

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\$3WbKfr1\$4vb1knvGr6FcDeF92R5xFn3mskfdnEn.....

- 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

- world's 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

- world's 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

```
1 #!/usr/bin/python2.7
2 # -*- coding: UTF8 -*-
```

```
from https://github.com/vvk-ehk/evalimine/
```

```
3
4 """
5 Copyright: Eesti Vabariigi Valimiskomisjon
6 (Estonian National Electoral Committee), www.vvk.ee
7 Written in 2004-2013 by Cybernetica AS, www.cyber.ee
8
9 This work is licensed under the Creative Commons
10 Attribution-NonCommercial-NoDerivs 3.0 Unported License.
11 To view a copy of this license, visit
12 http://creativecommons.org/licenses/by-nc-nd/3.0/.
13 """
```

```
14
15 def analyze(ik, vote, votebox):
16
17     # TODO: implement security checks
18     # such as verifying the correct size
19     # of the encrypted vote
20
21     return []
```

E-Voting in **Theory**

- Alice prepares and audits a ballot, then casts an encrypted ballot, which requires her to authenticate to a server.
- A bulletin board posts Alice's name and encrypted ballot. Anyone, including Alice, can check the bulletin board and find her encrypted vote posted.
- When the election closes, all votes are shuffled and the system produces a non-interactive proof of a correct shuffling. (zero-knowledge-proofs)
- After a reasonable complaint period to let auditors check the shuffling, all shuffled ballots are decrypted, and the system provides a decryption proof for each decrypted ballot. (zero-knowledge-proofs)
- Perform a tally of the decrypted votes.
- An auditor can download the entire election data and verify the shuffle, decryptions and tally.

A Brief History of Voting

- Athenians
 - show of hands
 - ballots on pieces of pottery
 - different colours of stones
 - “facebook”-like authorisation

problems with vote buying / no ballot privacy

- French Revolution and the US Constitution got things “started” with paper ballots (you first had to bring your own; later they were pre-printed by parties)

Ballot Boxes

Security policies with paper ballots:

- 1 you need to check that the ballot box is empty at the start of the poll / no false bottom (to prevent ballot stuffing)
- 2 you need to guard the ballot box during the poll until counting
(<https://www.youtube.com/watch?v=uP01swQVMoc&spfreload=10>)
- 3 tallied by a team at the end of the poll (independent observers)



Which security requirements do paper ballots satisfy better than voice voting?

- Integrity
- Enfranchisement
- Ballot secrecy
- Voter authentication
- Availability

Paper Ballots

What can go wrong with paper ballots?

Paper Ballots

What can go wrong with paper ballots?



William M. Tweed, US Politician in 1860's
"As long as I count the votes, what are you going to do about it?"

Paper Ballots

What can go wrong with paper ballots?

Chain Voting Attack

- 1 you obtain a blank ballot and fill it out as you want
- 2 you give it to a voter outside the polling station
- 3 voter receives a new blank ballot
- 4 voter submits prefilled ballot
- 5 voter gives blank ballot to you, you give money
- 6 goto 1

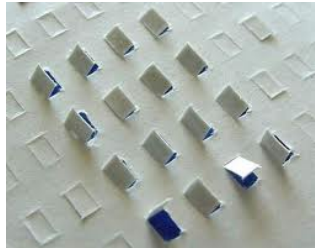
Mechanical Voting Machines

- Lever Voting Machines (ca. 1930 - 1990)



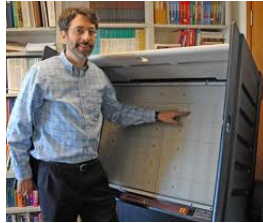
Mechanical Voting Machines

- Lever Voting Machines (ca. 1930 - 1990)
- Punch Cards (ca. 1950 - 2000)



Electronic Voting Machines

DREs

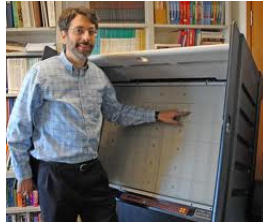


Optical Scan



Electronic Voting Machines

DREs



Optical Scan



all are “computers”

DREs

Direct-recording electronic voting machines
(votes are recorded for example on memory cards)
typically touchscreen machines
usually no papertrail



Diebold Machines

Alex Halderman:

- acquired a machine from an anonymous source
- they tried to keep secret the source code running on the machine

Diebold Machines

Alex Halderman:

- acquired a machine from an anonymous source
- they tried to keep secret the source code running on the machine
- first reversed-engineered the machine (extremely tedious)
- could completely reboot the machine and even install a virus that infects other Diebold machines
- obtained also the source code for other machines

Diebold Machines

What could go wrong?

