



## Account Hijacking Prevention With the Tricerion Strong Mutual Authentication (SMA) Server

### The Problem

Identity theft, in its broadest sense, cost US businesses and consumers almost \$50 billion in 2003.<sup>1</sup> "Account hijacking," through means such as phishing, shoulder surfing and keystroke logging, represents one of the fastest growing categories of identity theft.<sup>2</sup> Even though the problem of account hijacking is relatively small as a percentage of the total direct losses associated with identity theft, according to the Federal Deposit Insurance Corporation (the "FDIC"),

"[I]t is nonetheless serious for customers (both retail and commercial) and for financial institutions. The increasing access to alternative electronic payment systems means an increasing number of access points to financial institution systems, with each access point representing a pathway for a potential security breach. The increasing number of access points, coupled with the potential for anonymity afforded by electronic payment systems, facilitates electronic banking fraud. Yet customers expect financial institutions to ensure the safety and security of their financial transactions however those transactions are effectuated. Public confidence in the financial system is predicated on this type of trust."<sup>3</sup>

Gartner estimates the total direct costs of account hijacking in the US to be approximately \$1.2 billion. These direct costs, which may be underreported, primarily represent the out-of-pocket costs to financial institutions of reimbursing those customers who are the victims of phishing fraud. Today most banks fully reimburse all victims who report the fraud within 60 days. Worse than the direct costs, however, banking experts familiar with the problem fear that the pervasiveness and growth of these scams will stunt the growth of online banking and e-commerce, significantly limiting the economic potential of the Internet and fundamentally altering the e-commerce strategies of financial institutions. Many industry representatives and security experts believe that the indirect financial losses and public relations damage associated with publicity surrounding these scams may far outweigh the industry's direct financial losses.

In light of these facts, a cost-effective solution to the problem of account hijacking is fast becoming a first-order priority for most financial institutions and e-commerce merchants, as well as the bank regulatory community.

---

<sup>1</sup> *Putting an end to Account-Hijacking Identity Theft*, Federal Deposit Insurance Corporation, Division of Supervision and Consumer Protection, Technology Supervision Branch (December 14, 2004) (hereafter referred to as the "FDIC Report") at page 2.

<sup>2</sup> These terms are defined in the Glossary that follows this document. It is estimated that as of April 2004, approximately 4.5 million US Internet users had experienced unauthorized transfers from their checking accounts.

<sup>3</sup> FDIC Report, p. 6.

**Copyright © Tricerion Inc. 2005**

Tricerion, Inc., 2855 L'ville-Suwanee Rd, Suite 760-323, Suwanee, GA 30024, USA

Tricerion Ltd, Clarke House, 65 High Street, Egham TW20 9EY, UK

contact@tricerion.com ♦ www.tricerion.com

## Existing Solutions and their Limitations

Existing authentication and authorization solutions fall into three categories of credentialing:

1. The user's access is credentialed based on what the user knows – like a user name and password combination;
2. The user's access is credentialed based on what the user has – like a physical device, known as a “token,” that the user must somehow connect (either physically or through other electronic means, such as by entering a randomly generated password) to the computer in connection with the authentication routine; and
3. The user's access is credentialed based on what the user is – i.e., so-called biometric authentication based on the user's fingerprints, facial features or voiceprint.

Password-based systems are convenient, easy-to-implement and, at this juncture given their pervasiveness, cost almost nothing to deploy. Unfortunately, experts generally believe that password-based systems do not provide sufficient protection to users because they are vulnerable to a host of scams such as phishing, shoulder surfing and keystroke logging.

At the other end of the spectrum, token-oriented credentialing is quite secure in that it represents a so-called “two-factor” approach to authentication that requires the fraudster to both obtain the token and steal the password in order to compromise the user's account. But providing tokens to millions of online banking users is expensive. Moreover, tokens can be left behind, misplaced, forgotten and lost, with the net effect of reducing the utility and ubiquity of Internet banking and e-commerce if the token isn't readily at hand (and also, in many cases, requiring its replacement). Also, if tokens become pervasively used, the user's Internet experience is likely to be diminished as he finds himself forced to carry (and keep track of) multiple tokens to facilitate access to services supplied by different providers. Thus, notwithstanding the perceived security of two-factor, token-based systems, those systems have not been ubiquitously deployed, nor does it appear that they are likely to be broadly adopted in the near future because of the expense and user inconvenience of such a system.

