Secure Communication & Data Sharing with PGP

Bankim Tejani
Agenda

- Refresher on encryption basics
- Why protect your data?
- Why PGP?
- How do I use PGP?
- Uses beyond secure e-mail
Symmetric Encryption

- Typically private key or shared key
- Fast, efficient
- Only as secure as the key
- DES, 3DES, AES, Camellia
Asymmetric Encryption

- a.k.a. Public Key or Public/Private key pair encryption
- Trust & authentication
  - Certificate Authority
- Only as secure as private key
- RSA, PGP
Hashing

- One-way function
- Deterministic & efficient
- Small change to input creates dramatic entropy in output
- Fantastic for checksums
- MD5, SHA, MACs, signatures
Protect Your Data

- Data privacy laws - GDPR
- Privacy policy / Terms of Service
- Employment agreement
- PCI, SOX, other
- It's your data too!
- Don’t be evil…
Pretty Good Privacy (PGP)

- Developed 1991, P. Zimmerman
- Survived lawsuits, sanctions, corporate takeovers, and t-shirts
- “the closest you’re likely to get to military-grade encryption.”
  - Bruce Schneier
- Free!
Pretty Good Privacy (PGP)

- Asymmetric cryptography
- Hash-based signatures
- Public key repositories
- Web of trust
**Sender | Signing & Encryption Process**

- **Raw File**
- **Sender's Private Key**
- **Receiver's Public Key**
- **Signed & Encrypted File**
- **Email or FTP**

**Receiver | Decryption & Verification Process**

- **Email or FTP**
- **Signed & Encrypted File**
- **Receiver's Private Key**
- **Sender's Public Key**
- **Raw File**
Using PGP

- Get software
- Generate your keys
- Share & download public keys
- Encrypt & sign
- Decrypt & verify
- Share
Web of Trust

- Trust through network
- Sign others’ public keys to indicate trust
- Shared publicly via keyservers
Hey, I just got home from the party.

The one with the IRC folks?

Yeah.

How was it?

Got too drunk. I screwed up, bad.

What happened?

There was a girl. No idea who she was. Don't even know her name. I was too drunk to care.

And what, you slept with her?

No. I signed her public key.

Shit, man.
Innovative Uses

- Data pipelines
- Data sharing w/ partners
- Report / data protection
- Log protection / integrity
- Disk Images
I've been posting my public key for 15 years now, but no one has ever asked me for it or used it for anything as far as I can tell.

Maybe I should try posting my private key instead.