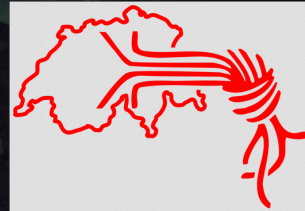


Postdemokratie mit e-voting

Der Traum der Geheimdienste



NSA: “e-voting bettelt darum, ausgebeutet zu werden”

«Internet-centric activities such as e-commerce, e-voting, and on-net industrial and utility control beg to be mined»

(aus: NSA: “(U) SIGINT Mission Strategic Plan FY2008-2013 [TOP SECRET//COMINT//REL TO USA, FVEY//20320108])



Ist e-voting nur scheinbar harmlos...



GILBERT nuclear physics
No. U-238

ATOMIC ENERGY LAB

PERFORMS OVER 150 EXCITING EXPERIMENTS!
FOR THE JUNIOR SCIENTIST

EXPLORE THE SECRETS OF THE ATOM!



Model of Alpha Particle
Made with Nuclear Spheres

- MOST MODERN SCIENTIFIC SET EVER CREATED!
- SEE PATHS OF ALPHA PARTICLES SPEEDING AT 12,500 MILES PER SECOND!
- WATCH ACTUAL ATOMIC DISINTEGRATION—RIGHT BEFORE YOUR EYES!
- PROSPECT FOR URANIUM WITH GEIGER-MUELLER COUNTER!



Measure radioactivity of Uranium and other ores with Gilbert Electroscopie, just like real scientists!



Thrilling to watch! Gilbert Spinthariscopes show you actual Atomic disintegration of radioactive material!



Prospect for Uranium and other radioactive Ores! Gilbert Geiger-Mueller Counter may win you \$10,000 Govt. bonus!

CONTENTS

No. U-238 GILBERT ATOMIC ENERGY LAB INCLUDES! GEIGER-MUELLER COUNTER + WILSON CLOUD CHAMBER + SPINTHARISCOPES + ELECTROSCOPE NUCLEAR SPHERES + ALPHA BETA AND GAMMA RADIATION SOURCES RADIOACTIVE ORES + THREE ILLUSTRATED BOOKS— "PROSPECTING FOR URANIUM", "HOW DAWOOD SPLIT THE ATOM", "GILBERT ATOMIC ENERGY INSTRUCTION BOOK".

\$10,000.00 REWARD

That's what the United States Government will pay to anyone who discovers deposits of Uranium! Get full details in the book "Prospecting for Uranium" packed with this Atomic Energy Lab.

Exciting! Safe!

ANOTHER GILBERT HALL OF SCIENCE PRODUCT

... oder haben Schweizer Forscher etwa den heiligen Gral gefunden?



Fast alle anderen Länder sind raus aus e-voting



e-voting Schweiz: die Befürworter

- «Computer sind unsicher? Wir schützen sie!»
 - Nicht einmal Banken schaffen es, ihre IT sicher zu halten – ständige “Leaks” und Einbrüche
 - Das Allermeiste wird vertuscht
- «Computern kann man nicht vertrauen? Dann nehmen wir mehr Computer, die sich gegenseitig überprüfen!»
 - “State Actors” aka Geheimdienste knacken nicht nur einzelne Computer. USA, Russland, China.



... doch IT-Sicherheit existiert nicht

- «Wir bieten eine Million, wenn jemand das System hackt!»
 - Mit Wahlen werden jährlich CHF 680 Milliarden entschieden, und nicht eine Million
- «Auch Wahlzettel kann man fälschen, genau wie unser System!»
 - ... doch Wahlzettelfälschen skaliert nicht



Hauptproblem: Skalierbarkeit

- Angriffe auf Computer skalieren mit $O(1)$
«konstant» bezüglich der abgegebenen Stimmen
- Angriffe auf Wahlzettel skalieren mit $O(n)$
«linear» bezüglich der abgegebenen Stimmen
- Erkennungsrisiko bei Wahlfälschung mit Zetteln
skaliert $O(n^2)$ «quadratisch»
- Erkennungsrisiko bei Wahlfälschung mit
Computern skaliert $O(1)$ «konstant»



Trick der Befürworter: Ausschliessliche Betrachtung der Software

- Betrachtet man innerhalb der Software, so sind die Verfahren gut
- Betrachtet man den Betrieb der Software auf echten Computern, so sind alle softwarebasierenden Verfahren völlig wirkungslos und damit hinfällig
- Es geht also um die Plattform
- Die Geheimdienste wissen das



Hauptproblem: unsichere Plattform

- “Reflections on Trusting Trust”
Ken Thompson, Turing Award 1984
- Moderne Computer:
 - Silicon
 - Microcode
 - Firmware
 - Operating System
 - Libraries
- e-voting-Programm nicht mal Open Source



Hauptproblem: Vertrauen der Bürger

- Demokratie befriedet: wichtig ist nicht nur, wer gewinnt, sondern auch dass der Verlierer die Entscheidung akzeptiert
- Wahlzettel, Bleistift, Kreuz
 - klar verständlich für jedermann
- Computer, Software, Kryptographie:
 - Kein Fachmann versteht alles, sondern es braucht hunderte Fachleute für alle Details
 - Laien haben gar keine Chance, auch nur die Grundlagen zu verstehen



Wie wird das Schweizer Volk entscheiden?

- Wird das seine letzte echte Entscheidung?

<https://blog.fdik.org/2018-01/s1515978869>

<https://blog.fdik.org/2016-08/s1471798246>

Volker Birk

Chaostreff Winterthur

CCC Schweiz

<mailto:vb@dingens.org> <http://blog.fdik.org>

<http://www.ccc-ch.ch>