Counter intuitively (given all of the publicity surrounding the future of biometrics), biometric authorization may represent the worst of all worlds. In most instances, in order for biometric credentialing to be viable, significant modifications need to be made to the user's computer system. Thus, this system suffers from the same economic objections associated with two-factor systems. Moreover, while a person's fingerprint may appear to be a relatively “safe” form of authentication, what happens if a hacker manages to secure a digital image of the user's prints? How does the user “change his password” to limit his risk in the future? For these and a host of other reasons, biometric credentialing is not widely deployed.

## The ultimate authentication system

The ultimate authentication system should, then, meet several important objectives:

First, it should provide real security to online banking and e-commerce users, rather than the mere appearance or veneer of security that existing password and pin systems provide today.



Second, it should be easy and relatively inexpensive to implement. Importantly, a system that is both truly secure and that avoids the expense of a “second factor” device would have a great deal of value.

Third, the ultimate account hijacking solution should effectively shift the risk of mis-authentication back from the financial institution to the consumer. For example, when an e-commerce transaction is effected today without the user’s signature or the presence of the credit card, it can be extremely difficult for the merchant to establish that the card user in this transaction was also the legitimate cardholder. Consequently, banks and merchants bear a disproportionate share of the costs of online fraud, and are looking to shift a portion of this risk back to the users.

Fourth, it should reduce the number of valid or potentially valid transactions that merchants deny because they do not have an adequate means of connecting the identity of the card user to that of the cardholder in online transactions. As it stands today, merchants deny an economically meaningful number of “card not present” transactions (and thereby forego revenue) because they cannot sufficiently connect the identity of the card user to that of the cardholder.

For these reasons, it is increasingly important that a system be brought to the marketplace that effectively, efficiently and securely provides for the authentication of e-commerce and online banking transactions, with a reasonable roll-out and ongoing price ticket.

### **The Tricerion SMA System**

A new entrant in the field, Tricerion, has developed an elegantly simple, yet highly effective, proprietary, server-based solution. The system relies on a number of innovations, in particular, Triangulation and Keypad Personalization, to prevent account hijacking from occurring in phishing, shoulder surfing, keystroke logging and screen capture scams and to increase the security and reliability of e-commerce transactions. Tricerion has filed patents on these innovations.

Tricerion’s online security innovations are embodied in a server, known as the ‘SMA’ or Secure Mutual Authentication server. The SMA is a robust, three-tiered server solution which is installed inside the financial institution’s firewall. This creates “triangulation” among the user’s computer, the bank’s online system and the SMA server. See Figure 1 below.



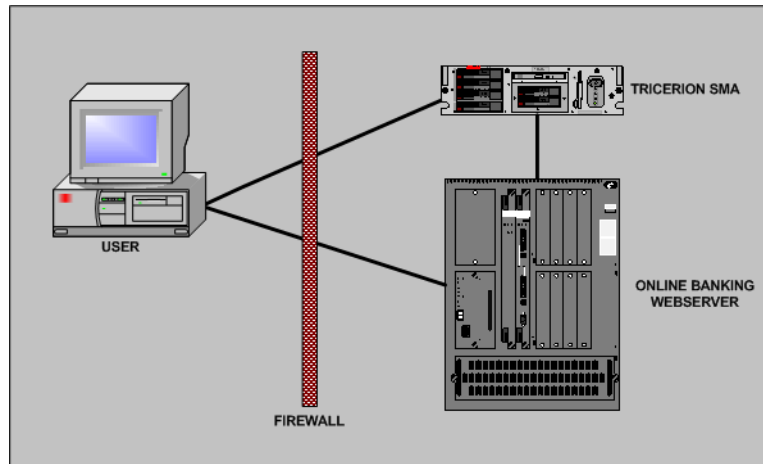


Figure 1: SMA system installation

The SMA's security enhancements rest on three key innovations: *triangulation*, *keypad personalization*, and *active countermeasures*.

