Securing Email

CS 594/Kent Law Privacy and security

2 Practical Uses of Crypto

- Securing data at rest on e.g., laptops, backup tapes, etc.
- Signature and/or encryption of email for:
  - Confidentiality
  - Integrity
  - Nonrepudiation

Email Crypto in Practice

- 2 Main systems:
  - PGP: "pretty good privacy": originally free, now company, also free GNUPG version
  - S/MIME standard: built into Outlook, Outlook Express, Mail.app, Thunderbird
    - Eventual standards war winner?

Your mission

- Send a signed (but not encrypted) email to sloan@uic.edu using S/MIME.
- Receive back a signed encrypted message from me.
- Send me another message that is both signed and encrypted.

Problem w/Email crypto

- Big conceptual problem is key management
- Web of trust model troublesome in practice at Internet scale—I trust who you trust who they trust who. . . ?!
- Certificate Hierarchy great inside one org; troubling inter-organization.

Keys in S/MIME

- Certificate Authority Model
- Two big well-known CAs give out free email certificates:
  - Thwate (owned by Verisign)
  - Comodo

About email

- Email provider (UIC, Gmail, Yahoo) stores the actual bits.
- 3 protocols—ways to get at them:
  - POP
  - IMAP
  - Webmail—read with web browser. This one is a problem with S/MIME.

POP, IMAP

- You read both of these with a mail reader, piece of software on your computer such as Outlook (Express) or Thunderbird
- POP (older): The bits get permanently moved from email provider to your PC
- IMAP: bits still live on their computer.

Notes

- Gmail provides both POP and IMAP access for free. Yahoo provides POP only for pay, and no IMAP option.