Chapter 13
Password Sharing and How to Reduce It

Ana Ferreira
Cintesis, Portugal & University of Kent, UK

Ricardo Correia
Cintesis, Portugal

David W Chadwick
University of Kent, UK

Henrique Santos
University of Minho, Portugal

Rui Gomes
Hospital Prof. Doutor Fernando Fonseca, Portugal

Diogo Reis
Hospital S. Sebastião, Portugal

Luis Antunes
Instituto de Telecomunicações, Portugal

ABSTRACT

Password sharing is a common security problem. Some application domains are more exposed than others and, by dealing with very sensitive information, the healthcare domain is definitely not exempt from this problem. This chapter presents a case study of a cross section of how healthcare professionals actually deal with password authentication in typical real world scenarios. It then compares the professionals' actual practice with what they feel about password sharing and what are the most frequent problems associated with it. Further, this chapter discusses and suggests how to solve or minimize some of these problems using both technological and social cultural mechanisms.

DOI: 10.4018/978-1-61692-895-7.ch013

INTRODUCTION

Health care is an industry sector considered to be exposed to high risks regarding information security. Nevertheless, today's technology and good practices provide a range of controls to mitigate (up to a certain level) most of those risks, especially those related to electronic health records. The biggest risk faced is a lack of understanding of the complex environments that our health services present and ensuring that users understand and comply with local policies. Convergence towards a viable universal solution is not imminent. Therefore trust in e-health is decidedly more fragile as compared with many other industry sectors. This can be explained by the constant challenges in system interconnectivity and an environment of continual changes in legislation (Croll & Croll, 2006).

A hospital is an environment in which sensitive information is the base of clinical decisions, so there is the need for a correct balance between the usability of information technologies and the security of the information (Kurtz, 2003). Hospital Information Systems (HIS) need to tackle security concerns regarding confidentiality (e.g. access control, and secure communications), integrity (e.g. data consistency, error correction, redundancy, and accidental or malicious alterations) and availability (e.g. continuous access to information by authorised users).

Confidentiality, which involves access control and secure communications, has been defined as ensuring that information is accessible only to those authorised to have access (ISO, 2000).

Access control relates specifically to confidentiality, and is a step performed after the identification and authentication of users is finished. Its purpose is to guard access to the patient records in the Information Systems (IS). Access control should start with a clear and succinct definition of an access policy (Blobel, 2000). This may seem easy to achieve, but usually does not exist, either because it can be very complex or simply because no one thought it was necessary to articulate it. In the healthcare environment, processes and people acting upon them may change very often and are, therefore, difficult to track. The primary cause of security breaches is insiders and the consequences in a healthcare environment can be more damaging than in any other organisation. Security should enable and not intrude in the daily workflow; otherwise people will try to bypass it just to do their work more easily. So, it is very important to assess and understand the reality of a working environment in a hospital.

Of the few published studies on the specific issue of password management and security in healthcare systems, a previous survey (Stanton & Stam, 2005) showed that end users do not comply with the regular security procedures that are necessary to keep their user accounts' information safe. This behaviour is closely related to the organization goals, so end users from organizations whose missions depend mainly upon security, behave better in performing security procedures. Nevertheless, training, awareness and knowledge of monitoring can also help in improving users' behaviour. Unfortunately, the downside of this is the fact that end users need to remember their chosen or assigned passwords so they tend to write them somewhere in order not to forget them. Furthermore, all the awareness and training of end users seems to be of little effect when it comes to password sharing behaviours.

This chapter addresses the topic of password sharing as follows. The Background section introduces some concepts related to Electronic Medical Record security. Password Sharing section confronts and analyses case study results of what happens in practice in terms of sharing passwords. It then compares this to what the healthcare professionals say happens and what their opinions and views on these issues are. The next section (Discussion and Recommendations) discusses the results in more detail and presents some recommendations for possible solutions to the problem of password sharing, in terms of both