Diebold Machines

What could go wrong? Failure-in-depth.

Diebold Machines

What could go wrong? Failure-in-depth.

A non-obvious problem:

- you can nowadays get old machines, which still store old polls
- the paper ballot box needed to be secured during the voting until counting; e-voting machines need to be secured during the entire life-time

Paper Trail

Conclusion:

Any electronic solution should have a paper trail.



Paper Trail

Conclusion:

Any electronic solution should have a paper trail.



You still have to solve problems about voter registration, voter authentication, guarding against tampering

E-Voting in India

Their underlying engineering principle is “keep-it-simple”:



E-Voting in India

Their underlying engineering principle is “keep-it-simple”:



Official claims: “perfect”, “tamperproof”, “no need for technical improvements”, “infallible”

Lessons Learned

- keep a paper trail and design your system to keep this secure
- make the software open source (avoid security-by-obscurity)
- have a simple design in order to minimise the attack surface

Lessons Learned

- keep a paper trail and design your system to keep this secure
- make the software open source (avoid security-by-obscurity)
- have a simple design in order to minimise the attack surface

But overall, in times of NSA/state sponsored cyber-crime, e-voting is too hard with current technology.

Online Banking vs. E-Voting

- online banking: if fraud occurs you try to identify who did what (somebody's account got zero)
- e-voting: some parts can be done electronically, but not the actual voting

Student In-Lecture Polling



- can guarantee anonymity
- integrity by electronic means
- how to achieve the same in “software”?

Anonymity

- anonymity through one-time pads

db OnlineBanking **Deutsche Bank**
Privat- und Geschäftskunden AG

Kil Kontonummer 000 000000 00 VB Nr. 001 TAN-Block-Nr. 004
Bitte beachten Sie diese Liste geschützt vor dem Zugriff durch Dritte/Unbefugte an sicherer Stelle auf

| | | | | | | | | | |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 790367 | 617389 | 257429 | 858743 | 065486 | 461758 | 572034 | 508458 | 446778 | 995261 |
| 488196 | 496225 | 928493 | 842280 | 512214 | 899713 | 629791 | 688926 | 386657 | 629294 |
| 067872 | 581255 | 633482 | 179631 | 928465 | 132456 | 428839 | 364093 | 772894 | 578293 |
| 123456 | 669926 | 262799 | 967799 | 298333 | 823675 | 852385 | 327601 | 944584 | 514088 |
| 355119 | 886791 | 320171 | 684843 | 411286 | 283685 | 434867 | 184638 | 561839 | 982316 |
| 948331 | 173865 | 260486 | 726175 | 085565 | 468229 | 815328 | 463697 | 682671 | 591326 |
| 388481 | 799524 | 136588 | 225965 | 878273 | 563495 | 596191 | 186662 | 274686 | 814639 |
| 331798 | 899818 | 186855 | 958438 | 565471 | 127630 | 427243 | 686387 | 780225 | 713897 |
| 846886 | 189915 | 198757 | 568579 | 169961 | 709665 | 878837 | 659491 | 821889 | 256687 |
| 772162 | 780865 | 487943 | 181667 | 149878 | 713321 | 879192 | 238808 | 575317 | 368287 |

Sie erhalten rechtzeitig vor Nutzung der letzten noch unverbrauchten TAN dieses TAN-Blocks automatisch einen neuen Folge-TAN-Block zugewiesen.

