



White Paper

Preventing Man in the Middle Phishing Attacks with Multi-Factor Authentication

Introduction

As businesses and consumers grow increasingly reliant on the Internet for conducting essential business transactions, new security threats are evolving that are harder to spot and harder to foil. No longer the purview of select security experts, new generation security risks such as “phishing” and “trojan horses” are now being discussed—and worried about—by the general public. Phishing, in particular, takes advantage of the trust a company has built with its customers, partners and employees to steal credentials the phisher can use to gain access to bank or brokerage accounts, internal systems and confidential information. They put a company’s assets and reputation at risk. They have also made email useless for business to consumer communication.

Recent media attention has shined the spotlight on new threats that are preoccupying security experts—including “man in the middle” phishing attacks—and the inadequacy of most existing technology to combat them. The emerging standard for security technology is “two-factor authentication”. Recognizing that simple passwords are too easy to discover, many companies are beginning to implement two-factor authentication systems—such as a password and a token that generates a new number every minute. However, security experts and journalists (see <http://www.computerweekly.com/articles/article.asp?liArticleID=137454&liFlavourID=1&sp=1> and <http://www.eweek.com/article2/0,1759,1776085,00.asp> for examples) have reported that basic two-factor authentication alone, though it solves many of the problems of a simple password, is not up to the challenge of today’s phishing attacks.

Is this new brand of phishing really the threat it’s made out to be and what can be done about it?

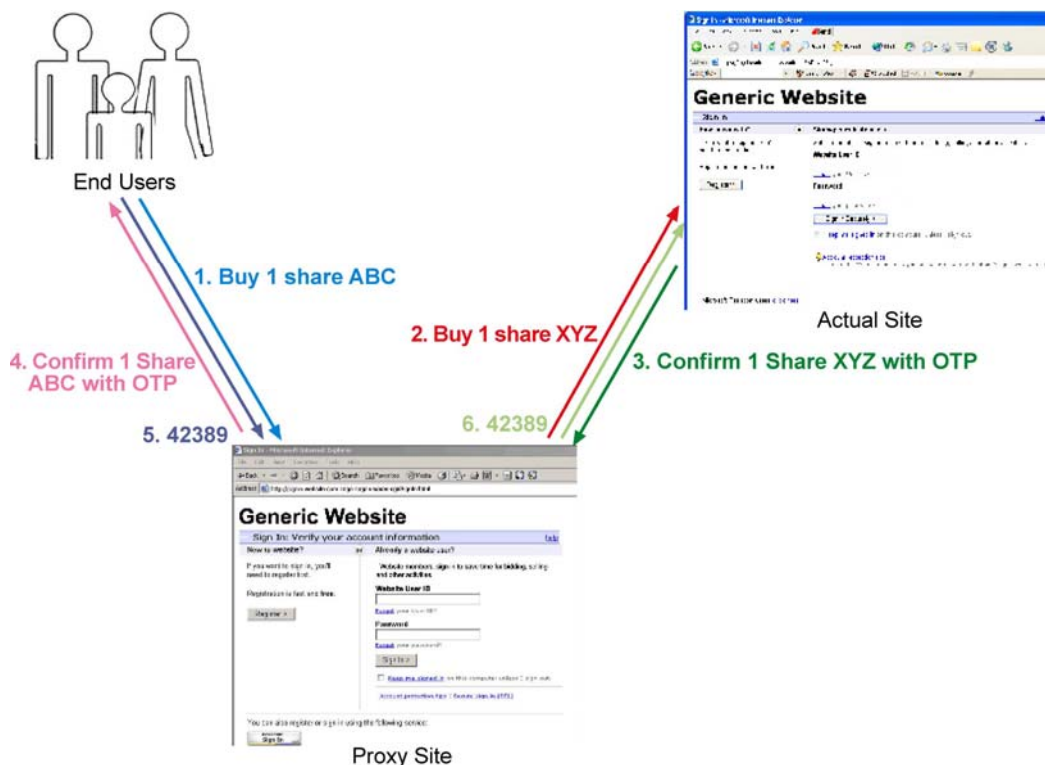
The Phishing Problem

The phishing threat is indeed real, and is of particular concern to those in financial services, e-business and ISPs where their business is directly affected.

