

Viewpoint

by MICHAEL CHERRY AND EDWARD IMWINKELRIED

Internet theft is avoidable

If the private sector cannot protect their sensitive information, citizens will turn to the courts. But internet theft easily can be avoided.

The number of recent, major breaches of computer security is alarming. Despite all the publicity, the situation appears to be getting worse, not better. This growing problem is affecting the legal system in particular as well as society in general. At the rate at which the problem is accelerating, the courts may soon be flooded with lawsuits based on security breaches or identity thefts and alleging statutory violations and common-law causes of action.

Since more and more consumers are losing faith in businesses' ability to protect their sensitive information, they are forced to resort to self-protection, sometimes daily checking their credit rating. Over time, this mass loss of faith will create a nightmare for the courts. If the private sector cannot protect their sensitive information and self-protection proves inadequate, predictably citizens will turn to the courts.

These facts strongly suggest that the current paradigm of computer security is ineffective; and all indications are that the situation will continue to worsen until we adopt a new paradigm. What would be the elements of a new approach? To begin with, companies and agencies ought to require a further authentication before permitting someone to access a specific database maintaining sensitive information. Many require a password at the initial logon but nothing later. Moreover, we should

make much more extensive use of encryption and not limit its use to the sending of information.

Simply stated, encryption modifies the form of computerized data by arithmetic means to render it useless to unauthorized persons. Authorized persons can access the information in useable form because they have a "key." The key unlocks the data; it is a mathematical tool for recovering the data in its original, unencrypted form. There are several varieties of encryption, and some are more effective than others. The National Institute of Standards and Technology has developed Federal Information Processing Standards (FIPS) 140-2 as a model for storing data.

There are several major advantages to widespread utilization of encryption. The most fundamental is that it removes the practical incentive for hacking. The hacker may succeed in penetrating the first line of defense, but cannot use the information. Without the key, the hacker has only nonsensical gibberish. In short, effective encryption removes the risk that the information will be used to the citizen's detriment. Further, in the long term encryption is a more cost-effective approach for companies and entities maintaining vast databases of confidential information. Encryption is a one-time labor cost. In contrast, periodic retesting and hardening of the network necessitates repeated expenditures.

Why then are we still relying on single password authentication and retesting? There are a number of contributing factors including inertia, but one is the perception among companies and entities that intensified authentication procedures and encryption will irritate their employees—so-called "password fatigue." That may indeed be true; employees undeniably appreciate "user friendly" systems. However, that view is myopic. It shifts the burden from the employees to customers who are forced to repeatedly check their credit rating.

The virtually daily, shocking reports of large-scale security breaches make it clear that we must revert to the computer standards we had before the 1990s when security was our top priority. The courts will soon face the question of whether a company's or agency's failure to implement encryption and additional authentication amounts to actionable negligence. The public and private sectors should get ahead of this issue by adopting security measures to safeguard our privacy. ❧

© Copyright 2008 Michael Cherry and Edward J. Imwinkelried, all rights reserved.

MICHAEL CHERRY,

President of Cherry Biometrics Inc., designs identity and security solutions. He is Vice Chairman, Digital Technology Committee, National Association of Criminal Defense Lawyers (NACDL) (mcherry@cherrybiometrics.com)

EDWARD IMWINKELRIED

is the Edward L. Barrett, Jr., Professor at the University of California, Davis, School of Law (ejimwinkelried@ucdavis.edu)