Global Information Assurance Certification Paper

Norma Jean Schaefer
Course: GSEC
Original submission

Knock Knock…Who's there? Do you know who is accessing your VPN?

Introduction

A virtual private network is several security technologies. These include encryption, authentication, and key management. The idea of the virtual private network is to give users of your data access securely whether they are across town or on the other side of the world.

While VPNs secure data by encrypting the data across public networks, potential information security risks are your remote users' networks, PCs, systems, etc. How do we know who is on the other end of the VPN? How can we make sure that the person or device on the other end is who they say they are? The answer is **strong authentication**.

Let's start with IPSEC

While there are several VPN solutions, this document will focus primarily on the IPSEC and IKE protocols standardized by the Internet Engineering Task Force. Products based on IETF standards benefit from a rigorous peer review by the best minds in the business, which is particularly important when it comes to encryption. A secure VPN solution that is designed in accordance with standards will integrate with a user's existing network security infrastructure now and for years to come.

IPSEC provides three basic capabilities:

- **Authentication**
  Authentication Header (AH) supports data integrity and authentication of IP packets. Data integrity helps identify undetected modification of packets in transit. The authentication portion authenticates users, prevents address spoofing attacks and guards against replay attacks.

- **Confidentiality**
  Encapsulated Protocol (ESP) supports two modes: transport and tunnel. Transport protects by encrypting the payload of an IP packet. It is used generally for client to server or workstation to workstation. Transport authenticates the IP payload but not the IP header.

  Tunnel mode protects the entire packet. Tunnel mode encrypts the entire original packet including IP headers. Encapsulation creates a new larger packet with different sources and destination IP addresses adding to the security.

- **Key Management**
  An integral part of any virtual private network (VPN) is key management. There are two types of key management used with IPSEC: manual and automated. Manual or Manual IPSEC requires a system administrator to manually configure each VPN gateway's local system keys and remote system keys.

  Automated or Internet Key Exchange (IKE), enable on-demand creation of keys. IKE is the

most flexible and scalable. IKE is IPSEC's default key management protocol. The IKE portion determines protocols, algorithms and keys and authenticates the two parties. The IKE protocol keeps track of the keys and updates them between any two-tunnel devices. However, setting up the tunnel involves moving the initial keys between tunnel partners so that they can start with secure communications. Once a secure channel is set up, IKE keeps things safe.

(Note: A new method of negotiating and managing keys is being developed to replace IKE. It is called Just Fast Keying (JFK). IETF may see it for the first time in December in Salt Lake City, UT. JFK is suppose to negotiate encryption keys with fewer messages possibly speeding up access to VPN sites.)

Authentication

In the beginning, there were only two standard forms of authentication used by IKE, pre-shared secret and digital certificates. Both of these forms of authentication can be used for remote users, as well as, remote devices such as another VPN gateway.

Now, there are several new proposed authentication methods that work with the IKE for remote users. Hybrid authentication, eXtended authentication (XAUTH), Challenge/Response Authentication of Cryptographic Keys **(**CRACK) and Pre-IKE Credential (PIC). All authentication methods are briefly described below.

Digital Certificates

Digital certificates are by far the most popular and secure. Secure if you know the person or device has not had their private key compromised. Digital certificates require a Certificate Authority (CA). A CA is a trusted third party who can vouch for the identity of people or systems. A CA is a defense against "man-in-the-middle" spoofing attacks during key exchanges.

IKE uses the industry standard X.509 certificate format. When someone initiates an IKE exchange with the VPN gateway or responds to one, the user signs the data first with their digital signature key. The gateway then checks an LDAP server and requests the certificate belonging to that user and verifies the certificate signature against the CA's signature. Then the gateway checks the person's signature that is part of the certificate and then checks the data that was signed. This whole process is done in the background and automatically.

Pre-Shared Secret

Pre-shared secrets are passwords. They are easy to deploy when used on gateway to gateway devices and in small numbers. For two points to communicate successfully, they must each know the same shared secret. But scaling to a large number of individual users can be a very large administrative and management task. Passwords, while inexpensive, are also weak as they are easily guessed, stolen or compromised.

It has been practice by some to deploy the same key for all users, but if there would be a

compromise of the pre-shared secret then a new secret would have to be created and all users would have to be notified of the new secret. This would lead to loss of productivity and user frustration with the system.

