01EDGE SE (Security Engine)

Problem:

- You want total security of classified documents in storage in the workstations and servers in the enterprise network.
- You want total security of all classified files in transit in the LAN and MAN.
- You want totally security of classified documents in transit between two workstations across the world connected through secure or even insecure networks.
- It should be practically unbreakable by any one in the world including technologically advanced western governments.
- You do not want to take the trouble of sending secret keys through secure channels

Solution

- Very high security Secret key system augmented by Public Key crypto system to encrypt the session key.
- Private key encrypted with password in the recipients computer.

Crypto Process:

- Generates RSA 1024 bit key pair (public key, private key pair)
- RSA Private Key is password-encrypted (PBEwithSHAAndTwofish-CBC)
- Public key is distributed outside the system.
- Sender encrypts a file using a 256 bit AES Key or other high security algorithms.
- This Key is then encrypted using 1024 bit or even 2048 bit RSA Public Key of the receiver.
- The encrypted file could be sent to receiver by mail/FTP/HTTP out side the system.
- At the other end, similar program is called to decrypt.
- Decrypts the file and saves it in the current directory

Key Highlights:

- Uses 256 bit AES Rijndael cipher or any of the other 8 algorithms for block encryption
- Being secret key encryption, it is reasonably fast.
- AES 256 bit is certified to be extremely secure, in fact the best available technology in the world as of 2003.
- 2^{256} key combinations or $1.1\text{x}10^{77}$ possible key combinations
- If a computer could crack DES by trying 2^{56} keys in 1 second, the same computer would require 149 trillion ($149\text{x } 10^{12}$) years to crack Rijndael 256 bit key. (For a comparison, the universe is estimated to be less than 20 billion ($20 \text{ x } 10^{9}$) years old)
- No secret key exchange as the secret key is encrypted with the RSA 1024 bit Public Key and appended to the encrypted file.

- Encryption of private key done with Twofish 256 bit hash key.

Rich Feature set includes:

1. Other encryption Systems based on DES, Triple DES, Blowfish, Twofish, IDEA, RC5 and RC6.
2. For extra security, multiple iteration of any algorithms up to 9 times (exactly as DES is to Triple DES)
3. Key generation of RSA keys 1024 and 2048 bits.
4. Shredding of input files by complete obliteration from the disk to make it totally non-recoverable.
5. Single cycle encryption even for multiple addressed documents using multiple public keys.
6. Digital signing of documents with ones private key for cent percent authentication and non-repudiation.
7. Fool proof verification of these digital signatures.
8. Enterprise internal CA (Certifying Authority) signing to facilitate internal cost effective PKI.
9. Time stamping of documents for proof of existence at points in time.
10. Time stamp verification of time stamped documents.
11. Establishment of a secured channel with Diffie-Hellman Key-agreement protocol based encrypted channel between two parties with out physical exchange of secret keys.

Value Proposition

- High security encryption needing no secret key exchange and providing security in storage and sharing.
- Choice of varying degree of security with a range of algorithms and multiple iterations all available for choosing.
- Shredding of input files providing total obliteration of input files.
- Every thing required for starting of an internal CA signature sytem and providing signed crtificates to internal professionals.
- Time stamping of internally generated documents for proof of existence
- Establishment of a secured channel with any one connected to the internet

CPC Nath,
Founder & CTO
01EDGE,
C 679 Sarita Vihar,
New Delhi 110044
India.
+91 11 2 694 8083
+91 908 020 2680
nath@computer.org