

Passwords 2.0¹

Norman Fraser PhD
Chief Executive Officer
Tricerion Group Plc

As in most areas of life, IT security has its fair share of cherished beliefs that happen to be wrong. One of the most pernicious of these is the myth that conventional passwords are good for securing network-accessible data or services. They're not, and this realization is now spreading. But when it comes to the vulnerability of passwords, a little knowledge can be a dangerous thing; some common 'password-strengthening' measures can actually reduce password security in online applications.

A password is only secure for as long as it remains secret. Once compromised it is worthless. There are two ways for a password to be compromised: it can be guessed or it can be disclosed. Let's consider password guessing and disclosure in turn.

Password guessing

It's not hard to design an unguessable password. Randomly select a sequence of 1,000 characters and, voila, you now have a password which is, for all practical purposes, unguessable. Unfortunately, you also have a password which is unusable. In the real world of conventional passwords, security and usability tend to conflict. In general, the higher the security, the lower the usability; the better the usability the worse the security.

Where users are allowed to choose their own passwords with complete freedom, they tend to favour usability over security, as a number of studies have shown. In one of these dating from 1990,² the average password length was 6.4 characters, and 24% of passwords could be guessed using a dictionary of only 63,000 words. More recently this data was re-analysed and with more advanced techniques 42% of the passwords were found to be readily crackable. A 1992 study yielded a data set in which 20% of passwords were guessable, and the average password length was 6.8 characters.³ In a 2006 study the average password length was found to be 6.8 characters, and using a commercially available password recovery toolkit 23% of the passwords were cracked in 30 minutes and 55% in eight hours.⁴ These studies demonstrated what hackers have long known – that users tend to behave like other users, including in their password choices. In a 2006 sample, collected from a phishing attack on MySpace.com, 0.34% of users used the name part of their email address as their password, 0.22% used password1, while abc123 and myspace1 were used 0.11% each. Individually these may look like small numbers, but put them together in a larger 'top 100' of popular password choices, and they become a gift to password crackers.

A common industry reaction is to protect users from their own unsafe choices by imposing structural constraints on what constitutes a valid password. For example, a corporate policy may decree that a password must be at least eight characters long, and must contain a mixture of alphabetic and numeric characters. This policy rules out most easily guessable passwords based on knowledge of the user, e.g. names of partners, children, pets, significant dates of birth, etc, but it also brings other guessable possibilities to the fore, e.g. home address (23eaststreet), or cultural preferences (starwars2). Enriching the password well-formedness constraints can further squeeze out meaningful and therefore guessable possibilities. For example, prohibiting passwords with clusters of digits at the beginning or end of alphabetic sequences helps reduce guessability.



Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldy, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Imposing minimum length and complexity constraints can be fairly effective in blocking dictionary attacks, so password guessing becomes a game of numbers. To crack a password it becomes necessary to iterate through all possible sequences allowed by the symbol set and policy constraints until the correct one is found. This is like clicking through every setting of a combination lock until it springs open. Short passwords composed from small character sets define a smaller search space than longer passwords composed from larger character sets, so they are theoretically more vulnerable. For example, the search space for a four-digit numeric PIN consists of 10,000 (10⁴) possibilities, whereas for a case-sensitive eight-character alphanumeric password it is 218,340 billion (628).

In the IT security business large numbers are comforting, so the arithmetic appears to drive us towards imposing longer, more complex passwords. But given that increasing the security of a password tends to diminish its usability, we need to ask: how secure does a password need to be, and how secure can it be before it starts to become unusable?

In an important paper published in 1959, the psychologist George Miller summarized evidence that most people can remember about seven chunks of information in working memory.⁵ Subsequent investigation has established that the number of chunks is actually closer to four.⁶ Thus, in order to remember longer strings of characters it is necessary to break them into a maximum of around four chunks. This is why we tend to segment telephone numbers into three or four clusters. But as passwords get longer, consisting of arbitrary sequences of characters with few mnemonic 'hooks', so it becomes harder to analyze them into memorable structures. Unfortunately, unguessable passwords also tend to be unmemorable and therefore unusable.

