Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Phishing is Yesterday's News – Get Ready for Pharming

April 2005

Entrust®
Securing Digital Identities & Information

Table of Contents

1 Phishing is Yesterday's News – Get Ready for Pharming

New Threats to User Identity and Information Demand New Security Approaches

From today's perspective, phishing attacks seem simpler and much less of a threat than the new breed of on-line attacks that are now being experienced. Phishing attacks, while adopting the persona of known on-line organizations, are easy to identify and can be shut down relatively quickly. Interestingly enough, organized crime has taken over perpetration of these attacks and their sophistication has increased significantly. Today, users face much more insidious forms of attack that are more difficult to detect and defend against.

2 A New Breed of Attack

This new breed of attack is commonly referred to as *pharming*. Instead of simply tricking the user to respond to a bogus e-mail which directs them to a counterfeit web site, *pharming* uses much more subtle ways to trick the user in to surrendering their identity and sensitive information. These attacks use Trojan Horses to install keystroke readers and redirectors that allow an attacker to capture passwords and credit card numbers without the user having to do anything out of the ordinary. Here are two examples of how this could happen:

1. The user opens an e-mail that looks legitimate, encouraging them to open the attachment which surreptitiously installs a key-stroke reader. When the user goes to their on-line bank, the key-stroke reader recognizes this and captures the user's keyboard entries as the name and password are typed in. This information is then transmitted to the attacker who uses it to access the user's account. A highly publicized case of this was recently reported with a Bank of America customer.

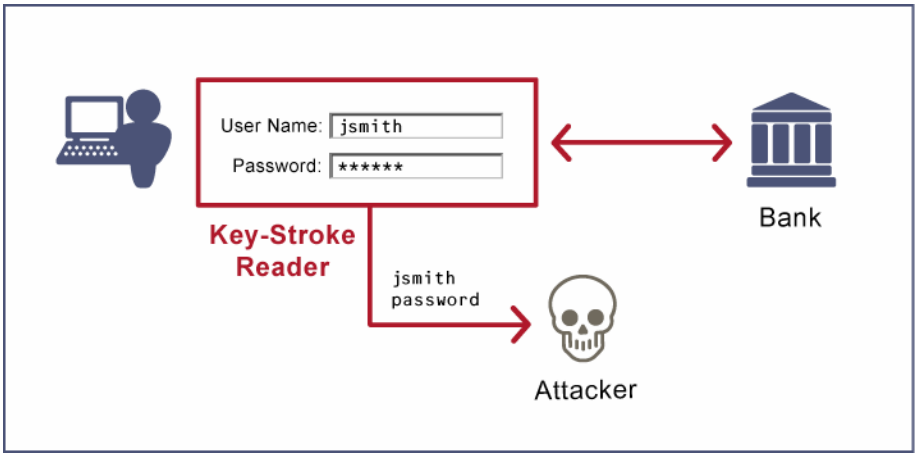


Figure 1

2. By downloading a file or visiting a web site with an ActiveX control, a user may unintentionally install a redirector which corrupts the user's HOSTS files and when the user goes to their on-line bank, the session is re-directed to go to an attacker's web site. This can also be accomplished by *poisoning* the DNS server which provides the address for the on-line bank. Sophisticated attackers can then redirect the session to the user's bank and while in the process is able to see all the traffic flowing back and forth – including passwords and personal information. The attacker has essentially inserted themselves in the middle between the users and their bank.

