ApTI
Asociația pentru Tehnologie și Internet

19 aprilie 2015

Răspunsul Asociației pentru Tehnologie și Internet (ApTI) la consultarea pe tema votului electronic lansată de Societatea Academică Română (SAR)

Un sistem de vot electronic prin Internet este nefezabil din punct de vedere tehnic în condițiile tehnice actuale, deci opțiunea votului electronic este o falsa ipoteza.

Astfel, sunt 3 elemente nesigure în comunicație:

1. Calculatorul de la care votul prin Internet se transmite nu poate fi sigur. Aceasta depinde doar de masurile de securitate ale calculatorului folosit pentru a vota (care sunt aproape imposibil de verificat pentru fiecare calculator în parte). Infectarea calculatoarelor cu sisteme de operare Windows (care sunt majoritate) este extrem de ușoară, de multe ori de-a dreptul trivială.
Explicat simplu: Tu votezi candidatul A și de pe calculatorul tău pleacă ca ai votat candidatul B.

2. Conexiunea prin care trimiți votul nu este sigura. Exista posibilitatea criptării end-to-end, dar tehnologiile de criptare nu au fost niciodată și nu au cum să fie, chiar și din punct de vedere teoretic, infailibile. Membrii comunității de securitate informatică știu asta de multă vreme iar pentru restul populației aceste lucruri au fost dovedite de ultimele revelații ale lui Snowden: comunicațiile pot fi accesate și modificate cel puțin de NSA și alte agenții de securitate externe.
Explicat simplu: Tu votezi candidatul A și de pe calculatorul tău pleacă ca ai votat candidatul A, dar ajunge la final ca ai votat candidatul B.

3. Calculatorul care primește votul cu software-ul care contorizează poate că e sigur (deși orice expert de securitate informatică va spune că nici un calculator conectat la rețea nu poate fi sigur). Softul de primire și contorizare a voturilor este imposibil de audiat perfect, astfel încât rezultatul votului poate fi ușor falsificat (indiferent de software-ul folosit), în special de națiuni care angajează hackeri (vezi incidentele recente cu Rusia sau chiar Coreea de Nord).
Dacă codul sursa al software-ului nu este public, acest software este, practic, o gaura neagră în care bagi votul și nu se știe ce iese.
Dacă codul sursa al software-ului este public, riscul este mai mic, însă posibilitatea de a găsi cineva o gaura de securitate pe care să nu o raporteze, ci să o exploateze în interes propriu este uriașă.
Vezi testul publicat specialiștii de la Universitatea din Michigan pentru încercarea de vot prin Internet din District of Columbia din 2010, prin care au făcut ca cel care a câștigat alegerile a fost Superman!
Explicat simplu: Tu votezi candidatul A și de pe calculatorul tău pleacă ca ai votat candidatul A, ajunge la calculatorul care face contorizarea că ai votat candidatul A. Cu toate acestea, în contorizarea voturilor, unde cineva cu interes a avut acces, se notează ca a fost votat B.

Mai sunt și multe alte probleme conexe:
- secretul votului nu poate fi asigurat.
Explicat simplu: Tu votezi candidatul A și cineva poate ști ca ai votat candidatul A.

- sistemul pe hârtie permite re-verificarea procesului și rezultatelor sistemului de votare de la un capăt la celalalt, pe când sistemul electronic nu permite această facilitate, datele electronice fiind în esența lor volatile, deci este foarte improbabila verificarea lui.
Explicat simplu: Cum poți verifica că cei care au votat candidatul A au fost înregistrați ca votând A.
- autentificare: cum trimiți datele de acces în sistem astfel încat nimeni sa nu aibă acces la ele în afara alegătorului? Experienta cu Posta Romana pentru trimiterea cardurilor de sănătate (total nesigura) ne arata ca statul român nu are o minima competența în acest sens.
- usability: Cum te asiguri că software-ul este făcut suficient de "pe înțelesul tuturor" astfel încât cel care votează A să înțeleagă că votează A și nu B.
- observatori: Cum găsești niște observatorii care chiar pot sa auditeze tot sistemul de la un capăt la altul
- tech support: Cum poți sa asiguri răspunsurile tehnice corecte și inteligibile la întrebările primite de la toți cei interesați?

Concluzie: Nivelul tehnic actual nu permite asigurarea unui sistem electronic de vot (și cu atît mai puțin a unui sistem de vot prin Internet) la un nivel de siguranță măcar acceptabil.

Va *imploram* sa citiți bibliografia științifică pe care ne bazam concluziile.

Bibliografie științifică:

1. Carleton Univeristy, „A Comparative Assessment of Electronic Voting”, Prepared for Elections Canada by Canada-Europe Transatlantic Dialogue, Februarie 2010, http://labs.carleton.ca/canadaeurope/wp-content/uploads/sites/9/AComparativeAssessmentofInternetVotingFINALFeb19-a.pdf
2. Dr. Paul G. Thomas (University of Manitoba) și Lorne R. Gibson (Former Chief Electoral Officer, Province of Alberta), „Comparative Assessment of Central Electoral Agencies”, A Report Commissioned by Elections Canada, Mai 2014, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote&document=index&lang=e
3. Elections BC, „Independent Panel on Internet Voting”, Februarie 2014, http://www.elections.bc.ca/index.php/voting/ipiv/
4. Jeremy Clark (Concordia University) și Aleksander Essex (Western University), „Security Assessment of Vendor Proposals - Final Report”, City of Toronto RFP #3405-13-3197, Februarie 2014, http://www1.toronto.ca/City%20Of%20Toronto/City%20Clerks/Elections/Accessibility/Files/TorontoVotingSecurity-FinalReport.pdf
5. The Carter Center, „Internet Voting Pilot: Norway’s 2013 Parliamentary Elections”, Martie 2014, http://www.cartercenter.org/resources/pdfs/peace/democracy/Carter-Center-Norway-2013-study-mission-report2.pdf
6. Scott Wolchok, Eric Wustrow, Dawn Isabel și J. Alex Halderman de la University of Michigan, Ann Arbor, „Attacking the Washington, D.C. Internet Voting System”, Proc. 16th Conference on Financial Cryptography & Data Security, Februarie 2012, http://www.ifca.ai/fc12/pre-proceedings/paper_79.pdf
7. J. Alex Halderman de la University of Michigan, Ann Arbor, „Lecture 8. Internet Voting? - 8.4 Washington D.C.”, Securing Digital Democracy video lectures,

https://class.coursera.org/digitaldemocracy-002/lecture/38
8. J. Alex Halderman, Drew Springall, Travis Finkenauer și Zakir Durumeric de la University of Michigan, Harri Hursti - Independent Security Researcher, Jason Kitcat de la Open Rights Group, Margaret MacAlpine - Post-Election Audit Advisor, „Independent Report on E-voting in Estonia", Mai 2014, https://estoniaevoting.org/findings/
9. Open Rights Group, „Findings of the Open Rights Group Election Observation Mission in Scotland and England", Iunie 2007, https://www.openrightsgroup.org/campaigns/e-voting/e-voting-2007/e-voting-main
10. Open Rights Group, „Electronic Counting", https://www.openrightsgroup.org/issues/e-counting
11. Vanessa Teague și J. Alex Halderman, „Security flaw in New South Wales puts thousands of online votes at risk", Martie 2015, https://freedom-to-tinker.com/blog/teaguehalderman/ivote-vulnerability/