KBA: Trustworthy and Usable Authentication

Dr. Michael Just and Dr. David Aspinall
mike.just@ed.ac.uk
http://www.inf.ed.ac.uk/

Authentication with Memorization

Authentication is central to computer security and almost every use of computerised systems. With the explosion of online e-commerce, banking, social web sites and governmental services, the problem of finding secure, usable and efficient authentication systems is more acute than ever. The risks of security failure are obvious, and unusable or inefficient systems additionally risk loss of customers or overly expensive support services managing password recovery.

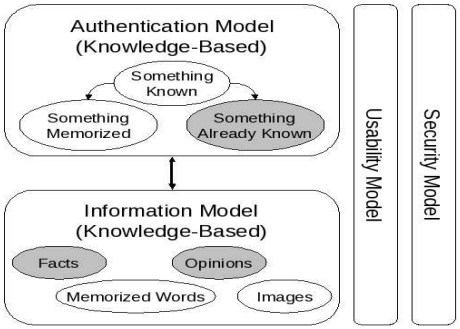
Within this dynamic environment, the mainstay for authentication remains the humble password. Years beyond its prime, passwords continue to control access to most information systems. Yet there is no hiding its failings as they are evident as much to everyday users as to academic researchers. The shortcomings of passwords might be best summarized as follows:*Passwords require 100% correct, unaided recall of a non-meaningful item.* (Prof Angela Sasse, 2003).

So we are left with the forlorn user, scratching their head to either understand the arcane rules for password generation (uppercase, lowercase, numbers, punctuation, don't reuse old passwords!) or to correctly recall one of dozens of passwords previously committed to memory. Inevitably, passwords are forgotten (or even lost, when written down) so that authentication mechanisms not similarly based upon memory are required to allow authentic access.

Authentication *sans* Memorization

While passwords remain the predominant form of Knowledge-Based Authentication (KBA), one can eschew the use of memorized information in favour of information *already known* to users. The most popular implementations use *challenge questions* and *answers*, and can be referred to as *cognitive passwords*. Questions such as *What is your mother's maiden name?* or *What was the name of your first pet?* are commonly used, though aren't necessarily secure or usable. The philosophy behind such forms of authentication is to reduce human processing capabilities during either the generation or recall of authentication information. In this way, the human brain can be leveraged for the knowledge it already contains for the purpose of authenticating, rather than introducing new, non-meaningful information.

Despite the ubiquity of such systems, there is a surprising lack of underpinning published research. Comparative studies, measures of usability and recoverability costs, scientifically justified guidelines for efficient implementation, are all lacking. Our research intends to fill this gap.



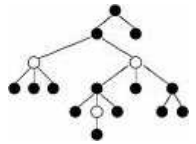
Our work will focus on developing the components in the above figure. An *Information Model* is key to this work, as it will categorize the different types of information that might be used for authentication purposes so that the security and usability can more easily be evaluated. The questions we hope to answer with our research include the following:

- Are current challenge question systems secure?
- Are current challenge question systems usable?
- Can we provide guidance to aid in developing such secure and usable systems?

Trustworthy Authentication

Traditional security analysis of authentication methods will focus on the *entropy* of the credentials used, determining how likely it would be for an attacker to *guess* a password, for example. With cognitive passwords, such as challenge questions, not only can the answers be guessed, but they can also be simply *observed* by an attacker. For example, information that is readily accessible from the Internet is often used.

Our *Security Model* will introduce some formality to the study of cognitive passwords to address these forms of attack by using *Attack Trees* to model the behaviour of an attacker and measure their likelihood for success. The attack trees will be instantiated by the different types of attackers that might guess or observe a cognitive password, including Strangers, Acquaintances, Colleagues, Friends and Family.



Usable Authentication

Usability testing of authentication solutions is relatively recent. Our work will build upon our previously established criteria for challenge questions (see below) in order to build a *Usability Model* for determining the suitability of our candidate solutions for the target communities of users.

Applicability Questions are relevant to the community of interest.

Memorability Users can recall original answers over time.

Repeatability Users can correctly repeat answers over time.

In addition, we're establishing processes to permit realistic and ethical testing of our candidate authentication solutions, qualities that have till now remained elusive to the research community.

Collaboration Opportunities

We're very interested in engaging others in order to test our candidate solutions, as well as discover new methods for authentication.

Validating our Solutions Engagement with organizations to validate our candidate solutions for their security and usability.

New Authentication Methods Engagement with cognitive researchers so as to discover alternatives for authentication information.

School of informatics