

EMAIL SECURITY

Navneet Scientist 'B'
Indian computer Emergency
Response Team

What is secure email?

- Login and passwords are encrypted
- Email contents are encrypted
- Authentication is required
- Cannot be “sniffed” by internal or external monitoring
- Does not rely on internal IT resources or employee honesty

Why is email security important?

- Regular email has no more security than a post-card
- Regular email can be easily “sniffed” from any PC on the network, ISP etc.
- Liability, lawsuits, exposure for failure to protect information
- Disgruntled employees, competitors

Choices available in the secure email

- PGP (Pretty Good Privacy)
- S/MIME
- SSL/TLS web-browser based email
- SSL/TLS POP/SMTP email

More about PGP

- Average users need extensive support
- Requires Key Exchange, Key management
- Not scalable
- Little industry support
- Can only exchange secure email with other PGP users

More about S/MIME

- Similar to PGP, requires administrator installation & configuration, support intensive
- User must download and install software
- Many installations have failed due to complexity
- Can only exchange emails with other S/MIME users

More about special providers

- Managed services using S/MIME with PKI key exchange
- Appliance based services with special hardware, requires integration
- Expensive, only starts becoming cost effective for systems with 500 + users

About secure webmail

- Nothing to download or install, no support issues beyond typical email
- Works with any web browser (Internet Explorer, netscape, Mozilla etc.)
- Uses SSL/TLS (RSA) security, same system used banks, VISA, etc.
- Easy to add, manage users
- No training needed - simple

About POP/SMTP secure email

- Works with all email programs (Outlook, Eudora, etc.)
- Uses SSL/TLS (RSA) security -same system used by banks, VISA, etc.
- Easy to set up, no downloads or installation, same support issues as traditional email

THANK YOU