ELECTRON GOVERNMENT AFFAIRS SYSTEM BASED ON VPN TECHNOLOGY

CHIH-YAO LO

Department of Information Management, Yu Da University

E-mail: jacklo@ydu.edu.tw

ABSTRACT

In the course of carrying out its mission the primary challenge facing e-gov is how to deliver secure online services to businesses and citizens. For this paper, the Virtual Private Network (VPN) will be the solution selected to deal with this challenge. VPN can resolve these issues by simplifying and speeding the delivery of on-line services and information to citizens, businesses, and inter-agencies safely and securely. The following paper is organized into seven sections: I) a brief introduction to e-gov; II) security and privacy of e-gov; III) Real World Case: Ontario, Canada; IV) VPN Technology and Network Security Protocols (VPN tunneling and VPN tunneling protocols through a look at their capabilities, advantages, and disadvantages); V) VPN Authentication, to include two-party and trusted third-party authentication and their capabilities, merits, and limitations; and VI) conclusion.

Keywords: *E-government, VPN, Secure, Online, Service*

1. A BRIEF INTRODUCTION OF E-GOV

In terms of providing services over the Internet, the concept of e-government (or e-gov) is very similar to that of e-commerce. Yet there are clear and important differences. What then exactly is e-gov? E-gov refers to a government's use of electronic technology – such things as the Internet, intranet, extranet, databases, decision support systems, surveillance systems, etc. – to formulate interaction between itself and its various agencies, citizens, and business enterprises in better and more efficient ways [14]. Thus, briefly stated, the aim of e-government is to facilitate interaction amongst three relationships: government and citizen (G2C), and government and business enterprises (G2B), and government and internal and external agencies of that government, i.e. government and government (G2G).

The goal of this new form of government is to augment convenience, decrease corruption and the opportunity for it, increase operational transparency, and to provide better and more efficient services and cost benefits to citizens, business enterprises, and internal and external agencies [14]. The electronic transactions and interactions between government and these three groups should be separate and be handled very

carefully. Before proceeding further, this section will briefly discuss the three major relations maintained by government.

A. Government and citizen (G2C). This deals with the relationship between government and the citizens it ostensibly serves, whether this be at the national or local level. E-gov allows government agencies to communicate with its citizens via a public network infrastructure such as the Internet. Furthermore, it also allows citizens to access public information and services instantly, conveniently at from anywhere and anytime that they can secure the necessary connection [13].

B. Government and Business Enterprises (G2B). G2B refers to the electronic interaction between the government and private businesses or organizations. This category allows electronic transaction initiatives, such as electronic procurement and the development of an electronic marketplace for government [13]. Furthermore, this G2B electronic communication will potentially help businesses to reduce costs and become more competitive [13].

C. Government and Government (G2G). This refers to the relationship between governments and other internal and external government agencies. This relationship will allow government departments and agencies to share databases, resources, and enhance the overall efficiency and effectiveness of their mission. It will make it easier for states and localities to meet reporting requirements and participate as full partners with the federal government in citizen services, while enabling better performance measurement, especially for grants. Other levels of government will potentially see significant administrative savings and will be able to improve program delivery due to the availability of more accurate data in a more timely fashion [13].

2. SECURITY AND PRIVACY OF E-GOV

Security and privacy constitute basic essentials for the successful functioning of e-gov. It is vital to its operations that a government protect the confidentiality of sensitive information belonging to citizens, businesses as well as its own operations while transporting it over a public telecommunications network. In other words, e-gov must guarantee the safe and reliable handling of crucial information while transporting it over the public telecommunication and be vigilant against the threat of cyber attack. Cyber attack is defined as any event or activity – deliberate or not – that has the potential of harming an IT system, any activity that involves unauthorized access to a private network or networks, and the access to or theft of classified information, even if traversing a public infrastructure network. This section will discuss the common issues of security and privacy.

Most government departments depend on email or network access for internal communication or to communicate with external government agencies. Therefore, it is important that email communications be secure. In many cases email that travels within an agency also traverses the Internet as it moves from one site to another, and

there is no assurance that the contents of a received email have not been altered. Therefore, it is important to implement a security solution to enable content scanning and virus scanning on encrypted messages. One of the solutions is to encrypt and digitally sign email messages [7]. This can ensure the privacy of email content and attachments, identify the email sender and recipient(s), and verify that an email message has not been tampered with in transit [7].

