Global Information Assurance Certification Paper

Timothy P Donahue: Version 1.2e for GSEC

Public Key Infrastructure (PKI) versus Virtual Private Networks (VPN) in the Department of Defense (DoD) environment.

Introduction

With the proliferation of automated information systems (AIS) and the supporting long haul communications that enables the transmission of information assets, DoD information has become subject to increased and more prevalent attacks on its confidentiality, integrity and availability. Recognizing a need for greater security within its information architecture, the Deputy Secretary of Defense determined in June 1998 that DoD would migrate to a PKI in compliance with Management Reform Memorandum (MRM) #16 establishing the requirements for the design, development and implementation of an approved PKI. At the time of this decision there were few viable options that could support the increased level of protection required for the transmission of DoD information assets. Outside of symmetrical encryption and its accompanying overhead in centralized key management, classified material storage (CMS) custodians, and storage facilities, PKI was the only viable option open to DoD. The primary concern of this paper addresses whether PKI still constitutes the only viable solution for greater confidentiality and integrity of information assets and if it provides sufficient return on investment.

In order to come to a reasoned decision on this issue, we need to understand what constitutes the architecture, the implementation and maintenance costs, as well as the benefits derived from a PKI. This in turn must be balanced against the architecture, implementation and maintenance costs, and benefits from a VPN secure transmission option that may be used in place of a Public Key Infrastructure.

Background

PKI definition:
A PKI allows users of an inherently non-secure network medium, such as the Internet, to securely and privately exchange data by the use of a public and a private and public cryptographic key pair. This is asymmetrical encryption. The key pair is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can uniquely identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. In short it is:
"The combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet."

DoD PKI definition:
"The DoD PKI will provide the data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature services for programs and applications which use the DoD networks." The intent is to provide a program that enables an individual with one certificate, to access and used multiple AIS within the DoD. The program is designed for the entire DoD and is intended to provide secured communications and transactions over unsecured networks.

DoD PKI Structure
PKI constitutes a framework and services that provide the generation, production, distribution, control, tracking, and revocation/destruction of public key certificates. The intent is to manage the keys in such a manner that the organizations within the DoD can achieve and maintain a secure networking environment. The public key infrastructure assumes the use of *public key cryptography*, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography involves the creation and sharing of a secret key for the encryption and decryption of messages. This secret key system has a couple significant concerns for large organizations with large numbers of users. Distribution and control of the private key becomes exponentially more difficult as the number of the recipients grows. It already assumes an existing relationship by the recipients of the private key. Retention or longevity of a private key must be factored in as well. A clearly defined and limited retention period for the secret key must be established to mitigate the risk of outside agencies cracking the key. The length of this retention period is dependent upon the strength of the key (56 bit keys are inherently weaker than 128 bit encryption keys, or the 156 bit 3DES key) and a subjective evaluation of what level of risk is associated with the retention time period. At the end of that cyclic period the entire process of secret key distribution must be completed again. Storage becomes an issue in that strict controls must be adhered to in order to prevent the private key from being compromised. In most cases this presumes an infrastructure in place, designed to support restricted access to the private key. Should the key be discovered or intercepted by outside agencies, messages can easily be decrypted. For these reasons, and the enormous number of active participants communicating on the INTERNET and NIPRNET, the public key infrastructure became the preferred approach.

A DoD public key infrastructure consists of:

- A certificate authority (CA) that issues and verifies a digital certificate (Digital certificates are electronic files that act like a kind of online passport. They verify the identity of the certificate's holder. They are tamper-proof and cannot be

forged.). A certificate includes the public key or information about the public key.

- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
- Numerous local registration authorities (LRA) that act as the individual verifier (requiring picture identification).
- One or more directories where the certificates (with their public keys) are held.
- A certificate management system.

How Public and Private Key Cryptography Works

Several basic factors must exist:

1. Each key is a unique encryption capability.
2. No two keys are ever identical. This is why a key can be used to identify its owner.
3. Keys always work in pairs. A private key, and a public key.

The concept is that any information that the public key encrypts, only the corresponding private key can decrypt, and vice versa. The public keys are freely distributed to those users who are validated for access to a DoD AIS and have the desire to exchange secure information with another user. Their private key is never copied or distributed and remains secure on their private key receptor (e.g. 3.5" floppy, token, smart card, etc.). By installing a private key on your computer or server, your computer now has its own private key. The matching public key is freely available as part of your digital certificate posted on your computer or web site. When another user wishes to exchange information with you, they access your public key. They use your public key to validate your identity and to encrypt the information they want to send you. Only your private key can decrypt this information, so it remains secure from inspection or tampering while traveling across the Internet/NIPRNET.

