Phishing Passwords
A Sevan White Paper

Microsoft's February 2004 patch to the Internet Explorer illustrates the gravity of *phishing*. A phishing attack attracts users to a malicious web site for the purpose of collecting sensitive information. Microsoft was compelled to modify IE even through they knew that this unscheduled patch would disrupt many reputable web sites. What is not mentioned is that this IE upgrade does not prevent phishing; it simply removed an exploit that cloaked the attack. Phishing will be with us for a long time, and only highly vigilant users can prevent it, which should not give us much hope.

Although most of the focus is on compromised credit cards and bank accounts, authentication passwords are most exposed. The reason is simple: users can be trained not to give up credit card numbers, but they don't have the luxury to withhold their passwords. Since passwords are required to access the legitimate web site, users have no option other than provide their passwords to a malicious spoofed web site. Once a user is fooled into authenticating to this malicious web site, his password is immediately compromised.

Don't let phishing undermine your security. Password and even OTP tokens are vulnerable. Fortunately, Sevan's certificate-based authentication is phish-proof. We don't prevent phishing. Rather, we prevent the malicious web site from stealing the user's identity. The attacker gets the user's certificate, but the certificate, by itself, does not provide access rights. This is because the user's identity is actually protected by his secret key, which is never sent to a web site, legitimate or malicious. This is the power of public key cryptography.

In summary, some day your employees, partners, and customers will be lured to a malicious web site for password harvesting. Sure, user training helps, but your only effective response is to abandon passwords and move to certificate-based authentication, such as provided by the Sevan WSA.

The illustrations show the difference between password authentication and certificate authentication in a phish attack. Illustration 1 shows that the malicious web site prompts the user for his name and password. Since the user thinks he is at the legitimate web site, he complies. The attackers now have the user's name and password, which can be used to attack the legitimate web site.

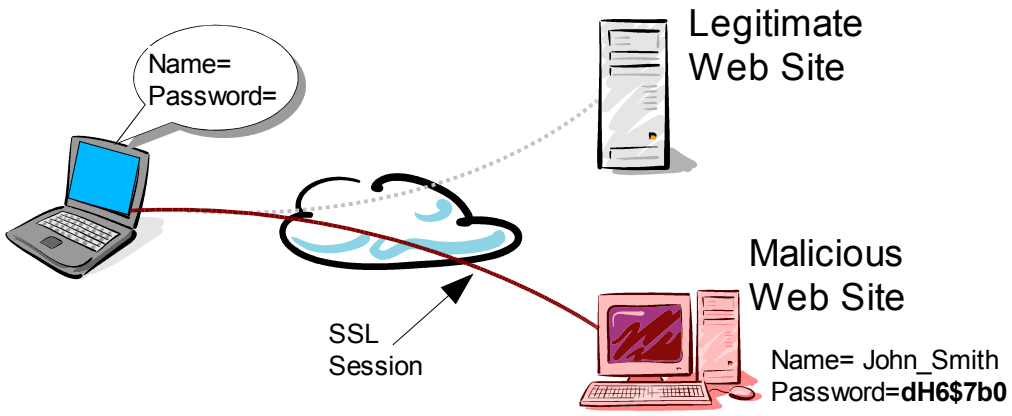

Illustration 1 Phisihing for a password -- user redirected to the malicious site and gives up password

Illustration 2 shows the same phish attack against a user protected by certificate-based authentication. As before, the user authenticates to the malicious web site. The difference is that the malicious web site gets only the user's certificate. The attacker cannot use the certificate to access the legitimate web site, since the attacker does not have the user's private key. The phishing attack was successful, but it yielded no useful

information. Both the user and the legitimate web site remain secure.

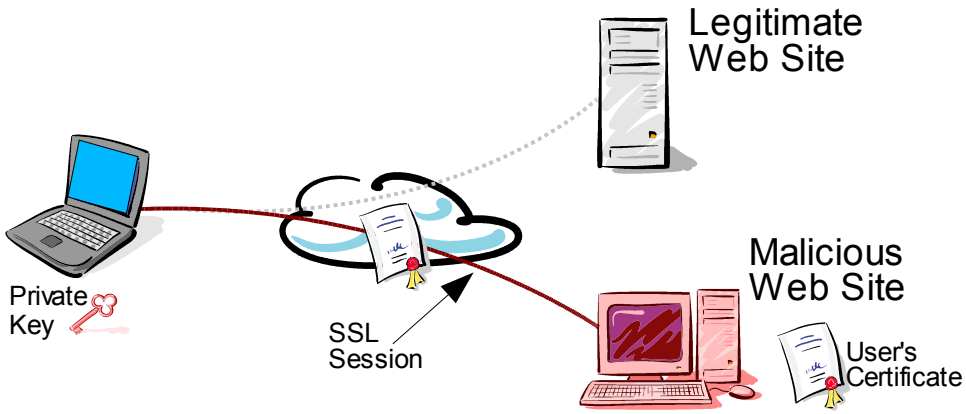

Illustration 2 Phisihing with certificate-based authentication -- user redirected to the malicious site but does not give up sensitive information

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com