G00124970
A. Allan

Research Note
6 December 2004

Passwords Are Near the Breaking Point

Mitigating authentication weaknesses by increasing password length and complexity will reduce security if passwords are pushed beyond the peak of their effectiveness. They are approaching this point now.

Core Topic
Security and Privacy: Security Administration

Key Issue
How will identity and access management evolve as an enterprise infrastructure?

Strategic Planning Assumption
By 2007, 80 percent of organizations will reach the password breaking point and will need to strengthen user authentication with alternative security methods (0.8 probability).

Passwords are a ubiquitous authentication method, despite many well-known vulnerabilities (see "Best Practices for Managing Passwords: Overview"). Password management was seldom a major issue in the desktop/tower PC world because an attacker needed physical access to the desktop PC, which wasn't easy to get. Thus, over-the-network attacks against vulnerabilities were the path of least resistance. However, it is much easier for attackers to gain physical access to laptops and personal digital assistants (PDAs) because these devices are portable and thus often lost or stolen.

Although stronger authentication becomes more important as the use of laptops and PDAs increases, most organizations are responding by making simple passwords longer and more complex. This also makes passwords more difficult to remember. Even with simple passwords, many users write down their passwords even when corporate security policies say they shouldn't, which reduces the security that passwords offer. Increasing the length and complexity of passwords will drive so many users to write down their passwords that it will yield a net *reduction* in security — the password breaking point.

Best Practices for Password Strength

Our recommendations for password length, as defined in "Best Practices for Managing Passwords: Formation," are:

- A password of eight or more characters is strongly recommended. A password of six or more characters is the minimum acceptable length.
- Sensitive systems or situations (for example, remote access) demand longer passwords — approximately twice as long as for nonsensitive systems.

Length is one of two criteria for password strength — the other is *complexity*. Our best practices provide seven rules for complexity, with the fundamental aim that a password should be as unlike a word, phrase, date or other string with semantic content as possible. Our password guidelines recommend that users construct passwords from the first letter of each word of a favorite song, poem, quotation or other source, and substitute numbers and other characters. Similarly, the United States Computer Emergency Response Team's Cyber Security Tip ST04-002 (11 February 2004) recommends that users "develop a mnemonic for remembering complex passwords" — for example, the phrase "I like to play basketball" could yield the password "iltpbb" or (better) "il!tpbb." An alternative approach is to use a very long but less-complex password, such as a "passphrase" (see Note 1).

Completely random passwords offer the most complexity. However, a password must be memorable to be useful, and many users would have difficulty remembering a random six-character password, nevermind a dozen or so that they may need to use. (A number of tools simplify password management for users; see "Take Care With Password Management Tools to Achieve Security" and "Enterprise Single Sign-On Tools Are Comprehensive but Costly.")

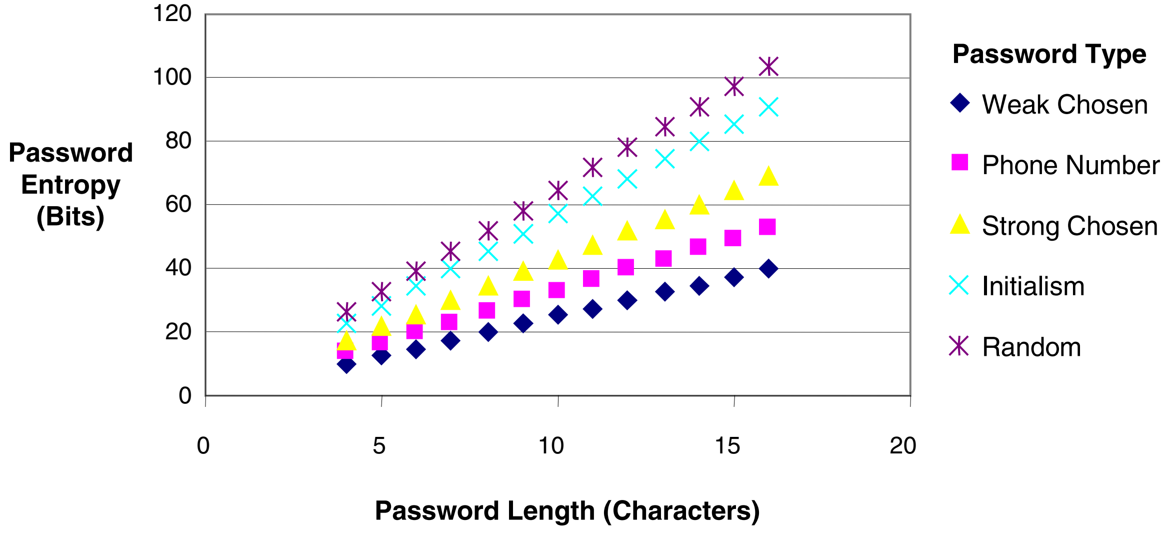
Note 1
Passphrases
The security of weak chosen passwords is low but persistent. Very-long chosen text — that is, a "passphrase" — may offer more security than a shorter complex password. However, the security of passphrases may be reduced by an increased susceptibility to shoulder-surfing attacks (and social engineering attacks), because passphrases take longer to type and may be more easily guessed by an attacker who sees only part of the phrase. Another barrier to the broad use of passphrases is the lack of support for long passwords. Although Windows operating systems, from Windows 2000 onward, support a maximum password length of 127 characters, many systems have much lower limits (for example, eight in z/OS RACF).