In public key cryptography, public and private keys are created simultaneously using the same algorithm by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). So, when I send you a message, I get your public key from a central repository, and encrypt a message to you using your public key. When you receive the message, you decrypt it with your private key. In addition to encrypting messages (which provides confidentiality), I could authenticate myself by using my private key to digitally sign the message. When you receive it, you can use my public key to decrypt it as indicated in the table below:

Action	Which key
Send an encrypted message	Use the receiver's public key
Send an encrypted signature	Use the sender's Private key
Decrypt an encrypted message	Use the receiver's Private key
Decrypt an encrypted signature (and authenticate the sender)	Use the sender's Public key

We now have a fairly accurate picture of the architecture of a DoD PKI, but still need to determine the cost. In July 1998 the Aberdeen Group published a white paper that evaluated the cost of ownership for a digital certificate project. They compared and contrasted the cost of ownership for three well-known products based on 5,000, 50,000, and 500,000 seat digital certificate capability. One of the products was VeriSign, which cut the end user cost for customers by providing the infrastructure themselves. The bullets listed below were directly taken from the white paper and provide the cost charges to the customer for a three year period based on seat requirements:

- $256,894 for 5,000 seats ($51.40 per seat);
- $541,127 for 50,000 seats ($10.80 per seat); and
- $1,276,904 for 500,000 seats ($2.60 per seat).

At that time, Netscape deployed only five and fifty thousand seat solutions as indicated below:

- $631,612 for 5,000 seats ($126.30 per seat); and
- $1,452,895 for 50,000 seats ($29.10 per seat).

The third product evaluated was Entrust, which had significantly higher costs because the customer had to buy the product and provide their own support and maintenance. The figure below bread\k down the per seat cost:

- $993,602 for 5,000 seats (198.70 per seat);
- $3,158,983 for 50,000 seats ($63.20 per seat); and
- $11,093,098 for 500,000 seats ($22.20 per seat).

Accepting these figures even in 1998 dollars, the cost of a PKI solution for the DoD, which comprises 1.2 million Active Duty, Reserve, and National Guard soldiers, sailors, and air men, as well as government civilian personnel would cost **$22,186,196.00** for the first three years. Naturally manpower and maintenance costs would be recurring, and it is probably safe to assume that PKI systems and client software would evolve and constitute additional costs during the life cycle of the PKI project. It is also safe to assume that the DoD would not out-source any of the PKI and would absorb all of the associated costs. This assumption is predicated on the DoD insistence that their information assets not migrate outside of the DoD environment. The Hard Disk Drive Disposal memorandum of 08 January 2001 mandated destruction of HDDs rather than allow information assets to migrate to civilian personnel.

The question now becomes what is our return on this investment, what benefits are accrued for the buy-in. The following are capabilities associated with a PKI:

- **Communicate securely with employees around the world.** A PKI offers users controlled access to your intranet for all your corporate information, such as HR data, secure email, and applications.
- **Exchange confidential data with business partners**. A PKI lets you create secure extranets and Virtual Private Networks that give select partners easy access to business-critical information stored on your internal network.
- **Safely, seamlessly integrate your supply chain.** A PKI provides a protected environment for safe information exchange at every stage of your manufacturing processes.
- **Take advantage of secure e-commerce**. PKI lets you offer a world of customers the confidence to purchase your goods and services on the web.
- **Provide non-repudiation.** A digital certificate allows a user to digitally sign and encrypt email messages, as well as allow them access to certain military web sites. The Defense Travel System is adopting the use of digital electronic signatures for travel. PKI certificates allow users to access their website and their digital signatures allow them to receive electronic authorization prior to a trip and permit them to sign their vouchers after the trip without actually having to sign a piece of paper. Their digital signature will verify the user is who they say they are. These electronic signatures create a secure and legal association between the travel and voucher information. The Defense Travel System is a practical approach for digital signature certificates, including commercial infrastructures and services, which could eventually be used in department-wide electronic commerce efforts.

That the digital signatures are legally binding is beyond question. The one hundred and sixth congress of the United States, during their second session (24 January 2000), enacted the Electronic Records and Signatures in Commerce Act (S. 761). The act specifically states:

"A signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforcement solely because it is in electronic form; and a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic record was used in its formation."

In effect providing a legally binding signature that is admissible in Tort and/or Contractual disputes.

We now know the architecture, presumed cost, and the benefits of a DoD PKI. Reduced to its lowest common denominator; a DoD PKI encrypts transmissions and ensures knowledge of who sent the transmission (non-repudiation).

VPN definition.

Since Virtual Private Networks are an emerging technology, there is no clear concise DoD definition of what constitutes a VPN. For the purposes of this paper the following definition will apply:

A VPN is hardware and software that will encrypt and encapsulate transmission packets of information, and using a suitable protocol tunnel through existing firewalls and security stacks. These encrypted and encapsulated packets will be recognizable only by a similar device that recognizes those packets. The requirements are listed below:

- Encryption: which disguises the data so that anyone interception the data cannot understand what they have acquired.
- Data integrity: which ensures that message being sent has not been corrupted or altered.
- Authentication: which ensure the validation of the sender and the receiver of the transmission.
- Access restriction: which ensures that transmissions are accepted from only know and approved sources within a specific community.

