Tricerion SafeLogin™ for Web

Product description

Tricerion's innovative SafeLogin product provides strong mutual authentication for accessing services such as online banking, e-commerce, ASP services, online communities, VPN, VoIP, and any other network-accessible service that requires user authentication.

Tricerion's approach to online authentication complements existing offerings and works well as part of a multi-layer solution. It enhances both actual and perceived security, without impairing user experience.

Tricerion's SafeLogin is a robust server solution, for installation inside the service provider's firewall alongside online application servers. Only modest adjustments to existing systems are required during installation, and no sensitive user data is ever transmitted from the application server to the SafeLogin server.

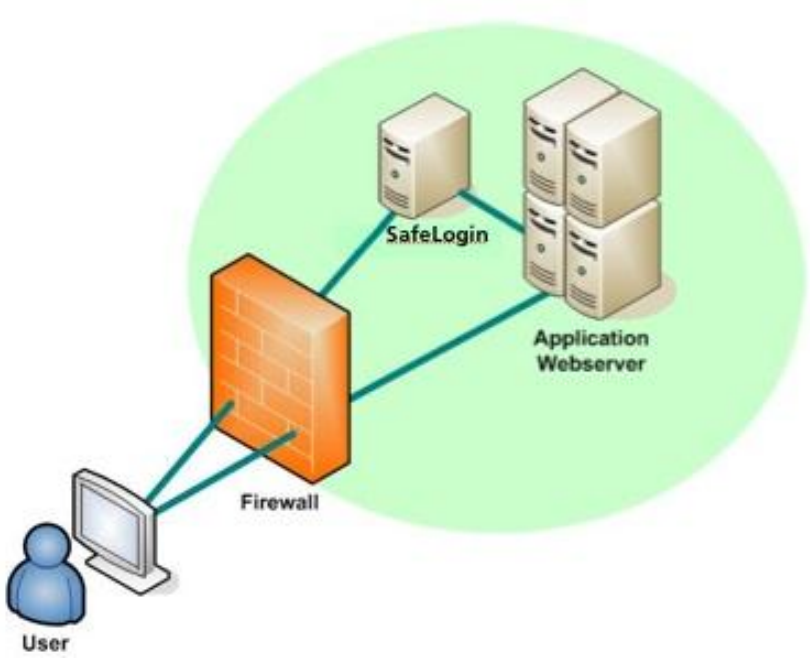

Figure 1: Tricerion SafeLogin server installation

SafeLogin enhances security by means of proprietary, patented *anti-phishing* and *transaction security* systems. Key innovations are SafeLogin's *Keypad Personalisation* and *Triangulation* technologies.

Tricerion Limited Science and Technology Centre, University of Reading, Earley Gate, Whiteknights Rd, Reading RG6 6BZ, UK
T +44 20 3286 5723
sales@tricerion.com www.tricerion.com

Keypad Personalisation

Reported instances of phishing attacks on banks, retailers, and other online service providers rose from almost none at the start of 2004 to over 37,000 different phishing sites by the end of 2006. This growing menace relies on a bogus email or letter being sent to a target population, requesting them to visit a fake website to be lured into unwitting disclosure of their authentication details to the phishing fraudsters.

Tricerion's Keypad Personalisation makes it significantly more difficult for phishers to deceive online users or for users to disclose their details inadvertently.

Keypad Personalization requires a two-step login. In outline, the procedure works as follows:

1. The user is prompted for their account name.
2. The account name gets passed to the SafeLogin server, along with a request for a keypad to be generated for this user and instance.
3. In the Tricerion approach to authentication security, PINs or passwords are always entered by means of a keypad, in which the key positions are shuffled for each occasion of use. Thus, instead of being offered the keypad in Figure 2, the user may see the example shown in Figure 3.

   This kind of one-time keypad is easy and intuitive to use without instruction. Direct entry of the PIN by typing is disabled, so the keypad must be used. When the user clicks keys on the keypad, what gets returned is not the selected values but the clicked co-ordinates relative to this one-time image. In order to use an intercepted click sequence maliciously it would be necessary to be in possession of the one-time image to which it relates, and to process a combination of digital and analogue information.

Tricerion Limited Science and Technology Centre, University of Reading, Earley Gate, Whiteknights Rd, Reading RG6 6BZ, UK
T +44 20 3286 5723
sales@tricerion.com www.tricerion.com

Figure 2: Conventional keypad

Figure 3: Tricerion one-time keypad
with randomized key positions

4. The 'plain vanilla' keypads shown in Figures 2 and 3 are for illustrative purposes only. When the web service requests a one-time keypad from SafeLogin, SafeLogin looks up the account name and retrieves personalization data for that user. This data is used to set keypad appearance properties. Permutation of these properties yields many distinct keypad 'look-and-feels'. Personalization values are fixed for each user, so users will become used to their own keypad look-and-feel.