Entropy as a Measurement of Password Strength

The strength of a password that follows from length and complexity can be measured by its *entropy*. The easiest way to express entropy is in terms of the number of bits of complexity that the password has. For example, a random password that is 8 bytes in length (with 8 bits per byte) would have 8 x 8 = 64 bits of entropy — typically, 2^{63} passwords must be tried before the password could be cracked. However, it is difficult to achieve 8 bits of entropy per character because keyboards restrict the number of characters that users can easily enter, and users have difficulty remembering passwords that don't have a structure.

Figure 1 plots *password entropy* against *password length* for "weak chosen" (2.5 bits of entropy per character), "strong chosen" (4.3 bits) and "random" (6.5 bits) passwords. It also shows estimates for passwords that follow our good password guidelines — that is, "initialisms." Because initialisms are not formed from English words, the entropy reduction due to patterning is greatly reduced, although initialisms are not truly random. The entropy per character is probably between 5 bits and 6 bits. (An analysis of a possible source of such initialisms — an English edition of Leo Tolstoy's "War and Peace" — yields 5.7 bits to 5.9 bits.) For comparison, Figure 1 also includes telephone numbers with an entropy of $\log_2(10) = 3.3$ bits per character.

Figure 1
Password Entropy vs. Password Length



Source: Gartner Research (December 2004)

"Treat Passwords as Ineffective on PCs" states that standard recommendations for password strength of between six and eight characters may no longer be sufficient for secure systems. Our "one month to crack," 46-bits-of-entropy target could be met by a password that follows our best-practice recommendations.

