In the first of these two short articles, I’ve been introducing e-voting. In this part, I summarize some key analyses of the security issues surrounding remote voting via the Internet.

In a July 2002 article posted on the BBC Web site, commentator Bill Thompson comments on a recent Green Paper proposal by Robin Cook, Leader of the House of Commons. Cook includes two methods for increasing the involvement of the public in government decision-making: “For the government, the two strands that make up e-democracy are ways to enhance participation (e-participation) and electronic voting (e-voting).” Thompson argues that the vulnerabilities of any e-voting system built in the next few years should preclude any use of such insecure technology. He writes that the consequences of fraud would be so serious that large amounts of investment would be profitable if they swayed the direction of an election. For example, “If we all use trusted processors then why not set up a production line to manufacture your own hacked chips? It would only cost a few tens of millions of euros. If all code has to be signed by some digital authority, why not spend a few million bribing the senior staff?”

A much longer and more detailed analysis of e-voting is from the respected scientist Avi Rubin of AT&T Labs. Rubin neatly summarizes the issues as follows [I have added the asterisks as bullets and slightly changed the punctuation]: “There are many aspects of elections besides security that bring this type of voting into question. The primary ones are

* coercibility – the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.

* vote selling – the opportunity for voters to sell their vote.

* vote solicitation – the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.

* registration – the issue of whether or not to allow online registration, and if so, how to control the level of fraud.”

Rubin then analyses the voting platform, the communications infrastructure, social engineering, and specialized devices (by which he means “tamper-resistant devices, such as smart cards.”) He discusses in some detail how programmatic attacks (viruses, worms, denial-of-service [DoS] attacks) could easily alter election results. Just imagine the consequences of, say, carefully-written Trojan horse programs, targeted DoS attacks on particular precincts on election day; Rubin writes, “In some close campaigns, even an untargeted attack that changes the vote by one percentage point could sway the election.” According to the notes in the source HTML for the document, that sentence was written a few weeks before the contested US presidential election of 2002. I strongly recommend Dr Rubin’s paper as foundation reading for anyone interested in e-voting.
Finally, I direct your attention to the immensely valuable annotated bibliography on electronic voting prepared by Rebecca Mercuri, PhD, Professor of Computer Science at Bryn Mawr College. Dr Mercuri has a distinguished record of contributions to the technical analysis of electronic voting; her Web site (see below) has many pages of news, essays, pointers to other e-voting sites, lists of her own and other scholarly works on the subject, and even pointers to e-voting humor.

***

I hope that these two short articles will increase readers’ interest in the trustworthiness of e-voting and that some of you will be able to contribute to a more informed discussion of this critically important issue in the future of representative democracy. I’m sure that I will be hearing from e-voting technology vendors clamoring for attention; if possible, I’ll write a follow-up column with some of their remarks.

***

For further reading:

[Note to avoid ambiguity: the string /1/ in this URL uses the lowercase form of the letter “L”]


[Note to avoid ambiguity: the string /1/ in this URL uses the lowercase form of the letter “L”]

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.