Phishing has evolved rapidly. Initially, users were lured to a phishing site where passwords were harvested. In the next phase, passwords were captured by blending phishing with spyware. Now, because more companies are deploying one time password tokens, phishers are able to use a far simpler “man in the middle” attack to strike organizations. With man in the middle phishing, all the phisher needs is a freely available web proxy server which is manipulated in minutes to set up an attack. Ironically, such attacks require far less sophistication than the initial phishing attacks. Here the attacker does not even have to take the trouble to copy the real web site—they simply proxy it and use it. Here’s how it works: In a man in the middle phishing attack, users are lured to a phishing site (such as a fake bank site) by an email or DNS caching attack where they enter their username, password, and the number from a one-time-password token. Rather than

simply a copy of the legitimate site, the phishing site is actually a web proxy server that connects to the legitimate site. The phisher’s server uses the information entered by the user to immediately log in to the legitimate site, then automatically either keeps the session open, pages the phisher, or alters the user’s transaction to benefit the phisher. The user surfs or transacts, unaware that they are not at a legitimate site. When the user logs off, the phisher remains logged on, refreshing the session with the legitimate site to keep it active.

Here’s one example of what man in the middle phishing can look like. In this case, the users think they have gone to a site and have purchased “ABC” stock. In reality, the phisher has purchased “XYZ” stock with their information.



Phishing represents an acute threat, with serious consequences. Phishers can wreak havoc with a user’s assets and a company’s reputation, by:

- stealing money from the user’s bank account
- manipulating the price of penny stocks
- gaining access to the user’s personal information, account numbers, etc. for identity theft

How to Solve the Problem

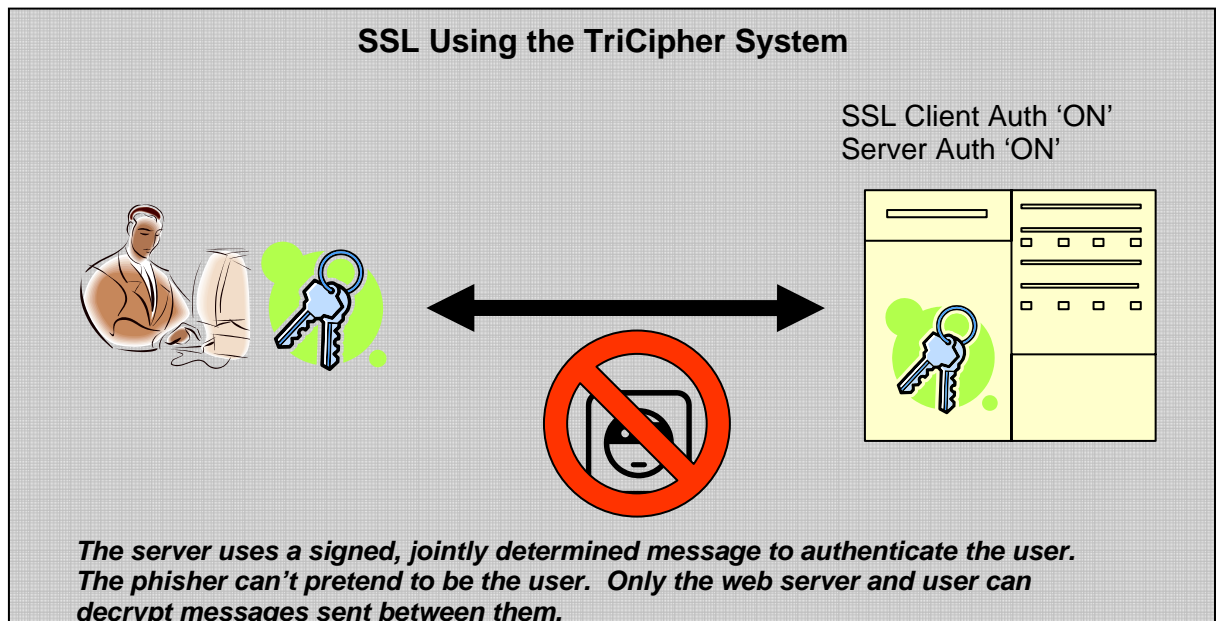
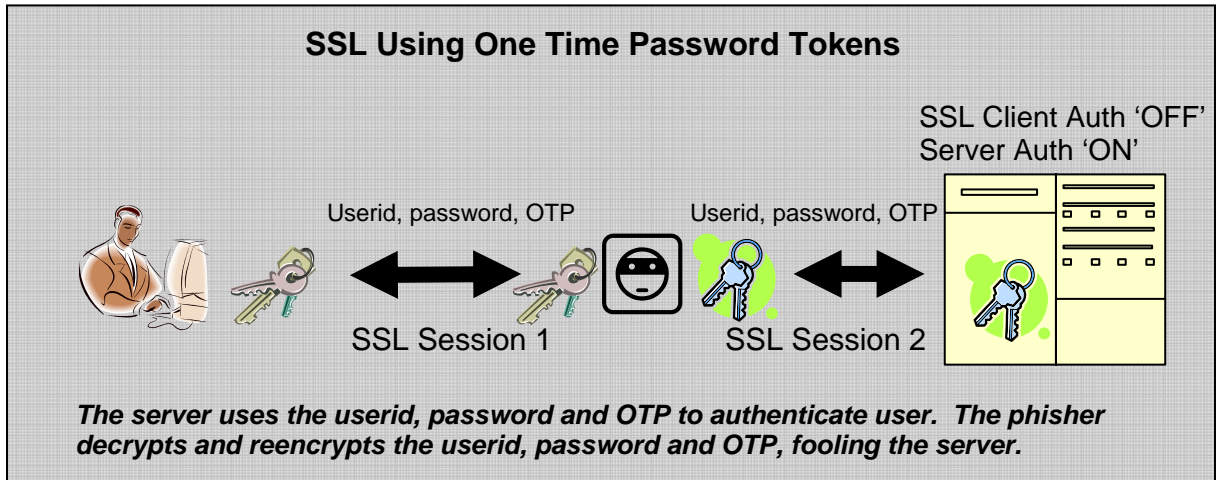
If one-time passwords and tokens can’t solve the problem, what *can* prevent phishing attacks? Because phishers always find new angles and have moved beyond reliance on user naïveté, education alone will not solve the problem. The best way to protect your