**Triangulation.** The Tricerion SMA system is built on a proprietary communications protocol we call Triangulation. Unprecedented levels of security in online transactions are achieved by moving from a conventional *dialogue* between the user and the institution's authentication server into a *trialogue* among the user, the institution's authentication server and the Tricerion SMA server. Even if a fraudster or hacker intercepts transmissions between two of the three points in the triangulated solution, they will still not be able to make sense of the information collected.

In a conventional online banking system, the user indicates their desire to login, and the system responds by prompting for an account name and PIN or password. The only protection against malicious interception of this highly sensitive information is provided by SSL encryption of the data, as in Figure 2.

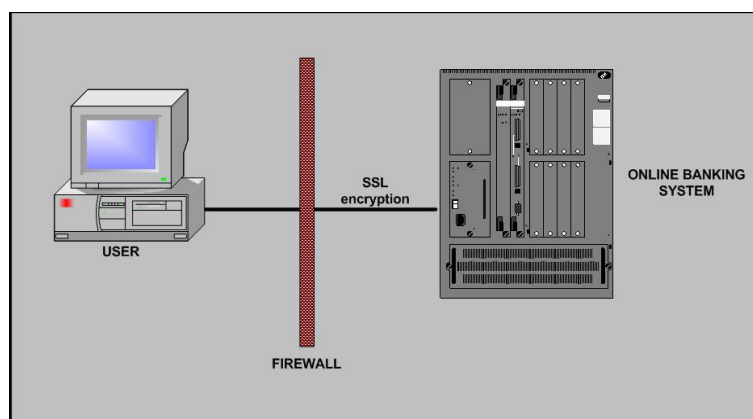


Figure 2: A conventional online banking system installation

While SSL is widely trusted as a secure encryption method, it does represent a single point of failure in conventional online systems. Most encryption schemes are ultimately cracked, and

usually much sooner than was originally predicted based on the mathematical properties of the encryption scheme. Strong encryption algorithms tend to be cracked not by brute-force testing of all possible settings, but rather by the fortuitous discovery of an unintended vulnerability, which dramatically reduces the security of the approach relative to the theoretical level.

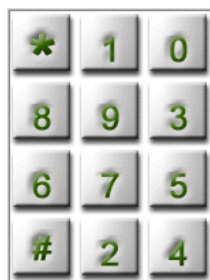
One of the better-known examples of this is the cracking of the World War II Enigma code after it was realized that certain messages routinely began with the day's weather report. Since the plain text of the weather report was known, it could be used as a key to unlock that day's encryption.

SSL is widely-used to encrypt highly structured information, including standards such as HTML and XML, and transaction standards relating to online banking. Though a PKI system like SSL is harder to crack than the Enigma code, it is fair to assume that sooner or later it will be compromised, whether by leveraging the high predictability of structured data or some other pragmatic weakness. The ever-increasing availability of cheap computing power, coupled with the ever rising financial value of SSL-encrypted transactions, provides strong incentives for would-be e-criminals to crack the code.

Tricerion's triangulation approach strengthens the encryption of all data transmitted, but its main contribution is to segment the data transmitted into discrete channels, such that compromise of one channel does not yield enough information to be useful.

Data flow between the user system, the bank system and the SMA system takes place as follows:

1. The user indicates that they wish to login to the bank system, e.g. by pressing a login button.
2. The bank system requests a new session from the SMA system.
3. The SMA system generates a new session and returns a one-time URL to the bank system.
4. The bank system transmits the elements of the login page to the user's browser, including the one-time URL.
5. In rendering the login page, the user's browser requests the one-time URL via the Internet, obtaining a randomized keypad directly from the SMA server, as shown in Figure 3.



