


White Paper

Is an SSL VPN really secure?



Although an SSL VPN provides excellent remote access capabilities, it is only as secure as the method used to prevent unauthorized access.

However, VPN access is increasingly simple for unauthorized users to get hold of a user's credentials and this means that an SSL VPN or any other security solution that relies on static passwords to authenticate users is extremely vulnerable. As high-profile breach reports make abundantly clear, preventing unauthorized access to valuable company data is no joke.

The business challenge

To stay competitive in today's dynamic global market businesses have to provide employees with easy and cost-effective remote access to applications and resources. As the demand for this functionality has increased, it has led to astounding advances in remote access technology. Businesses have transitioned from noisy modems at 2400bps with unreliable connections to expensive VPN access with poor throughput, and most recently to fast broadband connections using SSL VPNs (Secure Socket Layer/Virtual Private Networks). But no matter how remote access technologies have changed, one thing remains constant: To provide true security an organization must be able to positively identify every user attempting to access the system.

Although today's SSL VPNs from Cisco, Microsoft, network providers, and application developers appear at first glance to have made network access more secure than ever, the simple fact is that today's hacker is more capable than ever at defeating new security systems. And, as a result, static passwords pose the weakest link in any security solution, even SSL VPNs.

See it from the other side

"Just about every organization that I have ever visited in the past 10 years, including many Fortune 100 companies, have a high percentage of accounts with easily-cracked passwords," said Jason Hart, CEO, CRYPTOCard Europe, and a former ethical hacker for Ernst & Young. "The truth is that the sophistication of the increasing number of hackers who infiltrate company networks has far outstripped any advances in system security," Hart continued. "As a former ethical hacker I can tell you that it is increasingly simple for unauthorized users to get hold of a user's credentials, and this means that an SSL VPN or any other security solution that relies on static passwords to authenticate users is extremely vulnerable."

Just by typing in the word "login" into Google a hacker can list a vast number of businesses that are providing login portals for remote users. By simply visiting the site a hacker can easily get hold of a username from any listed email address, as the first part of the email address will usually be the user name. Alternatively, and just as simply, the illegal "user" can easily use Google to locate usernames by typing in "@business.com" (where "@business.com" is the domain name of the target). This search will also show interesting


information on the business' employees, such as whether they use their work email address to make postings within news groups, etc. Statistically, a whopping 80% of the passwords that a hacker needs to guess are related to people's interests and hobbies.

So, in a couple of easy steps the hacker has already got hold of a login portal, located a username, and found out the type of user background which often forms the basis for a password. Amazingly, at no point so far has the hacker had to do anything technical! Once a hacker has a username, it is very simple to use any number of freely available tools to secure the password. In fact, getting hold of user's credentials is so simple that it is the subject of hundreds of books that are readily available on the Internet!

This problem is further compounded when we consider an increasingly common occurrence; that the computer being used has a "keylogger" installed. A keylogger records all key strokes – including usernames and passwords. All the hacker needs to do then is reuse the user name and password that has been captured, and as far as the business is concerned the hacker is a trusted user. The same thing is true for shoulder surfing. As unsuspecting users sit in a coffee bar and access the network they can be oblivious to the fact that the person sitting at the table behind them isn't just sipping a Latte, but is actually making a note of all the passwords for the computer network, bank accounts, hotmail accounts, and so on.

This does not mean that SSL VPNs are not an excellent solution to remote access. Businesses of all sizes appreciate the fact that SSL VPNs are cost effective and that there is no need to deploy or manage software clients for remote users. This adds great flexibility as it enables people to work from hotels, coffee bars, and any other remote location. But, the simple truth is that the very simplicity of access which organizations have embraced cannot be adequately protected by traditional static passwords as any hacker with a stolen username and password can sit at any computer that has a web browser and gain access to a business' applications and resources.

"It is ridiculous and naïve for any organization to think that simply installing a SSL VPN will take care of access security if the gateway to the system is still protected by easily-cracked static passwords," commented Hart.



And yet despite numerous studies from firms such as Forrester Research which state that given the ability to do so, over 60 percent of users continuously use the same one or two passwords, the vast majority of businesses using technologies like SSL VPNs continue to rely on static passwords. This statistic is all the more frightening when you consider just how easy it can be for a hacker to steal a user's username and password.

So, it is clear that even today's SSL VPNs are still extremely vulnerable if organizations rely on static passwords. But, just as importantly, the cost of trying to protect access to the SSL VPN by making static passwords harder to guess can also be extremely prohibitive.

The Human Factor

Forcing users to come up with passwords that are hard to remember simply does not work because humans are not good at remembering a random string of numbers and letters. In fact, Gartner research found that password reset requests and other user identity-related problems can account for 15 to 35 percent of all help-desk call volume.

This significant cost is only worsened by the loss in productivity due to users not being able to access the system. As a result, overly-complicated, easily-forgotten passwords are often written down – just take a stroll around any office and you will see passwords in plain sight, and many more can be found by simply flipping over keyboards.

So, although an SSL VPN provides excellent remote access capabilities, it is only as secure as the method used to prevent unauthorized access. The question then is how can organizations eliminate the security flaw of static passwords without compromising the simple remote access capabilities that an SSL VPN provides?

Randomly-generated one-time passwords would eliminate the need for users to remember complex alphanumeric strings, and would make it impossible for hackers to steal a password for future use. A one-time password would also eliminate the risk associated with being shoulder surfed. And, surprisingly, the ideal technology has been around for quite some time.

The advantages of 2FA

Whether pressing a button or swiping a card to generate a random one-time password, two-factor authentication (2FA) tokens and smart cards are extremely simple for the user by eliminating the need to memorize complicated passwords. Also, as passwords are randomly-generated and only used once, they are impossible for a hacker to steal and reuse. It is not surprising that the ability to provide greatly-enhanced security without complicating the logon process is making two-factor authentication increasingly popular with security-conscious organizations.

"AEP's SSL VPN meets the industry's most stringent security standards, including ICISA TLS and government-level FIPS certification. However, offering the very best in network and application access security is only part of the story; there is still one weakness in the security chain – authenticating the user himself. Incorporating two-factor authentication plugs the security gap caused by static passwords for user authentication – allowing for more secure transactions – and is a fully complementary fit with our SSL VPN products," says Reggie Best, COO of AEP Networks. "The use of two-factor authentication takes care of the user threat adding yet another level of security to AEP's flexible working proposition."

"We have an increasing number of employee's who work from remote locations, including cafés and clients' premises," said Tom Chambers, Financial Controller of UK based Clifton Asset Management PLC. "Along with our security policy we have implemented a two-factor authentication solution to ensure that our shareholders have peace of mind that our information and database assets are secured." And, as many two-factor authentication solutions seamlessly integrate with today's SSL VPNs they are an attractive option for any organization looking to make the most of its investment by eliminating the weakest link in the security chain – static passwords. Because, as high-profile breach reports make abundantly clear, preventing unauthorized access to valuable company data is no joke!



CRYPTOCARD Europe

Tel: +44 870 7077 700

CRYPTOCARD North America

Tel: +1-613-599-2441

info@cryptocard.com www.cryptocard.com

