RIT professor recommends tougher computer security measures to beat hackers

December 3 2008

Hackers beware. A Rochester Institute of Technology professor knows how to thwart sophisticated and determined intruders from stealing personal and corporate information. His secret? Anchor your online activities to the physical world.

RIT scientist and entrepreneur Roger Dube takes a close look at user authentication and computer security in his recently published book "*Hardware-Based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography*" (Wiley).

Intended for information technology professionals and others responsible for implementing computer security, "*Hardware-Based Computer Security Techniques to Defeat Hackers*" is a complete review of different types of hardware technology that can protect computer systems.

"There are steps you can take to protect your computer so you can be certain an application you bring up is authentic and hasn't been replaced with something, for instance, that contains a Trojan horse—a virus that masquerades as a normal program," says Dube, research professor in RIT's Chester F. Carlson Center for Imaging Science, and president and chief scientist of Digital Authentication Technologies Inc.

"The protection that is available today is largely based on algorithms and secrets," Dube adds. "And the problem with secrets is that they have to be shared before they can be used. Poorly constructed secrets can be guessed, making systems vulnerable to attack. And poorly protected secrets can be stolen outright."

A recent example of this weakness made the news when a hacker gained access to Gov. Sarah Palin's Yahoo! account, weeks before the election, by pretending to be the Republican vice presidential candidate. The hacker used Palin's personal information reported in the news to answer the security question protecting her e-mail account.

Software approaches to computer security provide limited protection, Dube says. The problem is that encrypted keystrokes hiding the password/secret are transmitted over the Internet, and these passwords can be intercepted and broken.

Pseudo random number generators, algorithms that are often used to create passwords or disguise a password as a jumble of symbols and numbers, are inherently predictable and can be cracked. The commonly used two-factor form of authentication— username plus password, PIN number or pass phrase—is fragile. Today, more robust security systems require users to present their name and password, and something unique to themselves. The nation protects its top secrets with software and hardware security technologies considered to be astronomically difficult to break, Dube notes.

"You cannot use an algorithm to generate a true random number," Dube says. "It's going to be predictable because it's a calculation. It will create a number that looks random, but if a hacker commandeers the 'seed' condition, they've broken the code completely."

According to Dube, only hardware-based security applications can provide the strongest security systems possible—pattern-free and unpredictable. These methods connect a system or a person to the physical world, ensuring confidentiality and authenticity of communication in ways software applications cannot.

"We needed to tie our security system to something that has its roots in the physical world, rather than to make it purely algorithmic. The advantage is that you can find all kinds of random sources in the physical world that are completely pattern free, but the disadvantage is that they typically involved a piece of hardware. Until recently people have been reluctant to add another piece of hardware or to carry something around. But when the loss becomes too much, hardware-based protection becomes the answer."

In his book, Dube details security systems that generate "passwords" from the physical world such as advanced biometrics (fingerprint scanning and iris and retinal scans) and tokens, such as smart cards embedded with a secure electronic chip. He also discusses location technologies that determine if remote servers are legitimate or carefully constructed fakes commonly used in phishing attacks, as well as geolocation technologies, such as global positioning system technology. The book also discusses the potential vulnerabilities of each of these technologies.

Dube's own computer-security research focuses on location technologies and satellite timing signals. Contractors for the U.S. Department of Defense tested the security system Dube developed for Digital Authentication Technologies Inc. and found it robust.

"The technology gives us location awareness, but doesn't tell us where on the surface of the Earth we are," Dube says. "It's double safe in that way."

Source: Rochester Institute of Technology

Citation: RIT professor recommends tougher computer security measures to beat hackers (2008, December 3) retrieved 25 April 2024 from https://phys.org/news/2008-12-rit-professor-tougher-hackers.html