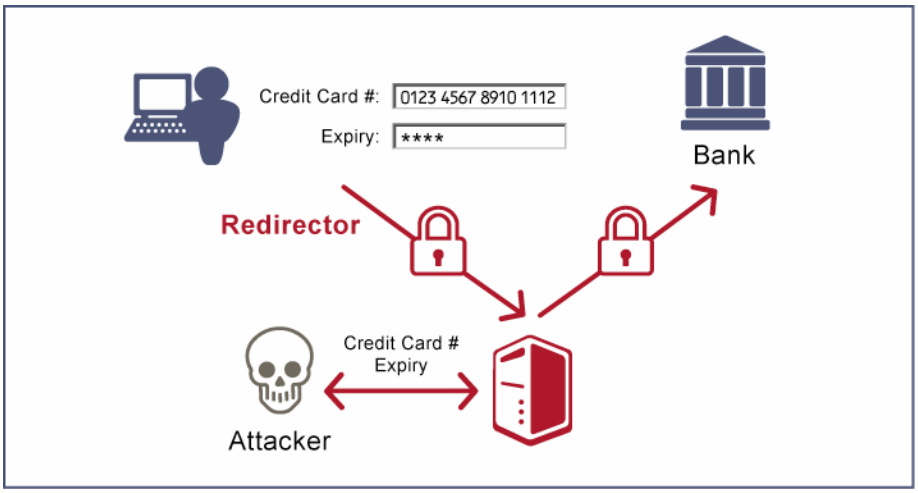


Figure 2

There is a well publicized case of these mechanisms being used by a company today for the purposes of gathering marketing data. MarketScore has raised concerns with many on-line service providers as under the guise of internet acceleration software, redirects Internet traffic through its site, giving it access to the user's passwords and sensitive information[1]. MarketScore does require users to accept an on-line agreement with the appropriate permissions although it is questionable whether they understand the full ramifications.

3 What Can be Done?

Historically, the security approach applied to these types of attacks has been similar to the concept of a *border guard*: stop malicious things from getting on the computer and stop the user from going to bad places. Tools such as anti-virus, anti-spyware, firewalls and intrusion detectors all take this approach. However, as attacks continue to evolve and become more sophisticated, the possibility of a key-stroke reader or a re-director successfully being installed despite these border guards cannot be ignored.

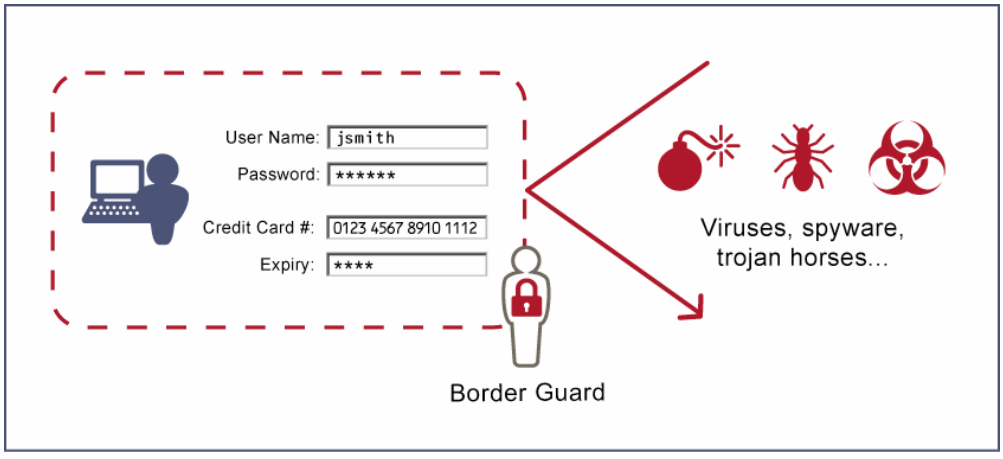


Figure 3

[1] *Marketscore monitors all of your Internet behavior, including … the activity you may have through secure sessions, such as when filling a shopping basket or filling out an application form that may contain personal financial and health information.* MarketScore Privacy Policy, 9 March 2005.

To deal with that possibility, a different security approach is required. In addition to the measures described above, the identity and information of users needs to be protected with "*body guards*". That is, security needs to stay with the user's identity and information regardless of the type of attacks and where user information flows. This type of security would provide "body guard" capabilities to a user identity, no matter where it travels even in the presence of key-stroke readers or with an attacker that is able to monitor internet traffic.

There are two security capabilities that can fulfill this "*body guard*" capability. The first is strong authentication. Today, users typically rely on a password to protect their identity but this is extremely susceptible to theft simply by having the attacker witness one login. Having an additional factor of authentication, something the user must physically possess in addition to something the user knows (i.e. the password), can help protect an on-line identity against attack. This is analogous to how users authenticate at an instant-teller bank machine: they have to both possess their banking card as well as know a PIN. With strong authentication, if a key-stroke reader is installed, it can capture only the password – not the physical factor used in the authentication process. Without that physical factor, the password alone cannot be used by the attacker to access the user's account.

The second important capability is persistent encryption. Today, Secured Socket Layer (SSL) protects information transmitted by users only as it is passed to the target server. For example, if a user inputs their password on-line it is available in the clear as soon as it reaches the web server on the other end. In the case of a re-director attack, the secure session ends at the attacker site before being forwarded to the legitimate on-line organization, leaving user data exposed. Persistent encryption can protect data regardless of the session security. User inputs are encrypted before they leave the workstation and can only be decrypted by the legitimate organization that has access to the back-end servers. Even if the communication is intercepted, the data will still be encrypted and of no use to an attacker.

