Computer scientists deploy first practical, Web-based, secure, verifiable voting system

March 5 2009

Computer scientists affiliated with the Center for Research on Computation and Society (CRCS), based at the Harvard School of Engineering and Applied Sciences (SEAS), in collaboration with scientists at the Université Catholique de Louvain (UCL) in Belgium, deployed the first practical, web-based implementation of a secure, verifiable voting system for the presidential election held at UCL earlier this week.

Called Helios, the system was developed by Ben Adida, a fellow at CRCS and an instructor/researcher at the Children's Hospital Informatics Program, Harvard Medical School. Professors Jean-Jacques Quisquater and Olivier Pereira and Ph.D. student Olivier de Marneffe at UCL worked closely with the UCL Election Commission to integrate Helios into the University's infrastructure, implement UCL's custom weighted tallying system, and optimize the verification tools for the election size.

"Helios allows any participant to verify that their ballot was correctly captured, and any observer to verify that all captured ballots were correctly tallied," said Adida. "We call this open-audit voting because the complete auditing process is now available to any observer. This revolutionary approach to elections has been described in the literature for more than 25 years, yet this is the first real-world open-audit election of this magnitude and impact of outcome."

The verifiable voting system, available as open-source/free software, implements advanced cryptographic techniques to maintain ballot

secrecy while providing a mathematical proof that the election tally was correctly computed.

Helios relies upon public key homomorphic encryption, a method where a public key is used to encrypt a message (in this case, a vote); messages can be combined under the covers of encryption (in this case, tallying the votes); and multiple independent private keys are required to decrypt the message (in this case, the election tally).

In an election, Helios works as follows:

• first, each voter receives a tracking number for his/her vote and the vote is encrypted with the election public key before it leaves the voter's browser;

• second, with the tracking number, a voter can then verify that their ballot was correctly captured by the voting system, which publishes a list of all tracking numbers prior to tallying; and

• finally, the voter, or any observer including election watchers from outside the election, can verify that these tracking numbers (the encrypted votes) were tallied appropriately. The election results contain a mathematical proof of the tally that cannot be "faked" even with the use of powerful computers.

"Because the tallying happens under the covers of encryption, the entire verification process is done without revealing the contents of each individual vote," explained Adida "Moreover, by using Helios, voters no longer need to blindly trust those supervising the election, as officials must provide mathematical proofs that everything was done appropriately."

The system was first tested in smaller elections throughout 2008 and

then, in early February 2009, on a population of 3,000 voters at UCL in anticipation presidential election held during the first week of March. The UCL Presidential election was available to 25,000 eligible voters, of which 5,400 registered and 4,000 cast a ballot.

More information: http://www.heliosvoting.org/

Source: Harvard University