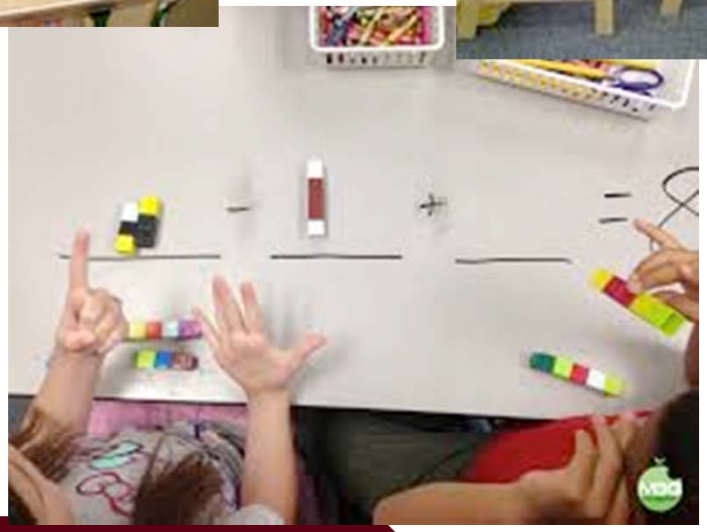
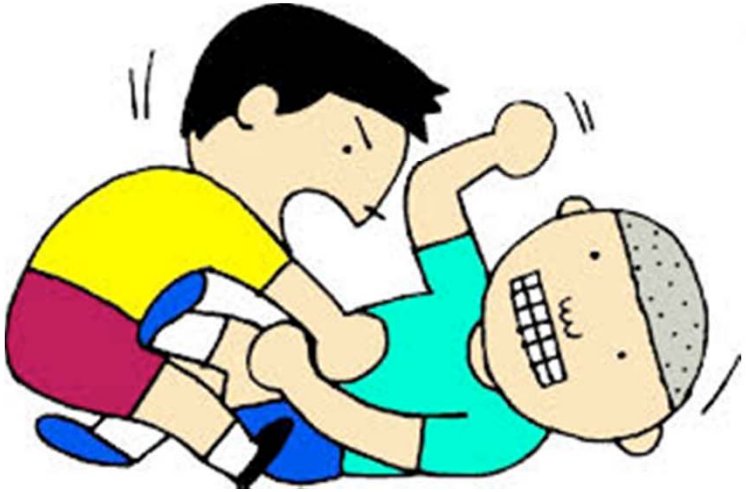
Internet Standards

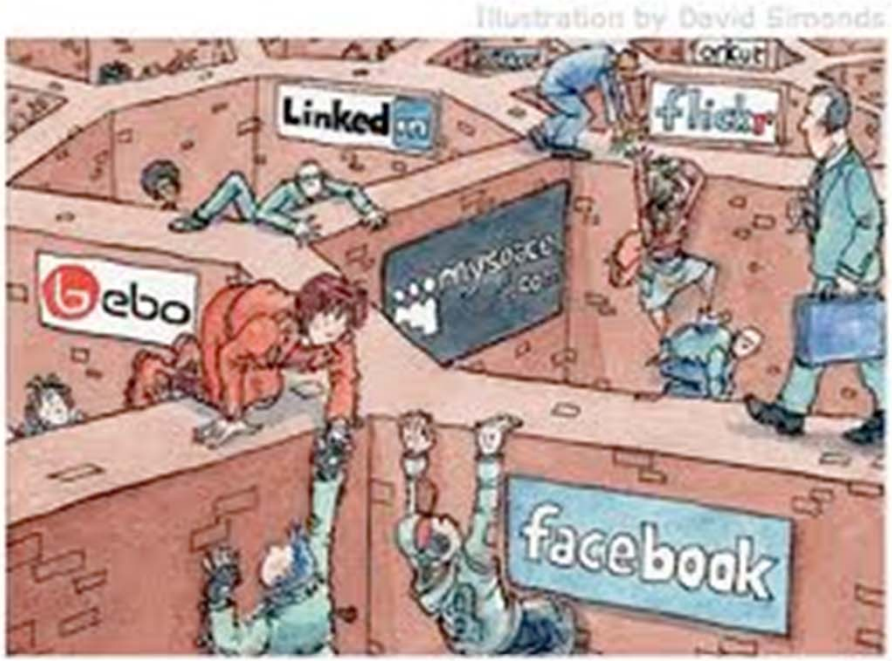
Sam Silberman, Constant Contact

What are Standards?