Furthermore, as e-gov expands, contractors and businesses will need to require secure access to agency networks. Agencies often need secure connections between remote sites. The common solution for this is to implement remote access VPN technology. Remote access VPNs enable user authentication and protect the data flow between the government network and its clients. Authentication may be accomplished via many different ways, which will be discussed later in this paper.

The Government Paperwork Elimination Act requires a significant paperwork reduction by all US federal agencies by October 2003 [7]. For this reason, many government agencies have turned to e-form. However, agencies must ensure the information on the e-form cannot be altered while also securing on-line form submission and delivery. Implementing digital signature technology will ensure information on e-forms is authentic and has not been tampered with. In other words, the contents of the form are fully protected with encryption during transmission and storage, and the identification of any government employee accessing the form's information is both authenticated and authorized to ensure privacy. Further, a digital signature also ensures the accountability of the submitter [7].

According to Entrust [7], one of the greatest challenges facing government in the delivery of on-line services is providing the privacy of information elicited from citizens, businesses, and other government agencies. Without that privacy, constituents and those doing business with government will not trust on-line services. In order to be successful e-gov must ensure the privacy of data is protected from end to end. End to End security means information remains confidential regardless of where it resides.

3. REAL WORLD CASE: E-GOV (ONTARIO, CANADA) IMPLEMENTS VPN SOLUTIONS

The Justice Department of Ontario (JDO) allows most of its attendant agencies to share criminal profile information, such as arrest records, personal information, fingerprints, photographs, etc. In order to protect such sensitive information, JDO uses the VPN solution offered by Nortel of Brampton. This solution allows only authorized users access to the system, and most importantly, it also ensures the privacy and security of the information and data being transported over the public network. The major merit with this VPN solution is that it also allows JDO to collect, store and transmit information to other agencies, such as the Drug Enforcement Administration, the Immigration and Naturalization Service, etc.

Nortel utilizes a full array of industry leading network components and equipment to provide high levels of security, flexibility, and reliability to

its e-gov solution. The components include Alteon* SSL VPN gateway, which provides secure remote access to web, clients, server, and mainframe application from any browser-equipped device. Services Edge Router 5500 (SER 5500), which is the platform that delivers network based IP-VPN service on either MPLS or conventional IP network, also provides a rich mix of IP services, security, traffic management, and quality of service (QoS) capabilities [14].

Furthermore, Nortel has also implemented its Nortel Network Multiservice Switches (MSS 7400, 15000, 20000) into the VPN solution. These switches provide a reliable IP-VPN service including rich mix of Layer 2 (ATM, FR, Ethernet), and "voice services as well as handling overlapping IP addresses in converged networks and simplifying the provisioning of multiple services on a single process" [14]. Implementing a VPN solution enables the JDO to conduct its transactions faster, more securely, and also more cost effectively than before. The following section will discuss the benefits of this solution.

A. Benefits of the VPN solution

VPN solution allows the JDO to simplify their business reporting, and most importantly to share information about criminals in a secure way. Furthermore, it provides a high level of security for extranet and intranet used for transactions among government departments and agencies, businesses, and citizens [14]. In addition, VPN solution also offers high-level network security capabilities, such as firewalls and denial of service protection to anti-spoofing, network address translator (NAT), end to end encryption capabilities, intrusion detection, etc. and applies them on a per-user basis [14]. JDO also enjoys the advantages of VPN tunneling options, including both virtual router based (RFC2764) and MPLS based (RFC2547). " Enjoying secure remote access options using IPSec client software or a "clientless" approach invoked with the SSL capability of deployed web browsers" [14]. All in all, VPN solution increases productivity and network security.

4. VPN TECHNOLOGY

A. A Brief Introduction to Virtual Private Network (VPN)

With the growth in popularity of the Internet many governments or government departments, organizations and enterprises have turned to it as a more cost effective way of extending their networks. The continuing popularity of the Internet has led to the evolution of the Virtual Private Network (VPN). VPN is a combination of software and hardware providing users with the ability of using an unsecured network to establish a secure private connection with a host network [17]. In other words, VPN uses a public telecommunication infrastructure like internet to connect from remote offices or individual users to a secure access to their organization's network, and enables users to send or receive sensitive data securely over public or shared networks such as the Internet.

VPN technology provides organizations a quick, inexpensive, and secure way to transmit their data across the nation and the world. Because of it flexibility, many government departments and organizations can easily communicate with other agencies and customers in a secure and cost

effective way while maintaining control and ensuring security. In other words, VPN gives government departments and organizations the same capabilities as private leased lines at much lower cost by using public or shared infrastructure. The most common VPN architectures can be divided into 3 common scenarios: (1) site-to-site intranet VPN, (2) remote access VPN, and (3) extranet VPN.