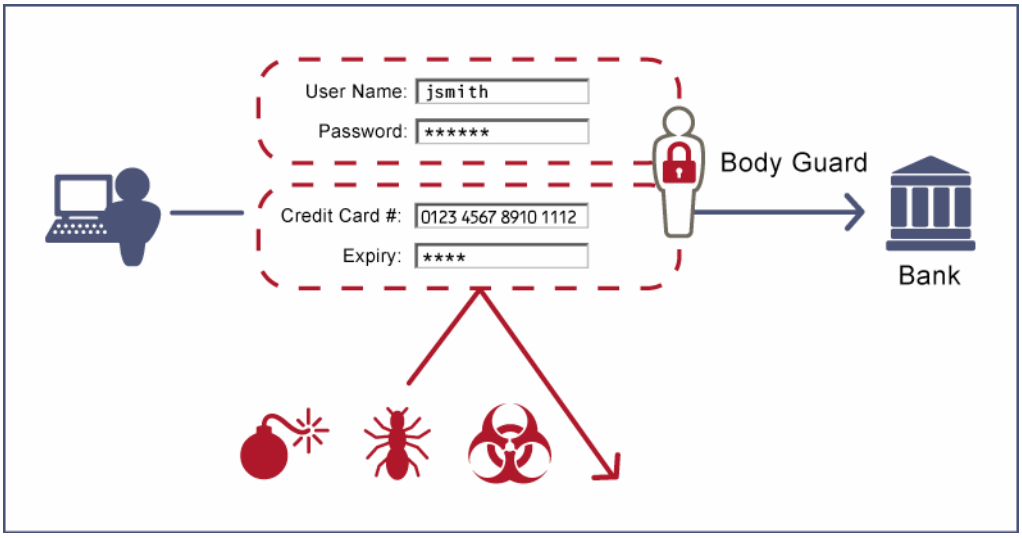


Figure 4

Together, these two capabilities can serve as body guards to protect both the user's identity and information in an increasingly hostile Internet.

4 Reality Check

There are several options that can provide "*body guard*" security but they must be evaluated using the real world requirements of the Internet. If a technology is too invasive to the end user, then it will not be adopted. If the technology is too expensive, then it will not be affordable to either the end user or the deploying organization.

There are several factors to consider when encouraging users to adopt technology:

- Client software – any requirement to download and install software is a barrier;
- Software interface – substantial complication of the existing user experience risks implementation; and
- Ease of use – especially for physical two-factor authentication, the ease of use including portability, durability and the user interface is a critical consideration.

Especially in large deployments, the cost of the approach is also paramount to its feasibility. If the total system cost is too high, then organizations face charging end users for the additional security to make an acceptable business case. This counteracts with the need to widely deploy the security to maximize the benefits as users are traditionally very resistant in paying additional service fees.

To be effective, "*body guard*" technologies must provide a high level of security while being both low-cost and easy to use and deploy.

5 How Entrust Can Help

Entrust has developed a solution to help you deal with this new, more menacing threat that combines security with low cost and low end-user impact. It provides the key security elements necessary to be the body guard for a user's identity and information**.**

Low cost, easy to use strong authentication. Entrust offers a range of strong authentication solutions that can significantly increase the security of an on-line identity. One example is Entrust IdentityGuard, which provides two-factor authentication at a fraction of the cost of traditional tokens and with minimal impact to the end user experience. By providing users with something they must physically possess in order to authenticate, it makes it more difficult to maliciously obtain a user's identity. Even if an attacker obtains a user's password, they will not be able to use it without the accompanying two-factor authentication.

Entrust IdentityGuard is easy to use and inexpensive to distribute to millions of users. Users continue to employ their user name and password but are also provided with a second, physical form of authentication based on an assortment of characters in a row and column format that is printed on, for example, a plastic wallet-sized card. When attempting to login or subsequently perform a high value transaction, users receive a coordinate challenge used to demonstrate that they are in possession of their unique card.

