Ralph Durkee
Independent Consultant
www.rd1.net

Security Consulting

Internet Systems Administration and Software Development

PGP Overview for Rochester ISSA Chapter

Agenda:

- Generic Public Key Encryption
- PGP Encryption
- Digital Signatures
- PGP Keys
- Key Management
- Discussion
- Demo if time / interest

Public Key a.k.a. Asymmetric Encryption

- 2 Keys used
  - 1 Public Key – Made publicly known
  - 1 Private Key – Carefully Protected
- Encrypted with either key (Public or Private)
- Decrypt with the opposite key used for encryption

Symmetric Encryption a.k.a. Shared Secret

- Encrypt and Decrypt with same key
- Problems
  - Have to securely pre-negotiate a shared secret
  - Sender can also decrypt messages.
  - Security depends on the strength of the secret
- Benefits
  - Symmetric Encryption is about 1000 times faster than Asymmetric Encryption

The Best of Both Worlds

Combine the Best of Public Key with the Best of Symmetric Encryption

2. Start off with PK to avoid a shared Secret
3. Use PK to authenticate parties
   (May be either Party or Both)
4. Generate a one time random session key
5. Share the session key via PK
6. Switch to Symmetric Encryption for better performance, using the session key

Combined A/Symmteric Encryption

- Common Reoccurring Design Pattern Used in
  - SSL
  - IPSec

And …

- PGP

PGP E-mail Encryption

1. Document is compressed
2. Random Session Key generated
3. Document is encrypted (symmetric) with the session key
4. Session Key is encrypted with the public key of every recipient.
5. Encrypted Key(s) and Document converted to ASCII Armor (RFC 2015)

Digital Signatures

- Digital signature is applied prior to encryption
  - Generate a Secure Hash of the entire document.
  - Secure Hash is kind of like a check-sum, but much better
  - The Secure Hash is encrypted with the signers private key.
  - Anyone with public key can decrypt the hash
  - Decrypted Hash is compared against recalculated hash to verify that the document hasn't been modified.
  - Provides non-repudiation as well as integrity.

Algorithm Details

- PGP like IPSec and SSL is really a collection or suite of Algorithms
- Choices of Algorithms (RSA & DH/DSS)
- Choices of key lengths
- Added Info included in the message
- Also included with the keys

PGP Keys -- What's in a key

- **ID** – Unique Identifier (0xDB93230C)
- **Type** – Algorithm Used (RSA or DH/DSS)
- **Size** – Key size in bits (usually 1024 and up)
- **Created** – Date Key was created.
- **Expire** – Date the Key expires
- **Cipher** – Symmetric Algorithm (CAST, IDEA or 3DES)
- Finger Print – Secure Hash of the key (Good for validating key)
- Validity – Valid only if signed
- Trust – Implies auto-trust of other keys signed

Key Management
Getting Keys

Getting a key is easy -- Via:

- E-mail
- Key Servers e.g. **wwwkeys.us.pgp.net**
- Off of a web site
- PDA transfer
- Most anyway a file can be received

Key Management Trusting Keys

- Methods of Validation
  - Face to with Photo ID (best verification)
  - Phone Call and read Key Finger Print (Good if you know the person)
  - Get key from multiple sources and verify (Good for verifying signatures from on downloaded files.)
- Signing the key ensure its integrity

Sample Key
ASCII Armor Format

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

mQGiBDrP1xURBADFhi5Aw9XQ2ULmCZne7aY4VlV2Iqvw8lkDZvVe+TbSE1sHu8qB
1IBqQETXCM4H3c/jdJyqR+He4J7R3rfy/f/uAJhKyI5oklr+r43ardotsvvXoFXb
7qaQMw5H8lPINAHzUey86kNem1ewwSnrkicdRWOTuAokZJhGIc1U3cEUrwCg/9yJ
imMOduXdVTk01Jy8BE6Lt9sEAMSHLGAdWz4sW3Mdc9KkVxDrWErY3SKTcLxpJ8B1
YTvHr7S+n66VK4mEzIrycTL4vG0WGpeKI+ga17fe/swYNz3TPhlJhwX3cvPI/37d
2Gqdie55qbYNyOgAO1oSLGWRqUc4nGkuwxA83uEwLHNRAIr/S+2gPRKWhxdCPN1T
3NR/A/934ervK95h+HtJwMmDopiPK1im3q4TuOoJSp/l0khBGUIrXHQJoKUXCDNb

 . . .
iEYEGBECAAYFAjrP1xUACgkQLNgy0NuTIwxlzgCg0f031ddKPROkmZPGnq+etlia
sgMAn0IQlK4flhVqi290Mw9jIeDo+FDR
=abqO
-----END PGP PUBLIC KEY BLOCK-----
```

Demo?

Discussion

- Any remaining Questions?
- OpSec Thought questions:
  - What are the weakness of PGP?
  - What attacks are likely if someone wanted to decipher PGP encrypted e-mail?
  - Is a Man-in-the-middle attack possible?
  - If not why not, or if so how could it be prevented?