

4-3-2 Safer EMail

The Key Points

Authenticity of Servers

Encrypted Transport

It's Easy

- Do not use pop, it is in the clear
- Use pop3s, port 995 over TLS/~~SSL~~
- Do not use imap, it is in the clear
- Use imaps, port 993 over TLS/~~SSL~~
- And they Authenticate the Servers using X.509 Certificates. CHECK IT!

Fetch Using IMAP4S

The screenshot shows the settings for an email account named 'randy@psg.com'. The 'Server Settings' section is active, showing the following configuration:

- Server Type:** IMAP Mail Server
- Server Name:** ran.psg.com
- Port:** 993 (highlighted with a blue oval)
- Default:** 993
- User Name:** randy

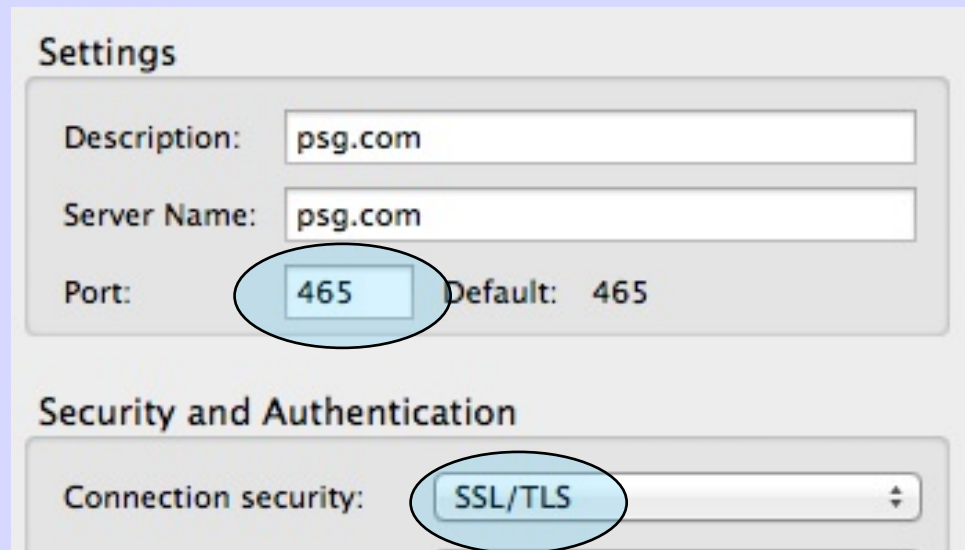
The 'Security Settings' section is also visible, with the following configuration:

- Connection security:** SSL/TLS (highlighted with a blue oval)
- Authentication method:** Normal password

The left sidebar shows a list of settings categories for 'randy@psg.com' and 'randy@iij.ad.jp', with 'Server Settings' selected for 'randy@psg.com'.

SMTPS over TLS/~~SSL~~

- Do Not Use Unencrypted SMTP/25



The image shows a screenshot of an email client's settings window. The window is titled "Settings" and contains two main sections: "Settings" and "Security and Authentication". In the "Settings" section, there are three fields: "Description:" with the value "psg.com", "Server Name:" with the value "psg.com", and "Port:" with the value "465". The "Port:" field is circled in blue. To the right of the "Port:" field, it says "Default: 465". In the "Security and Authentication" section, there is a "Connection security:" label followed by a dropdown menu. The dropdown menu is open, showing "SSL/TLS" as the selected option, which is also circled in blue.

