

# Applicable Password Authentication and User Acceptance

Gerhard E. Bruckner <gerhard@media.tuwien.ac.at>

June 20th, 2002

## Abstract

Even to date there are several noticeable distinct approaches towards computer security involving several disciplines: computer science, cognitive and occupational psychology. Computer scientists and software engineers focus on designing software enforced password policies and security mechanisms. In the process they often neglect psychological and organisational factors. Psychologists, on the other hand, analyse password memorability, user's password handling procedures, their perception of security, whilst not taking into account the technical demands involved. These groups seem to be adversaries, each camp giving suggestions and making demands which oppose the very goal of the others. Often, users are regarded to as 'weakest link' in the security chain which has constituted the traditional security approach: 'to address the problem by ever more complex technology' [5]. We state, that the most efficient solution is, to incorporate the key ideas of the different approaches to find an applicable trade-off between technical demands and users' (mental) work-load.

**Keywords:** Security, Passwords, Authentication, Security Awareness, Organisation factors, Passphrases

## 1 Introduction

Rapid growth of networked systems and the internet places many every-day tasks into the computer domain. Hence, the need for proper authentication - which is only an enabling task - and the different systems involved (e-mail, network-logon, netbanking, databases, ..) introduce huge demands on users' memory and produce additional work-load.

Considerable resources are spent designing and implementing secure authentication mechanisms, but 'the number of security breaches is still increasing' [1]. The '2002 Computer and Security Survey' [4] highlights this fact and states further, that eighty percent of their respondents acknowledged financial losses due to computer breaches, whereas more than half of the institutions questioned used encrypted logins and reusable passwords.

These results lead to the assumption that knowledge-based authentication is - inspite of aggressively promoted biometric authentication technologies - widely in use, with its de-facto implementation undoubtedly causing heavy problems in security and usability, which appears to have been addressed in contrary ways by the field of computer-science and applied psychology. The level of security

provided by this technique can vary greatly, depending on the individual user's password design experience, security awareness [1], the mental work-load forced onto the user by the security policy and the compatibility with work practices and organisational factors.

In this paper we will give an overview of the demands of both fields and the solutions they provide. Our goal is, to find applicable trade-offs between these contrary demands.

## 2 Technical Demands

In order to prevent unauthorized access, 'strong' passwords are required to withstand different kinds of attacks. When authenticating on a remote system, encrypted protocols are also required to prevent others to pick-up the credentials right from the network. For such a system to function, the (authentication) server must host a user/password database of some kind to verify whether a supplied user-id/password combination is valid or not. This database itself poses another point of weakness: If someone gains access to this database, he or she can launch a brute-force<sup>1</sup> attack against the encrypted passwords using a dictionary-based algorithm. This possibility, however, leads to the demand that passwords should be constructed of a high number of characters and a large character-set and must not contain any words that could be found in a dictionary in order to render these attacks inefficient and thus worthless.

The consequences of exponential improvements in computing power/cost-ratios [2] and development towards faster cryptographic algorithms and more effective (permuted) dictionary attacks lead to the idea of a 'maximally secure password', that 'would be one with maximum entropy: it would consist of a string as long as the system allows, consisting of characters selected from all those allowed by the system, and in a manner that provides no redundancy' [7].

Yet, all these requirements run **contrary to abilities of human memory**. Hence, from the technical point of view a 'good' password should:

- be constructed of a high number of characters: 8 or more as [2] recommend
- be constructed using a large set of characters: all printable or all 128 ASCII characters
- not contain any dictionary words, names etc.

In addition to that, there is often the demand to enforce more restrictive authentication regimes [1]:

- increasing change regimes: e.g. change password one a month
- reduction in allowed input error rates
- (different user-id/password combination for different systems)

There is no empirical evidence that such measures result in more secure user behaviour [1], but it is common belief that more restrictions in authentication mechanisms create more usability problems.

---

<sup>1</sup>Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

## 3 Psychologists' View

[1] states, that usability of security mechanisms has rarely been investigated - just regarding the user als 'weakest link' in the chain of security turns out to be just too simple when taking into account the huge demand on users' memory (e.g. multiple meaningless passwords that change frequently). In many cases, incompatibility between work-practices and security demands leave the employee with conflicting goals, so they often relegate security to second place [1], [5], resulting in undermining the security mechanisms.

### 3.1 Users' Behaviour

For the design of security mechanisms and the security policy of an organisation, the following issues have to be addressed:

- work practices (informal work procedures)
- organisational structure
- user's perceptions of password mechanisms
- user's perceptions of information sensitivity

Security machanisms incompatible with these issues may be circumvented by users and thereby undermine system security overall [1]. The two most common ways to circumvent security are 1) to write down 'difficult' or infrequently used passwords and keep the notes in an insecure place and 2) to construct related passwords in response to restrictive change-regimes or when having to handle a large number of different user-id/password combinations.

### 3.2 Memorability Issues

The very characteristics which make a password more secure (maximum entropy) also make it less memorable [1]. This becomes obvious when we confront the idea of a 'maximally secure password' with well-known properties of human memory; memory for sequences of items is temporally limited, when recalling, these items must be familiar chunks (words, familiar symbols) and human memory thrives on redundancy [7]. This, without fail, constitutes the fact that knowledge-based authentication techniques require some kind of trade-off between usability and security.