Anonymity

- anonymity through one-time pads

db OnlineBanking Deutsche Bank
Privat- und Geschäftskunden AG

Fl. Kontonummer 000 000000 00 VB Nr. 001 TAN-Block-Nr. 004
Bitte beachten Sie diese Liste geschützt vor dem Zugriff durch Dritte/Unbefugte an sicherer Stelle auf

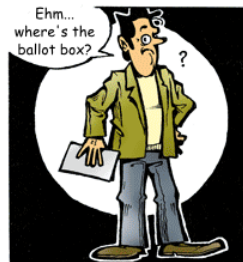
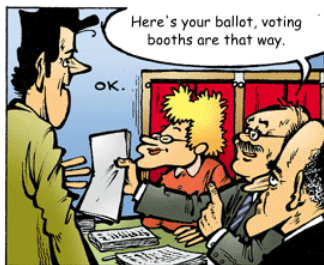
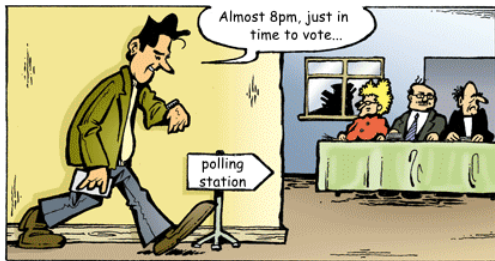
| | | | | | | | | | |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 790367 | 417389 | 257479 | 858743 | 045486 | 461758 | 572014 | 568458 | 446778 | 995261 |
| 480194 | 494225 | 928493 | 842280 | 512214 | 899713 | 629791 | 686926 | 386637 | 629294 |
| 407872 | 581255 | 433482 | 179611 | 928465 | 132456 | 428839 | 340593 | 772894 | 578293 |
| 123436 | 669926 | 262799 | 947799 | 298333 | 823675 | 832385 | 327681 | 949584 | 514088 |
| 385119 | 886781 | 320271 | 684841 | 411284 | 281845 | 414867 | 184418 | 561839 | 982314 |
| 490331 | 173863 | 282484 | 726175 | 055545 | 448229 | 815328 | 943697 | 482671 | 591326 |
| 380481 | 799524 | 136589 | 225965 | 878273 | 563495 | 596191 | 186862 | 274646 | 814639 |
| 331798 | 899818 | 156555 | 958618 | 565671 | 127630 | 427243 | 686347 | 780223 | 715897 |
| 840486 | 189915 | 198757 | 548579 | 169961 | 709465 | 874837 | 459491 | 821889 | 236487 |
| 772142 | 780885 | 487943 | 181647 | 149878 | 713321 | 879192 | 238808 | 575317 | 368287 |

Sie erhalten rechtzeitig vor Nutzung der letzten noch unverbrauchten TAN dieses TAN-Blocks automatisch einen neuen Folge-TAN-Block zugewiesen.

- solving the problem of distribution



The adventures of citizen Michael C. Robertson

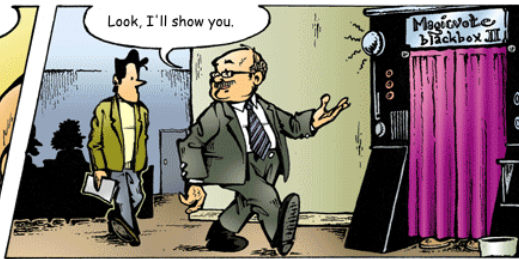


No, no, no, Mr. Robertson, we scrapped those for efficiency. We now have the latest in voting technology...

The MagicVote BlackBox II!



Look, I'll show you.



Just hold your ballot in front of this curtain, right about here.

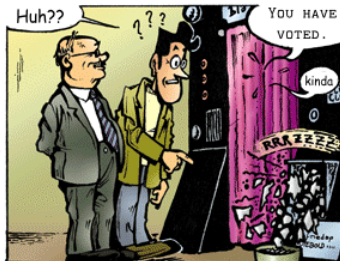


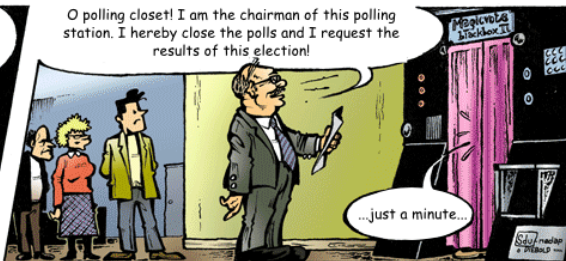
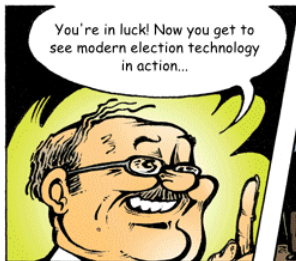
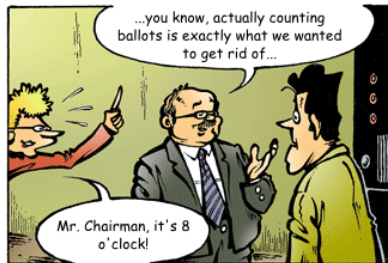
Huh??