Site-to-site intranet VPN. In this scenario, multiple network sites located at different geographical locations within the same organization are connected using a VPN. Each site can have multiple IP sub-networks that form a corporate intranet. A VPN is used to interconnect these sites to form a single large corporate intranet [20]. In the case of e-government, it allows a given government department and its multiple facilities to intercommunicate using the intranet VPN. Therefore, each location will have VPN devices implemented.

Remote access VPN. In this case, the VPN is used to connect a single remote network device to the corporate intranet. This single network device can be a portable computer accessing the network via the telephone network or a telecommuting computer accessing the network via a cable modem, DSL, or some other form of connectivity [20]. Remote access VPN works particularly well (and is particularly vital) for the operations of government law enforcement agencies, such as the police department or the Federal Bureau of Investigation, the main reason being it allows law enforcement officers remote access to the system via an unsecured network. In other words, remote access VPN enables secure information and sharing among all law enforcement agencies in the nation. The VPN solution allows the secure authentication of users, data encryption, secured email and information, and the digital signature of documents and communications.

Extranet VPN. In this scenario, network resources within one government department are opened for access to other agencies for various purposes, such as criminal reports, individual background check, etc. Such access differs from the intranet case in that it spans multiple administrative trust domains, and different types of resources are opened for departments' multiple agencies.

5. VPN TUNNELING PROTOCOL

In the terminology of the virtual private network "virtual" refers to tunnel and "private" refers to security. Just as the name suggests, VPN technology is based on tunneling protocol and security procedures to maintain the privacy and security of the data while transporting sensitive data using the public telecommunication infrastructure [1]. In other words, VPN creates secure connections called tunnels through public shared network, such as the Internet. These tunnels are not physical entities but logical constructs created using encryption, security standards, and protocols. The following section will discuss in more detail the VPN tunneling and its protocols, such as Point-To-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), Internet Protocol Security (IPsec or RFC), and Multiple Label Switching (MPLS), and follow by VPN security.

A. VPN Tunneling

Tunneling is use to transport a packet created by one protocol through a network comprising another protocol. In other words, it encapsulates the original packet within another packet. For instance, "to transport an Internetwork Packet Exchange (IPX) packet over the internet the IPX packet could be encapsulated within an Internet Protocol (IP) packet. At the destination, the IP header is removed and the IPX packet is delivered natively to the destination" (Izzo, 2000, p274). However, before the packet is encapsulated an important process of authentication, encryption, and compression needs to followed through (Izzo, 2000). The purpose behind this is to make it possible for the VPN tunnel to transport data across an unsecured network or public telecommunication infrastructure in a secure format. Furthermore, both ends/sites need to use the same tunnel protocol in order for the tunnel to function. There are two different VPN tunnel types: voluntary and compulsory.

Voluntary Tunnel. A voluntary tunnel requires clients have the ability to manage their own VPN tunnel. In other words, the client first needs to secure a connection to the carrier network provider (CNP) or Internet service provider (ISP), such as a local dialup ISP, digital subscriber line (xDSL), cable modem service, etc. Then the client application creates the tunnel to a VPN server over this connection. This configuration is particularly advantageous for a mobile workforce because the mobile/roaming users never know the source of their network connection (Izzo, 2000). Furthermore, a voluntary tunnel is also useful for telecommuters, especially if they are not physically located in the same geographic region. They can use any ISP and avoid direct long distance dialing to the corporate network.

Another advantages are that the VPN server does not necessarily have to be a router (it could be a web server or a workstation), and a voluntary tunnel is fairly easy and quick to set up [15][1]. But with every advantage there is always a disadvantage. The main disadvantage of the voluntary tunnel is that the user's computer must be equipped with special software to manage its own VPN [1]. Sometimes the deployment of this tunnel can be difficult or burdensome, especially adding it to a laptop that has already been deployed. The main reason is that the VPN client has to be nestled deep within the operating system, which can cause conflict with pre-existing services on the client's machine [15].

Compulsory Tunnel. The compulsory tunnel is just the opposite of the voluntary tunnel, and is also known as a mandatory tunnel. A compulsory tunnel is completely transparent to the end user [15]. The carrier network provider (CNP) or Internet service provider (ISP) manages the VPN connection. In other words, when the client first connects to the CNP or ISP, the CNP or ISP will in turn immediately broker a VPN connection between the client and a VPN server. This type of tunnel does not require the installation of special software on the devices on either side of the network, and it is also does not require reconfiguration in order to use the VPN. In other words, no client configuration is needed as long as the clients use the same ISP [15]. Furthermore, this type of tunnel is frequently used in all types of

VPNs: remote access, Intranet, Extranet, Voice, and enterprise VPNs [15].

