Security Engineering (2)

Email: christian.urban at kcl.ac.uk
Office: N7.07 (North Wing, Bush House)

Slides: KEATS (also homework is there)

This Course is about "Satan's Computer"

Ross Anderson and Roger Needham wrote:

> "In effect, our task is to program a computer which gives answers which are subtly and maliciously wrong at the most inconvenient possible moment... we hope that the lessons learned from programming Satan's computer may be helpful in tackling the more common problem of programming Murphy's."

This Course is about "Satan's Computer"

Ross Anderson and Roger Needham wrote:

> "In effect, our task is to program a computer which gives answers which are subtly and maliciously wrong at the most inconvenient possible moment... we hope that the lessons learned from programming Satan's computer may be helpful in tackling the more common problem of programming Murphy's."

Murphy's computer

Satan's computers

Defence in Depth

```
urbanc:$6$3WWbKfr1$4vblknvGr6FcDeF92R5xFn3mskfdnEn...:...
```

- hashes help when password databases are leaked
- salts help with protecting against dictionary attacks and help people who have the same password on different sites
- but they do not protect against a focused attack against a single password and also do not make poorly chosen passwords any better

Subtle Points

- in our web-application the salt needed to remain secret; in password files the salt is public

- the NYT has the "resource" unlocked at first and locks it depending on the cookie data
- our "web-application" has the resource locked at first, and unlocks it depending on the cookie data

Exam and Homework

- reminder...KEATS

Today's Lecture

online banking vs e-voting

solved unsolved

E-Voting

"Any electronic voting system should provide at least the same security, privacy and transparency as the system it replaces."

—Australian Voting Commission

Voting as Security Problem

What are the security requirements of a voting system?

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity

  - The outcome matches with the voters' intend.
  - There might be gigantic sums at stake and need to be defended against.

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy

- Nobody can find out how you voted.
- (Stronger) Even if you try, you cannot prove how you voted.

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy
- Voter Authentication

- Only authorised voters can vote up to the permitted number of votes.

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy
- Voter Authentication
- Enfranchisement

- Authorised voters should have the opportunity to vote.

Voting as Security Problem

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy
- Voter Authentication
- Enfranchisement
- Availability

- The voting system should accept all authorised votes and produce results in a timely manner.

Problems with Voting

Integrity vs. Ballot Secrecy

Authentication vs. Enfranchisement

Problems with Voting

Integrity vs. Ballot Secrecy

Authentication vs. Enfranchisement

Further constraints:

- costs
- accessibility
- convenience
- intelligibility

Traditional Ballot Boxes

Traditional Ballot Boxes

mechanical, but they need a “protocol”

Motives for E-Voting

- 76% of pensioners in the UK vote, but only 44% of the under-25s
- convenience
- speed

E-Voting

- The Netherlands between 1997 - 2006 had electronic voting machines
  (hacktivists had found: they can be hacked and also emitted radio signals revealing how you voted)
- Germany had used them in pilot studies
  (in 2007 a law suit has reached the highest court and it rejected electronic voting on the grounds of not being understandable by the general public)
- UK used optical scan voting systems in a few test polls, but abandoned any wide deployment

E-Voting

- US used mechanical machines since the 30s, later punch cards, until recently DREs and optical scan voting machines
- Estonia used in 2007, 2011 and 2015 the Internet for national elections (there were earlier pilot studies in other countries)
- The Australian parliament ruled in 2014 that e-voting is highly vulnerable to hacking and will not use it any time soon.
- Norway experimented with Internet voting, but e-voting is an incredibly difficult problem, even in such favourable circumstances...(voter turnout did not really increase)

E-Voting

- India uses e-voting devices since at least 2003 ("keep-it-simple" machines produced by a government owned company)
- South Africa used software for its tallying in the 1993 elections (when Nelson Mandela was elected) (they found the tallying software was rigged, but they were able to tally manually)

E-Voting in Estonia

- worlds first general election that used internet voting (2007, 2011, 2015)
- builds on the Estonian ID card (a smartcard like CC)
- Internet voting can be used before the election (votes can be changed an unlimited amount of times, last vote is tabulated, you can even change your vote on the polling day in person)
- in the 2011 parliamentary election 24% voted via Internet

E-Voting in Estonia

- worlds first general election that used internet voting (2007, 2011, 2015)
- builds on the Estonian ID card (a smartcard like CC)
- Internet voting can be used before the election (votes can be changed an unlimited amount of times, last vote is tabulated, you can even change your vote on the polling day in person)
- in the 2011 parliamentary election 24% voted via Internet

- needs to trust the integrity of voters' computers, central server components and the election staff