**Figure 3:** Tricerion one-time keypad

6. The user enters their PIN using the randomized keypad (direct typing of input is disabled).

7. Any conventionally-entered data is sent directly to the bank system (e.g. account name), but the click coordinates of the user's PIN selection on the one-time keypad is sent back to the SMA server.
8. The SMA server decodes the users' click coordinates relative to their one-time keypad and passes the user's PIN to the bank system *behind the bank's firewall*.
9. The bank system ascertains whether the user's account details are correct and either initiates an authenticated online banking session or rejects the login attempt.

Triangulation may seem like a simple modification to current practice, but it significantly enhances both the actual and the perceived security of the transaction in the following ways:

- Existing client-bank dialogues require only two SSL sessions to be cracked in order to access sensitive login details, whereas Tricerion dialogues require six SSL sessions to be cracked (two per channel), plus six further higher order encryption keys.
- This is an 'elsewhere' solution. Even if a channel is successfully cracked, there is always a piece of vital information 'elsewhere', and not in the cracked channel. The only two places where the information ever exists all together is in the user and in the bank system – the two places where it is supposed to be.
- This approach combines digital and analogue encodings at the same time, which greatly increases the difficulty of cracking the encoding for automatic systems. Conventional encryption combines with precise click position on a one-time keypad so that even if a criminal were to crack the encryption he would still have to find the correct one-time keypad and interpret the click coordinates manually or using sophisticated image processing software.
- In this approach the PIN never exists in digital form outside of the bank's firewall.
- The SMA server never 'knows' the significance of the data it handles. All it does is to generate keypads and decode strings against them. It has no idea if the PIN information is correct or incorrect, or which account it relates to. It provides a service to the bank system, but obtains no sensitive information from it. It does not store any state information which could be hacked and used maliciously.
- The scrambled keypad presents the user with very clear evidence that the bank takes security seriously, and that additional security measures are being used to protect the user's login details. However, the concept of a scrambled keypad is so easy to understand and use that users do not need any special training. (This is true for scrambled numeric keypads, but not scrambled alphabetic keypads, which are not practical.)

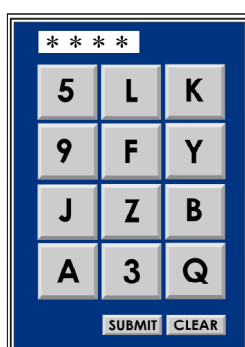
Triangulation is a simple, yet extremely powerful extension to online banking communication protocols.

**Keypad Personalization.** Tricerion's Keypad Personalization approach is built on a foundation of triangulation, and makes it significantly more difficult for phishing attackers to deceive the bank's customers or for customers to disclose their login details inadvertently.



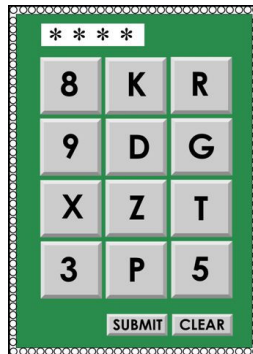
To gain the benefits of Keypad Personalization the existing customer account record held by the bank needs to be augmented by the addition of one extra field. Alternatively, this information can be stored in a separate database to prevent any changes to the main bank database. It is also necessary to implement a two-step login process. In outline, the process works as follows:

1. The user is prompted to input their account name.
2. The account name is used to retrieve a set of parameter values associated with that account name. This information may either be stored in a new field in the institution's Customer Account Record, or in the SMA server's own database, according to the institution's preferences. Parameters relate to keypad properties such as background color, border design, font, font size, font style, etc. Permutation of these parameter values yields many distinct keypad 'look-and-feels'. Parameter values are fixed for each user, so users will become used to their own consistent keypad look-and-feel. Since a mass phisher does not have access to each user's distinct keypad look-and-feel, the best they can offer in a spoof site is either a direct typing input or a plain vanilla keypad. In either case an input mechanism differing from the familiar keypad should alert users that something is wrong.
3. The Personal keypad approach can be extended further by issuing users with alphanumeric passwords. These are drawn from a set of 36 characters (A-Z, 0-9). Thus a user's password could be 'Y3JK'. One of the keypad personalization parameters stores the user's individual symbol set. This is a set of twelve symbols, made up of the user's password symbols, plus a random selection of other alphanumeric symbols. Thus a user whose password is Y3JK could be presented with a personal keypad as shown in Figure 4.



