

EMail Privacy Efforts

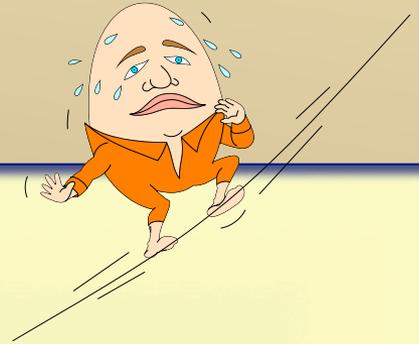
(ignoring secure sms/chat/im/social/...)

D. Crocker

Brandenburg InternetWorking

21 July 2014

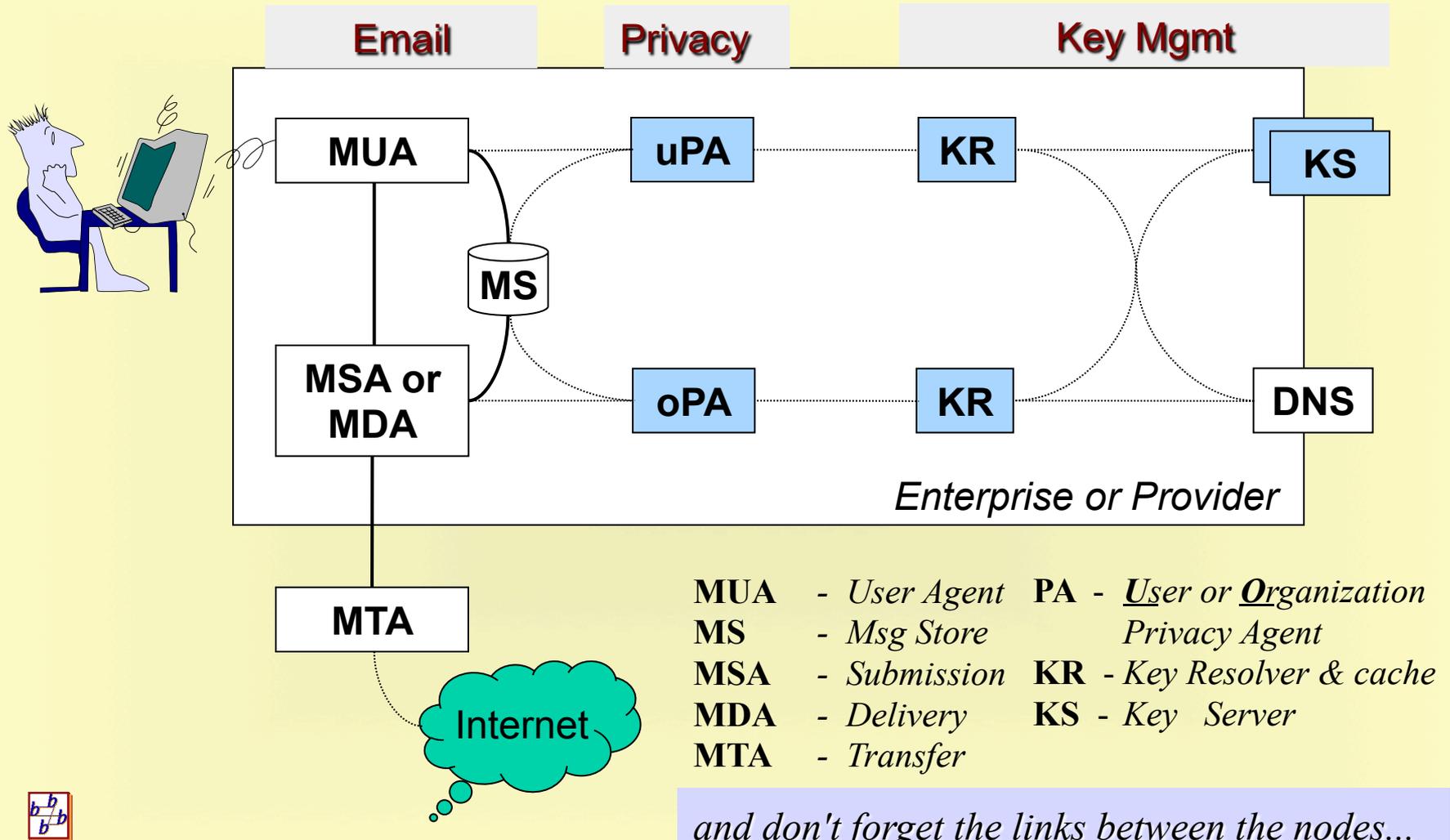
Threats



- **Author spoofing**
 - Is purported creator/submitter of message is the actual?
- **Service provider spoofing**
 - Is intended provider (mail, key, DNS) is the actual provider?
- **Message content disclosure**
 - Limit disclosure only to authorized parties -- recipients
- **Message structure disclosure**
- **Metadata disclosure**
 - Participant & message attributes, permitting social and network traffic analyses; relationships and activity

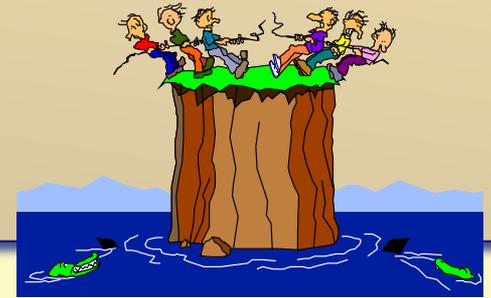


Basic Email Privacy Components



and don't forget the links between the nodes...

Vectors



- Password to account
- Key for signing/ encryption
- Certificate with key and attributes
- Key server
- Advanced Persistent Threats (APT)
- DNS and Domain Names
- Transmission Channel
- Mail Server
- Client

Who must you trust?
Who do you trust?
And with what?



TLS is good hygiene, but...



- **CA-based enforcement is lagging**
 - with 'opportunistic' meaning open to MITM
- **Leaves intermediaries vulnerable**
- **So what about...**
 - End-to-end protection that really is end-to-end?
 - *Wrap the message, not the channel!*



Long-Term Poor Adoption

- **Email content (body) encryption**
 - PGP
 - S/MIME
- **Barriers are systems-level, not crypto**
 - Key management at scale
 - User (and operator) usability limitations
- **Popular topic now, for some reason**
 - 100+ efforts around 'messaging', maybe 25+ for email

