Authentication Methods for Computer Systems Security

Zippy Erlich
The Open University of Israel, Israel

Moshe Zviran
Tel-Aviv University, Israel

INTRODUCTION

With the rapid growth of networked systems and applications such as e-commerce, the demand for effective computer security is increasing. Most computer systems are protected through a process of user identification and authentication. While identification is usually non-private information provided by users to identify themselves and can be known by system administrators and other system users, authentication provides secret, private user information which can authenticate their identity. There are various authentication approaches and techniques, from passwords to public keys (Smith, 2002).

This article presents the three main authentication approaches, their technology and implementation issues, and the factors to be considered when choosing an authentication method.

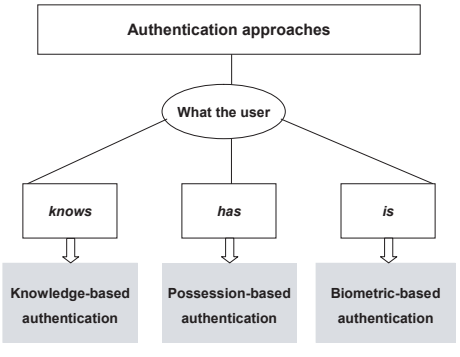
BACKGROUND

Even before computers came along, a variety of distinguishing characteristics were used to authenticate people. Computer systems have applied these characteristics for user authentication. The authentication approaches can be classified into three types according to the distinguishing characteristics they use (Menkus, 1988), as presented in Figure 1:

- What the user *knows*—knowledge-based authentication (e.g., password, PIN, pass code)
- What the user *has*—possession-based authentication (e.g., memory card and smart card tokens)
- What the user *is*—biometric-based authentication: physiological (e.g., fingerprint) or behavioral (e.g., keyboard dynamics) characteristics

As all these authentication types have benefits and drawbacks, trade-offs need to be made among security, ease of use, and ease of administration. Authentication types can be implemented alone or in combination. To strengthen the authentication process, the use of at least two types is recommended. Multiple layers of different types of authentication provide substantially better protection.

Figure 1. Classification of authentication methods



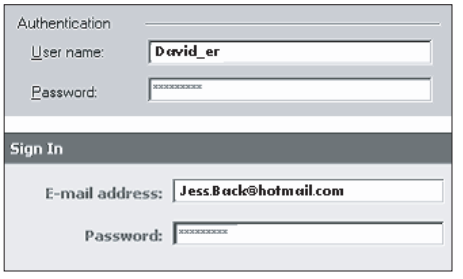
KNOWLEDGE-BASED AUTHENTICATION

The most widely used type of authentication is knowledge-based authentication. Examples of knowledge-based authentication include passwords, pass phrases, or pass sentences (Spector & Ginzberg, 1994), graphical passwords (Thorpe & Van Oorschot, 2004; Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005), pass faces (Brostoff & Sasse, 2000) and personal identification numbers (PINs). To verify and authenticate users over an unsecured public network, such as the Internet, digital certificates and digital signatures are used. They are provided using a public key infrastructure (PKI) which consists of a public and a private cryptographic key pair (Adams & Lloyd, 1999).

The traditional, and by far the most widely used, form of authentication based on user knowledge is the password (Zviran & Haga, 1993). Most computer systems are protected through user identification (like user name or user e-mail address) and a password, as shown in Figure 2.

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 2. Authentication through user identification and password



A password is conceptually simple for both system designers and end users. It consists of a secret series of characters according to some predefined rules. The user ID and password pair acts as user identification and authentication and serves to block unauthorized access to computing resources. In most systems, it can provide effective protection if used correctly.

However, passwords are known to suffer from a number of pitfalls due to human information processing limitations (Sasse, Brostoff, & Weirich, 2001; Yan, Blackwell, Anderson, & Grant, 2005). First, there is a trade-off between memorability and security. Passwords should be difficult to guess and easy to remember. The fact that difficult-to-guess and difficult-to-crack passwords are difficult to remember and that easy to remember passwords are easy to guess and easy to crack poses a dilemma for the generation of passwords. The most secure password is a random string of characters. Such passwords are difficult to guess by others, but at the same time are difficult to remember and thus compel the users to write them down, which impairs their secrecy. Moreover, most users have multiple passwords for different systems and applications, forcing them to remember several passwords. In order to help them to remember the passwords, they usually choose meaningful strings such as names, nicknames, or initials (Adams & Sasse, 1999), which are easy to remember but also easy to crack. They also tend to duplicate their passwords and thus cause the domino effect of password reuse (Ives, Walsh, & Schneider, 2004); namely, all the systems with the same password are no more secure than the weakest system using this password.

