Chapter 6
Play That Funky Password!
Recent Advances in Authentication with Music

Marcia Gibson
University of Bedfordshire, UK

Marc Conrad
University of Bedfordshire, UK

Karen Renaud
University of Glasgow, UK

Carsten Maple
University of Warwick, UK

ABSTRACT

Over the last few years, there has been emerging interest in authenticating users through the medium of music. Historically, developers of alternate modality systems have focused on image- and haptic-based techniques, instinctively shying away from music. This might be due to the inherently temporal nature of the listening task and the belief that this would be impractical and frustrating for users. In this chapter, the authors discuss and present new research in this field that, to the contrary, indicates that the "enjoyability factor" means users may be more willing to spend additional time authenticating with music than they would with other techniques. Although undeniably not the optimal solution in time-critical contexts, for many other pursuits music-based authentication could feasibly replace passwords, easing the number of secure strings the average user is expected to remember. Music may also offer a better solution for those suffering memory or cognitive impairments. This chapter incorporates discussion on recent advances in the field of authentication research within the context of a changing threat landscape. A prototype musical password system is presented and a summary of results from online user testing and a lab-based controlled experiment are presented which further reinforce the importance of accounting for "enjoyability" in the assessment of recognition-based authentication schemes.

1. 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

DOI: 10.4018/978-1-4666-7381-6.ch006

(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 in imprinting (Paivio, 1983) the password to memory.

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).

Another emerging issue is that web content is increasingly accessed via smartphones and tablets. Researchers at the Georgia Institute of Technology estimate that by the end of 2014 there will be more mobile devices on the planet than people (GTISC, 2013). Even though many of our online activities require authentication, using a password on these devices can be difficult or inconvenient due to their typically small screens and soft keyboards. Add to this the seemingly upward trend in frequency and scale of online password database breaches (and subsequent leaks) in recent years, and it is clear there is a very real problem where passwords are concerned. On the other hand, most if not all of these mobile devices have *audio* capabilities.

The aim of this chapter is to incorporate discussion on recent advances in the field of sound-based authentication research within the context of the changing threat landscape. We will detail one 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 online, and in a lab-based controlled environment, will be presented. Later in the chapter, implementation issues will be explored and opportunities for future research identified.

2. 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 usually be provided to the user during authentication, 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