Global Information Assurance Certification Paper

Overview of IPSEC
Manageability and Security

IPSEC (Internet Protocol Security) is a method to secure data transmissions between any two hosts. The data path may include one or more secure gateways. The beauty of IPSEC lies in its extensibility to new and stronger encryption and authentication methods. The Internet has always been a medium where information could be shared, but that freedom traditionally came with an associated cost to privacy and security. IPSEC changes the equation. It is now possible to exchange information across the Internet with a reasonable degree of certainty that no one but the intended listener can understand the data flow, while any unintended listener can only determine the origin of a packet and not its destination. IPSEC is not meant as a panacea to all the security exposures prevalent with the use of IP networking, but it can provide a framework to establish secure, authenticated, and reliable communication links. The most frequent use of this technology will be to create virtual private networks, but it can be used for such mundane tasks as encrypting traffic between hosts on the same subnet. Security and manageability affect the choices you make in configuring the Internet Security Association Key Management Protocol (ISAKMP), IPSEC mode, and selected encryption levels.

ISAKMP is the method by which security associations (SA) are formed and the process is independent of the manner in which any keys are passed. The Internet Key Exchange (IKE) defines the manner in which keys are passed. "A security association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely."[2408] "The ISAKMP SA is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication."[2409] A policy set is a defined data flow that looks and acts very much like an enhanced access list found on routers or firewalls. A data flow defines what specific source and destination IP protocol and service port pairs are to be used in a connection. Associated with the data flow in the policy is the type of security encapsulation that is to be used. Authentication Header (AH) and encapsulated security payload (ESP) are the two encapsulation types. AH is used primarily for authentication and anti-replay protection. ESP provides a mechanism where authentication, encrypted data payload, anti-reply services, or a combination of these features can be deployed. A single SA can have AH or ESP but not both. A security association is created in a two-stage process. The first stage in the construction of a security association is concerned primarily with authentication and the exchange of encryption keys. The second stage in building a security association addresses what traffic is to be protected and what encryption method will be used. "A single SA negotiation results in two security associations- one inbound and one outbound."[2409] The security and manageability associated with phase one of a SA is dependent on the authentication method chosen. An IETF implementation of ISAKMP must include pre-shared secret keys, it should include the Digital Signature Standard, and it may include public key encryption. Pre-shared keys are easy to manage for one or two devices since every connection in the SA must use the same key. The shared secret approach is not very scalable and when more than a few devices are in the same SA security can be lost because the key becomes too widely disseminated. Manageability and scalability increases markedly however if you

choose to implement digital signatures or public key encryption. The certificate methods provide a mechanism to quickly build individual SA's for the data flows between many devices with different security requirements.

IPSEC can be implemented in one of two modes. Transport mode is used when two hosts converse directly with each other. Tunnel mode is used when a host converses with another through one or more secure gateways. The fundamental difference between tunnel and transport mode is how the IP datagram is encapsulated. Tunnel mode must encapsulate one or more outer destination headers for use by the destination secure gateways and an inner IP destination header for the intended target. Manageability and scalability become issues when selecting a secure gateway. A secure gateway, if it is used in a large environment, must have the ability to form many types of associations. A VPN gateway may have to accommodate corporate remote users, vendors, business partners, along with the ubiquitous 'others'. Each of these user types has different security requirements and a secure gateway should meet every one or IPSEC may become expensive in terms of equipment and manpower. Access by any or all users may range from unlimited rights on the LAN to specific protocol service ports on designated machines.

Each phase in the creation of IPSEC SA's has an associated encryption level. IPSEC must include the following encryption or hashing methods: Digital Encryption Standard (DES) in cipher block chaining mode, MD5, SHA, and two Diffie-Hellman key sizes. Most implementations of IPSEC include 3DES. The weakest encryption method available, besides none at all, is DES. It has been repeatedly demonstrated that DES is vulnerable to be being cracked; however IPSEC has the ability to limit the life of a security association, so when it expires the SA is renegotiated. A timer can limit SA lifetimes and some implementations allow the lifetime to be set depending on the amount of traffic that passes between hosts. If the SA lifetime is kept sufficiently short DES is still a viable encryption method. If DES is vulnerable and 3DES is available, why choose 3DES? 3DES is computationally extravagant compared to DES. If a hardware encryption card is available for 3DES a similar one can generally be found for DES and the computational advantage of DES still applies. Hardware encryption cards are usually only found on secure gateway devices such as firewalls and routers. The MD5 hash has had an exploit demonstrated against it, however an IPSEC solution can be selected that implements the HMAC variant that has been shown not to be vulnerable to the exploit. As with encryption, the hash methods and Diffie-Hellman key sizes have different computational costs. SHA and the larger key are more expensive than MD5 and the smaller key size. Manageability is not an issue in choosing which encryption method, hash algorithm, and key size to utilize.

Manageability is the overriding concern in choosing which authentication method to use and how many types of users can be supported. In implementations that are going to experience only a few connections from a small number of users a pre-shared secret key

makes sense because the additional expenses of hardware, software and support are not needed for a public key infrastructure (PKI). In a setting where an implementation is going to have to be maintained with numerous users and many conflicting security requirements a PKI may be mandatory. Security is the chief consideration in choosing and implementing which encryption methods, hashing algorithms, and Diffie-Hellman key sizes to select. IPSEC can hide some of the difficulties now being experienced with DES, but the life span of DES is almost complete and AES will soon replace it. The tradeoff with using the components within IPSEC that are generally recognized as being more secure is how expensive they are computationally. If a system is perceived as awkward or slow, especially a security solution, then users will find a way to subvert it. A slow and difficult to use implementation of IPSEC will be of no benefit to the organization that implements it, so great care and consideration should be taken in selecting which IPSEC system to use and how it is configured.

Finally, there are two considerations every large-scale deployment of IPSEC for Internet VPN's must address. The first is extended authentication. Most vendors have included into their implementation of IPSEC the ability to perform additional authentication using RADIUS, TACACS+, biometrics, or one-time authenticators. Use of one or more of these services can make managing users easier and enhance overall security but the added manpower and infrastructure required to support them must be analyzed. The second consideration, which is possibly the most immediate security exposure to IPSEC, is how to protect a host computer that builds a VPN to a secure LAN from an exposed position on the Internet. Laptops and wide-band home users are going to be using IPSEC VPN's and how are you as a security professional going to prevent someone from hacking their machines in order to gain entry to your LAN? It appears the only solution is some type of personal firewall. IPSEC can protect a communication channel while it is in place, however it cannot protect a device that has already been compromised or prevent the exploitation of communications outside of the traffic defined in the SA. The configuration and management of a large number of remote firewalls should make everyone reflect long and carefully on how to implement IPSEC as a piece in a complete remote access solution.

References

Cisco Secure VPN Client Solutions Guide
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/index.htm

VPN-1 SecuRemote: Secure Virtual Network Architecture
http://www.checkpoint.com/products/vpn1/securemoteds.html

Etranet VPN: Extranet Security Manager Product Brief
http://www.hp.com/security/products/vpn/papers/brief/

[2401] Kent & Atkinson. "Security Architecture for the Internet Protocol". RFC 2401. November 1998.

[2408] Maughan, Schertler & Turner. "Internet Security Association and Key Management Protocol". RFC 2408. November 1998.

[2408] Harkins & Carrel. "The Internet Key Exchange". RFC 2409. November 1998.