customers, assets and reputation from phishers is with authentication systems that don't reveal secrets.

According to **Becky Bace**, President of Infidel, Inc., "The key to foiling these attacks is to take advantage of the existing SSL infrastructure to authenticate the client. SSL was designed to prevent man in the middle attacks and doesn't require the user to reveal the credential. Ideally, you would also like to make it impossible to steal the entire credential from the user."

Phishing occurs because...	To prevent phishing...
Only the server authenticates to create the SSL channel	SSL client authentication should be turned on
Phishers can intercept the user's "secret" login information	Choose a system that does not require the user to share their secret
With activity, sessions can be kept open for hours	Keep the session from being hijacked
Users are not sophisticated about looking for the SSL lock, or they are fooled by fake URLs	Educate users to check for the SSL lock and not accept unrecognized certificates—but don't rely on education alone to solve the problem

There are several vendors promoting technologies which do not strengthen client authentication, but instead try to educate users to make them less susceptible to being fooled by a fake site. We strongly encourage enterprises to adopt these technologies, which include improvements in the browser to help the user identify fake sites and improvements in firewalls that block access to known phishing sites. They are useful and further protect the enterprise. However, it would be a serious mistake to assume that these technologies are, by themselves, sufficient. At the end of the day, there is no substitute for strong authentication. And unfortunately, phishing targets the most gullible of users—the ones whom 'security awareness' techniques usually do not reach. Some users will always remain gullible, and the only way to keep their credential from being phished is to make it impossible for them to reveal their credential.



TriCipher Solution: The TriCipher Armored Credential System™ (TACS)

The TriCipher Armored Credential System (TACS) prevents proxied man in the middle phishing attacks by leveraging the Internet's existing SSL infrastructure, and combining it with a unique multi-part credential.

TACS creates a multi-part credential by splitting the user's credential between the user and a secure appliance kept in the enterprise's data center. Since the user doesn't have the entire credential, he or she can't give it away to the phisher, nor can the phisher steal it from their desktop. In addition, TriCipher's Double and Triple Armored credentials use

SSL client authentication, preventing a phisher from sitting in the middle of the user's session with the web server.

“To prevent phishing...SSL client authentication should be turned on”

SSL is standard software that exists in all web browsers and servers. The SSL software can perform three functions:

1. Authenticate the web server to the browser
2. Set up encrypted communications
3. Authenticate the end user to the web server