Settings

Description: psg.com

Server Name: psg.com

Port: 465 Default: 465

Security and Authentication

Connection security: SSL/TLS

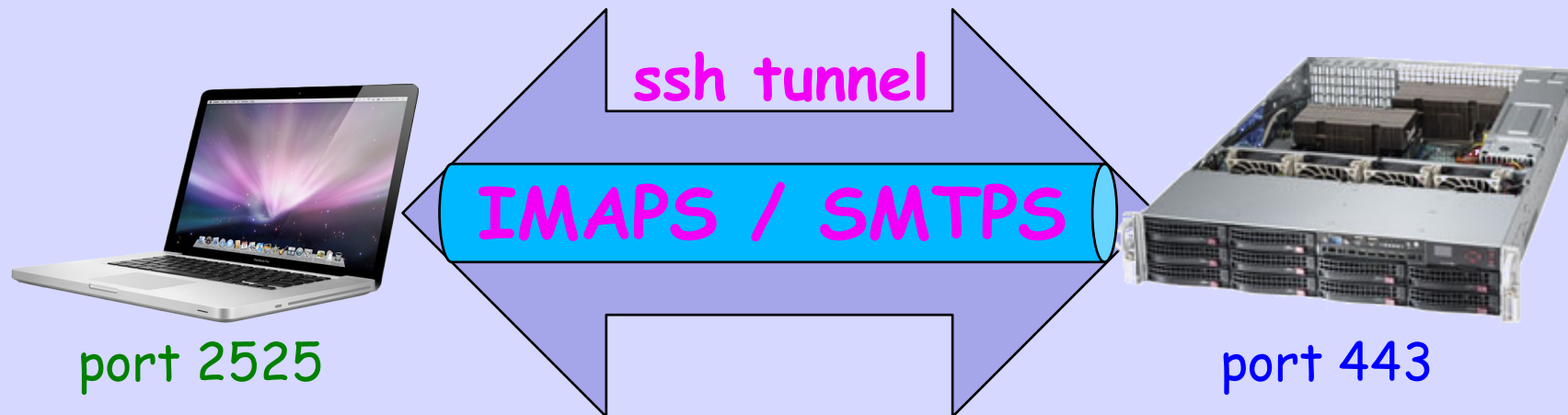
Authenticate Servers

- 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

I Tunnel & Use IMAPS



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

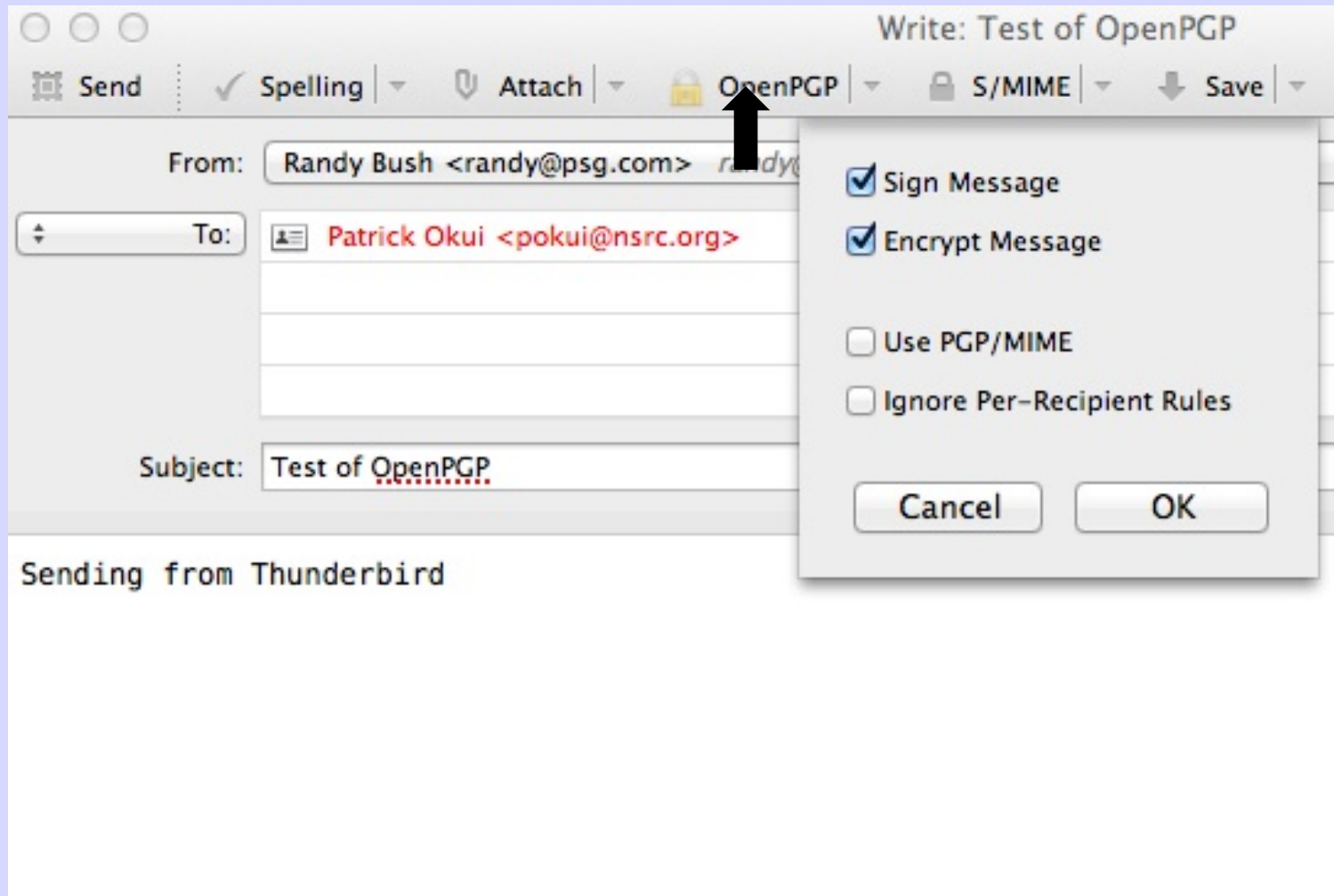
Target
Host

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