VPN Security and Methodology

Jason L Outen

East Carolina University

VPN Security

In this paper I will discuss what VPN's (Virtual Private Network) are and how they are best utilized by organizations and their personnel. I will include a timeline of the birth of the VPN up to its current state today to show the history of the concept and application. Then I will move on to discussing the various types of VPN's and their differences. This will include the topologies and implementations involved in constructing the VPN's. I will then delve into the myriad of security measures involved with VPN technologies ranging from protocols, authentication mechanisms, security measures, and certificates. The paper will also discuss the various manufacturers' involved with VPN's, costs of implementation, and the future of the VPN. This will include the current state of VPN technology and the ubiquity in which it is found within virtually all brands of security appliances sold today. The VPN is an often overlooked tool in the security toolbox and is currently a focal point of many compliance standards which may also make an appearance in this paper. Lastly the paper will look at the security risks and issues associated with VPN technologies since the inherent logic behind the VPN is to establish secure connections into networks but also provides a perfect venue for attack, penetration, and ultimately compromises.

What is a VPN

A VPN in essence is a means to use one's Internet connection as a virtual network cable to provide access to resources located on other networks securely and reliably. It is my wish and view that VPN's be used to replace or repurpose the existing insecure nature of the Internet and build it into a more secure model for the future. This would cut down drastically on the volume of theft of confidential data and serve to stifle attack vectors for hackers, by moving data into an encrypted state so that only those intended to read such data can. It is worth mentioning too that while a VPN may offer greater security and confidentiality that it is not foolproof. There are attacks and methods that can be used to break encryption, tear down the virtual constructs, and simply intercept data in the same manner as occurs over non-secure devices. The difference

being that most of the attacks are more complicated and in virtually all instances it takes additional time to decipher the data captured by thieves and eavesdroppers making costs higher for attackers.

Types of VPN's

The typical setup involves a VPN server at the site where the resources are to be accessed, and a VPN client at the location of the site that needs access to remote resources. This setup is referred to as a client to site VPN. Additionally VPN's can be used to share resources amongst two or more sites where two VPN servers connected together to create a secure WAN infrastructure. This setup is referred to as a Site to Site VPN. The "type" of VPN is associated with the protocol and encryption methods used to secure them. A few examples of VPN types are: SSL/TLS (Secure Socket Layer/Transport Layer Security), IPsec (Internet Protocol Security), PPTP (Point-To-Point Tunneling Protocol), IKE (Internet Key Exchange), and L2TP (Layer 2 Tunneling Protocol).

SSL/TLS.

SSL and TLS operate on the terms of CA's (Certificate Authorities) to authenticate that the certificate and encryption keys belong to who they are supposed to. This is the same as visiting an HTTPS website, but instead of using the certificates to secure communications with a single web server the technology is used to encryption transmissions to and from a VPN server or gateway. This does not provide for end to end encryption but rather only secures and encrypts traffic from a client to the target network where resources reside. Standard bit encryption for SSL/TLS is now normally set at 2048 bits to ensure acceptable levels of encryption and security. It is also worthy to mention that SSL/TLS operates at the application layer which makes it easier

to use. The transparency of SSL/TLS makes using VPN's as easy as surfing a secure website and requires little to no user interaction to utilize.

IPsec.

IPsec can be used as an end to end encryption protocol that operates at layer 3 of the OSI model. This leads to more robust security since layer 3 is the transport layer meaning that more information can be encrypted and self-contained authentication mechanisms can be utilized making third party authenticators such as CA's unnecessary. This is accomplished through the use of AH (Authentication Headers) and ESP (Encapsulating Security Payload) to mitigate threats such as MITM (Man in the Middle) and Replay attacks. Since IPsec operated at OSI layer 3 it is a protocol suite and has a counterpart known as IKE that facilitates the actual key exchange and encryption/decryption. Just as all layer 3 protocols, most notably TCP/IP, the actual suite is referred to as IPsec/IKE. IPsec establishes the link and transport while IKE performs the encryption and transmission of the secure packets, in much the same fashion that IP establishes the connections across ethernet cabling while TCP controls the sending/receiving of data packets.