B. VPN Tunneling Protocols

There are several widely used VPN tunneling protocols, such as Point-To-Point Tunneling Protocol (PPTP), Layer Two Forwarding Protocol (L2F), Layer Two Tunneling Protocol (L2TP), Internet Protocol Security (IPsec), and Multiple Label Switching (MPLS). Only IPSec, PPTP, L2TP, and MPLS will be discussed in this section.

Internet Protocol Security (IPSec or RFC2401). IPSec is a set of authentication and encryption protocols defined by the Internet Engineering Task Force (IETF) to secure communication at layer 3 (OSI standard network layer) between communicating peers. Layer 3, or network layer, is the lowest layer that can provide end to end network connectivity, therefore it requires that security measures be offered within IP [20]. Unfortunately, the Internet Protocol version 4 (IPv4 or RFC791) does not provide a built-in security mechanism. Therefore, the additional protocol and procedures are necessary. IPSec is designed to provide interoperable, strong cryptography based security for IPv4 or IP based networks [20] [15].

Furthermore, IPSec are also designed to address data confidentiality, integrity, authentication, and key management, and can operate as a compulsory or voluntary tunnel [17]. Because IPSec can be operated as either a compulsory or voluntary tunnel, just like other technologies, it must be agreed upon prior to the actual use of the protocol. According to VPN consortium, the IPSec typically works on the edge of a security domain, and IPSec encapsulates a packet by wrapping another packet around it. This is followed by encrypting the entire packet and this encrypted stream of traffic forms a secure tunnel over the public telecommunication infrastructure or unsecured network. The security protocols used in IPSec are Encapsulating Security Protocol (ESP or RFC2406) and authentication header (AH or RFC2402).

ESP primary provides confidentiality for IP traffic, such as authentication, data confidentiality through encryption, and optional anti-replay protection for IP packets [10]. The current standards for the IPSec encryption algorithm are Triple Data Encryption Standard (3DES), International Data Encryption Algorithm (IDEA), and the Advanced Encryption Standard (AES). These algorithms will be discussed in the next section.

AH provides per-packet authentication, which is data integrity and data origin authentication for the IP payload. In other words, the AH protocol makes sure that the data delivered within the IP packet is authentic and that it arrives at the destination without modification [10]. In order to do this, the AH includes a cryptographic checksum over the entire packet, and the receiver can use this checksum to verify that the packet has or has not been modified. ESP and AH can be used separately or together, depending upon whether the IPSec mode is the transport mode or tunnel mode. Usually, a client to local area network (LAN) connection uses the transport mode, while LAN to LAN connection uses the tunnel mode [10].

Furthermore, although the ESP and AH protocols specify how the data security services

should be applied to each IP packet, they do not tell how these security associations (SA) are actually negotiated. SA is central to IPSec. SA defines the kinds of security measures that should be applied to packets based on who send them, where they going and what types of payload they are carrying. SA can be manually configured by the system administrator or can be dynamically negotiated via a key management protocol such as Internet Key Exchange (IKE, or RFC2409 IKE, which is based upon the framework defined by the Internet Security Association Key Management Protocol [ISAKMP or RFC2408]). ISAKMP defines how the procedure by which the two communicating peers can secure the communication channel between them. In other words, ISAKMP provides the means for two peers to authenticate one another, exchange key management information, and negotiate security services (Yuan & Strayer, 2001). The main benefits provided by IPSec VPN technology is the tremendous saving cost over private wide area network connection, leased lines, or long distance phone charges. It has control over either granting or restricting network access to citizens, or internal or external agencies.

C. IPSec VPN Challenges

The major challenge of IPSec VPN is the hardware for the service providers and for organizations deploying IPSec VPN. These days it continues to have significant technical issues [10]. For instance, “the dynamic nature of IPSec implementation requires IPSec gateway vendors to continually verify their implementations' compliance with standards to ensure correctness and interoperability” [10]. Furthermore, the performance and scalability must also be constantly upgraded and verified to satisfy the growing needs of the IPSec VPN industry. For instance, the managed service providers and network managers must deal with the impact of IPSec VPNs on the performance of applications across the network, and with the interoperability of network elements and services in a multi-vendor environment.

