

## **E-Voting: The Security Perspective**

### **ALEXIOS BALLAS**

*Candidate for MSc*

*Department of Information Systems*

*London School of Economics*

E-Voting security has been at the forefront of a growing debate on e-voting systems. The academic community has recently begun exploring the issue and two main streams of thought have appeared. One supports universal and absolute security with the use of physical ballots and the other claims that such security is not a necessity in all contexts. Important aspects of the debate include voter authenticity, voter anonymity, system accountability, system disclosability and system availability. Theories used to present the argument include systems theory and structuration theory, but the theoretical underpinnings of the topic are still highly underdeveloped. The research methods are mostly interpretivist and include cases studies, qualitative analyses and action research. Future research on the topic should include case studies of open source systems implementations as well as research in how e-voting security should be handled in cases of weak democracies.

### **Introduction**

Election systems have traditionally been based on paper ballots and in some cases on mechanical devices such as lever and punch card machines. The last fifteen years following the wider trend of ICT adoption in government (e-government) some countries have started slowly adopting and in some cases fully substituting traditional voting systems with electronic voting systems (E-Voting). E-Voting comes in different forms and shapes. A general distinction could be made between electronic machine voting (eMV), which is voting on an election controlled device, and electronic distance voting (eDV), which allows voting remotely using mediums such as the Internet, Short Message Service (SMS), and interactive TV (Svensson & Leenes, 2003).

Following such developments and starting only six years ago the information systems' academic community is slowly beginning to explore the various aspects of e-voting. The research has touched on a wide range of issues including the reasons for and against adopting the different forms of the technology, whether the time is right for such an adoption, whether the technology is context specific, arguments for and against its centralized or decentralised management, whether and how it influences the election results and the use of open or proprietary source systems.

The most significant and most written about issue on the literature though is the security of e-voting systems. Elected governments in modern democracies derive their legitimacy from the electorate process. As such this process has an immense weight and importance and failing to secure its validity could undermine the system of government (Caltech/MIT Technology Project, 2001). The rest of this text will present and analyse the literature on e-voting security.

### **Security Debate**

#### *Overview*

Security in e-voting includes a wide range of issues and actors and is highly related to the type of technology used (Xenakis & Macintosh, 2004). It also relates to the procedures and standards that are put in place to overcome technological security

shortcomings (Mohen & Glidden, 2001; Williams & King, 2004; Xenakis & Macintosh, 2004). E-Voting needs to be secured from the voters, election officials, programmers, technicians and system administrators (Jones, 2004). The threats posed could be internal e.g. the vendor, election officials. Or they could be external such as individuals, well funded agencies, states, parties, criminals, terrorists, many of whom cannot even be prosecuted (Jefferson & Rubin & Simons & Wagner, 2004; Svensson & Leenes, 2003). The motives of the attackers range from publicity (Mayniham, 2004), to foreign intelligence and terrorist acts (Phillips & Spakovsky, 2001), to governments manipulating the system for their benefit (Mercuri & Camp, 2004).

The overall debate of the literature consists roughly of two main views. On one side the zealots of absolute security who do not trust that electronic means provide a sufficient level of transparency, privacy and reliability to be trusted by the electorate, and so always requiring some form of physical verifiability of the result. On the other side researchers whose main belief is that in specific contexts a sufficient level of security could be achieved through physical and electronic procedures and standards.

A comprehensive context of security issues is given by the CESG (Communications-Electronics Security Group) standard made for the UK Government (Xenakis & Macintosh, 2004) and includes voter authenticity, voter anonymity, data confidentiality, data integrity, system accountability, system integrity, system disclosability, system availability, system reliability, personnel integrity and operator authentication and control. The debate on the most controversial of these categories is presented below.

#### *Voter Authenticity*

E-Voting systems must ensure that only the eligible individuals are allowed to vote. Remote voting presents some challenges in doing so since the voter cannot be identified in person. This has led to a greater percentage of fraud in mail-in votes and suggestions that eDV will present the same weakness in a greater scale due to computer automation (Phillips & Spakovsky, 2001). A possible example would be a virus or a Trojan horse, which could spread to the victims' machines via

mass emails, presenting itself as the voter in order to manipulate the ballot according to its creator's intentions (Mohen & Glidden, 2001; Rubin, Simons & Wagner, 2004). Such a threat is significant and possible in major elections (e.g. US presidential election) due to its high popularity as a target of attacks, but it is argued that it is not a particular threat in smaller elections where the stakes and spread of the voters is different (Mohen & Glidden, 2001).

