



INTERNETA BALSOŠANA SABIEDRĪBAS DIENASKĀRTĪBĀ: PAR UN PRET

ANDRIS AMBAINIS

LATVIJAS UNIVERSITĀTE

PAR UN PRET

- Priekšrocības:
 - Vieglāk nobalsot (īpaši, esot ārzemēs);
 - Lielāka vēlētāju aktivitāte (nedaudz?);
- Trūkumi:
 - Drošība;

UZBRUKUMU LĪMENI₃

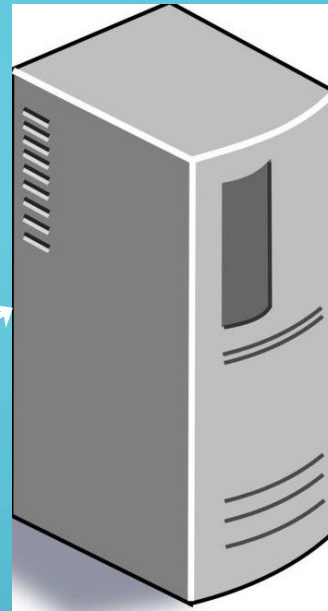
- Amatieris (script kiddie);
- Amatieru grupa;
- Drošības profesionālis;
- Organizēta noziedzīga grupa;
- Valsts.

VALSTS LĪMEŅA UZBRUKUMI

- Stuxnet, Irānas kodolprogramma, 1000 iznīcinātas centrifūgas (2010);
- Ukrainas elektroapgādes tīkls, 300000 cilvēku bez elektrības (2015);
- ASV vēlēšanu reģistrācijas sistēmas daudzos štatos (2016).

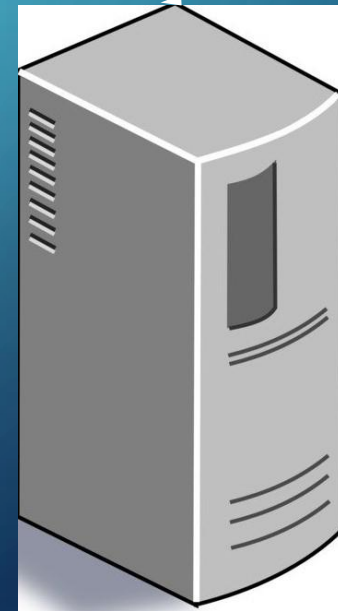
Ja var sekmīgi uzbrukt Irānas kodolprogrammai,
vai e-vēlēšanas Latvijā var būt drošas?

Balsu uzkrāšanas serveris



Lietotājs

Balsu skaitīšanas serveris



DRAUDI – VĒLĒTĀJA DATORS

- Vēlētājs neredz, vai nošifrētais balsojums, kas tiek nosūtīts uz CVK, sakrīt ar viņa balsojumu.
- Datorvīruss var inficēt balsošanas programmu.
- Inficēta programma var nomainīt vēlētāja balsojumu pirms tā nosūtīšanas uz CVK un pielietot pareizos autentifikācijas/šifrēšanas līdzekļus **nomainītajam** balsojumam.