How many symbols long does a password really need to be to deliver acceptable security? Most of us already trust access to our personal bank accounts to an ATM password that is only four digits long, i.e. to a search space of only 10,000. This is an acceptable level of security in this case because:

1. Physical possession of the ATM card (or a clone) is required before an attempt to crack the password can begin.
2. The maximum loss exposure if the password is cracked is low, tending to be capped by the account's withdrawal limit.
3. Most ATM accounts disable the card after about three failed attempts.

Given the capped loss exposure, most people are willing to accept a 1 in 3,333 (i.e. 3/10,000) risk that the password for a stolen card will be guessed correctly before the card is disabled. So if four-digit passwords are judged good enough for ATM transactions, how complex do passwords need to be for card-not-present Internet banking transactions, where the loss exposure is potentially much higher?

Password disclosure

Once we move beyond passwords that are trivially vulnerable to dictionary attacks (like password1), increasing the complexity of Internet passwords in sensibly engineered applications adds little to security and can actually cause a significant reduction in security.

The longer and more arbitrarily structured a password is, the less memorable it will tend to be. The less memorable the password, the more likely the user is to write it down. Indeed, some industry figures are even rejecting the conventional

wisdom that passwords should never be written down, and are now advocating precisely this. For example, Microsoft's Jesper Johansson has observed that the security industry has been giving out the wrong advice about passwords for 20 years: "I claim that password policy should say you should write down your password. I have 68 different passwords. If I am not allowed to write any of them down, guess what I am going to do? I am going to use the same password on every one of them".⁷

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Johansson is correct that only the rarest of savants is capable of the superhuman feats required to remember all the 'strong' passwords the average user has to manage. But he is also straying into perilous territory. A shelf-full of research shows that the majority of identity thefts begin with the theft of personal information by people close to the victim – family, friends and colleagues. For example, it has been claimed that up to 70 percent of identity theft occurs within companies.⁸ When Richard Smith explored a number of workplaces to see what he could find, his results were alarming:

Coincidentally, mouse pads are shaped like miniature doormats. Just as some people hide house keys under doormats, some hide passwords under mouse pads. [I] occasionally perform "mouse pad surveys" at companies using computer systems. The surveys look under mouse pads and superficially among other papers near workstations for written passwords.⁹

Smith's desktop surveys discovered ill-concealed passwords in up to 9% of workstations in companies that placed no requirement on users to change their passwords periodically. But amongst the companies Smith surveyed that force regular password changes, he discovered poorly hidden passwords at between 16% and 39% of workstations. (The widespread belief that forcing regular password change increases security turns out to be another of those plausible-but-false IT security myths.)

Increasing the length, complexity, and frequency of change of passwords may increase the arithmetic security of passwords, but these measures dramatically increase the probability that real users will compromise their own password secrecy. Any password policy that drives more than a third of users to disclose their passwords within easy reach of their office PCs is clearly still operating in the realm of idealized myth rather than hard-nosed reality.

Increasing the length, complexity, and frequency of change of passwords may increase the arithmetic security of passwords, but these measures dramatically increase the probability that real users will compromise their own password secrecy. Any password policy that drives more than a third of users to disclose their passwords within easy reach of their office PCs is clearly still operating in the realm of idealized myth rather than hard-nosed reality.

It is not just memory problems that cause users to disclose their passwords. The last few years have seen a dramatic rise in the number and ingenuity of Internet "phishing" attacks. One variety of phishing operates by luring Internet users to a fake copy of a real online service, such as an online bank. Users enter their login credentials in good faith, but in so doing they disclose their credentials to fraudsters who will gladly use them for criminal purposes. Academic studies have shown that "some visual deception attacks can fool even the most sophisticated users."¹⁰

One response to this kind of 'social engineering' phishing, is to deploy mutual authentication. One of the things that makes phishing possible is that in traditional logins users are required to authenticate themselves to the online service but the service is not required to authenticate itself to the user. The simplest variety of mutual authentication requires the user to store some personal information, such as a phrase or picture. When the service presents the user with a password entry screen it should display the user's pre-stored information (retrieved on the basis of the user's username) to prove that it is the authentic login site, and not some lookalike imposter. The rule for users to follow is simple: if you don't see your prestored site authentication data then don't enter your password – it's probably a phishing site. The weakness with this approach is that it attempts to combat a confidence trick by asking users to be careful, but good confidence tricks work precisely by deploying whatever means are required to make targets feel they are being careful, even as they are being scammed with eyes wide open. The first independent academic study of what can be called weak mutual authentication has shown that as many as 92% of users proceed to type in their passwords, even when the pre-stored site authentication data are not displayed.¹¹