**Figure 4:** Personal keypad including personal symbol set

The personal symbol set, like the keypad look-and-feel, is constant for each user, though the symbol positions are scrambled on each presentation. This serves not just to make it obvious to the user when a phishing attack is taking place (uninformed by the user-specific look-and-feel features), but also to render it *impossible* for most users to enter their password via a 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 36 available alphanumeric characters is only 1 in 119. Even if the user does not spot that they are being spoofed, they will not be able to enter their password via a realistic-looking keypad, because not all the necessary characters will be present. Figure 5 shows how immediately obvious a phishing keypad is relative to the usual one, and how impossible it can be to enter a password (e.g. Y3JK) using it.



**Figure 5:** Fake keypad with wrong look-and-feel and without necessary password symbols

- Of course, the user could still disclose their password by typing it into a phisher’s text input box or by including it in a reply email. Keypad personalization supports a further refinement to prevent even this kind of reckless self-disclosure. The requirement for this final level of security is that users be issued with password consisting of sequences of iconic pictures, such as those shown in Figure 6.



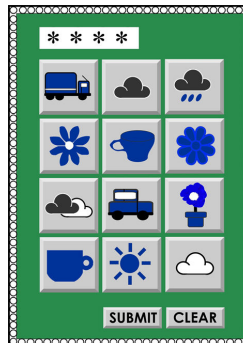
**Figure 6:** Pictorial password

- While pictorial passwords may initially seem odd, there is no reason why they should be. Learning Theory suggests that it is easier to memorize sequences involving shape, color and meaningful concepts, than arbitrary sequences of letters or numbers. 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 alphanumeric are used, the personal keypad will look like the example shown in Figure 7.



**Figure 7:** Personal keypad, using pictorial symbols

The chances of a user being able to enter their details via a phisher’s speculative keypad, such as the one shown in Figure 8 are extremely small.



**Figure 8:** Another personal keypad

Even though the phisher may, by sheer luck, generate a spoofed keypad having some features in common with the user's (for example, Figures 7 and 8 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 7 and 8 have different background colours and borders, and Figure 8 does not contain all the necessary password symbols). Once the move is made from alphanumeric to graphical symbols, there is no reason why the set of available symbols should not be very large. For example, there are  $6.1 \times 10^{28}$  combinations of 12 position keypads from a set of 256 symbols, and the chances of a randomly generated keypad containing all the symbols from a four-symbol password is 1 in 353,116.

**Active countermeasures.** Determined phishing attackers may try to subvert the anti-phishing system described here (e.g. by phishing the user's account name first, and then staging a full-blown targeted phishing attack) so the Tricerion SMA server includes an advanced set of active counter-measures to identify and disable attempted attacks. Whereas full descriptions of triangulation and pin pad personalization have been filed for patent, it is best to keep the details of countermeasures as secret as possible in order to stay ahead of the phishing community for as long as possible. Details will only be disclosed where absolutely necessary to parties who have signed a non-disclosure agreement.

**Implementation.** The Tricerion online security suite is implemented as a server solution, using two rack mount units (minimum installation), configured to provide:

- Dual redundant servers
- Load balancing
- Automatic failover
- Dual redundant power supplies in each server
- RAID 5 disks

No state information is stored in the SMA, so no backup regime is required (except in the case where institutions opt to store keypad personalization data in a Tricerion database, rather than in the institution's own Customer Account Records). No secret account information ever gets passed from the bank system to the SMA server, and the SMA

server never 'knows' the status or significance of the information it processes from the user. Thus the SMA server is incapable of compromising bank account details.