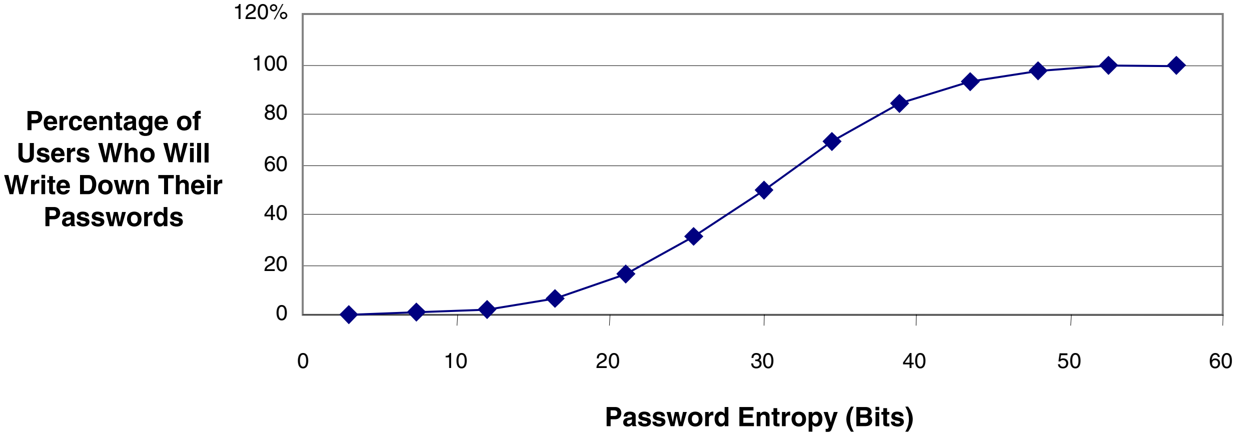
Entropy and Memorability

Higher entropy makes a password more difficult for a user to memorize. Therefore, you can't make passwords arbitrarily strong, even if your software allows it, because at some point you will get diminishing security return. We believe that this breaking point is only a little beyond current best practices.

The more difficult that a password is to remember, the greater the likelihood that a user will write it down — even when prohibited by an organization's information security policy. We hope that the egregious use of sticky notes on PC monitors is a vanishing practice, but other common hiding places, such as under mouse mats or tissue boxes, don't offer much additional protection. The majority of financially damaging security breaches are the result of insider attacks. Thus, writing down a password that could be obtained by an unscrupulous colleague is dangerous.

Figure 2 plots the *percentage of users who will write down their passwords* against *password entropy*. This is speculative, is based on anecdotal evidence and assumes a normal (Gaussian) distribution. Informal surveys tend to show that about a third of users write down passwords that follow "common practice" password rules — six characters, with some format restrictions, for 6 x 4.3 ~ 25 bits of entropy. A distribution with a mean of 30 and a standard deviation of 9 seems to be a reasonable, although simplified, assumption. Some users will be able to remember long, complex passwords or will be less likely to "misbehave" than others. Thus, there may be a more-attenuated distribution for high password entropy, perhaps following a Maxwell-Boltzmann distribution. For this research, we made the simplified assumption.