   Since phishing attackers do not have access to each user's distinct keypad look-and-feel, the best they can offer in a fake phishing site is a typing input interface or a plain vanilla keypad. In either case an unfamiliar input mechanism should alert users that something is wrong.

5. The Personalized Keypad approach starts to come into its own when users are issued with alphanumeric passwords. These are drawn from the set of a-z and 0-9 characters, (special characters may also be added). Thus a user's password could be 'Y3JK'. (Passwords of arbitrary length are supported). One of the stored personalization parameters defines the user's individual symbol inventory. This is the subset of alphanumeric symbols for presentation on this user's keypad, consisting of the user's password symbols, plus a selection of other 'padding' symbols. Thus a user whose password is Y3JK could be presented with a keypad as shown in Figure 4.

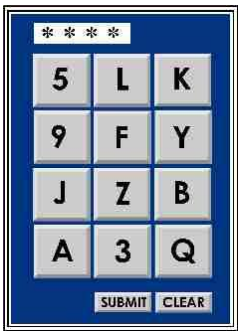

Figure 4: Personal keypad including individual look-and-feel and symbol set

The personal symbol set, like the general keypad look-and-feel, is constant for each user (though the symbol positions are shuffled on each presentation). Not only does this make it obvious to the user when they are being targeted in a mass phishing attack, it also renders it impossible for most users to enter their password via a generic phishing keypad. The chances of all the characters of a four-character password being present in a randomly generated 12-character keypad drawn from the (case-insensitive) 36 available alphanumeric characters is only 1 in 119. Even if the user doesn't spot that they are being spoofed, they will not be able to enter their password via a keypad, because the necessary characters will not be present.

6. Of course the user could still disclose their password to a phishing site by typing it into an input form or by writing it directly into a reply email. SafeLogin's approach supports a refinement to prevent even this kind of reckless self-disclosure. To support this highest level of security users are issued with passwords consisting of sequences of pictures, such as those shown in Figure 5.

Figure 5: Picture password

7. Picture passwords have much to recommend them. Experimental psychology has demonstrated that it is easier to memorise picture sequences involving shape, colour and meaningful concepts, than arbitrary text strings. Password administration procedures need not be significantly altered from present practice, e.g. new passwords can be printed and mailed to users, and users can reset their own passwords by selecting from a palette of available images. If images rather than alphanumerics are used, a user keypad might look like the example shown in Figure 6.

Figure 6: Personal keypad, using picture symbols

The chances of a user being able to enter their details via a speculative phishing keypad, such as the one shown in Figure 7, are extremely small. Even though the fraudster may, by sheer luck, generate a spoofed keypad having some pictures in common with the user's (for example, Figures 6 and 7 have some symbols in common), the chances of stumbling upon a viable personal keypad are vanishingly small and, in any case, will only work for one user (Figures 6 and 7 have different background colours and borders, and Figure 7 does not contain all the necessary password symbols). Once the progression is made from alphanumeric to picture passwords, there is no reason why the set of available symbols should not be very large. For example, there are 6.1 x 10^{28} possible 12 key keypads from a set of 256 available symbols, and the chances of a randomly generated keypad containing all the symbols for just a four-symbol picture password is only 1 in 353,116.

Figure 7: A phishing keypad

8. The SafeLogin picture keypad system effectively eliminates the possibility of conventional social engineering and keylogger Trojan attacks, but determined phishing attackers may attempt to subvert it by other means, e.g. man-in-the-middle attacks. To block such exploits SafeLogin includes an advanced set of active counter-measures to identify and disable attempted attacks.

Triangulation

The SafeLogin authentication solution is built on a proprietary transaction protocol we call *'triangulation'*. Unprecedented levels of security are achieved by graduating from conventional *dialogue* between the user and the online service to *trialogue* between the user, the online service, and the SafeLogin system (see Figure 1). Even if a malicious hacker were to intercept and decrypt one of the communication channels they would still not be able to make use of the information collected.

SafeLogin brings impressive levels of strong mutual authentication security to online transactions, in a way that is visible to the user without complicating usability. It does not require special user training, or additional enrolment. SafeLogin has been designed to be as easy to integrate into live online environments as possible; typically an initial installation into a live online service environment can be achieved in days rather than weeks or months.

Tricerion Limited Science and Technology Centre, University of Reading, Earley Gate, Whiteknights Rd, Reading RG6 6BZ, UK
T +44 20 3286 5723
sales@tricerion.com www.tricerion.com