Point-To-Point Tunneling Protocol (PPTP or RFC2637). The purpose of PPTP is to specify a protocol that encapsulates point-to-point (PPP) packets inside an Internet Protocol (IP) packet. It can be divided into two components: the transport (making the virtual connection) and the encryption (making it private). PPTP is developed by a consortium of vendors such as Microsoft, 3Com, ECI Telematics, Ascend, and Copper Mountain Networks. PPTP is one of the most popular protocols due to its easy configuration and low cost. It was the first VPN protocol supported by Microsoft dial-up networking [11].

Layer Two Tunneling Protocol (L2TP or RFC2661) acts as a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over a public network such as the Internet. L2TP is the standard of Internet Engineering Task Force (IETF), and it combines two of the best features of existing tunneling protocols: Cisco’s Layer 2 Forwarding (L2F) and Microsoft’s PPTP (Microsoft, 2000). L2TP encapsulates PPP frames to be sent over IP, X.25, frame relay, or asynchronous transfer mode (ATM) networks. L2TP offers the following benefits: vendor interoperability, potential use as part of the wholesale access solution, allowance of

ISPs to the service providers, offering VPNs to ISP and other service providers, and its potential to be operated as a client-initiated VPN solution.

Multiprotocol Label Switching (MPLS). The main purpose of MPLS is to reduce the amount of processing required at each router to forward a packet [6]. In other words, MPLS speeds up packet processing and the establishment of a traffic engineer path within a network. MPLS uses a label switching method to forward a packet through the network. The label is inserted in between the link layer header and the network layer header to the packet. Sometimes, it can also insert multiple shim headers, something commonly referred to as label stacking [6]. This label-based technique is based on an integration of layer two switching and layer three routing. It is specially designed for high-speed networks to use in a more efficient way to enhance switching performance while providing the scalability and flexibility of IP routing [3].

Furthermore, a major MPLS strength is its ability to integrate many different network technologies into a single interface with the IP layer [3]. This is due to the architecture of MPLS, which has been constructed using existing network typologies such as the packet organized from frame relay (FR), the file transmission size from IP, and the quality of service (QoS) goals from asynchronous transfer mode (ATM). The two major reasons MPLS is attractive as a VPN tunneling mechanism are that it provides a way to construct logically independent routing domains, and within a domain can map packets onto different levels of service, while it also provides a way to aggregate the traffic when the same security service can be applied to the already aggregated flow [20].

D. Advantages of L2TP and IPSec over PPTP

There are two major advantages of L2TP and IPSec over the PPTP. First, IPSec not only provides per packet data confidentiality, but also per packet data authentication and replay protection. By contrast, PPTP only provides data confidentiality. Furthermore, L2TP and IPSec connections provide much stronger authentication by requiring both computer level authentication through certificate and user level authentication through a PPP authentication protocol [11].

E. Advantages of PPTP over L2TP and IPSec

PPTP does not require a certificate infrastructure. That's why, the authentication process of PPTP is usually faster than L2TP and IPSec [11]. For instance, both L2TP and IPSec require the certificate infrastructure to the VPN server or other authenticating servers, and all VPN clients [11]. Furthermore, PPTP can be widely used in many different platforms, such as the windows series (XP, ME, 98, 95, 2000, NT, etc.). By contrast, L2TP and IPSec can be used with Windows XP and Windows2000 VPN clients only, the main reason being that only these clients support L2TP protocol, IPSec and the use of the certificate. In addition, PPTP can be placed behind the network address translator (NAT), whereas the L2TP and IPSec based clients cannot be placed behind the NAT unless it supports IPSec NAT traversal (NAT-T) [11].

6. VPN SECURITY

A. VPN Security

Since the VPN uses a public or shared network infrastructure to transport sensitive information, it is critical that it ensure the privacy and integrity of the data as it traverses such public or shared networks. The "private" its name implies is provided through the use of two security features: authentication and encryption. Authentication is the process that identifies an individual, while encryption is what keeps the data secret as it is transported over the public network [20]. The following subsection will discuss the authentication and security protocols.

Authentication. Authentication is typically a process of identification verification, and it ensures that the data is indeed coming from the source it claims to be [20]. Authentication methods can be broadly categorized into two types: two-party authentication and trusted third-party authentication.

