

AN EXPLORATORY SURVEY OF PASSWORD RE-USAGE

Ken Walsh, Blake Ives, Tim Louwers and Helmut Schneider

Although there have been recent significant advances in biometric access technology, some form of password-based access control system will always be necessary to secure information systems. Despite their ubiquity, such systems have been found to be vulnerable to both system security breaches and human error. In this paper, we discuss passwords in the context of the limitations of human information processing capacity. While users are estimated to routinely manage 15 password-based applications on a daily basis (Kanaley 2001), they can only be expected to effectively remember four or five passwords at a time (Adams and Sasse 1999). In order to determine the extent of the problem, we conducted a set of four surveys of users with varying levels of technological literacy. Based upon the responses, we conclude that users' most secure accounts are no more secure than those of the most poorly defended applications for which they reuse the same passwords. In other words, the problem of password reuse threatens to compromise our entire system of network security. We close with a discussion of the implications of our findings and some solutions.

Introduction

Although there have been recent significant advances in biometric access technology, password-based security systems remain the primary form of access control. Passwords, defined as “arbitrary strings chosen from a large character space [to] make a penetrator’s task more difficult” (Jobusch and Oldehoeft 1989a, 591), limit unauthorized access to personal computers, personal bank accounts, organization networks and intranets, application programs, subscriber web-sites – the list is endless. This boundless list of password-controlled applications that users face creates vulnerabilities beyond those of choosing an appropriate password. For password security to be effective, passwords must be difficult to guess, easy for the owner to remember, frequently changed, and well protected (Jobusch and Oldehoeft 1989b). The issue is that users must not only remember a unique specific string (at least eight characters in length) of numbers, letters, and symbols, but they must also remember a number of unique strings for each application they access. Unfortunately, human information

Ken Walsh is professor at the University of New Orleans in New Orleans, Louisiana.
 Blake Ives is professor at the University of Houston in Houston, Texas.
 Tim Louwers is professor at James Madison University in Harrisonburg, Virginia.
 Helmut Schneider is professor at Louisiana State University in Baton Rouge, Louisiana.