PPTP

Point to Point Tunneling Protocol operates at layer 2 of the OSI model giving it unparalleled granularity in the control of transmissions. Since this layer is the same layer that routers and switches use to negotiate traffic it also allows the VPN to act in the same fashion. This allows for multi-path VPN's or in layman's terms it allows for the routing and switching of encrypted traffic. It also facilitates for the use of authentication mechanisms to ensure the integrity of the data between senders and receivers in much the same manner as IPsec but allows for deeper authentication such as usernames and passwords to better facilitate policy

enforcement through native applications. These application protocols are PAP, CHAP, and MS-CHAP and are mostly used in Microsoft products, but are relatively insecure in and of themselves which can lead to security issues since while the VPN is encrypted user authenticator's most notably PAP sends credentials in clear text. This reflects a poor design model as ample security is available it just simply isn't utilized appropriately.

L2TP

L2TP is a method to reliably construct point to point connections and offers no authentication or encryption on its own. However it can be used to tunnel any protocol suite and is often used in conjunction with IPsec to secure the data within the connections it establishes. This feature allows L2TP to be more flexible as it can adapt security to whatever the need dictates and allows for VPN's to be more like virtual infrastructure instead of a construct that is built at will and makes it a great choice for site to site VPN's. L2TP is the offspring of PPP (Point to Point Protocol) and L2F (Layer 2 Forwarding) and is most commonly used by ISP's to divide existing cabling into virtual cables to provide pathways for multiple other carriers. This is how one carrier is able to send data across the network of another carrier.

VPN Security Methodology

SSL/TLS

SSL/TLS methodology is relatively straightforward and the protocol is built into so many applications natively most notably being web browsers for use in online purchases. In SSL/TLS there is a public/private key exchange that determines the encryption algorithm as well as provides data and client/server authentication via certificate exchange and validation against a certificate authority. The certificate authority is a third party that is trusted implicitly by the client/server using the certificate for validation. This is a two edged sword in that unless the CA

is spoofed, compromised, redirected then the trust is valid but recent attacks against SSL has been from attackers using forged certificates that tricked client/servers into divulging confidential data with attackers whom the security suite deemed legitimate. SSL/TLS encryption is performed using a predetermined algorithm based on RSA or AES as a mass exodus is underway to move from the compromised and vulnerable RC4 algorithm that was once the standard. SSL/TLS reliance and use of CA's is both the main strength and weakness of the encryption suite.

IPsec/IKE

IPsec methodology is strikingly more complicated than its VPN counterparts. It provides authentication, encryption, and tunnel creation from the suite without the need of application support as does SSL/TLS. Confidentiality and authentication is implemented via an AH (Authentication Header) or vie ESP (Encapsulating Security Payload). These create a hash from every packet so that the recipient can determine whether or not the packet has been damaged or altered. An important note to mention that using only AH will not allow NAT (Network Address Translation) to work properly since NAT appliances must alter the packet headers to match public facing addresses with their internal counterparts which would cause the authentication check to fail and those packets to be destroyed. ESP encapsulates the entire packet instead of just adding a header which allows for NAT traversal and the survival of the official header with the hash intact. Encryption algorithms are also user selectable and changeable on a moment's notice which allows for quick responses to encryption compromises. This is a feature that cannot be matched as easily with SSL/TLS since there is a time delay with the resetting of encryption and reissuing of certificates to validate the changes.

PPTP

Primarily only used by Microsoft products today as other entities have migrated to the improved L2TP, PPTP is still fairly widely used since it is built into all Microsoft operating systems. The methodology for it is relatively complicated and an encryption/authentication mechanism has to be selected as it does not natively feature those aspects, it merely constructs the conduit between two entities to generate a virtual cable. Authentication is handled by suites such as CHAP (Challenge Authentication Protocol), MSCHAP (Microsoft Challenge Authentication Protocol), EAP (Extensible Authentication Protocol), or PAP (Password Authentication Protocol). All of which have been compromised and are vulnerable since none of them employ encryption. The solution is to introduce an encryption agent such as PEAP (Protected Extensible Authentication Protocol) or SPAP (Secure Password Authentication Protocol (so that the actual stack looks like this PPTP-PEAP-MSCHAP. You can read it backwards to understand the encapsulation which goes like this Authentication packet (MSCHAP) is encapsulated by the encryption packet (PEAP) which is then encapsulated by PPTP. It is worth mentioning that SPAP and PEAP often use TLS to employ security which means that it is hands free encryption that is decided for the user easing configuration.