Two-Party Authentication. Two-party authentication can have either a one or two-way scheme. In a one-way scheme, a client must be authenticated to its server, but the server need not be authenticated to the client. However, in a two-way authentication scheme, the client and server must be mutually authenticated to one another [20]. Two party authentications basically rely on both the user and peer knowing one or more pieces of information that no one else knows, a so-called shared secret. Verifying this secret provides the proof of identity for the user. The authentication information can be either static or dynamic. In other words, the authentication function can be either symmetric or an asymmetric cryptographic algorithm.

Cryptography refer to the obfuscating of data so that it cannot be understood by anyone except those specifically intended to access it. Symmetric cryptographic algorithm is where the same shared key(s) are used for both encryption and decryption, whereas asymmetric cryptographic is just the opposite. It uses different keys for encryption and decryption [11]. There are several primary types of symmetric cryptographic algorithms in wide current use. These are Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RSA RC4 algorithm (RSA is named after its inventors Rivest, Shamir and Adelman), and skipjack encryption. The following section will discuss only DES and IDEA standards.

Data Encryption Standard (DES). In 1977 the United States National Bureau of Standards (also known as ANSI standard) published DES. DES uses 56-bit keys and maps 64-bit input blocks of plaintext onto a 64-bit output blocks of ciphertext [15] [16]. Although 64 bits exist in the key, eight parity bits are stripped off to form the well-known 56-bit key. The basic structure of DES encryption is as follows: The 64 bit input is first permuted, and then subjected to sixteen rounds, each of which takes the 64 bit output of the previous round and a 48 bit per-round key and produces a 64 bit output. "The per-round keys are different 48 bit subsets of the 56 bit key. After the 16th round, the 64 bit output is subjected to the inverse initial permutation. DES decryption is essentially done by running this process backwards" [16].

International Data Encryption Algorithm (IDEA). IDEA was designed by Xuejia Lai and James Massey in 1991. IDEA is a block cipher

and it was intended to replace DES [15]. IDEA's algorithm is a 64-bit block of ciphertext. It uses a 128-bit key to encrypt a 64-bit block of plaintext into a 64-bit block of ciphertext. The general foundation of IDEA is very similar to DES. With a 128-bit key, IDEA uses eight rounds to encrypt the data. Although this may be weak compared to DEA's 16 round ciphers, IDEA derives its strength from three incompatible types of arithmetic operations: XOR, modulo addition 16, and a multiplication modulo 216+1 [16] [15]. The main advantages of IDEA over DES are its "faster performance in software, the fact that aside from per-round key generation, decryption is identical to encryption, and finally the much bigger key size, ensuring greatly enhanced security" [16].

Two-party authentication schemes. There are many types of two-party authentication schemes, such as passwords, challenge/response, one-time password, token cards, etc. The following section will discuss in more details.

Passwords. Password authentication is the most common authentication scheme and has been used widely in two-party authentication. There is nothing really advanced in this type of authentication function, it is just a comparison operation. In other words, the user provides the password and compares it with the server. There are many disadvantages of using passwords authentication, to include:

(1) Passwords are often easy to guess or hard to remember
(2) Peer must store the password, so the user must rely on the server's physical security
(3) Passwords are transported over a network, so they depend upon the security of the network, i.e. the password may be subject to eavesdropping
(4) Peer does not have control or any way of disqualifying an attacker from simply submitting hundreds of guesses [20].

Challenge/Response. This scheme is also a password-based scheme, but in a different setting. The challenge/response scheme is basically the peer asking the user a question, which is presented as a challenge, and the user must then answer the challenge correctly or else fail in authentication [20]. Usually, this type of authentication information is dynamic. Further, peer and the user must share the same secret list. To take one scenario, the peer and the user use a shared secret as the key to an encryption algorithm. So the peer sends the user a random phrase, the user uses the shared key to process the result and then sends it back to peer. The peer compares the result with its own processed version of the result. If the result does not match, the authentication will fail. In this scheme, the peer can determine how many attempts the user is allowed before locking access to the resource for a predetermined time period [20].

One-Time Passwords. The major limitation of password schemes is that an attacker can learn the shared secret by eavesdropping on the transmission of the password from the user to the peer. One way to avoid this limitation is by using the one-time password scheme. This type of scheme is only valid for one authentication session. Therefore, the attacker can not replay an eavesdropped password or response. According to Yuan and Strayer[20], usually the list of one-time passwords is mutually generated by the user and

the peer, and the user uses the passwords in order and upon successful completion of a session using one password, it is crossed off the list and the next password is used for the next authentication session.