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Another variety of phishing has emerged more recently, in which a keystroke-logging virus infects a PC, where it quietly monitors user keyboard input until login credentials are typed. These are captured on input and immediately despatched over the Internet to the originating criminals, who can use them to access the user's account. A similar threat comes from keyloggers, which are tiny physical devices that can be discretely plugged into the back of user PCs, where they capture every keystroke for subsequent harvesting. In early 2007 a six year old child managed to plug a keylogger into the PC of Anne Milton, MP, when she left her computer unattended for 60 seconds inside the British Parliament building.¹²

The landscape of Internet password security has changed beyond recognition. In the age of phishing, old security certainties about what makes a password secure no longer apply. The greatest threat is no longer related to password guessability, but to password disclosure. A twelve-character alphanumeric password is no safer than a four digit numeric PIN to a wellconstructed phishing attack. In a world where users are freely able to disclose their own credentials, increasing the theoretical, arithmetic security of a password actually increases the likelihood that the user will disclose it. The simplest conceivable phishing attack involves a fraudster sending a victim an email requesting username and password by return. Bizarre as it may seem, a small percentage of users will reply sending their confidential details straight back. This vulnerability will continue for as long as we continue to base online authentication on conventional passwords.

We hear a great deal these days about Internet 2.0, the second wave of Internet technologies that moves from the primary focus of Internet 1.0 on information to much greater focus on value transactions. Conventional passwords have served us fairly well in the Internet 1.0 era, but with a changing threat landscape, and a growing requirement for secure transactional authentication, the time has surely come to start planning for a new generation in password authentication, Passwords 2.0.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Passwords 2.0

The Passwords 2.0 revolution has already begun. A range of one-time and multi-factor password offerings has been available for a while, making positive contributions to improved authentication security. While much of the progress has been laudable, today's leading Passwords 2.0 contenders still address only specialized niches rather than the problem in general. For example, PKI solutions offer impressive levels of security based on an authentication exchange involving public and private digital certificates under the supervision of an independent trusted authority. In practice the technical challenges of understanding, implementing and maintaining PKI solutions have meant that successful deployments are more or less confined to well-supported corporate environments. PKI, for all its security muscle, lacks a key component of the success of Passwords 1.0: simplicity.

Part of the security strength of PKI is that it hides a vital component of the identity credentials - the digital certificate - from the ordinary user, who may not even realize that it exists. This makes it difficult for users to disclose their authentication credentials inappropriately. One-time password tokens share the same property. In this approach, the user carries a small electronic key-fob which generates a fresh password every 60 seconds. The one-time password generator is synchronized with the online application, so that the user can gain access to the application only by entering the currently valid password during its short window of validity. Unwary users cannot definitively compromise their credentials because they don't know what their password will be in a minute's time, let alone in the general case.

Password tokens have found popularity with some online banking and enterprise network providers, but they are not without their problems. The initial capital cost of tokens is high, they are subject to a significant level of loss, they are battery-powered, so need to be replaced every three or four years, and it is necessary to have the token in one's possession on every occasion of login. Most devastating is that this is a solution that will not scale. The Microsoft executive quoted above

claimed to have 68 login accounts, so to secure these with one-time password tokens would require 68 separate physical devices, leading to what is sometimes called the 'cargo pants problem'.

Tricerion Group has developed a completely different and innovative approach to Passwords 2.0. Tricerion's SafeLogin™ solution is implemented as a piece of server-side software; installing it alongside the application web server in the serviceprovider's data centre makes it potentially available to all users, with no certificates to install, hardware devices to carry, or client-side software to be installed on user PCs. It is a rare example of what is sometimes called a 'zero footprint' solution, i.e. it is deployed solely through the user's existing browser, with no further setup required.