???

YOU HAVE VOTED.

kinda





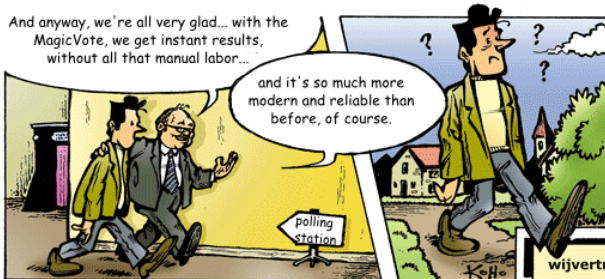


But... aren't you supposed to count those ballots? How do you know the guy in the closet counted right?

Well, honestly, we have no idea, but the government says it's all been taken care of, and the man behind the curtain has been extensively tested. I'm sure they know best.



And anyway, we're all very glad... with the MagicVote, we get instant results, without all that manual labor...



and it's so much more modern and reliable than before, of course.



wijvertrouwenstemcomputersniet.nl

Drawings: Koen Hottentot — Story: Rop Gonggrijp / Barry Wels — Color: Adam Swiecky — Translation: Jaap Weel

Buffer Overflow Attacks



first lecture

Buffer Overflow Attacks



first lecture



next

How to Salt?

1salt ⇒ 8189effef4d4f7411f4153b13ff72546dd682c69
2salt ⇒ 1528375d5ceb7d71597053e6877cc570067a738f
3salt ⇒ d646e213d4f87e3971d9dd6d9f435840eb6a1c06
4salt ⇒ 5b9e85269e4461de0238a6bf463ed3f25778cbba

- in Unix systems: hash(salt + password), or even hash¹⁵⁰⁰(salt + password)

How to Salt?

1salt \Rightarrow 8189effef4d4f7411f4153b13ff72546dd682c69
2salt \Rightarrow 1528375d5ceb7d71597053e6877cc570067a738f
3salt \Rightarrow d646e213d4f87e3971d9dd6d9f435840eb6a1c06
4salt \Rightarrow 5b9e85269e4461de0238a6bf463ed3f25778cbba

- in Unix systems: $\text{hash}(\text{salt} + \text{password})$, or even $\text{hash}^{1500}(\text{salt} + \text{password})$
- Bruce Schneier in cases messages are long:
instead of $m \mapsto \text{hash}(m)$,
use $m \mapsto \text{hash}(\text{hash}(m) + m)$

User-Tracking Without Cookies

Can you track a user **without**:

- Cookies
- JavaScript
- LocalStorage/SessionStorage/GlobalStorage
- Flash, Java or other plugins
- Your IP address or user agent string
- Any methods employed by Panopticlick
→ <https://panopticlick.eff.org/>

Even when you disabled cookies entirely, have JavaScript turned off and use a VPN service, and also ...

Verizon



1. Device sends an HTTP request.

2. Verizon injects an HTTP header ("X-UIDH"). It's a temporary ID, hashed or HMACed with a key.

3. Destination website (or third party) receives HTTP request with injected header.



4. Website directs request to advertising exchange.

5. Advertisers on the exchange can issue a paid API call to Verizon.

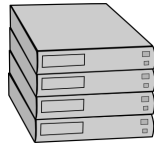
6. Verizon maps the header to a temporary ID, and returns the ID and/or advertising segments.

<http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works>

Web-Protocol



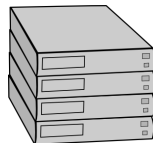
GET static.jpg



Web-Protocol



GET static.jpg

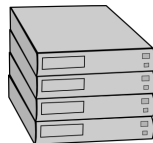


ETag: 7b33de1

Web-Protocol



GET static.jpg



ETag: 7b33de1

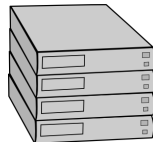
GET static.jpg ETag: 7b33de1



Web-Protocol



GET static.jpg



ETag: 7b33de1

GET static.jpg ETag: 7b33de1



HTTP/1.1 304 (Not Modified)