New e-voting system to flag up coercion

Posted on Tuesday 21st May 2013

SAN FRANCISCO – University of Birmingham (UK) computer scientists have devised an e-voting system that can identify and monitor any votes that could have taken place under coercion, they announced at the IEEE Symposium on Security & Privacy on 21 May 2013.

The internet-based system, called **Caveat Coercitor (http://www.gurchetan.com/papers/caveatcoercitor.pdf)** , is designed to flag up any votes made by voters that are coerced. For example, a coercer might change a legitimate vote by installing malware on the victim's computer, or vote on their behalf by stealing their voting password from the post. Such votes will be flagged up to the authorities so that they can be discarded, and their impact on the final result can be analysed. These analyses are made publicly available for anyone to verify.

Currently, in postal voting, there is no way of ascertaining whether a voter has been coerced or intimidated into voting a certain way, or choosing a particular candidate. The researchers are concerned about the potential for coercion in postal and internet voting, but so far it has proved very difficult to design voting systems which resist coercion completely.

Mark Ryan, Professor of Computer Security at the University of Birmingham, who led the design said: *'Instead of building in mechanisms that prevent coercion, our system tolerates coercion so that an evidence trail can be built up, and then the authorities can see how much coercion is taking place. Of course, all the while, people's votes are kept private.'*

Coercion can take many forms - voters can be coerced and intimidated by a family member, an employer, organized criminals or by illegal software installed on their computer. As well as making coercion evident, the researchers have used techniques to give voters the opportunity to verify that their vote is properly counted, and hasn't been altered once they have cast it. The proposed system combines coercion evidence and election verifiability.

Gurchetan Grewal (http://www.gurchetan.com/index.html) , who also worked on the project, said: *Malware on home computers could be used to coerce voters systematically. Making such coercion evident is an important check, which we have done in this work.'*

Ends

For further information Kate Chapple, Press Office, University of Birmingham, tel 0121 414 2772 or 07789 921164.