Authentication Practices from Passwords to Biometrics

Zippy Erlich
Mathematics and Computer Science Department, The Open University of Israel, Israel

Moshe Zviran
Faculty of Management, Tel Aviv University, Israel

INTRODUCTION

With the rapid growth of mobile devices and networked systems and applications, the demand for effective computer security is increasing. Our security is challenged increasingly by non-traditional threats from adversaries, from hostile regimes and international criminals and terrorists, who use new ways of attack by exploring new technologies and the world's increasing openness (Bosch, 2012). Thus, it is essential to devise security strategies to prevent cyber attacks on critical infrastructures and other essential information systems. 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 to system administrators and other system users, authentication is any protocol or process that permits one entity to establish the identity of another entity. The world of information technology offers a multitude of approaches and techniques, from knowledge-based authentication like passwords to biometrics-based authentication like physical fingerprints or touch screen tapping behavior (Erlich & Zviran, 2009). As mobile devices and smartphones become more widely used, receive regular data transitions from desktop systems and store increasing amounts of sensitive information, the imperative of ensuring their data security has become a major challenge. The ultimate goal for mobile devices is to provide the appropriate level of security and protection in a manner that the user can understand and use (Botha, Furnell, & Clarke, 2009).

This article reviews the three main approaches to user authentication: knowledge-based, possession-based and biometrics-based.

BACKGROUND

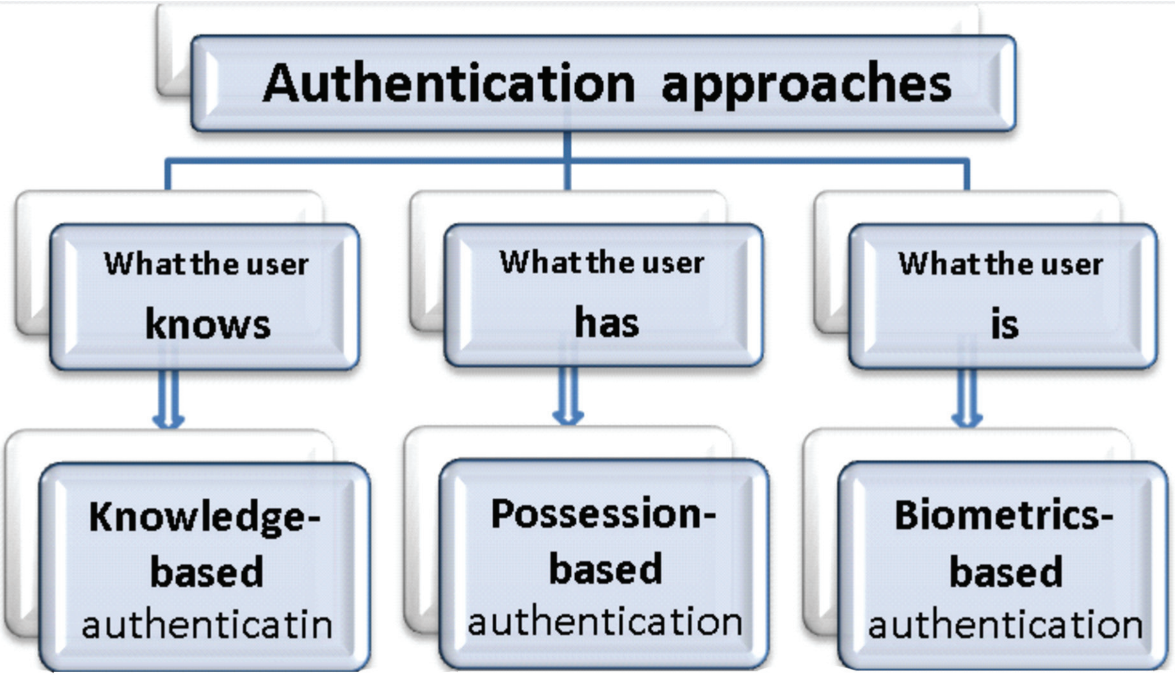
Information security involves blocking attacks and unauthorized malicious access to a system's resources and information (Erlich & Zviran, 2010). As mobile devices and smartphones are becoming widely adopted and affect almost every aspect of modern life, the imperative of ensuring organizational and personal data security has become a major challenge. The main goals of information security are confidentiality, integrity, and availability (Solomon & Chapple, 2005). Confidentiality means the assurance that access to information is granted only to users who have rights to access, integrity means the assurance that the data can be modified only by users that are authorized to modify it, and availability means the assurance that computer resources and information are available to authorized users whenever they are needed.

Access control supports both the confidentiality and the integrity goals of computer and information security. There are three main components of access control: identification, authentication and authorization (Zviran & Erlich, 2006). A user is typically equipped with a unique identifier, such as a user name. The process of authentication is used to verify the user's identity. The two phases of identification and authentication provide reasonable protection against unauthorized access to the computer system.

In choosing an authentication method a number of factors need to be considered: effectiveness, ease of implementation, ease of use and user attitude and acceptance (Furnell, Dowland, Illingworth, & Reynolds, 2000). This article focuses on the various authentication approaches.

DOI: 10.4018/978-1-4666-5888-2.ch417

Figure 1. Classification of authentication methods


Authentication approaches
What the user knows
What the user has
What the user is
Knowledge-based authenticatin
Possession-based authentication
Biometrics-based authentication

The authentication approaches can be classified into three types according to the distinguishing characteristics they use (Menkus, 1988), as presented in Figure 1 (Erlich & Zviran, 2009):

- **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:*** Biometrics-based authentication: physiological (e.g., fingerprints) or behavioral characteristics (e.g., keystroke or tapping dynamics).

As all these authentication types have benefits and drawbacks, tradeoffs need to be made among security, ease of use, and ease of administration. User attitudes are highly positive towards knowledge-based authentication and less positive towards possession-based authentication and biometrics-based authentication (Prabhakar, Pankanti, & Jain, 2003).

Authentication types can be employed 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 (Erlich & Zviran, 2010; Nischal, Gaikwad, Singh, & Devare 2013; Satheesan & Ilayarajaa, 2013).

KNOWLEDGE-BASED AUTHENTICATION

Knowledge-based authentication is the most widely used type of authentication. Examples of knowledge-based authentication include textual strings like passwords, pass-phrases or pass-sentences (Spector & Ginzberg, 1994), graphical passwords (Brostoff & Sasse, 2000; Fulkar, Sawla, Khan, & Solanki, 2012; Thorpe & van Oorschot, 2004; Sriram & Swetha, 2013; Towhidi, Masrom, & Manaf, 2013; Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005) and PINs. The various types of knowledge-based authentication are presented in Figure 2.

The traditional, and by far the most widely used, form of authentication based on user knowledge is the textual password (Erlich & Zviran 2010; Zviran & Haga, 1993). Most computer systems are protected through user identification (like user name or user email address) and a textual password.

Related Content