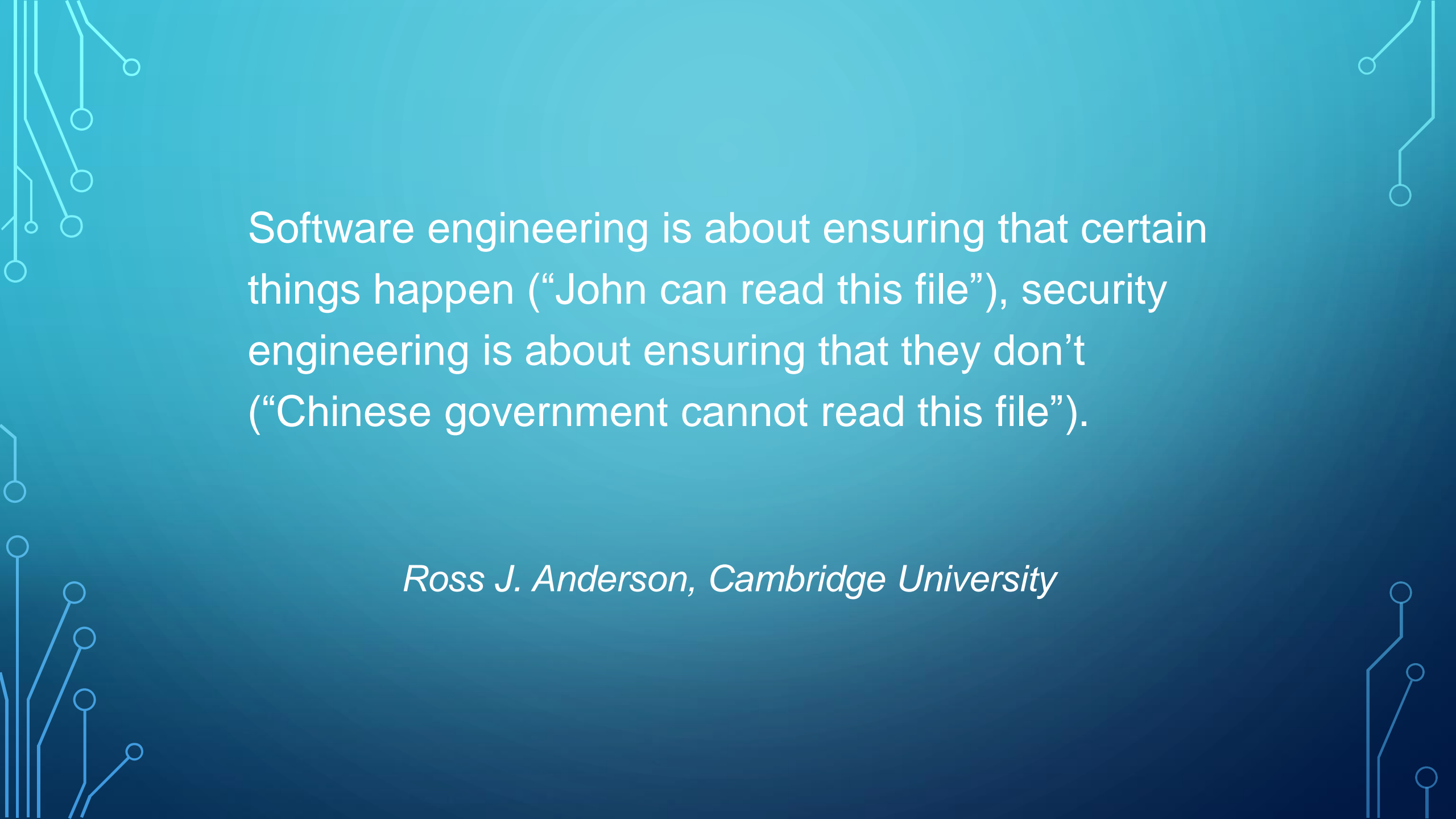
DRAUDI – BALSU SKAITĪŠANA

- Uzbrukumi no iekšpuses (personāls, kas iesaistīts sistēmas apkalpošanā);
- Uzbraukumi no ārpuses (drošības caurumi).

Sekas:

- Notikušie balsojumi var tikt mainīti;
- Var tikt pieskaitīti nenotikuši balsojumi.

Ielaušanās var tikt nepamanīta.

The background is a dark blue gradient. In the corners, there are decorative white and light blue circuit-like patterns consisting of lines and small circles, resembling a network or data flow diagram.

Software engineering is about ensuring that certain things happen (“John can read this file”), security engineering is about ensuring that they don’t (“Chinese government cannot read this file”).

Ross J. Anderson, Cambridge University

PASAULES PIEREDZE

- Igaunija – kopš 2005. gada;
- Norvēģija – 2011.-2013., netiek turpināts;
- Šveice – 2009.-2018., apturēts;
- Austrālija (New South Wales province) – kopš 2011. gada;
- ASV (Vašingtona) – tests 2010. gadā, izstrāde pārtraukta.

IGAUNIJA, 2014



A. Haldermans un komanda,
Mičiganas universitāte

Due to these risks, we recommend that Estonia discontinue use of the I-voting system. Certainly, additional protections could be added in order to mitigate specific attacks (e.g. [48]), but attempting to stop every credible mode of attack would add an unmanageable degree of complexity. Someday, if

Our disclosure is responsible. We have privately informed the Estonian Electronic Voting Committee of a number of technical issues in their systems, the details of which we have not made public.

ŠVEICE, 2019

Computing Mar 12

...

A major flaw has been found in Switzerland's online voting system

Verification: The specific issue is the way the system receives and counts votes before shuffling them and anonymizing voter details (everyone provides a birth date and an initialization code). Once they've been shuffled, the votes are counted and then decrypted. The trap door means someone could switch all the legitimately cast ballots for fraudulent ones, undetected.

ZELTA STANDARTS

- Individuāla verificējamība: vēlētājam ir iespēja pārliecināties, ka viņa balss ir pareizi saskaitīta;
- Universāla verificējamība: vēlētājam ir iespēja pārliecināties, ka visas balsis ir pareizi saskaitītas.

Netiek sasniegts nevienā realizācijā.

VERIFICĒJAMĪBA VS. AIZKLĀTĪBA

- Ja vēlētājs var pārbaudīt savu balsojumu, vai šo verificācijas mehānismu kāds nevar izmantot, lai pārbaudītu, vai vēlētājs «pareizi» nobalsojis?

ASV NACIONĀLĀ ZINĀTŅU AKADĒMIJA, 2018

Recommendations

5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.^{13,14} Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.¹⁵

The U.S. Election Assistance Commission, National Institute of Standards and Technology, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense should sponsor research to:

- assess the potential benefits and risks of Internet voting;
- evaluate end-to-end-verifiable election systems in various election scenarios and assess the potential utility of such systems for Internet voting; and

[Securing the Vote: Protecting American Democracy, 2018]