By Blake Ives, Kenneth R. Walsh, and Helmut Schneider

The Domino Effect of Password Reuse

One weak spot is all it takes to open secured digital doors and online accounts causing untold damage and consequences.

Password security is an essential form of user authentication both on the Internet and for internal organizational computing systems. Password protection schemes are used to protect relatively low-sensitivity systems such as access to online archives as well as highly sensitive corporate intranets or personal bank accounts. "Unfortunately the system of user name and password works less well than people believe," according to Bruce Schneier [10]. Moreover, the problem is escalating. The FBI found in a recent survey that detected system penetrations from outside the organization were reported by 40% of the organizations surveyed, up from 25% a year earlier [3].

Extensive literature on password security has evolved over the past 20 years. Much of it has been prescriptive, offering, for instance, advice for creating passwords and safeguarding them [7]. However, password vulnerabilities remain significant. Between 1989 and 1995, 22% of incidents reported to Carnegie Mellon's CERT Coordination Center (CERT/CC) involved password breaches [4]. The most common breach involved copying password files. It is now common to read news stories on password breaks such as the *Wall Street Journal's* report of NASA's loss of 6,000 passwords, or the Associated Press' account of the man who "pleaded guilty to federal charges of infiltrating sensitive computer systems, including those at Stanford University and NASA's Jet Propulsion Labora-

tory,"[1] or the use of an unauthentic request for bank customers to log onto a false Web site so the perpetrator could record passwords associated with online banking accounts [8].

In some more notable cases a security analyst in South Korea used an apparently stolen password from a rival to make a $22 million illegal trade; an admissions officer at Princeton was charged with using Social Security number passwords to pry into admissions decisions at Yale; and at least 21 students at Hofstra University were suspended and employees fired because of grade changes made with stolen passwords. Public access—now a common method for computer access—can be particularly susceptible to password theft due to potential weaknesses in the security of the workstation. For examples, a Kinko's facility was found to have keystroke-capture software installed, sending over 450 user names and passwords to a thief who subsequently used them for bank fraud [5]. Password vulnerability is not restricted to computer applications or operating systems. Indeed, a bug that released user passwords was found in the Netopia 650-T ISDB router firmware [11].

While password theft is a threat to the system from which the passwords were stolen, the network password vulnerability also threatens other systems. If users have many password-protected accounts and they reuse a password across more than one account, a hacker gaining access to one account may be able to gain access to others. If, for example, a hacker gains access to a weakly defended departmental file server and those passwords are stolen, those passwords could be used to gain access to a more secure corporate system. The hacker will reasonably anticipate that some users keep the same password on both systems. As e-commerce grows, the likelihood increases that a hacker who obtains access to passwords at a popular site might be able to use those user-IDs and passwords at another site. For example, there is an obvious and probably sizeable overlap between AOL and Citibank or BankOne and Amazon.com customers. A domino effect can result as one site's password file falls prey to a hacker who then uses it to infiltrate other systems, potentially revealing additional password files that could lead to the failure of other systems.

This is not just speculation. An intrusion was documented by the CERT/CC a few years ago in which a hacker was storing password files collected from several other sites on an intruded site. The hacker collected passwords from 186,126 accounts and had decrypted 47,642 of them. CERT/CC contends the passwords were then loaded into a password cracking tool [2].

[1] www.nytimes.com/2000/11/08/technology/08HACK.html

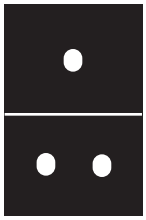
Hacking tools can give more people the capability of launching more sophisticated attacks. Some hacking tools can coordinate attacks from several intruded systems onto targeted systems. If hackers used this automation and coordination with the untold number of stolen password files (though not necessarily reported or even recognized as having been stolen), a strong new hacking tool could exploit a huge database of known user-ID/password combinations. A variation of the now common denial-of-service attacks could be applied, greatly enhancing the effectiveness of password attacks.

Such attacks are difficult to defend against. In many systems, if a hacker tool repeatedly attempts to use incorrect passwords to access a particular account, the system will, usually after several tries, shut down the account in defense. In this scenario where variations on both the user-ID and password are involved, no such defense will be effective and the hacker will be free to run long lists of such pairs. Once the user-ID/password pairs have been tested, a hacker could add database entries capturing identities of systems accessible by a particular pair. This database would then be a powerful tool for systems infiltration, with coordinated attacks arranged to maximize the damage before the problem is discovered.

