Lost Lessons: Election Systems

Peter G. Neumann, sidebar in IEEE Security and Privacy
Special Issue on Lost Treasures, November-December 2012, p. 18

This special issues collects some insights on computer security that happen to be particularly relevant to integrity of elections. Thus, it seems appropriate to consider some of the lost or hidden treasures in that context.

Past elections have illustrated a serious lack of commitment to total-system integrity, accountability, and privacy, as well as weak defenses against insider misuse. Essentially every step in the election process is a potential weak link, spanning registration and authentication of voters, ballot construction, the actual voting process, vote tabulation and canvassing, resolution of irregularities particularly in close elections, and remediation in the face of serious problems.

Many flagrant election irregularities have been observed, some of which are directly computer system related, others of which are procedural, operational, or seemingly extrinsic. These problems tend to arise because of the absence of or inadequacy of total-system requirements, flawed designs and implementations of computer systems, incomplete or misguided security evaluations, and so on.

Examples include significant tampering in the 1988 Florida Senate race (with a 14% drop-off in votes for that race compared with votes for president in the four punched-card counties, where there was essentially no drop-off in the non-punched-card counties) [1]; 22 people indicted in Louisiana in a bribery/kickback scheme in 1999; and nine people in Clay County, Kentucky (including election officials and a federal judge) indicted for election frauds in 2002, 2004, and 2006 [2]. The 2006 Kentucky fraud involved poll workers intentionally misleading voters about the user interface, informing them that clicking on the *cast vote* button would cast their votes, whereas a subsequent confirmation button was required with an alternative *back* button that allowed the votes to be altered by the poll workers. Of course, numerous other problems also arose in Florida in 1988 and 2000, Ohio in 2004, and so on, with registration, voter disenfranchisement and biased authentication, and vote counting. The past experiences – including the reports of the 2007 California Top-to-Bottom Review – all suggest that many of the lessons of the past have been almost completely ignored.

Various generic security principles in the literature are directly applicable to beginning-to-end and top-to-bottom election integrity, but have been largely ignored in commercial systems. Such treasures include Kerckhoff's Principle (avoiding security by obscurity), the Saltzer-Schroeder-Kaashoek security principles [6, 5], and the Clark-Wilson integrity properties [3]. In particular, the principle of minimizing the extent of the components what have to be trusted is flaunted by the reality in many of the systems in use today that essentially every step in the election process can be compromised, from establishment of standards to voter registration (disenfranchising, gerrymandering, etc.) to voter authentication (with multiple IDs required in certain cases) to vote casting (with machines observed switching votes) to vote tabulating and canvassing to remediation of disputes (especially in the absence of any meaningful audit trails – much less forensically meaningful nonsubvertible audit trails). Compromises are also possible at each layer of abstraction, from hardware to operating systems to election-specific software and data formats. Insider attacks remain particularly riskful [4], because of the opportunities presented and the ease of triggering serious irregularities.

There are many other application areas in which the lessons of this special issue are salient. However, election integrity is in some sense a paradigmatic example of why this special issue is more important than ever today. Specifically, revisiting some of the lost treasures and problems that might otherwise have been avoided suggest many deeper issues. To mention just a few, consider the risks of outsourcing functionality and responsibility to aunaccountable closed-source proprietary systems, short-sighted and unprincipled system development, lack of understanding of the risks, the continued lack of win-win solutions rather than debilitating tradeoffs among features, ease of use, accountability, cost savings, trustworthiness with respect to security and integrity, and so on. Unfortunately, trustworthiness is often the first to be reduced.

References

[1] P.G. Neumann, Computers in Elections, ACM Risks Forum, 7, 78, 1988; http://catless.ncl.ac.uk/Risks/7.78.html#subj1 .

[2] P.G. Neumann, Kentucky Election Fraud Indictments, ACM Risks Forum, 25, 76, 2009; http://catless.ncl.ac.uk/Risks/25.76.html#subj7 .

[3] D.D. Clark and D.R. Wilson. A comparison of commercial and military computer security policies. In *Proceedings of the 1987 Symposium on Security and Privacy*, pages 184–194, Oakland, California, April 1987. IEEE Computer Society.

[4] P.G. Neumann. Combatting Insider Threats. In *Insider Threats in Cybersecurity – and Beyond*. M. Bishop and C.W. Probst (editors), Springer Verlag, 2010.

[5] J.H. Saltzer and F. Kaashoek. *Principles of Computer System Design*. Morgan Kauffman, 2009. Chapters 1-6 only. Chapters 7-11 are online: http://ocw.mit.edu/Saltzer-Kaashoek .

[6] J.H. Saltzer and M.D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, September 1975.