

PKI-Enabled Network Security

Chii-Ren Tsai

Citigroup

Citigroup Information Security Office

12401 Prosperity Drive

Silver Spring, MD 20904, USA

chiiren.tsai@citigroup.com

(Extended Abstract)

EXTENDED ABSTRACT

Traditional network applications such as telnet, FTP, terminal servers, and client/server applications were designed without any built-in security measure to protect authentication data and sensitive information end-to-end. As a result, they are subject to various security attacks (e.g., spoofing, eavesdropping, replay, and unauthorized access). When the secret-key-based Kerberos authentication protocol had been invented by the MIT in the late 80's, it was quickly accepted by major vendors and triggered the creation of DCE (Distributed Computing Environment) as a secure platform for distributed applications. Kerberos/DCE requires significant efforts for application development and deployment, it had not been widely deployed before Internet e-commerce was on the horizon in the early 90's.

When the Internet and e-Commerce started to gain momentum in 1994, SSL (Secure Socket Layer) became the most popular protocol for server authentication and data confidentiality/privacy due to its simplicity and ease of deployment. It has been widely used for Internet e-commerce ever since and has been used as a vehicle for securing or tunneling a number of protocols such as telnet, ftp, and terminal emulation. It is fair to say that SSL is one of the most successful public-key-based protocols. SSL is running at the transport layer, it could secure applications at a higher OSI layer as long as they could be re-engineered to take advantage of SSL. However, it cannot benefit legacy applications whose protocols simply cannot be modified.

In the mid-90's IETF (Internet Engineering Task Force) was beginning to address IPv6 security and IP security protocols (IPSec) such as Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE), also referred to as ISAKMP/Oakley, were subsequently proposed and ratified. After that, IPSec has been subsequently implemented in most operating systems and platforms, and VPN (Virtual Private Network) became a major application of IPSec for securing remote access or building a secure tunnel between two points over the Internet or proprietary networks.

IPSec and VPN are non-intrusive to applications, and cost-effective, so that they could become a good alternative for protecting legacy applications without re-engineering the applications.

In this talk, we would briefly describe the above PKI-enabled security solutions with special focus on IPSec/VPN. In particular, we would describe the IPSec protocols and the notion of VPN, and discuss considerations related to their deployment. Besides, we would briefly articulate potential issues related to PKA (PKI-enabled applications) such as certificate chain spoofing.

KEY WORDS

Distributed Computing Environment, Internet Key Exchange, IPSec, Kerberos, ISAKMP/Oakley, Public Key Infrastructure, Secure Socket Layer, Virtual Private Network.