Token Cards. A token card generates a different octet stream every time it is used, and it is a special case of a one time password scheme. One of the important aspects of the token card scheme is that it keeps the token stream from being predictable by such devises as keeping the token generation algorithm secret or using secret seeds with known algorithms [20]. One of the more famous token cards is SecurID from RSA (RSA is named after its inventors Rivest, Shamir and Adelman) security. The SecurID card has a unique 64-bit seed value that is combined with a random number generator algorithm to generate a new password or code every 60 seconds. Only the associated peer knows what number is valid at that moment for that user and card combination [20].

This section will discuss authentication protocols. There are three widely used authentication protocols in two-party authentication, these are password authentication protocol (PAP or RFC1334), challenge handshake authentication protocol (CHAP or RFC1994), and extensible authentication protocol (EAP or RFC2284). PAP is the basic form used with point to point protocol. CHAP has more secure authentication over PAP, the reason being that by default CHAP will constantly challenge the host every two minutes to limit the exposure of a hijacked session [15].

Password Authentication Protocol (PAP or RFC1334). PAP provides a simple method for a user to establish their identity using a two way handshake, such as the user constantly sending their user ID and password as a pair to the peer until the authentication is acknowledged. This authentication is only done once at the initialization of the connection and it will remain valid as long as the connection is still on. This method of authentication is not a strong authentication because the user ID and password are sent without protection. Therefore, they are vulnerable to a hacker attack. Furthermore, the authentication peer has no control over the frequency of the authentication requests [20].

Challenge Handshake Authentication Protocol (CHAP or RFC1994). CHAP is a three way handshake. First, CHAP will verify the identity of the user on a point-to-point (PPP) link. After the link is established, the peer will issue or send a unique and unpredictable value as a challenge to the user. The user should use a keyed one-way hash function to calculate the value and respond or run over the challenge value (the key used in the one-way hash is the shared secret between the user and the peer). The peer will check the response against its own calculation of the hash value using the shared secret. If the value is a match, the peer replies with a success message or a failure message if it is not.

There are several advantages to using CHAP. First, the shared secret is never transmitted from the user to the peer. Playback protection is provided because each challenge value is unique and is valid only for that particular challenge [20]. Another advantage is the peer can control the timing and frequency of the authentication, so they can limit the number of challenges and ignore

users who habitually misbehave [15]. The main disadvantage of CHAP is that the shared secret must be stored by the peer and used in a cleartext form because the secret is the key to the one-way hash. Even if the secret key was in encrypted form, it would have to be decrypted for use [20].

Extensible Authentication Protocol (EAP or RFC2284). EAP is a three-way handshake general authentication protocol that supports multiple authentication mechanisms, and it runs directly over the link layer without requiring IP. Furthermore, while EAP does not select a specific authentication mechanism at link control phase, it will select one at the authentication phase. This allows the authentication to request more information before determining the specific authentication mechanism.

Trusted Third-party Authentication (TTP). A trusted third-party authentication scheme is when both users use this third-party trust to secure their interaction. In other words, a user must be authenticated to the peer, a trusted third-party can vouch for the user's identity or can provide information that can be used in such an authentication. They both must trust the third party to provide the service [20]. The schemes that TTP uses are symmetric and public key cryptography (PKC). PKC has a built-in mechanism for authentication, a form of cryptography which generally allows users to communicate securely without access to a shared secret key. There are many different cryptographic algorithms. This paper will only discuss public key cryptography (PKC) and secret key cryptography (SKC).

Public Key Cryptography (PKC). PKC was invented in 1976 by Whitfield Diffie and Martin Hellman. There are two keys in PKC: one is designated the public key and other the private key. Neither key is ever revealed to another party. For example, when A sends a secure message to B, A uses B's public key to encrypt the information. Party B then uses his or her private key to decrypt the message. Public and private keys are related in such a way that the public key can be used to encrypt messages but only the corresponding private key can be used to decrypt. Pretty Good Privacy (PGP) falls under this category of cryptography. PGP is very easy and extremely secure to use. PGP is a family of software systems developed by Philip R Zimmermann [20] and it uses an ad hoc approach for its authentication mechanism.