Figure 2
Users Who Write Down Their Passwords vs. Password Entropy

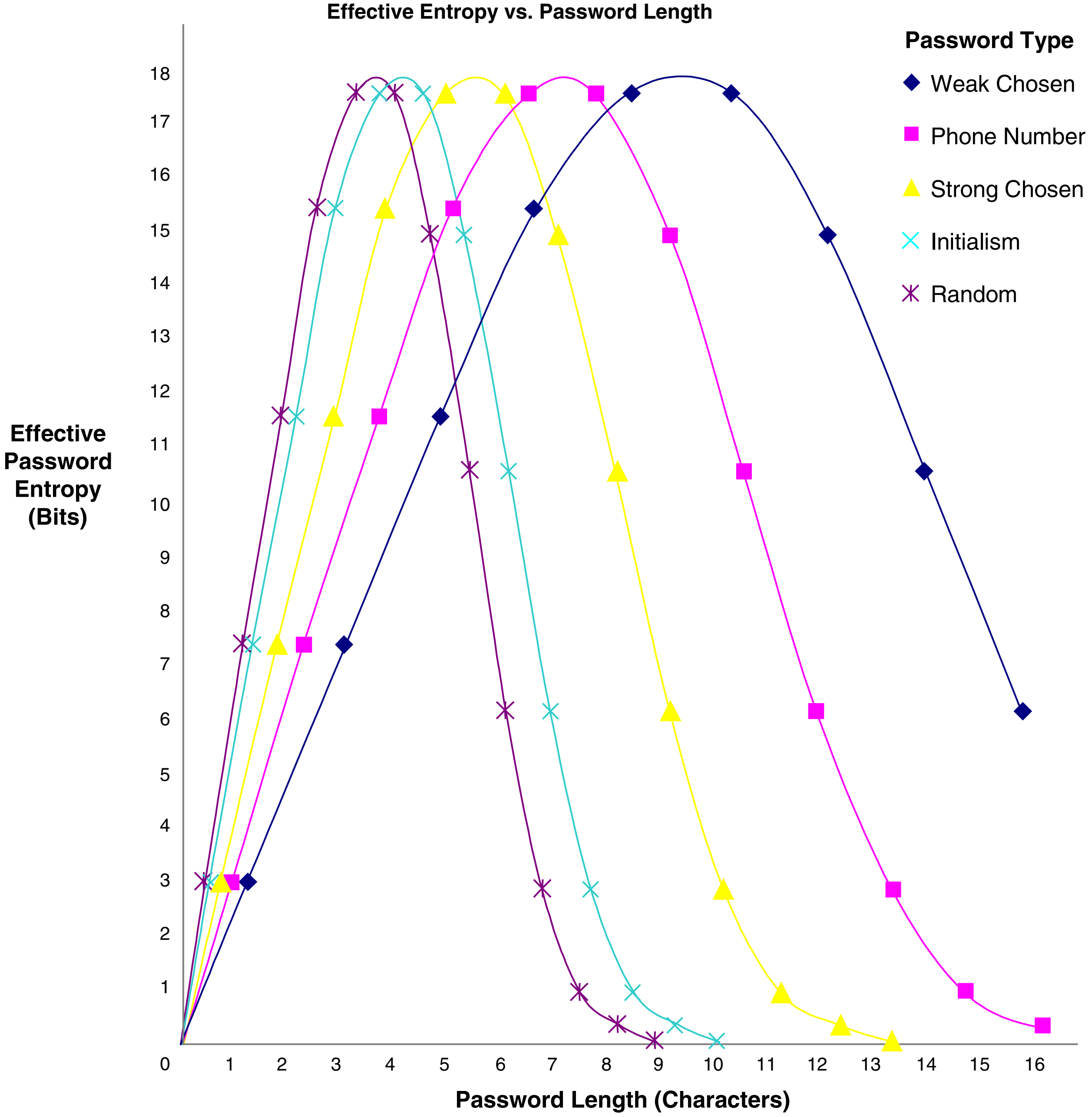


Source: Gartner Research (December 2004)

Difficult-to-Remember Passwords Are Less Secure

What is the impact on security if users write down their passwords? Figure 3 plots *effective entropy* — a measure of the true security afforded by passwords across many users in an organization — against *password length*. Effective entropy is calculated based on the fact that a password that is written down has zero entropy. This is another simplified assumption, because although an effectively hidden password will have an entropy that is higher than zero, most users choose easy-to-guess hiding places. Thus, the entropy of a password collapses to a close-to-zero value when it is written down. The percentage of users who write down a password is equal to the percentage reduction in entropy.

Figure 3
Effective Entropy vs. Password Length



Source: Gartner Research (December 2004)

Based on our assumed normal distribution, the maximum effective entropy of all types of passwords is about 18 bits. The number of characters required to reach maximum effective entropy for each password type is:

- Random — three to four
- Initialism — four
- Strong chosen — five to six
- Weak chosen — 10

If our assumptions are correct, then most organizations should have reached the breaking point of passwords. (Using a more-realistic Maxwell-Boltzmann distribution would have little impact on the maxima, although the distribution would be stretched out to the right of the peak.) However, this result doesn't fit with the apparent effectiveness of passwords. Perhaps we were too pessimistic in our simplified assumptions and, in fact, *less than a third* of users will write down their passwords, and users are *twice* as tolerant of password complexity. Using these revised assumptions, we can "smear out" the distribution in Figure 2 with a mean of 60 — that is, for a password entropy of 60 bits, half of users will write down their passwords — and a standard deviation of 19. The maximum effective entropy would then be about 35 bits, and the number of characters required to reach maximum effective entropy would be:

- Random — seven
- Initialism — eight to nine
- Strong chosen — 10 to 11
- Weak chosen — 18

Even with these more-optimistic assumptions, organizations that implement best-practice recommendations for password formation (eight-character initialisms) are close to the password breaking point.

The quantitative results may be inexact, but the qualitative result is sound: You can only push passwords so far. Best-practice password-formation recommendations appear to be approaching the limit. If you push passwords further, they will break and result in negative security return.

Bottom Line: Increasing password length and complexity can yield an increase in security, but it places additional burden on users. The breaking point is near, if not already reached. For stronger authentication, consider using stronger authentication methods, rather than increasing the length and complexity of passwords.