#### *Voter Anonymity*

Voter privacy is considered highly important in modern states and is a requirement on several international conventions (Svensson & Leenes, 2003). eDV though is unable in its own right to enforce ballot secrecy since the voter could exercise his or her right in any environment. This could compromise the vote secrecy and even force ballot casting to the preferred candidate of one's parent, spouse, employer, church and so forth (Phillips & Spakovsky, 2001; Xenakis & Macintosh, 2005). Lack of privacy in combination with weak voter authenticity on eDV could lead to more twisted effects in the election process such as vote selling, bidding and switching (Mercury, 2000; Jefferson et al., 2004).

In order to counter measure such effects various methods have been suggested such as strong legislation against vote coercion (Mohen & Glidden, 2001). Procedural solutions such as having a multi-modal multi-day election that permits voters to override any previous vote on the last day, which is set to only allow ballot casting in election centres (Svensson & Leenes, 2003).

#### *System Accountability*

A voting system should be able to detect malfunctions and possible manipulations, reconstruct the result and be capable of identifying its causes. Auditing the election process in terms of its electronic and physical processes help towards that goal (Jones, 2004; Phillips & Spakovsky, 2001).

Auditing though presents a major challenge in e-voting systems. The fact that voter anonymity needs to be maintained disallows the voter from receiving a receipt, like in financial transactions, that shows how he or she voted. Such a receipt could have then been checked against the actual results in order to verify their correctness (Jones, 2004).

In an attempt to adjust the financial receipt in the voting context the concept of voter-verified paper trail has been suggested. This only works in eMV as it requires the voter to get a printed receipt from the voting machine then check its correctness and place it in a ballot box (Grove, 2004; Jefferson & Rubin & Simons & Wagner, 2004). This allows for an end-to-end audit since both input verification and reliable recount becomes possible (Jones, 2004).

Lack of such receipts makes auditing less reliable (Mayniham, 2004; Grove, 2004; Jefferson & Rubin & Simons & Wagner, 2004; Jones, 2004). Suggestions to better this reliability concern propose recounts using a third party software mechanism that are different from the original in order to verify the result (Mohen & Glidden, 2001; Jones, 2004).

#### *System Disclosability*

On systems that voter-verified paper trails are not used, trust for the validity of the election outcome is shifted towards the software vendors and any possible subcontractors (Xenakis &

Macintosh, 2005). Such trust is not sufficient so standards for the external scrutiny of the vendors in terms of software and processes are put forward (Phillips & Spakovsky, 2001).

E-Voting systems need to be tested and certified by experts both in terms of code and functionality (Mayniham, 2004). There is a growing debate on whether these systems should be tested only on government approved specialised laboratories or whether they should be open source so that anyone could examine and critique them (Mayniham, 2004).

Open source supporters claim that open systems result in greater transparency, trust and confidence since there is universal scrutiny (Xenakis & Macintosh, 2005; Mayniham, 2004). They also suggest that such the oversight increases the incentive of the vendor to produce more secure code and fix errors in order to avoid negative publicity (Mayniham, 2004; Kitcat, 2004).

Open source opponents on the other hand claim that most open source projects are usually maintained by a single person and that the popular ones (for which public scrutiny really works) are only those that are actually used by the developers themselves. Since e-voting systems belong to the first category opening their source will not provide any benefits in terms of security (Kitcat, 2004). They also claim that even if the code developed is open source its hard to ensure that the code used on election day has not been altered as was the case with the Diebold e-voting scandal in the US (Mayniham, 2004; Kitcat, 2004).

In terms of the procedural measures suggestions have been made for public observers to monitor the process either through specially created computer monitors (Phillips & Spakovsky, 2001) or through a series of logic and accuracy tests of the machines on election day (Williams & King, 2004). Other researchers have though disregarded them as inadequate and contributing more towards feeling rather being secure (Mayniham, 2004; Phillips & Spakovsky, 2001).

#### *System Availability*

E-Voting systems need always to be available. Failure to do so could result in voter disenfranchisement. One of the most significant issues with eDV and most particularly with Internet voting is the Denial Of Service (DOS) attacks. These are a fundamental problem of the Internet architecture and although preventative measures could be employed (Mohen & Gliddens, 2001) there is no absolute guarantee of safety (Mercury, 2000; Mohen & Glidden, 2001; Xenakis & Macintosh, 2005). DOS attacks are always a threat to interrupt the e-voting service. In order to minimise the risks, procedural measures have been suggested. These ask for a multi-day multi-modal voting process that reserves the last day only for eMV. This will ensure that no matter the disruptions on the eDV the last day could ensure that all voters do cast their ballots normally (Mohen & Glidden, 2001; Xenakis & Makintosh, 2004).

