# Chapter 46
# Music is the Key:
## Using our Enduring Memory for Songs to Help Users Log On

**Marcia Gibson**
*Institute for Research in Applicable Computing, University of Bedfordshire, UK*

**Marc Conrad**
*Institute for Research in Applicable Computing, University of Bedfordshire, UK*

**Karen Renaud**
*University of Glasgow, UK*

**Carsten Maple**
*Institute for Research in Applicable Computing, University of Bedfordshire, UK*

## ABSTRACT

*Devising access control systems to support needs and capabilities of users, as well as the security requirements of organisations, is a key challenge faced in many of today's business environments. If users are to behave securely, they must not be overburdened with unworkable authentication policies and methods. Yet the prevailing alphanumeric password can be a double-edged sword: secure passwords are inherently difficult to recall and vice-versa. Consequentially, a growing number of alternatives are emerging. In this chapter, the authors describe one novel scheme - a musical password. Musipass was designed with the user in mind and is tailored toward the task of authentication on the Web, where biometric and token-based systems have proved unsuccessful in replacing the flawed, yet prevalent traditional password. This chapter, which includes discussion on current thinking in the field of authentication, will be of interest to information managers, security practitioners, and HCI professionals.*

## INTRODUCTION

The most widely employed method of establishing an individual's eligibility to access an online file, site or service is to test their knowledge of a secret key: the familiar alphanumeric password. The level of security passwords offer against brute-force and dictionary attacks theoretically depends upon the degree of informational *entropy* (Shannon, 1948) they contain. However, it is widely acknowledged that passwords constructed of random letters, digits, and special characters are difficult to recall (Yan, Blackwell, Anderson, and Grant, 2004). For this reason, naïvely selected passwords are often derived from meaningful objects (Brostoff and Sasse, 2000), or will contain predictable patterns. These passwords offer reduced entropy, although they assist imprinting (Paivio, 1983) the password to memory.

DOI: 10.4018/978-1-4666-2919-6.ch046

Organizations often impose password construction policies. This seems a fitting strategy given that the rationale for password use is usually to protect assets. However, these policies usually revert a password to its prior arbitrary and unmemorable format. When faced with onerous password policies, users cope by writing passwords down or sharing one password over numerous accounts; therefore a policy intended to enhance security will often weaken it in practice (Inglesant and Sasse, 2010).

These issues become exacerbated on the web. This may emerge from the absence of security cultures which could be fostered in other settings (Johnson and Goetz, 2007), large numbers of sites requiring registration for trivial purposes (Renaud and De Angeli, 2009), user's perceptions of the economic costs involved in adhering to policy as greater than the costs of not following it (Herley, 2009), difficulties in visualizing online threats (Gaw and Felten, 2006) and because many websites are accessed infrequently; whereas the neural pathways through which memories are accessed deteriorate without frequent use (Sapolsky, 2005).

The objective of this chapter is to provide a summarized and updated follow-up to research originally published as (Gibson, Renaud, Conrad and Maple, 2009). We will discuss recent advances in the field of authentication research and in particular detail a novel approach: the *musical* password, which aims to address the weaknesses of the alphanumeric scheme while remaining suitable for inclusion in online environments. A prototype system, "*Musipass*" will be presented and a summary of results from user testing presented. Later in the chapter implementation issues are explored and opportunities for future research identified.

## BACKGROUND

There are two reasons that we forget; either the information no longer exists ("*trace-dependent forgetting"*); or it exists, but cannot be retrieved ("*cue-dependent forgetting"*) (Tulving, 1974). Trace-dependent forgetting happens when an item is not imprinted strongly enough, if the item has not been successfully consolidated or has become corrupted by other memory items ("*interference*"). Cue-dependent forgetting occurs when a retrieval trigger ("*cue"*) is not associated with the item.

It is difficult to generate a cue for a random password and cues cannot be provided to the user during authentication (i.e. it requires *"free-recall"*), as it cannot be ascertained whether the user is a friend or a foe. When John in accounts creates the password "Fluffy" based on his pet's name or writes passwords down, what he is really trying to do is provide himself with a cue as insurance against forgetting. So what happens when John has three pets, Fluffy, Lois and Ruff? In this case interference may be experienced, where John is able to recall numerous passwords, but not the precise one to access the system in question. When an individual reuses a password over numerous accounts he or she is effectually limiting the effort required to generate and memorize the password, as well as the possibility interference will occur.

Passwords must be recalled precisely and entered correctly without feedback (i.e. they are obfuscated to shield against observation). This makes passwords more difficult to enter, especially for users with cognitive, physical or other impairments who often experience usability issues on the web more severely than others (Petrie and Keir, 2007). A wide range of factors can impact an individual's ability to use passwords: Dyslexic users often spell words unpredictably, dyspraxic users experience difficulties sequencing, users may have developmental or language difficulties (Schmidt, Kölbl, Wagner, and Strassmeier, 2004), elderly users often have difficulties retaining newly learned information (Small, Stern, Tang, and Mayeux, 1999) and some have poor reading skills (Schmidt, et al., 2004) or are unfamiliar with the designated alphabet script (Mendori, Kubouchi, Okada and Shimizu, 2002).