

Phishing for an Answer

In search of a single sign-on solution

One of the fundamental flaws in IT security systems is that clients and servers authenticate themselves to each other in different ways. As a result, when you log into your bank account, your bank can be sure it's you logging in if you provide the right password. You, however, can never be sure if you have logged into your bank or just some site that looks like your bank's.

Unfortunately, financial institutions, retailers, and the computing industry are not addressing this common problem in a unified way. Rather, they are independently trying to find a solution. Some are focusing on educating the consumer, believing that training customers to recognize certain clues on a Web page will help ensure they are secure. Industries and companies are on the defensive, each trying to adapt faster than the attackers who have learned to exploit their individual weaknesses.

Maybe it's time to take a look at Kerberos, a 20-year-old open-source authentication protocol, which allows servers to authenticate clients (and vice versa) with a single sign-on capability. Named after the three-headed dog from Greek mythology who guarded the gates of Hades, Kerberos was developed by the Massachusetts Institute of Technology (MIT) in the 1980s as part of a distributed computing experiment. It now ships standard with every single copy of every major operating system. Not surprisingly, it's been used for a decade internally by most of the major investment banks to safeguard their billions.

Why isn't everyone using it?

While the protocol is mature, much development work still needs to be done to make Kerberos interoperable across all systems and devices.

Since Kerberos is open source, there isn't a financial incentive for companies to invest in programming that then could be used by everyone for free.

Also, many companies have a love-hate relationship with open-source software: They love the price tag but hate the informal support organization.

Vendors, reacting to the perceived needs of the marketplace, have done the minimum necessary to make Kerberos a ubiquitous authentication method. While they may ship Kerberos, they often do not support or fully integrate it. Kerberos deployments are often not up to date with standards, and there is no guarantee of timely bug fixes. As a result, Kerberos is judged not by the potential of the protocol, but rather by the limited functionality MIT has been able to fund.

In the absence of a universal solution, the authentication and authorization wheel is repeatedly re-invented and continues to fracture. Meanwhile,

If business wants it, the vendors will provide.

one high-profile security compromise after another continues to erode faith in electronic commerce.

Maybe this is where the world's financial institutions, retailers, computer industry, and even governments could unite in a common cause. If business wants it, the vendors will provide.

Maybe the European Union could flex its considerable muscle and legislate a Kerberos solution. MIT could continue to act as the neutral agent and create a consortium like the World Wide Web Consortium to do the development work, interoperability testing, and certification, while also encouraging the building of the necessary support organizations. It may take a few years, but in the end, we would have a robust, universal authentication system and a single sign-on solution for the world's computer networks. ■



By Stephen C. Buckley

▶ Read online:
www.symantec.com/ciodigest/thinktank/buckley

Stephen C. Buckley is associate director of the Center for Digital Business at the MIT Sloan School of Management in Cambridge, Massachusetts. He can be reached at sbuckley@mit.edu.