### **Theories**

The majority of the e-voting literature does not employ any of the widely used IS theories. This is probably the result of the fact that the literature is still in its early stages. The papers that do so use the structuration theory (Svensson & Leenes, 2003), systems theory (Mayniham, 2004), principal-agent theory (Mayniham, 2004), computer science theory (Mercuri

& Camp, 2004) and social identity theory (Oostveen & Besselaar, 2005).

In security, aspects of the systems theory such as the natural accident theory and the high reliability theory are applied. E-Voting systems are viewed as highly complex systems that according to natural accident theory make accidents inevitable. Minor errors in various parts of the complex and closely coupled system could result in unexpected feedback loops. As a result errors in e-voting systems cannot always be predicted and their probability becomes almost inevitable as the complexity of the system increases (Mayniham, 2004).

Election systems though must be reliable and failure to be so could undermine the system of government (Caltech/MIT Technology Project, 2001). In an attempt to resolve the unpredicted system errors the high-reliability theory is employed. This theory is viewed by Mayniham as complementary to the natural accident theory although there is an academic debate on whether they are complimenting (LaPorte, 1994) or contradicting (Sagan, 1999) each other. The theory advocates that building a highly reliable system requires high levels of technical competence acquired through an environment that rewards error reporting and promotes continuous system improvement. The fact that elections are infrequent and use temporal stuff makes it hard to build the appropriate technical knowledge base required (Williams & King, 2004). The theory's requirement for transparency and error reporting favours an open source implementation of e-voting. High-reliability theory also advocates high level of redundancy on the system in order to be able to recover from the unavoidable system errors, such redundancy could be achieved using data audits as well as software and hardware recovery systems (Mayniham, 2004; Jones, 2004).

Structuration theory is also used to demonstrate and explain why different countries employ different forms of e-voting systems and security measures. So according to the theory these measures are distinct as the actors' decisions over time and in each country are influenced by different social and institutional contexts, which are in turn change influenced from these decisions (Svensson & Leenes, 2003). So security in e-voting is influenced by a country's norms, the electoral interests of dominant political actors, industrial and economic pressures and general policy ambitions such as attitudes towards e-government (Svensson & Leenes, 2003). Structuration theory could be considered as complementary to the system theory perspective described above as it looks at the political context.

### **Epistemology and philosophical assumptions**

Most research methods in the literature use interpretivist methodologies. These include many cases studies (Jefferson & Rubin & Simons & Wagner, 2004; Xenakis & Macintosh, 2004; Larsen, 1999; Deutsch & Berger, 2004; Coggins, 2004; Xenakis & Macintosh, 2005), few qualitative analyses (Mercury, 2000; Phillips & Spakovsky, 2001; Mercury & Camp, 2004; Jones, 2004; Svensson & Leenes, 2003) and some action research (Mohen & Gliddens, 2001; Kitcat, 2004; Williams & King, 2004).

Positivist's research methods are also employed to a lesser extent in the form of experiments (Herrnson, et al., 2005; Oostveen & Besselaar, 2005), quantitative analysis (Phillips &

Spakovsky, 2001; Mayniham, 2004) and an empirical survey (Herrnson, et al., 2005).

In more detail almost all the security related research uses interpretivist methods, which seems to derive from the fact that it is hard to quantify security related issues. In the only case that quantitative analysis has been used (Mayniham, 2004) residual votes have been wrongly identified as a factor of reliability. Wrongly because it did not take into account the fact that residual votes could also be cast as a protest vote (Mercuri & Camp, 2004). On the other hand all research related with e-voting usability uses positivist research methods such as experiments and empirical surveys.

### **Conclusions**

The e-voting research as a whole is mostly critical though there are some normative elements trying to influence the course of things especially in the US context. At the moment and since this is still a new field the research is not very well interlinked. This is apparent since there is currently no theory sharing among the papers, excluding those produced by the same authors (Xenakis & Macintosh, 2004; Xenakis & Macintosh, 2005).

The subject's literature volume though seems to increase every year. At the same time the importance of the research is stepped up as a growing number of governments are considering e-voting in the next few years (Svensson & Leenes, 2003). These factors combined with the fact that the field is relatively unexplored makes up for a vibrant future debate.

