Chapter 33
Organizational Password Policy

Alex Ozoemelem Obuh
Delta State University, Nigeria

Ihuoma Babatope
Delta State University, Nigeria

ABSTRACT

The purpose of this chapter is to provide an overview of password policy. It specifically identifies some basic elements of password policy, password and password policy life cycles, essence of password policy within an organization, password policy usability considerations, implementation/enforcement of password policies within organizations, the importance of access control in relation to password policy and computer security, and future trends in password policy are set forth. Generally, the absence of a password policy leaves a large void in any organization's ability to operate effectively and maintain business continuity, and allows for ad-hoc decisions to be made by unauthorized personnel.

INTRODUCTION

The ubiquity of passwords is a fact of the present age. Authentication is usually executed by using the combination of a user name and password (Vu, Proctor, Bhargav-Spantzel, Tai, & Cook. 2007). Thus, password is often a major barrier between a potential attacker and a victim's information. Knowing a person's password allows an attacker to impersonate that person in an online setting, or access sensitive data intended only for that person. As society becomes increasingly dependent on passwords for security, it also becomes vulnerable to those passwords becoming compromised.

Previous works have shown that users, when given the option, tend to create simple passwords (Yan, 2001; Summers & Bosworth, 2004; Leyden, 2003). However, simple passwords are especially vulnerable to attackers (Yan, 2001; Vu, Proctor, Bhargav-Spantzel, Tai & Cook. 2007). Therefore, many groups and organizations develop password policies which impose restrictions on the passwords a user may create and how those passwords are used. A well-written policy may increase an organization's security (Polstra, 2005; Summers & Bosworth, 2004; Vu, Proctor, Bhargav-Spantzel,

DOI: 10.4018/978-1-61520-847-0.ch033

Tai & Cook. 2007; Kuo, Romanosky & Cranor, 2006).

A large portion of password policies is usually related to the creation of passwords. For example, a password creation policy may require that passwords be at least six characters long and contain at least one numeric character. There are, however, several other facets in a password lifecycle for which password policies are relevant (Weirich, 2005).

In the design of a password policy, it is crucial that human factors be considered in addition to technical factors. While a password policy may specify the encryption to be used on the password, an overly complex password may be written down on paper by its users because they fail to memorize it (Summers & Bosworth, 2004). Likewise, many password policies specify with whom a user may share passwords, and under what circumstances an administrator is to be contacted. There are many organizations using passwords for security, but no widely-accepted unified context under which all of those password policies may be understood and compared. Such a unified context would enable both the creation of better password policies and a better understanding of password policies (Summers & Bosworth, 2004).

Passwords are the most common authentication for accessing computer systems, files, data, and networks. But are they really secure? According to Wakefield (2004), the SANS Institute indicates that weak or nonexistent passwords are among the top 10 most critical computer vulnerabilities in homes and businesses. A compromised password is an opportunity for someone to explore files and accounts, and even obtain administrative privileges, undetected. Federal regulations mandate the security of confidential client information. The rising threat of litigation is prompting organizations to seriously evaluate computer security measures. Creating impenetrable passwords is a reasonable measure to enhance system security. Security breaches not only put firms at risk of litigation for failing to protect confidential information, they can also lead to financial losses (Wakefield, 2004).

Passwords are commonly used to gain access to websites storing confidential financial information. They often enable users to execute and authenticate commercial and financial transactions. A compromised company password may lead to fraud, illegal activities, unauthorized transactions, or public disclosure of private information. The most common password vulnerabilities include user and administrative accounts with weak or nonexistent passwords and the lack of company policy to adequately protect passwords. Effective measures to reduce network vulnerability and increase security include the implementation of policies that outline important password habits, and proactive verification of password integrity (Polstra, 2005; Summers & Bosworth, 2004; Vu, Proctor, Bhargav-Spantzel, Tai & Cook. 2007; Kuo, Romanosky & Cranor, 2006).

The objectives of this chapter are to: X-ray literature on system security policy dwelling particularly on password policy within organizations; identify the various stages of password policy life cycle, and features, guidelines, policy usability considerations and implementation.

BACKGROUND

A 'password' is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource. The password must be kept secret from those not allowed access (Wikipedia, 2008).

The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword. Sentries would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable television decoders,