In order to improve password security and protect it from dictionary and brute force attacks, password policy should implement rules for choosing and maintaining passwords (Smith, 2002). The major rules are:

- Non-dictionary and no-name passwords.
- Long enough passwords with mixed types of characters.
- Password ageing and not reusing.
- Complex passwords using acronyms, rhymes, and mnemonic phrases, which are difficult to guess and easy to remember (Carstens, McCauley-Bell, Malone, & DeMara, 2004; Yan et al., 2005).
- Passwords should not be shared and should not be written down.
- The number of unsuccessful authentication attempts should be limited by the system.
- Passwords should never be stored in clear text; they should be encrypted or hashed.

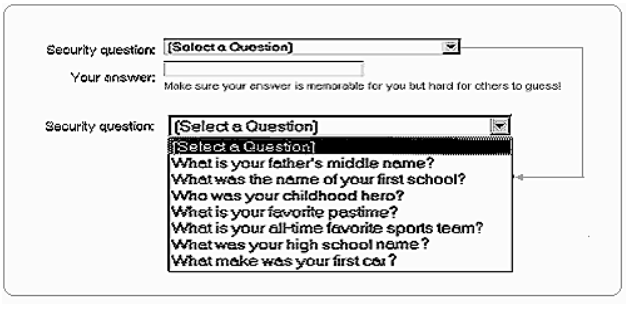
Passwords based on the aforementioned rules are more effective, more difficult to identify and to determine by cracking utilities. To overcome the problem of sniffing passwords when authentication is performed over the Internet, one-time passwords are used. The one-time password can be implemented using smart cards—a kind of possession-based authentication discussed hereafter.

Passwords, used as the first level of authentication, that allow access to information system resources through operating systems are commonly referred to as *primary passwords*. Passwords used as the second level of authentication, for further control and protection of multi-level access to segments of these resources, such as sensitive applications or data files, are commonly referred to as *secondary passwords* (Zviran & Haga, 1993).

In determining primary passwords, the operating system manufacturer uses system-generated passwords or user-generated passwords with predefined rules. User-generated passwords are shown to be easier to remember but less secure than system-generated passwords as they can be easily guessed (Lopez, Oppliger, & Pernul, 2004).

In order to overcome the difficulty of remembering passwords, a *question-and-answer password* method has been suggested (Haga & Zviran, 1991). This method is mainly used for secondary passwords. It involves a dialogue between the user and the system, as shown in Figure 3.

Figure 3. Example of a question-and-answer password



4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/authentication-methods-computer-systems-security/13587

Related Content

Model-Supported Alignment of IS Architecture
Andreas L. Opdahl (2005). *Encyclopedia of Information Science and Technology, First Edition (pp. 2012-2017).*
www.irma-international.org/chapter/model-supported-alignment-architecture/14554

Social Issues in Electronic Commerce: Implications for Policy Makers
Anastasia Papazafeiropoulouand Athanasia Pouloudi (2001). *Information Resources Management Journal (pp. 24-32).*
www.irma-international.org/article/social-issues-electronic-commerce/1190

IT in Improvement of Public Administration
Jerzy Kisielnicki (2002). *Annals of Cases on Information Technology: Volume 4 (pp. 131-140).*
www.irma-international.org/chapter/improvement-public-administration/44503

The Effect of Level of Negotiation Support Systems and Cultural Diversity on Coalition Formation: A Content Analysis
Xiaojia Guo, John Limand Fei Wang (2008). *Information Resources Management Journal (pp. 84-96).*
www.irma-international.org/article/effect-level-negotiation-support-systems/1352

IT Industry Success in Finland and New Zealand
Rebecca Watson (2005). *Encyclopedia of Information Science and Technology, First Edition (pp. 1714-1720).*
www.irma-international.org/chapter/industry-success-finland-new-zealand/14501