The rapid increase of e-commerce has fostered a proliferation of password protected sites. Forrester Research [6], for instance, reports that active Web users manage an average of 15 passwords on a daily basis. Unfortunately, Adams and Sasse [1] report that four or five passwords are the most a typical user can be expected to use effectively. Users are thus poorly equipped on a cognitive level to deal with today's need for multiple passwords, thus leading to password reuse on different systems. One source speculated that reusing a password is akin to revealing a password, thus potentially shifting legal liability for misuse to the user.

Users who reuse passwords often fail to realize their most well-defended account is no more secure than the most poorly defended account for which they use that same password. Unfortunately, the latter accounts may be quite weak as sites fail to implement the kinds of secure authentication methods now standard at the operating systems level. For instance, a journal editor given top-level access to a reviewing system was startled to discover he could see the passwords of the several hundred users of the system.

Risks will grow exponentially as password-protected systems proliferate, particularly among small e-commerce sites. Indeed, this problem inspired the title of our article—for with the falling of the weakest domino, other systems will follow, yielding new password information from which still more systems will fall. Today,



We believe it is imperative that e-commerce security systems move expeditiously to either augmented password security systems or alternative security schemes such as smart cards or biometrics.

in an increasingly connected world, this recognition is also essential for, but largely ignored by, everyday users. Sasse et al. [9] trace many password weaknesses to the way in which passwords systems are implemented and call for greater collaboration between security administrators and users. Since issues such as poor password choice have been recognized for more than 20 years without major changes in user behavior, this does not appear to be an adequate general solution, although organizations should heed their advice to make the best use of current password systems.

Despite the apparent high costs and the given limitations of password security systems, we believe it is imperative that e-commerce security systems move expeditiously to either augmented password security systems or alternative security schemes such as smart cards or biometrics. Here, we describe alternatives to password security schemes, discussing both the strengths and weaknesses of those systems and including recommendations for practice and research for what should be done given the identified vulnerabilities.

Alternative Security Schemes

While there are numerous alternatives to password security systems, each involves trade-offs. Among the considerations are the cost to implement, the time required to use, any special considerations regarding place of use (for example, must it be from a particular computer), ability to change the scheme if it is compromised, physical limitations, health considerations (for example, a fingerprint reader on a public site), nontransferability, time stamped, and so on. It is beyond the scope of this article to thoroughly explore each of these alternatives and their limitations. However, the main classes of alternative technology are discussed to demonstrate their potential.

In public-key encryption (PKE) the user is authenticated by the private key used to encrypt a message to the server. While similar to a password, the private key has two features that increase its security. First, the private key is stored on a client computer or smart card and can be of considerable length, thus eliminating the need for the user to memorize the code while also avoiding the possibility of the user generating an easy to guess code. Second, the server verifies the code by correctly decrypting certain information sent by the client rather than comparing to a password file thus eliminating any server-side storage of passwords, encrypted or not. However, a user's private keys must be protected on the client side, thus changing the location of a potential theft.

Public-key infrastructure (PKI) uses PKE to authenticate users across a number of different applications or systems. A PKI can be set up by an organization to be used across its various systems or it can be set up by a third-party vendor to provide authentication services to many vendors. PKI can allow a user to have a single private key that can be used across some or all of the user's needs, simplifying key management for the user. In this situation, loss of the user's private key can make several or all of the user's systems vulnerable in a similar way as when a user chooses the same password to enter for multiple systems. However, in this case, greater emphasis may be placed on making sure the system is difficult to penetrate with responsibility for the key remaining in the hands of the user. Further, a method of centrally revoking a key can be put in place so that a stolen key can be quickly disabled for all systems. Despite some positive attributes, PKI systems are so difficult to use and so poorly implemented, they are usually viewed as ineffective. Indeed, according to one observer, "digital certificates provide no actual security for electronic commerce; it's a complete sham" [10]. Education and improvements in standards and technology may make this approach more effective in the future.

Biometrics involve some form of data obtained about the user's physiology such as scanning an eye, fingertip, or face, or capturing patterns in voices or motions made while signing a document. Again, a biometric can be seen as another form of password, in this case generated by the interaction of a human and a scanning device. While convenient, the digital scan or pattern is vulnerable to network analyzers and, unlike a password, cannot be changed once stolen. This generally limits the use of biometrics to scenarios where the network and biometric capture device are secure.