PKC offers a useful and powerful mathematical tool to facilitate authentication, and public key infrastructure (PKI) is the set of services and policies that lays the framework for binding a public key to an identity and distributing that binding. Furthermore, PKI manages the public keys for everyone in such a way that a powerful statement of authentication could be made [20]. PKI has three processes: certification, validation, and certificate revocation. Certification is the binding of an identity to a public key. In other words, the public key and the identity are placed inside a digital document and this is called a certificate. Then a trusted third party digitally signs the certificate, vouching for the correctness of its contents. This trusted third party in PKI is also known as the certification authority (CA) [20]. Validation is the process of verifying the

authenticity of the certificate. This process involves the verification of the signature of the CA. In order to verify the signature, the process uses CA's own public key to verify while also checking the certificate against a certificate revocation list (CRL). CRL is the list that contains a list of certificates that have been revoked by the CA. This indicates that the binding is no longer valid. Furthermore, the validation process also checks the validity period contained in the certificate itself. Certificate revocation is the process of rejecting a previously issued certificate before its expiration date. The CA must keep track of all the certificates it has issued and must be prepared for revocation [20].

Secret Key Cryptography (SKC). SKC, also known as symmetric cryptography, is a much traditional form of cryptography compared to PKC, the reason being that SKC uses a single key to encrypt and decrypt a message. SKC deals with encryptions and also authentication. It uses the technique called message authentication codes to archive the authentication. SKC also employs other techniques, such as block ciphers and stream ciphers. A major problem with SKC is getting the sender and receiver to agree on the secret key without anyone else finding out. This requires a method wherein the two parties can communicate without fear of eavesdropping. Among its merits is that SKC is generally faster than PKC.

7. CONCLUSION

All in all, the VPN solution provides government with secure private networking for multiple agencies and agencies across a shared network. Furthermore, it also allows citizens and businesses to communicate with government in a very sufficient and private way in terms of sending sensitive information over a public network. The bottom line is it gives government more flexibility, delivering scalability, reliability, and a secure network infrastructure capable of supporting any network protocols at anytime. Such security goes to the very heart of e-gov's mission. Without the security provided by VPN the integrity of e-gov would be as vulnerable as the information it handles.

REFERENCE

[1] Adtran, (2001). Understanding virtual private networking. Retrieved from http://www.vpnc.org/

[2] Bhatnagar, S. C. (2004). E-Government from vision to implementation: A practical guide with case studies. Sage Publications.

[3] Cisco, (2003). Layer 2 Tunnel Protocol. Retrieved from http://www.cisco.com/univercd/home/home.htm

[4] Cisco, (2003). IPSec. Retrieved from http://www.cisco.com/univercd/home/home.htm

[5] Cisco, (2004). Creating an intelligent platform for operational excellence in E-government. Retrieved from http://www.cisco.com/

[6] Encore Network, (2004). Preserving end-to-end quality of service for IP VPNs over MPLS satellite networks. Retrieved from http://www.vpnc.org/

[7] Entrust, (2003). Information Security Solution for E-Government. Retrieved from http://www.entrust.com/

[8] Gollner, M. (2004). Taiwan launches nation-wide PKI project for an "Electronic Identity Smart Card" based on StarSign token. Industry & Government, 2, 14-15.

[9] Holmes, D. (2001). eGov: eBusiness strategies for government. London: Nicholas Brealey Publishing.

[10] Kalidindi, S., & Stewart, E. (2003). IPSec Virtual Private Networks: Conformance and Performance Testing. Ixia Company.

[11] Microsoft, (2000). Virtual Private Networking in Windows 2000: An Overview. Retrieved on November 10, 2005 from http://www.microsoft.com/windows2000/server

[12] National Research Council, (2002). Information technology research, innovation, and E-Government. Washington D.C.: National Academy Press.

[13] Ndou, V. (2004). E-Government for developing countries: Opportunities and Challenges. The Electronic Journal on Information systems in Developing Countries.

[14] Nortel, (2004). Nortel Network E-Government Solution. Retrieved from http://www.nortelnetworks.com

[15] Quiggle, A. (2001). Implementing Cisco VPNs: A hands-on guide. McGraw-Hill. New York:NY.

[16] Steffen, D. (1999). Cryptography. Retrieved from http://www.maths.mq.edu.au/~steffen/old/PCry/report/node7.html

[17] VPN Consortium, (2004). VPN Technologies: Definitions and requirements. Retrieved on November 10, 2005 from http://www.vpnc.org/vpn-technologies.html

[18] WordBank, (2005). Word Bank. Retrieved from http://www1.worldbank.org/publicsector/egov/definition.htm

[19] Wood-Haper, T., Ibrahim, O., & Ithnin, N. (2004). An interconnected success factor approach for service functional in Malaysia electronic government. ICEC'04 Sixth International Conference on Electronic Commerce, 446-451.

[20] Yuan, R., & Strayer, W. T. (2001). Virtual Private Networks: Technologies and Solutions. Addison-Wesley. NY:New York.