edge
- The malicious firmware modifies the votes cast by users, causes denial of service attacks, and otherwise disrupts the election

Scenarios

- Changing votes scenarios:
  - The trusting voter
  - The careful voter
  - The fleeing voter
  - The fake fleeing voter
  - After-the-fact vote
  - Bypassing physical security

YouTube Video

ES&S Virus Attack

- DTD is modified to contain malicious firmware
- Modified DTD installs virus on DRE during ballot loading
- During prelat DRE performs correctly, but during voting phase it changes votes
- When master DTD used to collect votes, the DRE infects the DTD, which infects other DREs and the EMS
- Virus remains dormant in EMS until next election

Lessons Learned

Lesson 1

Poor integration leads to insecurity

If reuse of a piece of code proves to be necessary or helpful, then the whole system design must be taken into account

Lesson 2

Cryptography is hard to get right

A mindful usage of strong encryption algorithms with strong, well-protected keys along with data signing are a must for building secure voting systems

Lesson 3

Unfounded trust assumptions enable compromise

One of the main premises for building a secure voting system is the absence of any unfounded assumptions and thorough checks of all input

Lesson 4

Certification and standards that are currently used are not enough for security

A more thorough and security-oriented certification process for evaluating voting systems is needed

Lesson 5

Logic and accuracy testing gives a false sense of security

The only way to make logic and accuracy testing realistic is to, at the very least, have the firmware totally unaware of any testing mode

Lesson 6

COTS components are difficult to configure in a secure way

When COTS components are used, the vendors should either provide a pre-configured component or they should provide detailed configuration specifications

Lesson 7

Voting procedures underestimate the power of potential adversaries

Procedures should never be relied on as the only guarantee of system security. Each component should implement a complete set of security mechanisms necessary for its protection

Lesson 8

Security training of electronic voting system developers is not sufficient

Knowledge of basic security concepts, their application, and defensive programming practices should be prerequisites for the developers of critical systems such as an electronic voting system

Conclusions(1)

- We performed a red teaming assessment of the Sequoia voting system as part of the California Top-To-Bottom Review and of the ES&S system as part of the Ohio EVEREST project
- We found a number of significant security issues in both the physical and software protection mechanisms in both systems
- We demonstrated our findings showing numerous scenarios through which election results can be controlled by an attacker

Conclusions(2)

- We developed a number of special purpose tools to perform the required analysis
- There is a need for drastic changes in the way that electronic voting systems are designed, implemented, and tested
- Unless voting systems are held up to standards that are commensurate with the criticality of the tasks that they have to perform, the very core of our democracy is in danger

Credits

Team:

- Davide Balzarotti
- Greg Banks
- Marco Cova
- Viktoria Felmetsger
- William Robertson
- Fredrik Valeur

Team leaders:

- Giovanni Vigna and Dick Kemmerer

More Information

- California Top-To Bottom review
  http://www.sos.ca.gov/elections/elections_vsr.htm

- Ohio EVEREST project
  http://www.sos.state.oh.us/sos/info/everest.aspx

- ISSTA08 paper on special purpose tools and testing methodology developed
  http://issta08.rutgers.edu/

More Information

- California Top-To Bottom review
  http://www.sos.ca.gov/elections/elections_vsr.htm

- Ohio EVEREST project
  http://www.sos.state.oh.us/sos/info/everest.aspx

- ISSTA08 paper on special purpose tools and testing methodology developed
  http://issta08.rutgers.edu/

More Information

- YouTube videos

http://www.youtube.com/watch?v=SWDEZqqqBHE

http://www.youtube.com/watch?v=moEsgdzZ19c&feature=related

What do you think?

Are your votes really counted?

Questions?