ECE455 Week 2 Readings

Jonathan Lam

09/15/21

Contents

1 Analysis of an electronic voting system

Kohno et. al, 2003

- Criteria for a good voting system:
  - Anonymity of ballot
  - Tamper-resistant
  - Human factors – comprehensible by all users
- Direct recording electronic (DRE) voting systems eliminate papor ballots from voting.
- It is useful to have a sheet of paper printed alongside each ballot to confirm the user's intent
- **"Security through obscurity"**
- Voters can easily programim their own smartcards to simulate the behavior of valid smartcards used in the election

- Anyone with physical access to the machine (janitors or poll workers) could do the same
- Smartcards do not perform any cryptographic operations, which is an immediate red flag
  - This ability sets them apart from magnetic stripe cards.
- A MITM attack can be performed to determine the protocol if it is not known a priori.
- The system only keeps track of the votes from people who cancelled their votes, rather than counting the number of people who do vote.
- PIN is sent in plaintext from the card to the terminal; attacker could read the input and try all 4-byte consecutive substrings
- Can trick Windows into thinking that a second flash storage device was inserted, even when there wasn't one; this increases the chance of data loss through hardware failure
- **"Sneaker net"** – when data is transported physically, e.g., hard drives carried from one location to another
  - These can just as easily be perpetrated by MITM attacks
- Registry information is stored in plaintext
- "We believe the Diebold system violates the FEC requirements by storing the protected counter in a simple, mutable file."
  - "In fact, the only solution that would work would be to implement the protective counter in a tamper-resistant hardware token" – **how would this work?**
- Ballot definitions are not encrypted nor checksummed
- Candidate information is not stored in the results file; only the numeric index of the candidates; even rearranging the ballot definition file would change the results
- Information about the backend server is stored in plaintext on the terminal, and is also stored on the ballet definition file
- Vote records and the audit logs are encrypted and checksummed before being written to the storage device. However:

  - All encryption is done with a single, hardcoded DES key
  - DES is not a strong encryption (triple-DES or AES are better)
  - DES used in CBC mode requires a random initialization vector to ensure security, which is not performed
  - **16-bit cyclic redundancy check** (CRC) – an unkeyed, public function vs. first encrypted the data to be stored and then to calculate a keyed cryptographic checksum.

- Votes are recorded sequentially, which can link voters with their votes
- Votes are given "random" serial numbers after they are sent to the tabulating server
  - A LCG (not cryptographically secure) is used with a static seed with information about the voting terminal and the election
- A log is sent as a stream to a printer but this isn't stored in a persistent place (e.g., to a file); if the printer is unplugged then the logs are lost
- Some of the files are very old (such as the files generating the DEC and CRCs)
- Poor documentation can lead to misunderstanding of intent
- There do not seem to be regular internal testing processes, or a bug tracking system; there are also no design specifications
  - "Virtually any serious software engineering endeavor will have extensive design documents that specify how the system functions, with detailed descriptions of all aspects of the system, rnaging from the user interfaces through the algorithms and software architecture used at a low level"
- **Trusted computing base (TCB)**: the set of software that can compromise the security of a program

2 Checks and balances in electionsequipment and procedures prevent alleged fraud scenarios

Diebold Elections Systems, 2003

- Checks and balances in the election cycle:

  - Equipment certification
  - Equipment purchase
  - Equipment receipt
  - Ballot preparation
  - Equipment preparation
  - Election day
  - Election results
  - Election canvass

- Diebold assumes that there is no collaboration by malevolent insiders or voters

- **Mercuri method** (having a paper trail association) reduces the situation basically down to that of a paper system, but it does have the stated benefits, but also its own downsides

- The certification authorities are not named – they are simply lisetd as "certification and testing bodies," and are noted as third-parties

- Diebold claims that "The source code for ballot tabulation systems is generally required by statute or regulation to be placed in a third party escrow facility, to be examined only upon court order or the vendor's failure to suppor th

  - **Is this true?**

- Response to unencrypted networks: they claim that all uploading is done on point-to-point networks and not through the Internet or dial-up

  - **Is this secure? Was this true? Is this practical on a large scale?**

- **The general rebuttals created by Diebold are roundabout: they don't deny the vulnerability but instead say that there is no way to prove that it has been exploited; they also stake themselves on the no malevolent actors in the election process or within the company**

- Assumption that ballot definitions are not always pre-installed is probably correct, especially in the case of last-minute changes or multiple ballot definitions used in a machine – rebuttal is clearly wrong?

- "which are locked inside the physical Ballot Station and continuously controlled by local election officials"
  - This assumes that physical locks and local election officials are not vulnerabilities that could pose a threat
- "Hypothetically, it would be possible to reverse engineer the password the password using the means described. But to describe the describe the process as 'easy' is an exaggeration." (about homebrew smartcards) – **this doesn't address the problem at all! In fact, it acknowledges the vulnerability**
  - "Roster reconciliation" to detect errors
- About hardcoded passwords – it has since been fixed, which means that they acknowledge the problem
- Many of the arguments are based on the fact that the poll machines don't transfer data over the Internet

3 Response to Diebold's Technical Analysis

Kohno et al., 2003

- Diebold misunderstood many technical details
  - "Safe" language was misunderstood: type and memory safe
  - Not being transmitted over the Internet is irrelevant – the networking protocols are still the same
  - Running on a different platform doesn't matter
- Argument: "no one correct way to do cryptography" doesn't mean that they do it right – logical gap
- Do not explain how key management was resolved
- CRCs versus MACs (**Message Authentication Codes**); latter is more secure
- "Unlike traditional software engineering, where testing can be used to show that a feature functions correctly under normal circumstances, security engineering is concerned with *abnormal circumstances*. Thus, testing can only be used to show that a system is not vulnerable to a given set of attacks, not that a system is secure."

- Another logical gap: not offering evidence of such an exploit or failure is not solved unless they prove the lack of such exploits or failures
- **Holt bill?**

3.1 Questions to ask of vendors:

- Has your system been reviewed by multiple outside credited security experts? Are these reports available?
- Can the public review the security of the system? Is there security through obscurity? If so, what happens if the code gets leaked, or if there's a malicious insider?
- Credentials of software developers w.r.t. cryptography and computer security?
- Do you offer guarantees (e.g., refunds plus "damages") if the equipment is found to be insecure or attacked?
- Is a manual recount possible?