If you are going to deploy IPSEC using pre-shared secret(s), then policies are a must in dealing with this type of authentication method. Policies should be established to determine:

- how many characters and how complex the pre-shared secret should be.
- who is responsible for the exchange of the pre-shared secret.
- how the pre-shared secret will be exchanged.
- how often the pre-shared secret will be changed.
- if this exchange is by phone, how do you verify the person on the other end.
- how will each location deal with employee turnover. If the VPN tunnel is set up between two different organizations, what is the process of re-verifying employees identity who is responsible for supporting pre-shared secret changes.

Extended Authentication (XAUTH)
Xauth is an Internet draft for the purpose of leveraging legacy authentication methods (LAM). This would allow third-party authentication services such as RADIUS and SecurID within the IKE protocol. The concern with this protocol is that it offers a change to IKE, which may leave the protocol insecure.

You can follow the process of this draft at: http://www.vpnc.org/draft-beaulieu-ike-xauth

Hybrid Authentication
Hybrid authentication allows users to utilize existing third-party authentication services such as RADIUS and SecurID. The Hybrid Authentication uses the digital certificate on the gateway server. The client uses challenge/response authentication.

You can follow the process of this draft at: http://www.vpnc.org/draft-zegman-ike-hybrid-auth

Challenge/Response Authentication of Cryptographic Keys (CRACK)
CRACK requires only a certificate on the server. The client may use a Xauth or Hybrid authentication method such as RADIUS or SecurID tokens or username and passwords. The server authenticates to the user using certificates. The user authenticates to a LAM service. Security properties of IKE are retained.

You can follow the process of this draft by searching on D Harkins, B Korver, D Piper, "IKE Challenge/Response for Authenticated Cryptographic Keys", draft-harkins-ipsec-ike-crack-00.txt (work in progress).

Pre-IKE Credential (PIC)
This proposed protocol would allow IPSEC authentication by an Authentication Server (AS) and third-party protocol such as RADIUS. The client authenticates to the AS using a key

exchange protocol where only the server is authenticated, and the derived keys are used to protect the legacy user authentication. The AS then provides the client with IKE compliant credentials, which can be used to then authenticate to an ISPEC gateway. PIC is favored, as it requires no modification to IKE.

You can follow the process of this draft at: http://www.vpnc.org/draft-ietf-ipsra-pic

What is Strong Authentication?

You have now seen the different options for authenticating devices and users within IKE. If digital certificates and pre-shared secrets is not an option for your organization due to cost, administration, management, then it is nice to know you can look at other solutions for authenticating to an IPSEC VPN. And possibly you already have an authentication method in place such as SecurID.

You will want to avoid passwords as used in pre-shared secrets, as they are the weakest form of authentication. Passwords are subject to being stolen, guessed, or brute force attacked. You want to look toward strong authentication methods that you can use within IPSEC.

Strong Authentication is the using of two or more of the following methods of identifying an individual or device and is critical to maintaining security of your network. When considering authenticating to your network through a VPN, you should consider some form of strong authentication.

- Something you have - smart card or token
- Something you know – password or PIN
- Something you are – fingerprint or biometrics

All of the authentication methods listed above, with the exception of pre-shared secret, can use solutions that are based upon strong authentication. These new proposed authentication methods enhance the security in the VPN when used with strong authentication.

- Digital certificates take something you have - private key and something you know - pass phrase. This solution coupled with complex passwords is a good solution. Digital certificates can also be located on a smart card.
- SecurID - Something you have - token or smart card and something you know - PIN number.
- Biometrics - Something you are - fingerprint to authenticate to something you have - digital certificate.

Which authentication do you use with which VPN solution?

Digital Certificates

- A gateway to gateway VPN scales very well using digital certificates. Instead of keeping track of a separate key for each tunnel device, each tunnel device in the VPN only has to keep track of its own key pairs. Some gateway solutions provide a mini-PKI to allow you to setup a CA and issue certificates to VPN gateways.
- Client to server scale very well using digital certificates as well. These digital certificates can reside on the PC or on smart cards.

Pros

- Strong Authentication
- Key pairs generated and kept on a smart card are more secure as they never leave the card. Combine smart cards and two-factor authentication and you have a very secure solution.
- Scalable

Cons

- The weakest link to using digital certificates is the location of the key pairs and especially the private keys. If these keys reside on the PC then it runs the risk of being compromised due to the lack of security on the PC. Private keys that are kept on the PC are more likely to use a pass phrase to unlock the key. This pass phrase is subject to keyboard monitoring, remote access Trojan attacks, being stolen and brute forced attacked.
- A downside to smart cards is deploying the smart card readers. There is a level of complexity and administration overhead with maintaining the reader software and hardware on every device that connects to you.

