4-3-1 Safer EMail

The Key Points

Authenticity of Servers

Encrypted Transport

It's Easy

- **Do not use pop, it is in the clear**

- **Use pop3s̲, port 995 over TLS/S̶S̶L̶**

- **Do not use imap, it is in the clear**

- **Use imaps̲, port 993 over TLS/S̶S̶L̶**

- **And they Authenticate the Servers using X.509 Certificates. CHECK IT!**

Fetch Using IMAP4S

▼ **randy@psg.com**	**Server Type:** IMAP Mail Server
Server Settings	**Server Name:** ran.psg.com Port: 993 ↕ Default: 993
Copies & Folders	
Composition & Addressing	**User Name:** randy
Junk Settings	
Synchronization & Storage	**Security Settings**
OpenPGP Security	Connection security: SSL/TLS ↕
Return Receipts	
Security	Authentication method: Normal password ↕
▼ randy@iij.ad.jp	
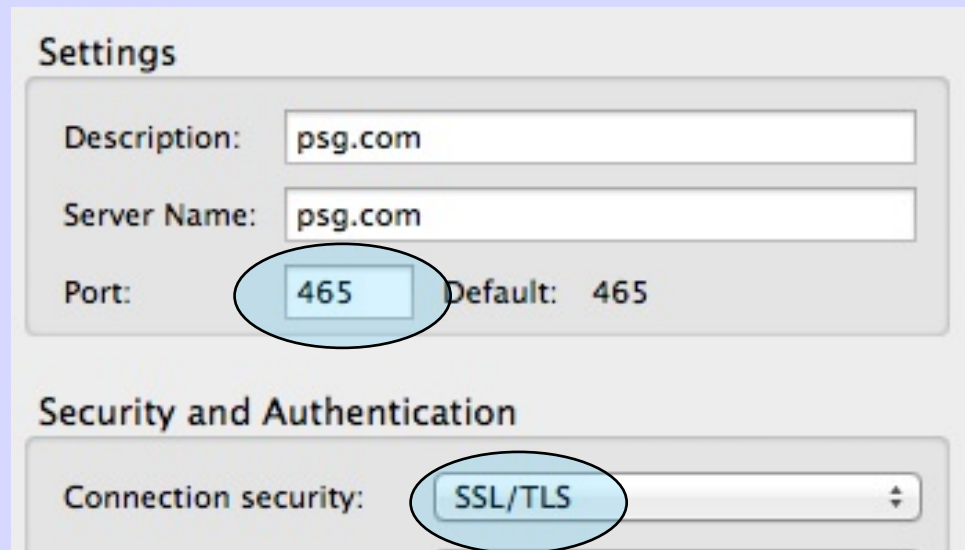
SMTPS over TLS/~~SSL~~