Tricerion SafeLogin replaces conventional alphanumeric passwords with picture passwords like the one shown in Figure 1 below:



Figure 1: Picture password

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Cald, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

People who have never seen picture passwords before nonetheless immediately know how to use them, since their function and purpose are obvious by analogy with conventional passwords. At login time users type in their username, and are then presented with a password entry keypad, like the one shown in Figure 2:



Figure 2: Password entry keypad

The pictures that make up the password should be clicked in sequence on the keypad, followed by 'Submit'. This is an example of that rarest of artifacts - the self-documenting interface. Users who have received no training intuitively know how to proceed, and can enter their picture password almost as fast the first time they encounter this login method as they can after becoming experienced users.

The password entry keypad seen by any given user is personalized in two important respects. First, the look-and-feel of the keypad background is selected by the user at set-up time, and may be reset subsequently at will. For a minority of users this personalized look-and-feel will provide important reassurance that the login site is genuine and not a faked phishing site. If these users see a keypad look and feel other than the one they have previously selected they will immediately terminate the login process without disclosing their password. For the majority of users, though, the look-and-feel personalization will be no more than a pleasing design feature.

The second variety of personalization in the keypad is much more important from a security standpoint. Any given user will always see the same set of keys on their keypad, though the key positions will be shuffled on each presentation. Thus the set of keys User A sees will contain all the keys necessary for User A to enter their password, plus some 'padding' keys to bring the total up to the number of key positions in the keypad (in this case 12). User A will always see these same 12 keys on every login occasion, though their positions will be shuffled on each presentation. User B may see a partially, or completely, different set of keys on each login occasion.

This login method can be used from any Internet access device that supports a browser, it requires no special equipment to be carried by the user, and it is no harder to use than a conventional password. In fact, it is somewhat more user-friendly than conventional passwords due to a fact discovered by experimental psychologists almost 50 years ago.¹³ People tend to remember information presented visually more reliably than information presented textually or verbally. The truth of this finding, known as the picture superiority effect, is already familiar to anyone who knows they have previously met the person in front of them, but cannot recall their name. A part of the brain specialized in perception recalls previously seen visual items; a completely different part of the brain remembers verbal or textual information. Visual perception is much more efficient and reliable than non-visual memory, so Tricerion SafeLogin passwords provide a real help to users struggling with the problem of too many passwords to remember.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldy, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Suppose a user has 68 different login accounts. The user enters their username for one of these accounts and immediately sees their own personal password-entry keypad for that account. Prior to starting the login procedure the user may not have had any recollection of their password, but as soon as they see the collection of keypad images which they only see for this account, they receive strong visual cues which prompt recall of the appropriate password for this service. This is rather like the person who says, "I couldn't give you directions for how to get there but I could take you there." Our brains devolve some of the burden of visual recall out into the world - when we see enough visual cues in the world this triggers recall of the rest. So when I see the visual specifics of the password entry keypad for my 46th login account, it triggers painless recall of the appropriate password associated with that account.

This works particularly well when the user consciously constructs a mnemonic story around the picture password. One such story for the password shown in Figure 1 might be, "I drove to the coffee shop; it was raining as I got out of my car and I got soaked by a passing truck." Once such a mnemonic story has been constructed it is very difficult not to remember it on subsequent presentation of the relevant keypad.

Shuffling of the key positions does not appear to impact the effectiveness of recall, so long as the number of keys in the keypad does not exceed about 16. Key shuffling adds important security elements, helping to protect against shouldersurfers (password thieves who watch over user's shoulders as they enter credentials) and against certain kinds of Trojan virus. When a key symbol is clicked what gets returned over the Internet is not the value shown on the key but rather the coordinates of the key location that was clicked on this one-time keypad. This means that the password never exists in digital form outside the service provider's firewall; only inside the firewall are the clicked coordinates resolved into password values.

How guessable are picture passwords? This is harder to answer than in the alphanumeric case. In general, the probability of correctly guessing a password of length L from an available alphabet of N symbols is 1 in N^L . However, in the case of Tricerion SafeLogin, the set of all available symbols will be unknown to the criminal attempting to guess the password. Unlike in conventional passwords where the number of available symbols is limited to those that are easily typeable on a QWERTY keyboard, the Tricerion SafeLogin symbol set is open-ended, and may be very large indeed. In the abstract, the chances of guessing a password of seven symbols from a 1,000 symbol set of available symbols is 1 in 1000^7 , which is 1 followed by 21 zeros, i.e. a very large number indeed.

