Computers & Security (2005) **24**, 546–560

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Query-directed passwords

Lawrence O'Gorman*, Amit Bagga, Jon Bentley

Avaya Labs Research, 233 Mt. Airy Road, Basking Ridge, NJ 07920, USA

Received 30 July 2004; revised 21 April 2005; accepted 16 June 2005

KEYWORDS
User authentication;
Passwords;
Knowledge-based authentication;
Challenge questions;
Password reset;
Password creation;
Call center authentication

Abstract A classical tradeoff in the field of user authentication is between user convenience and system security. Should users authenticate themselves with their mother's maiden name, which is easily recalled but not very secure; or should they memorize a long, random password that is secure but unmemorable? In recent years, tokens and biometrics have been offered as the answer to this convenience-versus-security conflict; however, these require infrastructure modifications.

We introduce query-directed passwords (QDP), an authentication procedure based on questions and answers — where the answers are *known*, not memorized. QDP is particularly convenient for infrequent use, such as monthly or yearly authentication to seldom-accessed accounts. Applications are described that capitalize on advantages of QDP. One of these is an automated password recovery system where testing showed a reduced use of Help Desk personnel for repeated, forgotten passwords from 20% to 2.7%. We discuss other applications, experimental results, and future research directions.

Introduction

User authentication involving queries into personal knowledge has received a bad reputation in the security world — and rightly so. Authentication questions about social security number,[1] mother's maiden name, and date of birth are stereotypes of security by obscurity, and have security as well as privacy shortcomings (US Social Security Administration, 1997). Yet, this type of information is used widely because it is easier for the user to recall than memorized passwords. Passwords are often forgotten, and this is exacerbated by the facts that we are told not to write them down, not to reuse the same password for multiple hosts, to change passwords frequently, and to use increasingly stringent password composition rules (Morris and Thompson, 1979; Riddle et al., 1989; Jobusch and Oldehoeft, 1989; Feldmeier and Karn, 1990; Bunnell et al., 1997; Furnell et al., 2000; Pond et al., 2000; Yan et al., 2000).

* Corresponding author. Avaya Labs Research, 233 Mt. Airy Road, Rm 2A33, Basking Ridge, NJ 07920, USA.
E-mail addresses: logorman@avaya.com (L. O'Gorman), bagga@avaya.com (A. Bagga), jbentley@avaya.com (J. Bentley).

[1] ''Social security number'' is a US term, but will be used here generally to connote any national identification number.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.06.006

Knowledge-based authentication includes passwords and personal knowledge Q&A (questions and answers). It is instructive to compare these two. Whereas the former was designed for authentication, the latter was not. Passwords are secrets shared between two parties for the purpose of proving an authorized user's identity. In contrast, the answers used for personal knowledge authentication are not secret. For instance, you don't invite friends to your birthday party, and then say you can't reveal the date because you use it for authentication. A password can be changed if compromised. You can't change your mother's maiden name. We are instructed to use different passwords for different hosts to eliminate cross-attacks. For personal knowledge Q&A, since the number of questions and answers is traditionally small, what do you do after you've used social security number for Host A, mother's maiden name for Host B, and date of birth for Host C? Finally, the password authentication process does not provide a hint of the password. In contrast, personal knowledge Q&A does provide a hint. This is a convenience for the legitimate user, but offers a standing target for attackers. An attacker needs to only find out that Host X *always* asks for address and date of birth, and then he knows what information must be discovered to successfully attack this account.

Instead of questions relating to personal data (e.g., address, mother's maiden name), some personal knowledge Q&A schemes allow the user to create questions on their own (e.g., what was the name of my first pet?). However, simply ceding the job of Q&A creation to users will not result in uniformly better questions and answers. The general user is not a security expert and it is difficult to measure how ''good'' is a user's question and answer. (This is in contrast to passwords where resistance to attack can be quantitatively estimated (Bishop and Klein, 1995).)

There are alternatives to knowledge-based authentication (O'Gorman, 2003). Tokens and smart cards can create and store strong passwords so there is no need for memorization. However, there is a significant expenditure to provide tokens and readers to all users. Biometrics has some convenient advantages, but suffers the same drawback due to the cost of providing capture devices and has reliability and logistic drawbacks (O'Gorman, 2002; Dorai et al., 2004).

Because of deficiencies with the alternatives, we revisit knowledge-based authentication. As maligned as passwords may be, they do have a number of good properties. Like the biometric, you've always got them (once memorized). Unlike tokens and biometrics, you don't need special readers because computer keyboards and telephone keypads are ubiquitous. Passwords, when used correctly, can have very strong security. The keyspace of a well-chosen password can be as high as that offered by tokens and much higher than the effective keyspace of most biometrics, which succumb to false matches at a rate similar to the guessing rate of a 4- or 5-digit PIN (O'Gorman, 2003).

The work described in this paper falls into the category of knowledge-based authentication, and mainly into the subcategory of personal knowledge Q&A, although there is overlap in the password category. The goal of our work is to obtain stronger security from personal knowledge Q&A, while retaining its inherent convenience. This work is not intended to replace your primary one or two passwords that you may use multiple times a day. Instead, it is most applicable to your many other secondary passwords that you use less frequently, perhaps to your health insurer, financial service, a web service, etc. It can also be used as a backup access mechanism, such as for password recovery or reset, of your primary or secondary passwords.

After describing related background work in the section Background, we describe the QDP framework in the section Query-directed passwords (QDP). This includes how QDP fits into the hierarchy of authentication types, specifications on design of QDP Q&A, and QDP system specifications. In the section QDP in applications, we mention three QDP applications, and more deeply in detail a fourth application, QDP for computer passwords. Section Experiments describes experiments with QDP involving user recall rate, imposter rate, and usage statistics. Finally, we discuss our results and describe some future challenges in the section Discussion and future work.

Background

Attempts to make personal knowledge Q&A stronger are not new. Ellison et al. (2000), proposed a method called *personal entropy*. This is based upon Shamir's secret-sharing scheme, also called a (t,n)-threshold scheme, where a secret is distributed into n shares of which at least t of these are needed to reconstruct the secret (Shamir, 1979). The n shares are encrypted and decrypted using personal knowledge Q&A. Frykholm and Juels (2001) proposed the *error-tolerant password recovery (ETPAR)* method. One portion of the method is similar to the personal entropy method, distributing the answers to personal knowledge questions