TechnologyReview.com

YOU VS ALL-OR-NOTHING SOA SOLUTIONS
Take the IBM SOA Self-Assessm

Print | Forums

The Password Is Fayleyure

By Michael Schrage March 2005

Replay
Tivoli.
IBM TIVOLI IT SERVICE MANAGEMENT
MINIMIZES TIME AND LABOR COSTS
TIGHTLY INTEGRATES TECHNOLOGY, PROCESSES, AND PEOPLE
BOOSTS SECURITY
IBM.
Get the white paper

Under Review: Password selection for Yahoo! Mail etc.

PokeKey1...ou812$...twasbri11ig!. All were favorite passwords of mine long ago. The first is the name of the puppy I briefly had as a child. The second was shamelessly lifted from a Van Halen album cover. The third, you'll recall, opens *Jabberwock*y. I must have typed each one hundreds of times.

Looking back, I feel like an idiot for believing my wittily "unguessable" passwords enhanced my security in any meaningful way. Password protection is pervasive, annoying, inconvenient, and does little to deter anyone intent on doing harm. But you can't gain legitimate access to many services without it.

Yahoo Mail registration, for example, has come a long way from being an open invitation to spammers and spoofers. Who would argue that its automated "ID/password" reminders are not a boon for the lazy and aphasic among us? But Yahoo's relentless reliance on password protection is a security patch that feels more like a challenge to evildoers than a serious deterrent. And Yahoo Mail is among the better ones in a pretty bad lot.

Today's password authentication schemes are little more than security placebos. They perversely inspire abuse, misuse, and criminal mischief by deliberately making users the weakest link in the security chain. Greater teleprocessing power has made stealing or cracking password sequences ever faster, better, and cheaper. Security guru Mark Seiden observes that many hack attacks have nothing to do with how "strong" a target password is, because these attacks rely on brute-force discovery of alphanumeric sequences. "The bad guys are really attacking your keyboard," he says. That security system administrators make users jump repeatedly through digital hoops to defend the "integrity" of our four- to 12-character sequences falls somewhere between insult and joke.

If a company wanted to design a security system that made a mockery of everything we know about human behavior, cognitive psychology, and cryptographic analysis, it would come up with our contemporary bit-based babel of passwords. As authentication expert Richard E. Smith has observed, the logical conclusion of most "strong password" policies—don't use names of family members or pets; don't use birthdays or calendar dates; use randomized sequences of special characters; don't use your password for more than one or two sites; change your passwords several times a year; don't put your password(s) in your PDA or cell phone—is that passwords should be impossible to remember and should never be written down.

Somehow, the world's ATM banking systems have managed to get by with a bare minimum of fraud for more than 20 years by relying upon only four-digit codes. So what do the banking geeks grasp about password management?

The obvious answer: the stronger and more complex the password scheme, the lazier and more technically incompetent the security system administrator. As Smith demonstrates in a series of keen analyses, the rise of plain-text "sniffer" technology combined with computationally enhanced processing power makes traditional password protection ever weaker and more fragile.

So why are we demanding that millions of people spend more and more time and memory on a security procedure that yields less and less protection? The world doesn't need "better" or "more secure" passwords; it needs to wean itself from passwords and PINs as the medium of authentication. We'd be far more secure with more layered approaches to authentication—"suspicion engines" on the lookout for deviant behaviors—and more subtle yet persistent ways of tracking and challenging online identities.

The global silliness of the password mentality was beautifully highlighted in a survey conducted last year that found 70 percent of those asked said they would reveal their computer passwords for a bar of chocolate. Sweet. A third of those surveyed volunteered their passwords to interviewers without being offered a bribe. Yet another survey discovered that fully 79 percent of people questioned on the streets of London revealed such desirable security-sensitive data as mother's maiden name and birth date. "We are amazed at the level of ignorance from consumers on the need to protect their online identity," sniffed a spokesman for RSA, the pioneering encryption firm that sponsored the research.

Actually, I'm amazed by the laziness of global enterprises that make their users primarily responsible for the security and integrity of complex systems. If passwords are anywhere near as important to online authentication, identity, and security a decade hence as they are today, it will be the clearest possible signal that the virtual world has become an even more dangerous and volatile place for both transactions and interactions.

Michael Schrage is a researcher and consultant on innovations economics and the author of Serious Play *(2000).*

55.397454259909
CATEGORY_KEYWORDS:SOFTWARE