World without Standards





We live in a connected world

Topics

- DMARC (Indirect flows)
- Security/Privacy
  - TLS over SMTP
  - End-to-end encryption
- SMTP over IPv6
- Activities in the IETF APPSAWG

How does DMARC work?

- Organization publishes a DMARC policy on their domain
  - P=none
- Participating ISPs sends the organization authentication and forensic reports
- Organization audits their outbound sending practices
  - Centralizes outbound mail
  - DKIM signs all outbound mail
  - Publishes/updates SPF
  - Repeat
- Only after exhaustive analysis, organization can enable DMARC p=reject

Who should enable DMARC?

- Large organizations who's brand (domain name) is used as part of a phishing scam.
  - Banks (Bank of America, Amex)
  - Popular brands (PayPal, Ebay, Amazon)
  - Government agencies (IRS)

Who should not use DMARC?

- When individuals within the org need to send mail via indirect flows
  - Mailing lists
  - ESPs
  - Proxy/forwarders
- Any organization where the mailbox owner requires to send mail via Indirect flows.
  - Mailbox service providers (ISPs)
  - Large corporations (no brand risk)

Proposed Mitigations

- Customer use non-DMARC hosted mailbox
- Proxy FROM address (Address re-write)
  - FROM “Sam” sam+yahoo.com@ccsend.net
  - Reply-To: sam@yahoo.com
- Obtain permission to DKIM sign on behalf of ISP
  - AOL.COM CS.COM AIM.COM
- Relay through domain owner’s SMTP server

Proposed Mitigations

"Delegating DKIM Signing Authority”
draft-kucherawy-dkim-delegate-01 (work in progress), June 2014.

"DKIM Conditional Signatures”
draft-levine-dkim-conditional-00 (work in progress), June 2014.

"A List-safe Canonicalization for DomainKeys Identified Mail (DKIM)”
draft-kucherawy-dkim-list-canon-00 (work in progress), June 2014.

"Recognized Transformations of Messages Bearing DomainKeys Identified Mail (DKIM) Signatures”
draft-kucherawy-dkim-transform-00 (work in progress), April 2015.

"Third-Party Authorization Label”
draft-otis-tpa-label-00 (work in progress), May 2014.

Reference: https://datatracker.ietf.org/doc/draft-ietf-dmarc-interoperability/

Security / Privacy

- Session (point to point) encryption TLS
- End-to-end encryption

Security / Privacy

The DNS Based Authentication of Named Entities (DANE)

Session (point to point) encryption TLS

- DANE Opportunistic TLS
  - SMTP security via opportunistic DANE TLS
    - draft-ietf-dane-smtp-with-dane-16

- DANE published keys
  - TLS Protocol using TLSA record in DNS
  - RFC 6698 (was draft-ietf-dane-protocol)

Security / Privacy

End to End Encryption

Dane

- Using DANE to Associate OpenPGP public keys with email addresses
  - draft-ietf-dane-openpgpkey-03

- Using Secure DNS to Associate Certificates with Domain Names For S/MIME
  - draft-ietf-dane-smime-08

Security / Privacy

End to End Encryption

De facto standards (browser plug-ins)

- Google
  - https://github.com/google/end-to-end/wiki
- Yahoo
  - https://github.com/yahoo/end-to-end

SMTP over IPv6

- **SMTP IPv6 to IPv4 Fallback**
  - http://tools.ietf.org/html/draft-martin-smtp-ipv6-to-ipv4-fallback-01
- Required authentication (best practice)
  - Linkedin position
    - https://engineering.linkedin.com/email/sending-and-receiving-emails-over-ipv6
  - Google's position
    - https://support.google.com/mail/answer/81126?p=ipv6_authentication_error&rd=1#authentication

Activities in the IETF APPSAWG

Message Disposition Notification (updates for gateways and I18n)

http://datatracker.ietf.org/doc/draft-ietf-appsawg-mdn-3798bis/

Message Header Field for Indicating Message Authentication Status

draft-ietf-appsawg-rfc7001bis-07

Email Authentication Status Codes (SPF AND DKIM)

RFC 7372 (was draft-ietf-appsawg-email-auth-codes)

Next Steps

- Get Involved

- DMARC
  - Speak up about indirect flows
  - Propose solutions
- SMTP Encryption
  - Implement Opportunistic TLS

Questions?

Sam Silberman
ssilberman@constantcontact.com
@samuelsilberman