Encryption Algorithms for VPN Protocols

There are many notable encryption algorithms available but the most widely and accepted two are SHA and AES. Other algorithms that may be used but not discussed here are; RSA, RC4, DH, DES, 3DES, Blowfish,

SHA-2.

SHA-2 is the replacement of the older encryption SHA based encryption algorithms, it is recommended that no one employ the use of the older algorithms any longer. SHA-2 has a

simple yet computationally complex method to provide encryption. A message to be encrypted is divided into multiple 512bit blocks M1, M2, M3… respectively with the last padded with extra bits as needed to force it to be 512bits long. The equation for encrypting is as follows:

$H^{(i)} = H^{(i-1)} + CM^{(i)}(H^{(i-1)})$; where $H^{(i)}$ is the encrypted message, $M^{(i)}$ is the plain text message, and C is the compression function and the + signs means MOD 2^{32} word sizes. So each hashed message is then added to the next message and so on and so forth. The compression algorithm contains the encryption and outputs a hash value for error checking and authentication. The compression is usually handled by employing XOR (exclusive OR's) or bit shifting to render the original message indecipherable unless you are the intended recipient. SHA-2 has so far never been cracked but as computational power increases in machines the time calculated to crack the encryption has deemed the creation of a replacement algorithm necessary which is dubbed SHA-3 and is proposed to be released for use in 2014.

AES.

AES cipher XOR's works by employing an ECB style cipher. The plaintext message blocks are placed into a row and column format the columns and rows are then shifted. XOR'ng is used with a temporal key that is used on the first block to determine subsequent keys and hide the temporal key from interceptors. AES is not arithmetically difficult cryptography in the $2+2MOD^{32}$ sense but rather relies on a fixed key used to determine how far column and row shifts occur which in turn permutated the key for the next set of XOR and shifts that correlates with adding, subtracting, and multiplying bytes and words as opposed to simply applying functional variables with ready known values. Which consequently makes it computationally quick for encryption and slightly less quick to decrypt. AES can also be utilized as an effective stream based cipher if the ECB mode is altered to OFB.

References

AES encryption. (n.d.). *AES encryption*. Retrieved April 12, 2014, from http://aesencryption.net/

Arora, M. (2012, May 7). How secure is AES against brute force attacks?. *EE Times*, *5*. Retrieved April 10, 2014, from http://www.eetimes.com/document.asp?doc_id=1279619

Cruz, J. (2013, May 7). Keccak: The New SHA-3 Encryption Standard. *Dr. Dobbs*, *4*. Retrieved April 10, 2014, from http://www.drdobbs.com/security/keccak-the-new-sha-3-encryption-standard/240154037

IPsec. (2014, September 4). *Wikipedia*. Retrieved April 12, 2014, from http://en.wikipedia.org/wiki/IPsec

Implementing PEAP-MS-CHAP v2 authentication for Microsoft PPTP VPNs. (n.d.). *Microsoft Support*. Retrieved April 12, 2014, from http://support.microsoft.com/kb/2744850

Mason, A. (2014, April 7). VPNs and VPN Technologies. *ciscopress.com*. Retrieved April 12, 2014, from http://www.ciscopress.com/articles/article.asp?p=24833

Next Generation Encryption. (n.d.). *Cisco*. Retrieved April 12, 2014, from http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Song, S. (n.d.). SSL VPN Security. *Cisco*. Retrieved April 12, 2014, from http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html

Stallings, W., & Brown, L. (2012). Symmetric Encryption and Message Confidentiality. *Computer security: principles and practice* (2nd ed., pp. 623-650). Boston: Pearson.

Tyson, J., & Crawford, S. (2011, April 11). How VPNs Work. *HowStuffWorks*. Retrieved April 12, 2014, from http://computer.howstuffworks.com/vpn1.htm

draft Publications. (n.d.). *NIST Computer Security Publications*. Retrieved April 12, 2014, from http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-52-Rev.%201