## Conclusion

The combination of Triangulation, Keypad Personalization and Active Countermeasures delivers unprecedented levels of protection against account hijacking in a relatively inexpensive and simple-to-deploy single-factor system:

- From the perspective of a large financial institution that may support millions of online banking users and desires not only to reduce its direct risk of loss from account hijacking, but whose online banking clientele demand to know that their online transactions are safe and secure, the SMA solution is secure, cost-effective and innovative; and
- From the perspective of e-commerce merchants, who are seeking a better means of validating online transactions, both to reduce fraud and to reduce the rate at which they may be denying *bona fide* transactions.

The direct and indirect economic implications of online fraud and account hijacking are massive. Several solutions will emerge, but the prevailing solution will have all of the characteristics of the SMA solution: it will be simple; it will be easy and relatively inexpensive to deploy; it will provide unprecedented levels of security; and, from the user's perspective, it will be simple, intuitive and convenient, yet provide a level of justifiable comfort that the online environment is a safe place to transact. Tricerion believes it represents the winning solution in this marketplace.



## Glossary

**Account Hijacking** A form of identity theft in which the fraudster assumes, through one or more different scamming techniques, the customer's identity in order to access and then abuse a valid financial account.

**Authentication** The process by which a user is admitted to his or her account through the use of credentials.

**Authorization** A permission, based on the user's identity, to take certain actions once admitted to an account. For example, once authenticated, most online banking users also have the authorization to make electronic payments or transfers.

**Biometric Authentication** A form of authentication in which the principal form of credentialing is a biometric "signature," such as a fingerprint, a voiceprint or faceprint.

**Credentials** The unique identifier that is used to authenticate an account user. Credentials can be user name and pin, biometrics or possession of a physical token.

**Identity Theft** The general category of consumer fraud that involves stealing the user's financial identity and then abusing the underlying accounts. The FDIC estimates that in the United States, the direct costs of identity theft in 2003 were almost \$50 billion.

**Keystroke Logging** A form of account hijacking in which spyware deployed on the user's computer picks up and transmits to a fraudster the keystrokes that provide access to the user's financial accounts. The same effect can also be achieved by attaching a physical keystroke recording device to the user's computer.

**Phishing** A form of account hijacking in which a fraudster creates a spoofed email or website appearing to be from a real financial institution, and solicits the recipient and potential victim of the fraud to provide the user's online credentials, ostensibly to allow the putative financial institution to fix some problem with the user's account. Phishers "mass mail" this form of fraud to millions of email accounts in the hope that some percentage of users will fall for the scam. Phishing is a rapidly growing problem. It is estimated that about 20% of those who have received these scams have clicked on a link in the phishing email and that up to 5% of phishing recipients respond to these scams by providing their credentials.

**Keypad Personalization** An innovative form of credentialing from Tricerion that creates a personalized, randomized pin pad that serves as the core credential for each authentication event.

**Shoulder Surfing** A simple, but nonetheless effective, form of account hijacking in which fraudsters steal a user's user name and password credentials by looking over the user's shoulder in a public place in which those credentials are entered (such as at an ATM machine).

**SMA Solution** The innovative, three-tier credentialing solution from Tricerion.

**Token** A device, such as a random pin generator or smart card, which is used, in combination with other credentials, to authenticate the user of a financial account. Tokens represent the "second factor" in a two-factor credentialing system.



**Triangulation** Another SMA innovation that establishes a *trialogue* among user, banking authentication servers and the SMA server in order to establish a much higher level of online security than is available in a system predicated on a *dialogue* that occurs between the user and the authentication system. With triangulation, even if a fraudster intercepts transmissions between two of the three points in the triangulated solution, they will still not be able to make sense of the information collected.

**Two-Factor Systems** Systems of credentialing that rely on two factors for authentication, such as a user name/password combination, plus with some form of device. For example, ATM cards represent “tokens” that are part of a two-factor system. While two-factor systems significantly increase the security of the authentication process, they are expensive to deploy (because all online users of a given institution need to receive the token) and they may reduce the usability of online accounts since the user must carry the token in order to be able to access their account.