In reality this is a meaningless figure, since Tricerion SafeLogin passwords cannot be guessed in the abstract - they can only be entered via a specific, personal password entry keypad. If we assume that the user's username has been compromised such that the criminal has access to the user's password entry keypad, the chances of the criminal being able to guess a seven-symbol password from a twelve-key keypad are 1 in 35.8 million.

Tricerion SafeLogin passwords are realistically unguessable, even when the appropriate personalized keypad has been compromised. However, as we have seen, it is not the guessability of passwords so much as their disclosability that determines their effective level of security in today's threat landscape. Tricerion passwords provide excellent resilience to disclosure attacks, since users find it exceptionally difficult to reveal their secret passwords in the absence of their own personalized login keypad.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Consider the challenge faced by a phishing attacker trying to obtain the login credentials of a user protected by Tricerion SafeLogin. Suppose a user has the password shown in Figure 1. How will a criminal go about phishing this? They could try luring the user to a fake login site, but this fake site must provide the user with a means of entering their password. The password capture method used by almost all phishing fake sites today is to ask the user to type their password into an input form. However, this user's Tricerion picture password cannot readily be typed, since there is not a match between typeable characters and Tricerion pictures. Instead, the criminal could try presenting a randomly generated speculative password entry keypad, such as the one shown in Figure 3.



Figure 3: A faked password entry keypad

The user being phished ought to notice that this keypad has a very different look-and-feel from the one they usually see (i.e. the one shown in Figure 2). Even if the user fails to notice this and tries to proceed with password entry, they will fail at the very first symbol, since this is missing from the fake keypad shown in Figure 3. Indeed, one of the problems a phishing attacker faces is that they don't even know how many symbols are available in the password 'language', far less which ones are relevant to any given user.

Suppose for the sake of this example, the password 'language' consists of 1,000 pictures. Leaving aside the difficulty a phisher would face in discovering this, the chances of a phishing attacker's randomly generated twelve-key password entry keypad containing all four symbols necessary for a user to disclose the password shown in Figure 1 would be infinitesimally small, and for a realistic seven symbol password it would be orders of magnitude smaller again. In the general case, if:

m = the total number of symbols in the password 'language'

n = the number of keys shown on the keypad

q = the number of symbols in the password

p = the probability that a randomly generated keypad will contain a particular password then:

$$p = \frac{(m-q)!n!}{(n-q)!m!}$$

Under realistic conditions the chances of a user being able to enter their password on a phishing attacker's randomly generated password entry keypad are vanishingly small.

Since phishing by keypad guessing is impractical, how about other social engineering means? The phishing attacker could request that the user describes their password in some way. The simplest and most obvious way to do this is by reference to keypad position (e.g. "the first symbol is in the top left of the keypad") but of course this will be meaningless due to the shuffling of key positions on each presentation.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Alternatively, the user could offer a short verbal description of the password symbols. For example, the password in Figure 1 could be described as “car, cup, cloud, truck”. This is not as useful as it might at first appear, since there are 18 different sequences that correspond to this description in the keypad shown in Figure 2, only one of which is correct. If the account locks after three failed login attempts it remains unlikely that the phishing attacker will be able to access the account, even after the user has attempted to disclose the password. (Note that there are also 10 possible “car, cup, cloud, truck” sequences in the phishing keypad shown in Figure 3, none of them correct.)

The user might try writing a more detailed description of the symbols, e.g. “the first symbol is a blue car, with round headlamps, facing head-on towards you...”. However, in the unlikely event that the user can be persuaded to go to all this trouble to disclose their password, it can be argued that this is willful, not accidental disclosure, which has implications for who pays in the event of loss.

A further benefit of Tricerion SafeLogin is that it is immune to most Trojan virus attacks, which steal login credentials by capturing keystrokes and sending them back to the criminals. With picture passwords there are no keystrokes to capture, and any more sophisticated image capture Trojans (of which few have been recorded) will require human processing of data to extract useable results. Since phishing is a numbers game, anything that significantly decreases the automatability of attacks increases the likelihood that sites with this protection in place will be left alone in favour of easier targets.