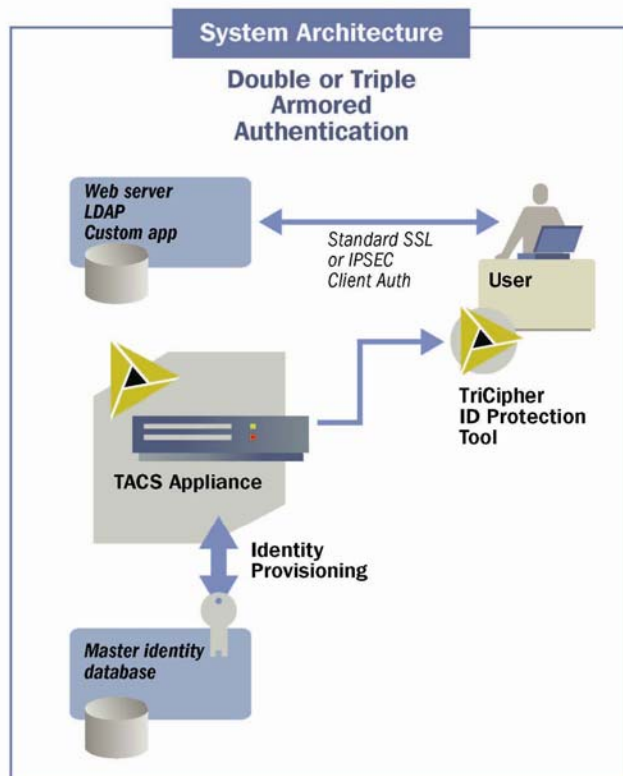
While every web server has the ability to do all three, most only use functions 1 and 2, and rely on weak user IDs and passwords to achieve end user authentication, leaving them open to attacks such as phishing. To use the TACS system, at a web server the administrator simply “turns on” the third feature - no software to install.

Client side SSL is not vulnerable to man in the middle attacks for the following reasons:

- With SSL client authentication turned ON, the web server knows who it's talking to, so the phisher cannot impersonate a legitimate user. The way SSL is typically used today (server authentication only), the user authenticates the server to set up the SSL session, but not the other way around.
- With TriCipher's Double and Triple Armored credentials, the user's authenticating information is *not sent to the web server*. With a one-time password (OTP) token, the userid, password and OTP are all sent to the web server over SSL. Since the SSL session is set up without authenticating the client, a man in the middle attack is possible.
- The message to be signed to set up the SSL session with the web server is *jointly agreed* by the server and browser. The message between the phisher and web server is different than that between the phisher and user. So, the phisher cannot pass through the signature, nor can he get the user to sign the wrong message so he can pass it along.

“To prevent phishing...Choose a system that does not require the user to share their secret”

If the entire credential were stored with the user, then an attacker who compromises that PC can usually steal it (even if it is encrypted). Whereas in the TACS approach the part of the credential stored securely on the TACS-Appliance blinds the attacker for a wide variety



of attacks against the part the user holds.

Double Armored Credentials

A Double Armored Credential can be seamless for the user, but does require a small CAPI driver on the client, the TriCipher ID Protection Tool. The tool automatically pops up when the user goes to a page that is protected by SSL client authentication. The tool collects the user's id and password, then signs (encrypts) the password using a key stored in the Trusted Platform Module (TPM) or Windows® Key Store. This key is completely invisible to the user. The login is completely familiar. The ID Protection Tool authenticates the user to the TACS Appliance which checks that the user's credential is still valid. To sign the jointly agreed message in SSL (the running hash), the ID Protection Tool sends the hash to the Appliance, which uses its part of the credential to sign. This partially signed has is returned to the desktop, where the ID Protection Tool signs with the user's part of the credential. The fully signed hash is then returned to the web server for verification.

At \$5/seat, Double Armored Credentials provide a secure, two-factor solution that does not require the user to carry a token or smartcard, yet cannot be phished – a cost effective, highly secure alternative to time synchronous or challenge response one time password systems.

Triple Armored Credentials

A Triple Armored Credential works just like Double Armored, except a third factor (besides the user's password and a key stored on the PC) is required. Often this is a smartcard, but it could be a biometric or a simple USB memory stick used to store a key pair (this is secure in our system for reasons we won't go into here). When the user enters their password, it is signed using both the key on the PC and this second key. This raises the bar for an attacker. They not only have to steal the password and get access to the PC, they have to steal the smartcard, too.

Our patented technology fills the gap between authentication systems that are either not secure enough or too hard to use and deploy. TriCipher's innovative approach to strong multi-factor authentication protects against phishing and eliminates dictionary attacks.

Deployment

TACS is designed to work with your single sign on, identity management, provisioning, authorization and directory systems. TACS integrates through a simple provisioning plug-in to your directory, and authentication plug-in at your identity management system. At the web server or any relying system, all that's required is to turn on support for SSL/IPsec client authentication or X.509 certificates.

Contact Us

Contact us for more information on TriCipher's strong authentication system and how it can help your business defeat phishing.



TriCipher, Inc.
1900 Alameda de las Pulgas
Suite 112
San Mateo, CA 94403

+1.650.372.1300 tel
+1.650.372.1301 fax
www.tricipher.com