ACCURATE

A CENTER FOR
CORRECT, USABLE,
RELIABLE, AUDITABLE,
AND TRANSPARENT ELECTIONS

Report on the California top-to-bottom review

David Wagner
University of California, Berkeley

www.sos.ca.gov/elections/elections_vsr.htm

Earlier this year, California Secretary of State Debra Bowen commissioned the University of California to examine 3 voting systems.

Diebold


Accu-Vote
PLACE BALLOT INSIDE TO KEEP VOTING SECRET
After Voting is Completed:
INSTRUCTIONS TO VOTERS
When inserting ballot into Accu-Vote Machine,
GRIP BELOW
DOTTED LINE

Hart InterCivic

Sequoia Voting Systems

Teams

Matt Bishop, PI:

- Accessibility
- Red teams

David Wagner, PI:

- Document review
- Source code review

Teams

Matt Bishop, PI:

- Accessibility
- Red teams

David Wagner, PI:

- Document review
- Source code review

Team members

- Diebold, Hart: *Bob Abbott,* Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi, Jacob Stauffer
- Sequoia: *Dick Kemmerer, Giovanni Vigna,* Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, William Robertson, Fredik Valeur
- Diebold: *David Wagner, Alex Halderman,* Joe Calandrino, Ari Feldman, Harlan Yu, Bill Zeller
- Hart: *Eric Rescorla,* Sreenu Inguva, Hovav Shacham, Dan Wallach
- Sequoia: *Matt Blaze,* Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, Ping Yee

We found…

We found… significant security problems in all 3 systems.

Crypto was often severely flawed, or missing entirely.

Sequoia

Sequoia invented their own password encryption algorithm.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password "**`sekret`**" encrypts to "**`sekretXYZ`**"*.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password "**`sekret`**" encrypts to "**`sekretXYZ`**"*.

** Obfuscated for 'security'; "XYZ" are not the real letters.*

Sequoia

"We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended."

— Sequoia source team

Diebold

One of Diebold’s passwords was

Diebold

One of Diebold's passwords was "**`diebold`**".

Hart

In some places, Hart avoided trivially broken crypto by…

Hart

In some places, Hart avoided trivially broken crypto by…
omitting it entirely.

Hart

In some places, Hart avoided trivially broken crypto by… omitting it entirely.

When you connect a polling-place machine to the county's central PC, it trusts the PC implicitly.
The county PC can instruct the machine to overwrite its software, and it will blindly comply. (No authentication!)

Diebold and Hart's systems don't adequately protect the secrecy of the ballot.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record…

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record… but the seed is known to officials, enabling them to recover the order votes were cast in.

Diebold

The Diebold touchscreen stores vote records in the order they were cast.

A crypto PRNG is used to generate unique IDs, stored with each vote record… but the seed is known to officials, enabling them to recover the order votes were cast in.

Each vote record is time stamped.

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

But it stores the CRC of each vote record in the audit log…

Hart

The Hart e-voting machine stores vote records in a pseudorandom order.

But it stores the CRC of each vote record in the audit log… and audit log entries are stored in the order they're logged.

The code fails to follow sound engineering principles expected of security-critical systems.

Diebold

```
TCHAR name;
_stprintf(&name, _T("\\Storage Card\\%s"),
   findData.cFileName);
Install(&name, hInstance);
```

All 3 systems allow malicious code to propagate virally.

Diebold

The Diebold code that reads data off the memory card has buffer overruns and other vulnerabilities.

Diebold

1. Attacker writes malicious data onto a memory card.
2. Uploading results at county HQ on election night infects county machines.
3. County machines can write malicious data and code onto memory cards that will infect all polling-place machines in the county in the next election.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

The voting machine can exploit buffer overruns in the code on the PC to take control of the PC.

Hart

1. Attacker installs malicious code onto a voting machine.
2. When connected to the county PC, it hacks the PC.
3. The county PC then installs malicious code onto every voting machine subsequently connected to it.

A single individual, with no special access, could introduce a virus onto a single voting machine,

A single individual, with no special access, could introduce a virus onto a single voting machine, and this virus could infect every machine in the county.

- “We found pervasive security weaknesses throughout the Sequoia software. Virtually every important software security mechanism is vulnerable to circumvention.”
- “Our study of the Diebold source code found that the system does not meet the requirements for a security-critical system. It is built upon an inherently fragile design and suffers from implementation flaws that can expose the entire voting system to attacks.”
- “The Hart software and devices appear to be susceptible to a variety of attacks which would allow an attacker to gain control of some or all of the systems in a county. [..] Many of these attacks can be mounted in a manner that makes them extremely hard to detect and correct. We expect that many of them could be carried out in the field by a single individual, without extensive effort, and without long-term access to the equipment.”

Results

Results

On August 6th, California Secretary of State Debra Bowen imposed new conditions on the use of these 3 voting systems.

Questions for the panel?

Matt Blaze — Sequoia source code team

Alex Halderman — Princeton source code team

Giovanni Vigna — Sequoia red team

Dan Wallach — Hart source code team