The limitations on this literature review have been mainly the language and the space available. Language because only English papers could be searched and so limiting access to papers from Brazil and maybe India where e-voting is already happening in full scale. Space as it did not allow for a more complete discussion on the literature debate.

Although the user-verified paper trail form of the technology is presented as the only valid universal solution for e-voting in the majority of the literature, one could recognize that the opposite side of the argument is highly underrepresented. E-Voting without user-verified physical audits could have a place in some particular contexts and countries especially if transparency through open source technology is maintained.

Future research in e-voting needs to be extended beyond the US context. It should check on the results of open source implementations in elections like Australia. It should widen its scope by looking at issues raised in non typical western countries e.g. e-voting in India and Brazil that have already full scale e-voting systems. Finally e-voting security research could be combined with concepts like e-oppression in an attempt to determine the role of international organisation like the UN in observing elections in weak democracies where the loss of privacy and government intervention could have severe effects.

### **References**

Altman, M. and G. M. Klass (2005). "Current Research in Voting, elections, and technology." *Social Science Computer Review* 23(3): 269-273.

- CalTech (2001). Voting: What is, What Could Be, Report of the CalTech MIT Voting Technology Project, MIT Voting Technology Project.
- Coggins, C. (2004). "Independence of voting systems." *Communications of the ACM* 47(10): 34-38.
- Deutsch, H. and S. Berger (2004). "Voting systems standards and certifications." *Communications of the ACM* 47(10): 31-33.
- Franco, A. D., A. Petro, et al. (2004). "Small vote manipulations can swing elections." *Communications of the ACM* 47(10): 43-46.
- Grove, J. (2004). "ACM Statement on Voting Systems." *Communications of the ACM* 47(10): 69-71.
- HERRNSON, P. S., B. B. BEDERSON, et al. (2005). "Early Appraisals of Electronic Voting." *Social Science Computer Review* 23(3): 274 - 292.
- Jefferson, D., A. D. Rubin, et al. (2004). "Analyzing internet voting security." *Communications of the ACM* 47(10): 57-64.
- Jones, D. W. (2004). "Auditing elections." *Communications of the ACM* 47(10): 46-50.
- Kenski, K. (2005). "To I-Vote or Not to I-Vote." *Social Science Computer Review* 23(3): 293-303.
- Kitcat, J. (2004). "SOURCE AVAILABILITY AND E-VOTING AN ADVOCATE RECANTS." *Communications of the ACM* 44(10): 65-67.
- LaPorte and R. Todd (1994). "The Strawman Speaks Up: Comments on The Limit of Safety. *Journal of Contingencies and Crisis Management*." *Journal of Contingencies and Crisis Management* 2(4): 207-11.
- Larsen, K. R. T. (1999). "Voting technology implementation." *Communications of the ACM* 42(12): 55-57.
- Mercuri, R. (2000). "Voting Automation (Early and Often?)." *Communications of the ACM* 43(11): 176.
- Mercuri, R. T. and L. J. Camp (2004). "The code of elections." *Communications of the ACM* 47(10): 53-57.
- Mohen, J. and J. Glidden (2001). "The case for Internet voting." *Communications of the ACM* 44(1): 72-85.
- Moynihan, D. P. (2004). "Building Secure Elections- E-Voting, Security, and Systems Theory." *Administration Review* 64(5): 515 - 528.
- Neumann, P. G. (2004). "The Problem and potentials of voting systems." *Communications of the ACM* 47(10): 29-31.
- Oostveen, A.-M. and P. V. D. Besselaar (2005). "Trust, Identity, and the Effects of Voting Technologies on Voting Behaviour." *Social Science Computer Review* 23(3): 304-311.
- Philips, D. M. and H. A. V. Spakovsy (2001). "Gauging the risks of internet elections." *Communications of the ACM* 44(1): 73-85.
- Sagan and D. Scott (1993). "The Limits of Safety: Organizations, Accidents and Nuclear Weapons. Princeton." NJ: Princeton University Press.
- Svensson, J. and R. Leenes (2003). "E-voting in Europe: Divergent democratic practice." *Information Policy* 8(1): 3-15.
- Williams, B. J. and M. S. King (2004). "Implementing voting systems- the Georgia method." *Communications of the ACM* 47(10): 39-42.
- Xenakis, A. and A. Macintosh (2004). *Procedural Security in Electronic Voting. 37th Hawaii International Conference on System Sciences.*
- Xenakis, A. and A. Macintosh (2005). "Trust Analysis of the U.K. e-Voting Pilots." *Social Science Computer Review* 23(3): 312-325.