Hybrid Authentication, Xauth, CRACK, PIC

The newly proposed authentication methods are to be used by remote users. There are no card readers to install, no foot print on the PC. Solutions using SecurID are flexible, scalable and you have strong two-factor authentication.

Pros

- Client to server scale very well using SecurID tokens and RADIUS. Especially if users are already accustomed to using these forms of authentication.
- You can use SecurID and RADIUS to authenticate to other business application.
- SecurID privdes strong authentication

Cons

- Expense of token systems

Conclusion

VPNs are only as secure as the protocols, size of encryption keys, key management and authentication chosen. Strong authenticating to the VPN is a must to identify who is accessing your network and systems remotely. By using strong authentication, one can control access to resources, create user accountability and a reliable audit trail. Combine a strong authenticated VPN with a firewall and you have a good method of controlling access to the VPN.

There are four new proposed methods of authentication that help leverage existing or newly purchased strong authentication systems. You are no longer limited to pre-shared secrets and digital certificates anymore if using IPSEC like I was in the beginning.

Strong authentication is a must for good access control to a VPN, but we can not forget about information security in layers. You combine good VPN standards and perimeter defenses along with a good security policy for accessing your network and systems, good procedures, and client-side security such as virus software and a personal firewall and you are going to be more confident as to who is on the other end of your VPN. You won't have to ask who's there anymore.

References:

1 Beaulieu, S. Pereira, R. "Extended Authentication within IKE (XAUTH)." Cisco Solutions. Internet draft: <draft-beaulieu-ike-xauth-02.txt>. October 2001. URL: http://www.vpnc.org/draft-beaulieu-ike-xauth.

2 Crume, Jeff. "Inside Internet Security, What Hackers Don't Want You To Know." Addison-Wesley. 2000. 102-122, 132, 243-251.

3 Greene, Tim. "Standards work should reinforce VPNs." Network World, Nov. 5, 2001. URL: http://www.nwfusion.com/news/2001/1105specialfocus.html.

4 GTE Internetworking International. "IPsec VPNs with Digital Certificates: The Most Secure and Scalable Approach to Implementing VPNs." 1999. URL: http://www.firstvpn.com/papers/gte/GTE%202.pdf

5 Harkins, Dan. "CRACK: The new VPN authenticator." Network World. May 28, 2001. URL: http://www.nwfusion.com/news/tech/2001/0528tech.html

6 Intel. "How do I design and build a secure web site and network? Building a secure e-business: the case for strong user authentication." 2001. URL: http://www.intel.com/eBusiness/technology/implement/2/hi15012_p.htm

7 Litvin, M. Shamir, R. Zegman, T. "A Hybrid Authentication Mode for IKE." Check Point Software. <draft-zegman-ike-hybrid-auth-00.txt>. June 2001. URL: http://www.vpnc.org/draft-zegman-ike-hybrid-auth

8 Macleod, Alan. "Protecting the 'private' in VPN." Network World. Sept. 27, 1999. URL: http://www.nwfusion.com/news/tech/0927tech.html

9 RSA Security. "Implementing a Secure Virtual Private Network." 2001. URL: http://www.rsasecurity.com/solutions/vpn/whitepapers/ISVPN_WP_0501.pdf.

10 Schneier, Bruce. Secrets & Lies, Digital Security in a Networked World. John Wiley & Sons. 2000. 193-194, 135-150.

11 Scott, Charlie. Wolfe, Paul. Erwin, Mike. Virtual Private Networks, Second Edition. O' Reilly & Associates, Inc. 1999, 1998. 6, 23.

12 Sheffer, Y. Krawczyk, H. Aboba, B. "PIC, A Pre-IKE Credential Provisioning Protocol." Microsoft. <draft –ietf-ipsra-pic-04.txt>. November 2001. URL: http://www.vpnc.org/draft-ietf-ipsra-pic

13 Silvia, Lori. "Simplify PKI with Hybrid Auth, Xauth." Network World, Aug. 28, 2000. URL: http://www.nwfusion.com/news/2000/0828tech.html