CSci 4271W
Development of Secure Software Systems
Day 28: Usability and voting

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Usable security example areas, cont'd

Logistics, evaluations break

Elections and their security

System security of electronic voting

Spam-advertised purchases

- "Replica" Rolex watches, herbal `V!@gr@`, etc.
- This business is clearly unscrupulous; if I pay, will I get anything at all?
- Empirical answer: yes, almost always
  - Not a scam, a black market
  - Importance of credit-card bank relationships

Advance fee fraud

- "Why do Nigerian Scammers say they are from Nigeria?" (Herley, WEIS 2012)
- Short answer: false positives
  - Sending spam is cheap
  - But, luring victims is expensive
  - Scammer wants to minimize victims who respond but ultimately don't pay

Trusted UI

- Tricky to ask users to make trust decisions based on UI appearance
  - Lock icon in browser, etc.
- Attacking code can draw lookalike indicators
  - Lock favicon
  - Picture-in-picture attack

Smartphone app permissions

- Smartphone OSes have more fine-grained per-application permissions
  - Access to GPS, microphone
  - Access to address book
  - Make calls
- Phone also has more tempting targets
- Users install more apps from small providers

Permissions manifest

- Android approach: present listed of requested permissions at install time
- Can be hard question to answer hypothetically
  - Users may have hard time understanding implications
- User choices seem to put low value on privacy

Time-of-use checks

- iOS approach: for narrower set of permissions, ask on each use
- Proper context makes decisions clearer
- But, have to avoid asking about common things
- iOS app store is also more closely curated

Trusted UI for privileged actions

- Trusted UI works better when asking permission (e.g., Oakland'12)
- Say, "take picture" button in phone app
  - Requested by app
  - Drawn and interpreted by OS
  - OS well positioned to be sure click is real
- Little value to attacker in drawing fake button

Outline

Usable security example areas, cont'd

Logistics, evaluations break

Elections and their security

System security of electronic voting

Supplementary office hour

- Prof. McCamant tonight 6:00–7:00pm
- Same Zoom room as regular office hours

SRT logistics

- All online this semester
- Requested but not required; can't affect your grade one way or the other
- Primary evaluation combines Prof. McCamant and the course
- Please also evaluate Saugata separately if you have comments or suggestions about his performance
- Open through the last regular class day

SRT URL

- `https://srt.umn.edu/blue`
- We'll take a 15-minute break in class material that we request you use for filling out the evaluation

Outline

Usable security example areas, cont'd

Logistics, evaluations break

Elections and their security

System security of electronic voting

Elections as a challenge problem

- Elections require a tricky balance of openness and secrecy
- Important to society as a whole
  - But not a big market
- Computer security experts react to proposals that seem insecure

History of US election mechanisms

- For first century or so, no secrecy
  - Secret ballot adopted in late 1800s
- Punch card ballots allowed machine counting
  - Common by 1960s, as with computers
  - Still common in 2000, decline thereafter
- How to add more technology and still have high security?

Election integrity

- Tabulation should reflect actual votes
  - No valid votes removed
  - No fake votes inserted
- Best: attacker can't change votes
- Easier: attacker can't change votes without getting caught

Secrecy, vote buying and coercion

- Alice's vote can't be matched with her name (unlinkable anonymity)
- Alice can't prove to Bob who she voted for (receipt-free)
- Best we can do to discourage:
  - Bob pays Alice $50 for voting for Charlie
  - Bob fires Alice if she doesn't vote for Charlie

Election verifiability

- We can check later that the votes were tabulated correctly
- Alice, that her vote was correctly cast
- Anyone, that the counting was accurate
- In paper systems, "manual recount" is a privileged operation

Politics and elections

- In a stable democracy, most candidates will be "pro-election"
- But, details differ based on political realities
- "Voting should be easy and convenient"
  - Especially for people likely to vote for me
- "No one should vote who isn't eligible"
  - Especially if they'd vote for my opponent

Errors and Florida

- Detectable mistakes:
  - Overvote: multiple votes in one race
  - Undervote: no vote in a race, also often intentional
- Undetectable mistakes: vote for wrong candidate
- 2000 presidential election in Florida illustrated all these, "wake-up call"