Smart cards can be used in a number of ways, from simply storing a password to performing complex encryption such as PKE on the card. In fact, a PC can be used as a smart card when electronic purse software is used to store passwords. While the PC itself is vulnerable to network attack, threats to the server side and client side are drastically reduced if a tamper-resistant card employs internal PKE and an algorithm that does

not require the user's private key be transmitted from the card or stored on a server. The private key, which replaces the password, is only used within the card. This technology appears promising if the client-side device remains in friendly hands. Tokens that generate changing codes over time are resistant to network analyzers and, if implemented in a convenient manner, may offer some promise for effective e-commerce security. So too, in the long run, might systems involving trusted intermediaries. As solutions arise, however, so do new problems. For example, if smart card technology were well developed, privacy concerns might increase.

Recommended Courses of Action

While there is no silver bullet solution to the user authentication problem, it is still important to work toward improvements in password usage, security systems, and understanding threats. Improvements to authentication systems can be made by both practitioners and researchers and must be addressed from many points of view. Here is a summary of recommendations for improved practice and further research.

Recommendations for practice:

- Improve password guidelines to include a recommendation to limit the repetition of passwords across sensitive systems.
- Improve audit methods to audit current use of passwords and other identification schemes with emphasis on weaknesses at the user, client, network, and server interfaces.
- Improve security education to train and educate the general public as well as universities, e-commerce merchants, governments, and other organizations. Further, users should be trained in more advanced methods such as biometrics, PKE, and smart cards to be better prepared to use such technology as needed.
- Improve security education for application developers on systems design security issues.

Recommendation for research:

- Conduct research into the practices of security management at multiple levels in the organization including planning, implementation, and maintenance.
- Conduct research into alternative technologies including research that considers the user aspects of its implementation.
- Continue research into what influences user security behavior including policies, education, and incentives.
- Continue research into user password behavior including password reuse behavior and the potential impact of training schemes.
- Conduct research to better understand what security weaknesses are most useful to the hacker and what might be future hacking trends.
- Conduct research into trends in system break-ins. Analyze the extent to which security measures are becoming stronger or weaker over time.

Conclusion

Password security today is the perception of security rather than the reality. Indeed, the Emperor really does have very few clothes. The growth of e-commerce has led to a huge increase in the numbers of passwords required by individual users—very often duplicated over and over throughout the Web. In such an environment, a password, and all the accounts it provides access to, are no more secure than the weakest system using that password. Like dominos, when a weak system falls prey to hackers, information will be revealed that will aid the hackers in infiltrating other systems, potentially leading to the fall of many other systems, including systems with far better security than the first. Until these problems are addressed, there remains a very real threat to the fabric of our increasingly electronic society. C

References

1. Adams, A., and Sasse, M.A. User are not the enemy. *Commun. ACM 42,* 12 (Dec. 1999), 40–46.
2. CERT. CERT Incident Note IN-98.03, Password Cracking Activity. CERT Coordination Center, Carnegie Mellon University, 1998; www.cert.org/incident_notes/IN-98.03.html.
3. Harreld, H. Security: An uneasy alliance. *Infoworld 23*, 13 (Mar. 26, 2001), 42–44.
4. Howard, J.D. An analysis of security incidents on the Internet, 1989-1995. Dissertation, Engineering and Public Policy, Carnegie Mellon University, 1997.
5. Jesdanan, A. Spy case shows public risk: Names, passwords stolen at Kinko's Internet terminals. *South Florida Sun-Sentinel* (July 23, 2003).
6. Kanaley, R. Login error trouble keeping track of all Your sign-ons? Here's a place to keep your electronic keys, but you'd better remember the password. *San Jose Mercury News* (Feb. 4, 2001).
7. Morris, R. and Thompson, K. Password security: A case history. *Commun. ACM 22,* 11 (Nov. 1979), 594–597.
8. Needham, K. Internet banking passwords stolen. *The Sydney Morning Herald* (Mar. 19, 2003).
9. Sasse, M.A., Brostoff, S., and Weirich D. Transforming the "weakest link"—A human/computer interaction approach to usable and effective security. *BT Technology Journal 19*, 3 (July, 2001), 122–131.
10. Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. Wiley, New York, 2000.
11. Security Focus. Netopia 650-T ISDN Router Username/Password Disclosure Vulnerability. bugtraq id 1952, 2000; www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D1952.

Blake Ives (bives@acm.org) is a professor at C.T. Bauer College of Business, University of Houston, TX.
Kenneth R. Walsh (kwalsh@uno.edu) is an associate professor in the College of Business Administration, University of New Orleans, LA.
Helmut Schneider (hschnei@lsu.edu) is a professor at Ourso College of Business Administration, Louisiana State University, Baton Rouge, LA.