While Tricerion SafeLogin offers industry-leading authentication security, it also opens up the possibility of enriching the user’s experience of the service provider’s brand during login. For example, Figure 4 shows how a vintage car company could add its distinctive branding to its login experience.



Figure 4: A vintage car company password entry keypad

Figure 5 illustrates how an online video game company might brand its logins.



Figure 5: An online video game password entry keypad

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldy, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

Migrating users from conventional alphanumeric passwords to Tricerion SafeLogin picture passwords can be managed in easy steps so as to retain user support and maintain smooth operations. Perhaps the simplest approach is a two-step process in which users are first upgraded to keypad entry of their existing alphanumeric password, using a personalized alphanumeric password entry keypad like the ones shown in Figures 6 and 7 (where the look-and-feel and key set are personalized to the user).



Figure 6: An alphanumeric password entry keypad



Figure 7: Another alphanumeric password entry keypad

Once the users have grown accustomed to entering passwords by clicking on a personalized keypad, in a second step the passwords can be upgraded to picture sequences, with the concomitant change to picture keys on the keypad, but the general keypad look-and-feels previously selected can be retained. This effectively reduces the scale of each change step to manageable proportions, and increases the users' sense of continuity as they migrate from lower to higher security.

Conclusion

In today's threat landscape, organizations that implement Password 1.0 security and rely on old IT security orthodoxies to protect their user authentication are leaving themselves exposed to serious risk of compromise. A new generation of Password 2.0 solutions is required to meet this threat. One of the first of these, Tricerion SafeLogin with picture passwords, effectively kills social engineering and Trojan phishing attacks, whilst increasing the memorability of passwords and decreasing the possibility that users can inappropriately disclose their passwords through written, typed or spoken means. These benefits can be easily deployed from the server side, require no special user training, and do not negatively impact usability. On the contrary, they offer service providers with a new tool for brand reinforcement during the user login process.

Password security used to be all about making passwords unguessable; now they also need to be undisclosable in order to be secure against the latest attacks. Tricerion SafeLogin provides unparalleled protection on both fronts with minimal implementational or operational overhead and a highly cost-effective pricing model.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Cald, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com

References

- 1 An abbreviated version of this paper appeared in Financial Sector Technology, May/June 2007, p.59.
- 2 Klein, Daniel V. (1990) Foiling the Cracker; a Survey of, and Improvements to Unix Password Security, Proceedings of the United Kingdom Unix User's Group, London, July.
- 3 Spafford, Eugene H. (1992) Observations on reusable password choices. Proceedings of the 3rd Security Symposium. Usenix, September.
- 4 Schneier, Bruce (2006) MySpace Passwords Aren't So Dumb. Wired, December 14.
- 5 Miller, George A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.
- 6 Cowan, Nelson (2001). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. Behavioral and Brain Sciences, 24, 87-185
- 7 Kotadia, Munir (2005) Microsoft security guru: Jot down your passwords. CNET News.com, May 23.
- 8 Collins, Judith (2005) Identity Theft: Now It's Your Problem. Microsoft.com.
- 9 Smith, Richard E. (2002) Authentication: From Passwords to Public Keys, Addison-Wesley.
- 10 Dhamija, Rachna, J.D. Tygar & Marti Hearst (2006) Why phishing works. Proceedings of the Conference on Human Factors in Computing Systems (CHI2006).
- 11 Schechter, Stuart E., Rachna Dhamija, Andy Ozment & Ian Fischer (2007) The emperor's new security indicators: an evaluation of website authentication and the effect of role playing on usability studies. IEEE Symposium on Security and Privacy, Oakland, May.
- 12 www.bbc.co.uk/pressoffice/pressreleases/stories/2007/03_march/23/keylogger.shtml
- 13 Shepard, RN (1967) Recognition memory for words, sentences and pictures. Journal of Verbal Learning and Verbal Behavior 5: 201-204.

Castleforce IT Consultancy Ltd

Registered Office: The Summit, Thorsway, Caldby, Wirral, CH48 2JJ Tel: 0151 2031400

Sales Office: Enterprise Centre, University of Reading, L33 London Road Campus, London Road, Reading Berkshire, RG1 5AQ Tel: 0118 9071600

Company Registration No: 5935861 VAT No. 899948123

Email: info@castleforce.com Web: www.castleforce.com