Fortress Technologies produces a device titled the NetFortress box, which satisfies the definition above. The box is a plug and play with a port in and a port out for communications. Each NetFortress box purchased for a particular organization has a unique digital signature burned into the box. No other organization may obtain that unique digital signature, so that transmissions are only accepted from boxes within the organization's architecture. The boxes each have a permanent public and private key that are unique to that particular box. Each box constructs its personal 512 bit public key when first powered up. When the boxes attempt to exchange information they each determine that they have the appropriate organizational signature, and then they exchange

their public keys and calculate a permanent common secret key for the communication transmission unique for those two boxes. This key is permanently stored on the each box. For Dynamic key exchange, the boxes generate a random dynamic private key, which is frequently changed. The public keys are derived from the private keys. After the initial session where the 512 bit keys are exchanged the boxes enacts a Diffie-Hellman protocol using the dynamic keys, but the protocol is encrypted using the permanent common secret key. The new exchange produces a 128 bit common secret key that has a random life cycle and is used to transmit network traffic destined for other sites within the organization. The end result is a renegotiation for each transmission that effectively eliminates a possible man-in-the-middle attack.
Headers of the standard IP packet structure are modified and rearranged to hide the original intent of the packet. The information is then compressed to disguise the original size of the packet and NetFortress protocol is place in the header, which has the effect of hiding information about the host. The entire packet is then encrypted and sent down the line to a like (with the same organizational signature) NetFortress box. The transmission box then calculates a checksum in the header. The receiver checks the checksum after decryption to ensure data integrity. A second encrypted checksum on the sender's side is the means of authentication since only the two boxes involved in the transmission know the static and dynamic encryption keys used in the exchange. The MAC header address is replaced by the MAC address of the targeted NetFortress box, so that no one outside of the organization can tell what is behind the device. The unique organizational digital signature prevents spoofing from similar boxes.

With this understanding of our VPN architecture we would need to know the cost to make a valued comparison of benefits to a PKI solution. The Army Distance Learning Program (TADLP) currently uses the NetFortress VPN devices are part of their security architecture. The boxes are installed at each geographic location, and in some cases because of the distances between facilities at particular locations more than one box is used. Projected costs to the government is as follows:

NetFortress 10 (10mb throughput) setup and maintenance is $6,023.

Benefits derived is the secure transmission by encryption of DoD data assets

Conclusion

Using TADLP as a microcosm of the DoD, a value decision on what constitutes the best fiscal approach can be determined. TADLP incorporates 220 sites scattered worldwide supporting seven to twelve thousands seats, with an active user base of 1.2 million.
It has already been determined that a PKI designed to support such a system architecture would cost the Department of Defense:

$22,186,196 for the initial three year investment.

The cost of the VPN solution to support the TADLP system architecture would be as follows:

$6,023 X 242 sites (this assumes a ten percent site requirement of localized geographically diverse facilities) = **$1,457,566**.

The primary difference between the two solutions is the capability for non-repudiation associated with a PKI. The essential question now becomes whether non-repudiation is worth **$20,728,630**. It is my contention that it is not. While some organizations within DoD may benefit from a non-repudiation capability (e.g. supply, acquisition, contract managers, etc.) the vast majority of DoD does not. Certainly not at a $20.7M price tag. By incorporating a combination of the two technologies the DoD could provide the necessary capabilities required. Using the Aberdeen Group white paper on PKI costs we can still support 50,000 users with a PKI at the following cost:

$3,158,983 for 50,000 seats ($63.20 per seat).

If we combine the cost of the Fortress Technologies VPN solution (**$1,457,566**) with the cost of a 50,000 seat PKI solution (**$3,158,983**) using the Entrust figures (DoD acquires and manages all aspects of the PKI) we have a combined cost of **$4,616,549** for the first three years. This is still a significant savings ($17,569,647) over the cost of implementing the $22,186,196 DoD wide PKI solution. By accepting the limited seat approach for PKI, and a VPN solution across DoD, the government can save $17.5M within the first three years of investment. We still achieve the benefits of legally binding digital signatures and significant cost savings. We simply target those agencies within DoD that would achieve tangible benefits from a non-repudiation capability vice a full DoD implementation.

References

1. "Frequently Asked Questions (FAQs): DISA customer support site. Https://disa-ca.dtic.mil/wobin/WebObjects/PKIfaqs.wo
2. Assistant Secretary of Defense memorandum: "DoD Public Key Infrastructure (PKI)", August 12, 2000.
3. Evaluating the Cost of Ownership for Digital Certificate Projects: The Aberdeen Group, July 1998. http://www.verisign.com/library/reports/aberdeen/cost/index.html
4. "Public Key Infrastructure Roadmap for the Department of Defense": DISA customer support site, December 18, 2000. https://iase.disa.mil
5. "S. 761 Title I-Electronic Records and Signatures in Commerce": DISA customer support site, January 24, 2000. https://iase.disa.mil
6. "Secure Packet Shield Technology: The NetFortress VPN Secret": Fortress Technologies. http://www.fortresstech.com

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event