#SECURITY #DEMOCRACY

Why the answer to how to strengthen public trust in elections is… SEEV

7 May 2019

ELECTION SERIES #3

The traditional pencil-and-paper method to mark your vote in the polling booth has been gradually replaced by electronic voting machines in many countries, in Europe and beyond. Ensuring the security of electronic voting machines and quelling fears of vote-rigging have become ever more important. One ERC-funded researcher has been working tirelessly to develop such an e-voting system through two projects, SEEVS and its follow-up SEEVCA.

We live in politically volatile times. This is an age of social media dominance, fake news and paranoia from many sections of society that the political system is somehow built to be aligned automatically against their fundamental interests. For liberal democracy to survive and flourish, the fundamental premise on which it is built – regular, open and free elections to choose your political representatives – must be trusted. If election results are questioned, this undermines the credibility of the entire democratic process.

Introducing you to SEEV

This is why Professor Feng Hao, an ERC grantee, now with the University of Warwick (and previously Newcastle University), has been investigating a new type of e-voting systems that are end-to-end (E2E) verifiable, but in contrast to all previous E2E verifiable voting systems, they do not require any trustworthy authorities, called ‘self-enforcing e-voting’ (SEEV).

“All previous E2E verifiable voting systems require a set of tallying authorities, who are supposedly trustworthy individuals with cryptographic and computing expertise and tasked with performing complex cryptographic operations,” explains Prof. Hao. “In essence, the systems we’ve been developing completely remove the need for any such tallying authorities, meaning that every voter is able to count votes themselves and verify the integrity of an election process in real-time, whilst preserving the privacy of each individual vote.”

Prof. Hao asks us to imagine a picture of the Manhattan skyline formed of millions of pixels. Each voter holds the key to one pixel which is their vote. Each pixel is encrypted so it doesn’t reveal any private information about the vote, however when all pixels are formed together, a detailed image is revealed, showing the election tally. “If an attacker attempts to tamper with pixel values, or modify the election result, it will be publicly detectable because the mathematical relations between pixels will fail to be verified,” says Prof. Hao. “Our experience really shows that by removing tallying authorities, the voting process can be automated and managing an election is almost effortless.”

Addressing challenges, finding solutions

There are still some challenges though to iron out before wider commercialisation can be pursued. First, the notion of privacy protection if an electronic voting machine is hacked. “The initial design of a SEEV system works on pre-computing the ballots before an election, but it requires securely storing the pre-computed ballots. We addressed this issue by opting for a real-time computation strategy and built a new end-to-end verifiable voting system without any tallying authorities,” explains Prof. Hao. “In this new system, when the e-voting machine is completely compromised, the tallying integrity of an election remains preserved and what the attacker can learn is strictly limited to the partial tally at the time of compromise.”

Then probably the next fundamental challenge is the human factor: would voters actually accept such a system? “In particular, our system is based on cryptography to enable every voter to verify the integrity of an election system, but ordinary voters do not understand cryptography, and many of them do not bother to perform any verification,” says Prof. Hao. “We carefully took into account these human factors in the SEEV prototypes, so that the verification task for individual voters is kept minimal. The point of an election is to convince the loser; hence at least the loser of the election will be motivated to perform such a verification to check if they indeed have lost.”

Full steam ahead for SEEV!

Moving forward, Prof. Hao’s team also intends to apply their work to India (the world’s largest democracy) where, through a new project funded by the UK Royal Society, they will adapt SEEV to cater to the specific conditions in the country. Secondly, they intend to commercialise SEEV for internet voting applications, focusing initially on online shareholder voting, through a project funded by the Innovate UK Academic Start-up Programme. And finally, they plan to extend the underlying cryptographic design principle of SEEV to other applications such as auction and decentralised payment.

Overall, Prof. Hao is most proud of the fact that he and his team actually built concrete systems that could be used in real-life elections. “For me personally, the proudest moment was arguably when we showed our system to an election official in Newcastle who responded: ‘This is the future’,” he concludes.

Project information

http://www.ncl.ac.uk/

SEEVS
Self-Enforcing E-Voting System: Trustworthy Election in Presence of Corrupt Authorities

Researcher:
Feng Hao
Host institution:
University of Newcastle upon Tyne, United Kingdom

Call details
ERC-2012-StG, PE6

ERC funding
1 484 713 €

Related links

See all ›

22 May 2024

Studying gangs from the inside

#CITIES #SECURITY

31 May 2023

Wildfire recovery: Lessons from animals

#ENVIRONMENT #DIVERSITY #SECURITY

10 Nov 2022

Low-carbon transition at least cost to society

#ENERGY #CLIMATE #SECURITY

31 Jan 2022

Who controls the blockchain?

#ARTIFICIAL INTELLIGENCE #SECURITY #DEMOCRACY