


SE-4920: Lecture 15

PGP (Pretty Good Privacy)

- Reading
 - Chapter 22
- Today's Outcomes
 - Give an overview of the history and current application of PGP


1



Background

- First available in 1991
 - By Phil Zimmerman
 - Encrypt files, often used in email
 - Intended to be freely distributable
- IDEA for SK operations (*e.g.*, encrypting data)
- RSA for PK operations (*e.g.*, encrypting IDEA key)
- Encumbrances
 - RSADSI patent on RSA algorithm (US only)
 - Debates about whether permission was granted
 - Resulted in fork: US version with shareware RSA implementation
 - Expired in 2000, no longer an issue
 - IDEA patents in numerous countries
 - Last expire in 2010-2011
 - Government
 - Criminal investigation of Phil Zimmerman in early years
 - Munitions control regulations for encryption stronger than 40 bits
 - US policy liberalized in late 1990s
 - By 2000, export was legal


2



OpenPGP

- Open standard for PGP interoperability
 - Proposed in July, 1997
 - RFC 2440 ratified by IETF in July, 1998
 - As of early 2006, an updated standard is being finalized
- Asymmetric algorithms
 - To RSA, adds DSA (signing) and Elgamal (encryption)
- Symmetric algorithms
 - To IDEA, adds Triple-DES, Blowfish, and others
- Hash algorithms
 - To MD5, adds SHA- {256,384,512} and others
- Compression algorithms
 - To ZIP, adds zlib and BZip2


3



PGP use

- Common uses are encrypting files and email
- PGP plugins are available for most email programs
 - Some security experts have concerns about the use of plugins. Exposing unencrypted data to the email program, which may not be trusted, is the major concern.
- GUI and command line versions are available, both commercially and freely
 - GPG (GNU Privacy Guard) is the leading free implementation, with GUI add-ons and email plugins available
- A commercial DLL is also available for Windows software development
 - EasyByte's Cryptocx


4



Key distribution

- PGP uses an "anarchy" model for keys
 - Certificates can be issued by any user for any user
 - Identity only
 - Trust to sign other keys ("introducer")
 - User indicates the keys he trusts
- Easy to use "out of the box", but may have scaling issues
 - Multiple chains to recipient
 - Multiple keys for some recipients
- Untrusted keys can be used, but software will warn
- Latest versions of PGP also include more PKI-like features

5



Key distribution

- Public keys published on servers (central or your own)
- Can verify with 128-bit cryptographic hash (fingerprint)
- Keys have name and email address fields
 - Disambiguate people
 - Still need to check fingerprint

6



Efficient encoding

- PGP supports various compression methods (originally ZIP only)
- RFC 3156 specifies a multipart MIME for PGP-encrypted data, using Base64 encoding
 - Eliminates many old problems with breaking of text lines, etc.
 - A 1-bit change will invalidate the signature

7



Certificate and key revocation

- A certificate can be revoked by the signer
 - Does not mean that key is necessarily invalid
- Only the owner can revoke a key
- Certificates and keys have optional expiration dates
- Distribution is informal
 - E.g., <http://pgp.mit.edu/>
 - Some newer products have PKI-like features


8



Signature types

- When signing, PGP includes a field indicating whether a message or certificate is being signed
 - Guard against chance that a message would mistakenly be interpreted as a certificate


9



Private key

- PK pair not needed if you only need to verify others' signatures
- PK pair needed
 - To sign
 - To receive encrypted mail
- Private key password
 - MD5 hash is IDEA key to encrypt private key
 - 64-bit CFB with random IV (stored with private key)


10



Key rings

- Data structure containing keys and perhaps certificates
- Private key rings
- Public key rings
 - Can share to distribute all public keys and certificates


11



Object formats

- Encrypted messages with multiple recipients
 - One IDEA key, encrypted with each recipient's public key
- Other formats...
 - Signed messages
 - Encrypted and signed messages
 - Signed human-readable messages
 - Do not compress, plaintext readable if the recipient does not use PGP

12



RFC3156 encrypted example (not signed)

```

From: Michael Elkins <elkins@ero.org>
To: Michael Elkins <elkins@ero.org>
Mime-Version: 1.0
Content-Type: multipart/encrypted; boundary=foo;
        protocol="application/pgp-encrypted"

--foo
Content-Type: application/pgp-encrypted
Version: 1


--foo
Content-Type: application/octet-stream
-----BEGIN PGP MESSAGE-----
Version: 2.6.2

hWGV32hYOCER8GAA/Wcu7d45aDxP4Q08KJpD3v529K1YcUJ2fve871MD1x40j
eM4GDSF1b1b7YVp13H19GL8e/AqbyyJH4a5Y0rK10Q9m8vJY8nL3M0X3Z
qVYQzFcdyryXmyYU8A1d8G8u8Aq9u08K1a2HfcrYy0p0g1b46ev1E29YA
AA8H8byATY4uT1tNCWE11BoqyC6Iqy7UQ21sBrXg6Cuk588bukLeauQW3
1y11d70JulaChm8/ZnaD9vDVCv0010C18+
+BAK
-----END PGP MESSAGE-----

--foo--

```

13



RFC3156 signed example (not encrypted)

```

From: Michael Elkins <elkins@ero.org>
To: Michael Elkins <elkins@ero.org>
Mime-Version: 1.0
Content-Type: multipart/signed; boundary=bar; micalpgp=mt;
        protocol="application/pgp-signature"

--bar
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

>Ahhhh!

Did you know that talking to yourself is a sign of sanity?

It's generally a good idea to encode lines that begin with
From: because some mail transport agents will insert a greater-
than (>) sign, thus invalidating the signature.

Also, in some cases it might be desirable to encode any >20
trailing whitespace that occurs on lines in order to ensure >20
that the message signature is not invalidated when passing >20
a gateway that modifies such whitespace (like BITNET). >20

me


--bar
Content-Type: application/pgp-signature
-----BEGIN PGP MESSAGE-----
Version: 2.6.2

1Q79w08N1vEF28v8Bp0f0Ag00g0c17u8v08jy48zG81b3h3G1X/LC//
3Y78bW4210P1d8aT1p8b08y9v1d388zG08v08A+78b08C7C418q
u8b08v0c17118b08v1g/287PzP881aT70/77p08d0w/08f11788w
K08a4b4z+
+BAK
-----END PGP MESSAGE-----

--bar--

```

14



Additional references

- http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
- http://en.wikipedia.org/wiki/Pretty_Good_Privacy

15