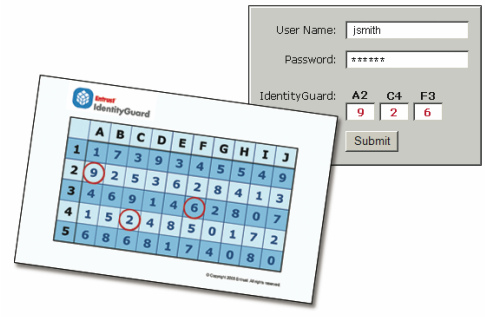
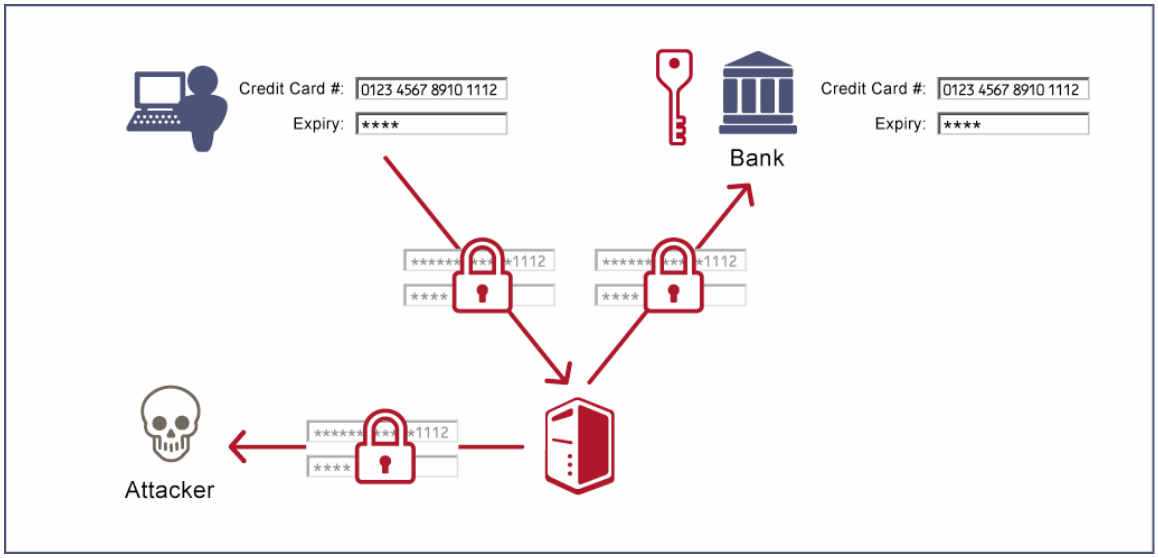


Figure 5

As illustrated in Figure 5, the challenge consists of coordinate prompts that the end user looks-up on their individual card. In this example, the response to the challenge "A2", "C4" and "F3", would be "9", "2" and "6". These numbers are entered by the end user demonstrating that they are in possession of their Entrust IdentityGuard grid.

Entrust IdentityGuard is an easy to use two-factor authentication method at a fraction of the price of a battery-powered token.

Transparent, end-to-end persistent encryption. Using Entrust TruePass™, user information is protected with an extra layer of encryption allowing the information to be accessed by the authorized back-end application. As soon as the user submits data it is encrypted before leaving their workstation. The encryption is done transparently without the user having to install any software or deal with any additional user dialogues.



Even if a user submission is maliciously routed through an intermediate site where the SSL session protection is terminated, user input is not accessible. Only the legitimate back-end application has the necessary key to decrypt the data.

Together, these two capabilities are provided in an affordable and deployable package and are combined with a level of security designed to address these new challenges.

6 Summary

As Pharming continues to grow, organizations will need to proactively mitigate the risk with a stronger form of authentication that is easier to use and less costly to deploy. Entrust IdentityGuard addresses this need by providing a simple, and inexpensive way of increasing security and defending against attacks with two-factor authentication. The Entrust TruePass product is designed to protect user information with an extra layer of encryption making it more difficult for thieves to steal authentication information. As soon as the user submits data it is encrypted.

Organizations taking action to address identity theft attacks such as phishing and pharming have the opportunity to reduce financial losses experienced as a result of these attacks, as well as provide users with confidence to continue using on-line services.

Entrust IdentityGuard and Entrust TruePass are part of Entrust's Secure Identity Management solution and can be used independently or integrated providing stronger authentication and access control elements. For more information on how Entrust IdentityGuard can help you minimize phishing and pharming concerns, please visit: **http://www.entrust.com/IdentityGuard/.**

7 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities.

For More Information

For more information on how Entrust can help secure digital identities and information, visit www.entrust.com or call 888-690-2424.