E-mail List Services (ELSs)

- ELs enable users to easily exchange emails
  - LS bears all the overhead
- Increasingly popular for exchange of both public and private content; i.e., security is an important concern
  - E.g., there are over 300,000 registered lists on LISTSERV while only 20% of them serve public content
- Little or no work in providing security solutions for ELs
  - We provide SELS: Secure Email List Services

Security Requirements in ELs

- Confidentiality: only authorized users (i.e., list subscribers) should be able to read emails - list server is excluded; e.g., Security lists concerning infrastructure protection
  - Executives lists concerning corporate strategies
  - Collaborative healthcare lists concerning patient data
- Integrity: receivers must be assured that email has not been modified in transit
- Authentication: receivers must be able to verify the identity of the sender

Proxy Encryption

- Allows transformation of a cipher-text encrypted under one key, say PK_U, to a cipher-text encrypted under a different key, say PK_U', without access to the clear-text
- Cipher-text C_K of clear-text M encrypted under ElGamal public-key PK_LK = g_LK
  \[ C_{LK} = (g^{rL_K} \cdot M, g^r) \]
- Transformed cipher-text C_U of clear-text M encrypted under ElGamal public-key PK_U = g^U
  \[ C_U = ((g^{rL_U})^{-1} \cdot (g^{rL_K} \cdot M, g^r)) = (g^{rU} \cdot M, g^r) \]
where LK = U + U' and transforming agent (LS) knows U'.
- Applications - file-sharing, key-escrow, secure and certified e-mail mailing lists
- SELS is the first deployable Proxy Encryption application

Secure List E-mail with SELS

- Key Store: Members’ corresponding private keys K_U

SELS Architecture

- Goals
  - Compatibility with existing e-mail infrastructure
  - Use of COTS security tools and components
- Design approach
  - Build on GPG for integration with client MUAs
  - Develop plugins for List Servers/MTAs; e.g., Mailman
- SELS Compatibility
  - Client side: Works with Emacs, Mac Mail, Mutt, Outlook, Thunderbird
  - Server side: Works with Mailman, Sendmail
- Status
  - List Moderator (LM) software released
  - Test List Server operating at NCSA
  - List Server (LS) software release forthcoming

Software Development

- Key Store: (PK_L, SK_L)
- Transform k w/ K_U' (SELS Proxy Re-encryption)