USA.. Switzerland.. Germany.. India..

Ramsoft

Productization of PCSKIP

SunScreen SKIP-E+ (Simple Key management for Internet Protocol) is a single user software, which can be used to secure the transactions of the user through the public and local area networks. This software uses the SKIP specification developed by Sun Microsystems. SKIP is a way of protecting network traffic through management of keys and encryption. SunScreen SKIP-E+, which protects a single user, would hence work as complimentary to SunScreen, which protects the network. SKIP was developed for an American client.

Highlights:

- Global productization
- Extensive testing anddocumentation
- Entirely done off-shore

Key features of SKIP:

Compliance to SKIP Protocol: It implements all features of SKIP versions 1 and 2.

Certificate Management: It recognises certificates in X.509 formats V1 and V2. The software also supports unsigned Diffe-Hellman certificates. Raw modesupport for ESP and AH is also present.

Data Encryption/Decryption: The software supports the algorithms for key and data encryption as per the specifications of SKIP. The algorithms supported at present are:

- DES-CBC-64/56 bit (key, traffic)
- 3 Key Triple DES-CBC (key, traffic)
- RC4-40 bit (traffic)
- 2 Key Triple DES-CBC (key, traffic)
- RC4-128 bit (traffic)
- DSA (signature)
- Keyed MD5 (authentication)
- MD5 (key separation)

The system running this product will be able to use different algorithms to interact with different systems. The software has a cryptographically secure random number generator for the generation of unpredictable keys.

Authentication: The software ensures that the data is coming from the expected source, which is performed as per the SKIP specifications for authentification.

Configuring Remote sites: Users will be able to define information on all remote sites with whom they are going to have transactions.

Configuring Connections: Connections are the currently active remote sites. User can define the currently active remote sites. They should also be able to specify different algorithms for different connections.

Context - Sensitive Help: All screens have context-sensitive help and the users are able to activate them through an option on the screen.

Warnings and Error Messages: The system displays self-explanatory error messages in a separate window.

User Messages: Users get the messages on the current state of the software, next action to be taken and specific precaution.

Monitoring Facilities: Users are able to watch the global security policies and also monitor the traffic as per the global policy settings.

Independent Certificate Generation and Maintenance: User will be able to generate certificates along with the capability to manage certificates independently.

Productization

Technical Information		
Technology	⇨	Windows Virtual Device driver (VxD), SKIP
Environment	⇨	- Windows 95 - De lphi - C++/C

SunScreen SKIP-E+ works transparent to any application. It operates at the network layer and inspects all the data that passes between network interface and IP layer. Thus SunScreen SKIP-E+ provides protection to user applications such as HTTP browser, Telnet, E-mail client etc. without the knowledge of the application. It thus is application independent and hence transparent to the applications. Since SunScreen SKIP-E+ implements SKIP protocol versions 1 and 2, it is compatible with SunScreen SPF-100 Sunscreen EFS-100 and SKIP for Solaris devices.

SunScreen inspects all IP data passed to and from the network interface layer and protects it using the SKIP v1 and v2 protocol implementations embedded in it. SunScreen SKIP-E+ employs encryption of messages, or packets, using randomly generated packet keys. Each packet key, in turn, is then encrypted using the

Diffie-Hellman (DH) Shared Secret Key. The latter, which is generated using the public key-private key pair concept, is used to encrypt the key belonging to the packet that is being transmitted over the network. At the receiving end, the Shared Secret Key, which is also generated utilizing a complementary DH pair of keys, is used to decrypt the packet key. Subsequently, the packet is decrypted, thus enabling the recipient or remote party to view its contents.

Execution road-map:

Ramsoft was engaged by the client to transform the existing code into a global product to be supported on the Windows 95 and Windows 3.11 environments. The process of productization began with a thorough understanding of the technical specifications. This was then followed by a review of the source code. A detailed functional specifications document was generated to serve as the criteria against which the source code could be validated and tested to determine the extent to which the source code satisfied the product specifications.