VPN SECURITY

N.RUBA*
DR. M.KARTHIKEYAN**

*Ph.D., Research Scholar, Himalayan University, Arunachal Pradesh, India
**Head, Dept of Computer Science, Kandasamy Kandar’s Arts and Science College, P.Vellur, Namakkal, Tamil Nadu, India

ABSTRACT

Because the Internet facilitates the creation of VPNs from anywhere, networks need strong security features to prevent unwelcome access to private networks and to protect private data as it traverses the public network. After all, companies that have expectations of privacy over their own networks have the same expectation when the Internet is involved. Unfortunately, as data travels between users and their remote offices, it can pass through 25 or more different servers around the world before reaching its final destination. With so many potentially prying eyes, the data should be secured through some form of encryption.

KEYWORDS: Encryption, Cryptosystems

ENCRYPTION

A key component of a VPN solution is providing data privacy. Without an explicit way to provide data privacy, information traveling over an unsecured channel like the Internet is transmitted in clear text. Data transmitted in clear text can be viewed or even stolen through common “sniffing” programs and/or devices that monitor data traveling over a network. Tools such as a protocol analyzer or network diagnostic tools built into today’s operating systems can easily “see” the clear text information as it is transmitted. Companies are also concerned that some private data may not be encrypted by the VPN before it is transmitted on the public wire. IP headers, for example, will contain the IP addresses of both the client and the server. Hackers may capture these addresses and choose to target these devices for future attacks.

To ensure data privacy and protect valuable transmitted data against “man-in-the-middle” attacks, encryption techniques are required to scramble clear text into cipher text. Encryption scrambles a message into cipher text. The cipher text is then sent to the recipient, who decrypts the message back into clear text again [8]. This encryption/decryption process on the parts of the sender and receiver of the message combine to form a cryptosystem.

www.jiarm.com
There are two types of cryptosystems:

- **Private key cryptosystems:**
- **Public key cryptosystems:**

**Private Key (Symmetric) Cryptosystems**

A private key cryptosystem uses the same secret, fixed-length bit string as a key for both encryption and decryption. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the private key.

![Private Key Cryptosystems Diagram](image)

Figure 1 shows an example of how data flows in a private key cryptosystem. In this example, the originator encrypts the message “abc” using the secret key, transforming it into “!&#”. Anyone that has the same secret key can then decrypt the message “!&#” back into the original message of “abc”. Some common symmetric encryption algorithms include:

- **Data Encryption Standard (DES)**
  - DES takes a 64-bit block of data and a 56-bit key and produces a 64-bit block of encrypted data.

- **RC4**
  - An alternate to DES that uses the same key to scramble and descramble packets. RC4 uses either 40- or 128-bit encryption and is approximately 10 times faster than DES.

- **Triple-DES (3-DES)**
  - An even more highly sophisticated encryption mechanism that uses three keys instead of one, thereby providing a much higher level of security than DES. Each of these algorithms differs in bit length (or "strength"). The strength of the algorithm establishes the amount of effort required to break the system. The longer the bit length, the “stronger” the encryption algorithm and the greater the effort
required to break the system. A private key cryptosystem suffers from the following drawbacks:[5]

- Since the “secret key” is used for both encryption and decryption, anyone who steals the key can steal all the data that is currently or had already been encrypted, jeopardizing all present and past communications using the shared key.
- Because of this danger, the keys must be delivered in a protected manner such as a direct face-to-face negotiation or a telephone call exchange. Since the privacy of all data communications is based on the integrity of the secret key, it is important to replace keys periodically. Replacing keys on a frequent basis presents hackers with a very small window of access to the system, thereby providing a greater level of privacy.

Public Key (Asymmetric) Cryptosystems

A public key cryptosystem uses a pair of mathematically related keys:[18]

- A private key that is kept secret within the system, and
- A public key that can be made known to the public.

Because one of the two elements, the public key is made available to the general public, the initial creation and exchange of a “shared secret key” that is used for secure communications can be accomplished more easily than with a private key cryptosystem. Two public key cryptosystems that are commonly used within VPN solutions today are Diffie-Hellman (DH) and Rivest Shamir Adlemen (RSA).

Figure 2 shows an example of a private key (symmetric) cryptosystem.[5]
USER AUTHENTICATION AND ACCESS CONTROL

Up to this point, discussed about the encryption aspects of VPNs. Equally as important is the process of ensuring that users are who they are. The following sections describe the steps taken to address and resolve these security concerns.

Internet Protocol Security

Internet Protocol Security (IPSec) is a framework of open standards developed by the Internet Engineering Task Force (IETF) to ensure data privacy, data authentication, and user authentication on public networks. It is a robust standard that has withstood extensive peer review and emerged as the clear industry standard for Internet VPNs. One of the advantages of IPSec is that it operates at the network layer, whereas other approaches insert security at the application layer. The benefit of network layer security is that it can be deployed independently of applications running on the network. This means that organizations are able to secure their networks without deploying and coordinating security on an application-by-application basis.

Data and User Authentication

Data authentication methods can be used to verify that communications have not been modified in transit. With user authentication, the identity of the remote user must be verified before that user is granted access to the corporate network. With this method, unauthorized individuals are denied access to the network. This process is arguably the most important element of any VPN solution.

There are a number of user-authentication methods. These include:

- **Pre-shared secrets**
  
  Pre-shared secrets are passwords that are distributed to users “out of band,” or independent of the VPN technology infrastructure. They offer an easy way to deploy VPNs quickly to a limited number of remote users. However, shared secrets do not provide robust scalability for large remote user environments.

- **Digital certificates**
  
  Digital certificates are electronic credentials for proving user identity. These electronic credentials can be stored on the remote computer or on tokens carried by the user. Management of digital certificates, including distribution and revocation, is automated by a
Public Key Infrastructure (PKI). PKIs offer a stronger and more scalable authentication infrastructure than shared secrets, but are more expensive and complex to deploy.

- **Hybrid Mode Authentication**

  Hybrid Mode Authentication allows organizations to integrate legacy authentication schemes such as Secure ID, TACACS+, and RADIUS with VPNs. Without Hybrid Mode Authentication, these schemes must be replaced by shared secrets or digital certificates to deploy a VPN, which can be a complex and costly process.

**CONCLUSION**

Whenever there are competing protocols for a certain application, the most obvious question that arises is what protocol is best suited in a certain scenario? In the case of VPN security protocols, there are three major protocols and a company or an individual trying to install a VPN solution would be faced with this question. Unfortunately, there is not one single “magic” answer to this question. The protocol selection depends on various factors. As a conclusion in this report, some pointers that can assist in this selection process are discussed. The protocols running on the internal network of the company, looking for a VPN solution, will play a major role in this decision. This is because IPsec and other VPN protocols are not compatible with every other protocol. NetBEUI or IPX/SPX-based networks will have a limited number of options if VPN solution requires those packets to be tunneled to another site, in this case, best bet would be to go with either PPTP or L2TP.

**BIBLIOGRAPHY**

5. Network Magazine Title: “SSL VPNs driving remote Networking ” – volume no. 7 February 2004 , page no: 14