- ## Do Not Use Unencrypted SMTP/25

Settings

Description: psg.com

Server Name: psg.com

Port: 465   Default: 465

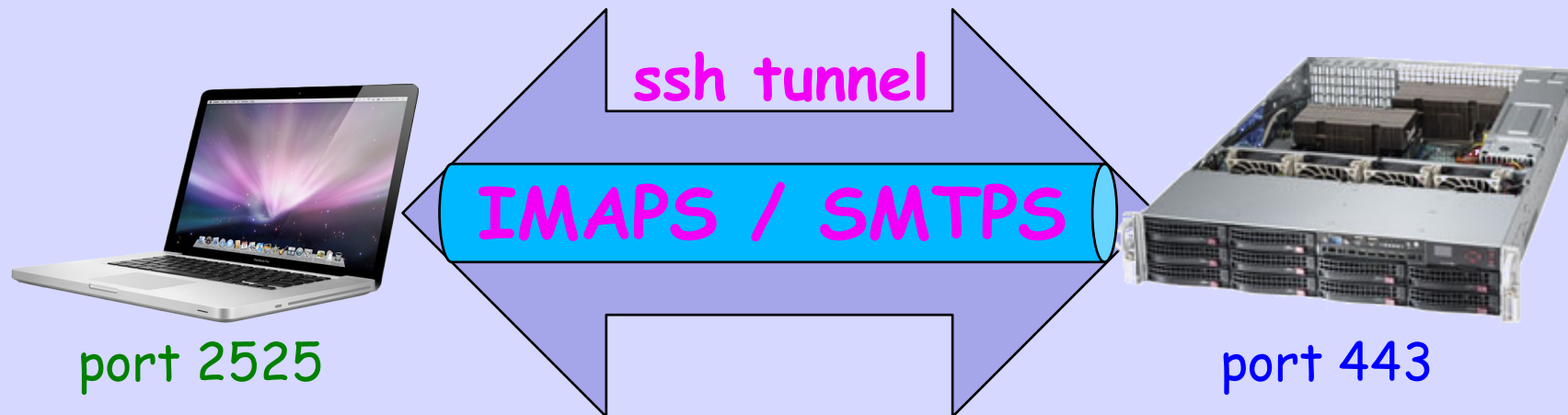### Security and Authentication

Connection security: SSL/TLS

Authenticate Servers

- **Assume the Wire is Tapped**

- **Assume Someone will Spoof Servers**

- **Know Your Servers' Root Certificates**

- **Confirm Certificates on Configuration**

- **Choose Good Passphrases**

Encrypt Critical EMail

- **Assume the Wire is Tapped**

- **Use a Personal X.509 PKCS#12 User Certificate with SMIME – T'Bird etc.**

- **Use a PGP key with Enigma – T'Bird**

Creative Commons: Attribution-NonCommercial-ShareAlike

I Tunnel & Use IMAPS

ssh tunnel

IMAPS / SMTPS

port 2525

port 443

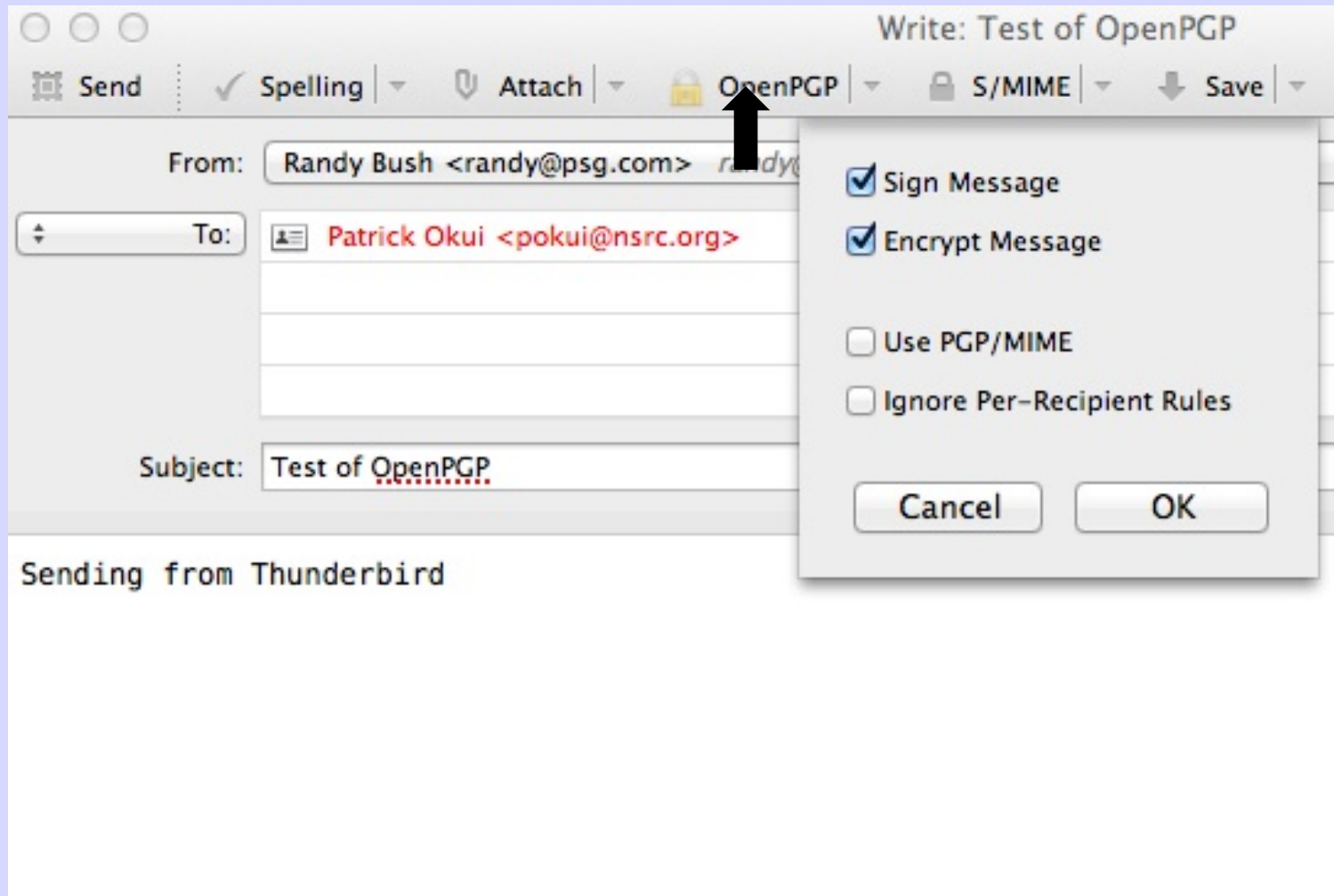`$ ssh -N ssh.psg.com -p 443 -L 2525:127.0.0.1:25`

Target
Host

Tunnel
Port

Port on
MacBook

Tunnel
EndPoint

Using PGP

Of Course
All Our Mail Goes To The NSA, GCHQ, PLA, …

Or You Can Give It To The World's Largest Spy Agency Google / GMail