Shifting politics of elections

- Until recently, concerns about electronic voting security were more associated with Democrats/the left
  - Including larger proportion of academics
- But more prominently voiced by Republicans in 2020
- Ideal: system needs to demonstrate security to a skeptical but good-faith observer

Precinct-count optical scan

- Good current paper system, used here in MN
- Voter fills in bubbles with pen
- Ballot scanned in voter's presence
  - Can reject on overvote
- Paper ballot retained for auditing

Vote by mail

- By mail universal in OR, WA, CO, HI, UT
  - Many other states have lenient absentee systems
  - Some people are legitimately absent
  - Big for a one-time reason in 2020
- Security perspective: makes buying/coercion easy
  - Doesn't appear to currently be a big problem, though worse than in-person

Vote by web?

- An obvious next step
- But, further multiplies the threats
- No widespread use in US yet
- Unusual adversarial test in D.C. thoroughly compromised by U. Michigan team

DRE (touchscreen) voting

- "Direct-recording electronic": basically just a computer that presents and counts votes
- In US, touchscreen is predominant interface
  - Cheaper machines may just have buttons
- Simple, but centralizes trust in the machine

Adding an audit trail

- VVPAT: voter-verified paper audit trail
- DRE machine prints a paper receipt that the voter looks at
- Goal is to get the independence and verifiability of a paper marking system

Outline

Usable security example areas, cont'd

Logistics, evaluations break

Elections and their security

System security of electronic voting

Trusted client problem

- Everything the voter knows is mediated by the machine
  - (For Internet or DRE without VVPAT)
- Must trust machine to present and record accurately
- A lot can go wrong
  - Especially if the machine has a whole desktop OS inside
  - Or a bunch of poorly audited custom code

Should we use DRE at all?

- One answer: no, that's a bad design
- More pragmatic: maybe we can make this work
  - DREs have advantages in cost, disability access
  - If we implemented them well, they should be OK
  - Challenge: evaluating them in advance

US equipment market

- Voting machines are low volume, pretty expensive
- But jurisdictions are cost-conscious
- Makers are mostly small companies
  - One was temporarily owned by the larger Diebold
- Big market pressures: regulations, ease of administration

Security ecosystem

- Voting fraud appears to be very rare
  - Few elections worth stealing
  - Important ones are watched closely
  - Stiff penalties deter in-US attackers
- Downside: No feedback from real attacks
- Main mechanism is certification, with its limitations

Diebold case study

- Major manufacturer in early 2000s
  - During a post-2000 purchasing boom
  - Since sold and renamed
- Thoroughly targeted by independent researchers
  - Impolitic statement, blood in the water
- Later state-authorized audits found comprehensive problems
  - Your reading: from California

Physical security

- Locked case; cheap lock as in hotel mini-bar
- Device displays management menu on detected malfunction
  - Can be triggered in booth by unspecified use of paperclip
- Tamper-evident seals? Not a strong protection

Buffer overflows, etc.

- Format string vulnerability
  - `"Page %d of %d"`
- Was this audited?

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

Web-like vulnerabilities

In management workstation software:

- SQL injection
- Authentication logic encoded only in enabled/disabled UI elements
  - E.g., buttons grayed out if not administrator
  - Not quite as obviously wrong as in web context
  - But still exploitable with existing tools

OpenSSL mistakes

- Good news: they used OpenSSL
  - Bad news: old, buggy version
- Insufficient entropy in seeding PRNG
  - Good interface from desktop Windows missing in WinCE
- Every device ships with same certificate and password

Election definitions

- Integrity "protected" by unkeyed, non-crypto checksum
- Can change bounding boxes for buttons
  - Without changing checksum!
- Can modify candidate names used in final report
  - E.g. to fix misspelling; security implication mentioned in comment

Secrecy problems

- Limited, since the DRE doesn't see registration information
- But, records timestamp and order of voting
- Could be correlated with hidden camera or corrupted poll worker

Voting machine viruses

- Two-way data flow between voting and office machines
- Hijacking vuln's in software on both sides
- $\rightarrow$ can write virus to propagate between machines
- Leverage small amount of physical access

Subtle ways to steal votes

- Change a few votes your way, revert if the voter notices
  - Compare: flip coin to split lunch
- Control the chute for where VVPAT receipts go
- Exchange votes between provisional and regular voters