Psychological Acceptability Revisited

COMPUTER SCIENCE DEPARTMENT

Usable Security and Privacy

Dr. Abdallah Karakra

Thursday, November 7, 2024

THE PRINCIPLE OF PSYCHOLOGICAL ACCEPTABILITY

"It is essential that the **human interface be designed for ease of use**, so that users routinely and automatically apply **the protection mechanisms correctly**. Also, to the extent that **the user's mental image of his protection goals matches the mechanisms he must use**, **mistakes will be minimized**. If he must translate his image of his protection needs into a radically different specification language, **he will make errors.”**

Jerome Saltzer and Michael Schroeder

PSYCHOLOGICAL ACCEPTABILITY : Detailed Description

- This principle recognizes the **human element** in computer security.
- Applying the principle of psychological acceptability requires taking into account **the abilities**, **knowledge, and mental models of the people** who will use the system.
- The principle of psychological acceptability states that security mechanisms **should not make the resource more difficult to access than if the security mechanisms were not present.**

Example (1) : Passwords

- Passwords are a **mechanism designed to authenticate a user .**
- Password **is a sequence of characters that confirms the user's identity**. If an **attacker guesses the password associated with an identity, the attacker can impersonate the legitimate user with that identity**.

Problems with passwords

- Many passwords were **easy to guess.**
- In the early 1990s, CERT announced that many attackers were using **default administrative passwords to enter systems.**
- In the early 2000s, a CERT advisory reported a **"back door"** account in a database system with a known password.
- Accounts with **no passwords** or with **passwords set by the vendor.**

CERT: Computer Emergency Readiness Team

Problem to solve

How can passwords be made easy to remember, yet difficult to guess?

One difficulty in solving this problem lies in **balancing the ability of a human to remember a password that an attacker will find difficult to guess** against the ingenuity of the attacker.

Not secure:

The users typically picked dictionary words, names, and other common words

Different ideas

Different users have of what constitutes a password that is difficult to guess:

1. When warned not to use names as passwords, one user **changed his password to "Barbara1“, or use Foreign words** .

   - **System administrators, system programmers** usually **understand the need for passwords that are difficult to guess comparing with the users of home systems**, who surf the Web, exchange email, write letters, print cards, and balance budgets, **may or may not understand the need for good passwords**, and almost always underestimate how resourceful attackers can be.

2. Attempts to **educate users to select good passwords**.

Different ideas

3. The proper selection of passwords is a classic **human factors problem** . Assigning **passwords selected at random can be shown to maximize the expected time needed to guess a password**. **But passwords with randomly selected characters are difficult to remember.**

- **Approaches from different companies to solve remembering password problem:**

  Microsoft, Apple, and other vendors, is to supply a **"wallet" or "key ring"** for passwords. **The user enters her passwords, and their associated target**, into the key ring, and chooses **a "master password"** to encipher the ring. Whenever a password is needed, the user supplies the **single master password**, and the system deciphers the appropriate entry in the ring. This allows the user to **save many passwords at the price of remembering only one**.

Different ideas

- **Advantages of the "wallet" or "key ring" approach**
  - This approach tries to **implement the principle of psychological acceptability** by **making passwords as invisible as possible**. The **user needs to remember only one password for all her different systems**. But **an attacker without access to the key ring must discover a different password for each system for that user**. If the **passwords are chosen randomly, and the set of possible passwords is large enough, guessing the chosen password is highly unlikely**.

Different ideas

- **disadvantages of the "wallet" or "key ring" approach**
  - The first lies in the phrase "without access to the key ring." **If the attacker gains that access, she/he needs to guess only the master password to discover all the other passwords**. So, the **problem of password guessing has not been eliminated**; it has been reduced to the user having to select one password that is difficult to guess.
  - The second problem springs from this need. **What happens if the user forgets his/her master password? In most implementations of the key ring, the system cannot recover the master password** (because if the system can do so, an attacker can also). Hence, the user must change all passwords on the key ring, as the originals cannot be recovered either, and select a new master password.

Are the previous approaches satisfying the principle of psychological acceptability?

- This demonstrates **a failure to meet one aspect of the principle of psychological acceptability. If the security mechanism depends upon a human, what happens if the human fails?** Logic dictates that this should never happen, and if it does, it is the **human's problem**. But logic must account for the frailties of human beings, and the principle of psychological acceptability speaks to human failure. How do you recover?

How to make the previous approaches satisfying the principle of psychological acceptability?

- Another approach is to **base authentication on criteria in addition to a password**, such as possession of **a smart card or a biometrics measurement.** In principle, **if a password is discovered, the attacker cannot immediately gain access to the protected system.** Again, the principle of psychological acceptability comes into play; **the additional requirement must be acceptable**. Swiping an identification card, or entering a number displayed on a token, might be acceptable.