[5] points out that memorability is strongly connected to password design. The most important issues regarding passwords are ([5], remarks in brackets by the authors):

- the capacity of working memory is limited (password length, multiple passwords)
- memory decays over time, frequently recalled items are easier to remember (frequency of password use/change regimes)
- recognition of familiar items is easier than unaided recall (character-set)
- people cannot 'forget on demand' (change regimes)
- items that are meaningful are easier to recall (entropy)

## 4 Finding Trade-Offs

In the context of knowledge-based authentication with passwords, we identified the process of **password design** as the key element where improvements can be achieved with reasonable effort. However, without educating users on data and information security, policies, standards and guidelines, all attempts to implement security - even with reasonable usability considerations - will be virtually worthless [3]. So the second key element is communication.

### 4.1 Password Design

A huge number of techniques ranging from optimized machine-generated pseudorandom passwords to composite weak authentication<sup>2</sup> (including cognitive passwords<sup>3</sup>, associative passwords<sup>4</sup> and systems based on recognition of visual items) are currently under discussion, not to mention the field of biometrics. All these techniques still need to be evaluated and implemented into operating systems and applications currently in use. Moreover, most of them are expensive and not suitable for common business and educational environments. It is more than obvious, that users are familiar with the knowledge-based authentication mechanisms (userid/password-combination) in place and that this mechanisms will be commonly in use during the next years.

The question of the trade-off we seek is clearly expressed in the question raised in [5]: 'Can passwords be strong and memorable'. It seems that the answer to this is not an easy one. Password design techniques should be applied somehow adaptive in regard to how frequent a password will be used, the number of passwords, the security demands of the environment and information sensitivity.

### 4.2 Security Awareness

According to [3], a successful security awareness program should comply with the following characteristics (remarks in brackets by the authors):

- educate and inform users, at the very minimum: all employees must fully understand the reasons underlying the security policies, standards and guidelines
- achieve a workable balance between security and productivity (authentication is only an enabling task)
- communicate to individuals the importance and general concepts of security
- bridge cultural divides between the information security team and others (common goal)
- the mindset of the individual must be addressed ([5] regards to this by 'accountability')

---

<sup>2</sup>several weak but memorable items

<sup>3</sup>involve a series of questions about the user's personal preferences and history

<sup>4</sup>employ word pair or phrase association whilst avoiding association stereotypes

- social engineering<sup>5</sup> should be addressed in depth
- physical password protection

[5] states that identity issues, social issues and accountability have to be addressed when designing a security awareness program, which itself should not result in a single meeting or conference but in terms of an 'effective security awareness program' [3] as a definite institution within an organisation.

## 5 Conclusion

With the given password mechanisms implemented in commonly used systems (Unix, Windows) and the users' experience, we can achieve immediate results in password quality by suggesting a password design method which has empirically proven high usability and a reasonable improvement in security. The pass-phrase approach as explained and conducted by [7] produced remarkable results: Passwords were even harder to crack than user-generated random passwords and did not introduce additional overhead. We suggest that passwords designed using this method contain a higher number of characters than conventional numbers and the likelihood of constructing a dictionary word is very low. [7] explains how to construct a password to the subjects of the empirical study:

'A good technique for choosing a password is to use the first letters of a phrase. However, don't pick a phrase like 'An apple a day keeps the doctor away' (Aaadtka). Instead, pick something like 'My dog's first name is Rex' (MdfniR) or (My sister Peg is 24 years old' (MsPi24yo).'

As we pointed out, **password length** may no longer be a serious problem. It is easier to construct long memorable passphrases than meaningless sets of characters. In terms of the technical demand for a large **character-set**, users must additionally be educated to use digits and meta-characters, such as punctuation marks etc. **Multiple passwords** remain an obstacle, but can be managed by constructing related passphrases which result in unrelated passwords. In any case, the resulting password is only **meaningful** to the specific user.

Additionally, users can be guided and supported through the process of password design by the means of a 'proactive password checker' [6]. By doing so, a user constructing a password which is regarded as insecure gets immediate feedback about his or her choice. This includes not only password length or character-set, but dictionary tests and other algorithms. The *cracklib* contained in most linux distributions is a common example for such practices.

To conclude this, we must underline that it is imperative to educate users not only about password design and selection, but on general security issues related to their workplace in order to prevent a lack in security consciousness [3]. The problem of computer security and security in general is a prime example for the human-computer-interaction design approach<sup>6</sup>.

---

<sup>5</sup>relief on lies, bribes, falsehoods to trick people to reveal information

<sup>6</sup>The HCI design approach takes into account that users and technology work together completing a task in order to achieve a goal in a physical and social context [5].

## References

- [1] Anne Adams, Martina Angela Sasse, and Peter Lunt. Making passwords secure and usable. In *Proceedings of the HCI'97 Conference on People and Computers XII*, pages 1–19, 1997.
- [2] David C. Feldmeier and Philip R. Karn. UNIX password security – ten years later. In Giles Brassard, editor, *Advances in Cryptology – CRYPTO ' 89*, volume 435 of *Lecture Notes in Computer Science*, pages 44–63, Santa Barbara, CA, USA, 1990. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany.
- [3] Katherine Ludwig. Security awareness: Preventing a lack in security consciousness. *SANS Institute Reading Room*, May 2001.
- [4] Richard Power. CSI/FBI computer crime and security survey. *Computer Security: Issues & Trends*, VIII, No. 1, 2002.
- [5] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19, July 2001.
- [6] Jianxin Yan. A note on proactive password checking. In *ACM New Security Paradigms Workshop, New Mexico, USA*, September 2001.
- [7] Jianxin Yan, Alan Blackwell, Ross Anderson, and Alsdair Grant. The memorability and security of passwords - some empirical results. Technical Report 500, Computer Laboratory, University of Cambridge, 2000.