<https://github.com/OpenTechFund/secure-email>

<http://cups.cs.cmu.edu/soups/2014/workshops/effcup.html>



(Some) Current Projects

- **Web Mail**

- Lavaboomb
- Mega
- PrivateSky
- ProtonMail
- Scramble
- Startmail
- Whiteout

- **Browser Extensions**

- Mailvelope
- End-to-End

- **Self-Hosted Email**

- Dark Mail Alliance
- FreedomBox
- Mailpile
- Mail-in-a-box
- kinko



(Some) Current Projects

- **Mail Clients**

- Bitmail
- Mailpile
- Parley

- **Email Infrastructure**

- Dark Mail Alliance
- LEAP Encryption Access Project

- **Post-email alternatives**

- Bitmessage
- Bote mail
- Cables
- Dark Mail Alliance
- Enigmabox
- FlowingMail
- Goldbug
- Pond



Basic Email Message Components

- **Envelope** (*rcpt-to, mail-from*)
 - Difficult to deliver if dest address not in the clear...
- **Header**
 - User (*to, from, cc, date, subject...*)
 - Ops (*received, return-path...*)
- **Content**
 - Body - Attachments
 - Body - Structure



Key Management



- **Assignment**
- **Discovery**
- **Validation**
- **Availability**
- **Revocation**
- **Rollover**



Example work



- **Walled garden**
 - Product / Service
 - Address book vs. transport
 - E2E protection
- **Better**
 - Crypto (OTR, PFS, ...)
 - Cert mgmt (Revocation, structure, TOFU, Bitcoin clone-ish...)
 - Packaging (TOR-ish)
- **Usability**
 - Automatic key mgmt
 - Automatic key use
 - Safety flags & signals
- **Storage**
 - Encrypted
- **P2P exchanges**
 - Key 'invitation'
 - Transport
- **Replace**
 - Certs (DNSChain,...)
 - Transport (eg, TOR)
 - SMTP
- **OpenPGP**
 - Integration
 - Facilitation
 - Turnkey & sanitized

