Pushing The Envelope

The state of DMARC and the future of email

Jesse Thompson
Solutions Architect
DoIT User Services
What is DMARC?

Domain-based Message Authentication Reporting and Conformance

1. Authenticate Domain to Message
2. Reporting:
   - Visibility
   - Feedback
3. Conformance:
   - Protection
   - Governance

DMARC
(SPF is valid OR DKIM is valid)
AND SPF/DKIM domain is aligned with From domain

RFC 7489

dmarc.org
Mail Flow

- **Inbound spoofing**
  - On-Prem MTAs (Oracle, Sophos)
  - Inbound mail flow

- **World**
  - DMARC Spoofers

- **Office 365**
  - Exchange Online Protection
  - Exchange Online
  - Intra-user mail flow

- **G Suite**
  - G Suite Scanning
  - Google Groups
  - Outbound mail flow

- **WiscList, SMTP Auth, SMTP Relay**

- **Outbound mail flow**
State of DMARC - @wisc.edu

External spoofing protection (via SPF and DKIM)
- \( p=\text{quarantine} \ pct=50 \) (100% in July)
- [DNS query](https://dns.google.com/resolve?name=_dmarc.wisc.edu&type=TXT)
- No loosely-integrated cloud services
- SPF limit - means that subdomains are necessary

Inbound protection (via local policy)
- Tagged with [CAUTION: External]
- And From header is rewritten
- We will allow exemptions

[go.wisc.edu/email-authenticity](go.wisc.edu/email-authenticity)
DMARC - subdomains

New! General purpose - e.g. brand@u.wisc.edu

Or bring your own - e.g. something@brand.wisc.edu

Why are subdomains good?
Compartmentalizes risk, visibility, and manageability

Dmarcian service

Consultation from DoIT. Contact: dmarc@doit.wisc.edu
DMARC next steps

1. wisc.edu DMARC to pct=100
2. DMARC consultation as a service
3. Backfill subdomain DMARC records
4. Protect unused subdomains from spoofing
5. subdomains DMARC to pct=100
6. Leverage Dmarcian (or successor)
7. (Dynamic SPF?)
8. (Dmarcian successor?)
DMARC Forwarding challenge

example.com IN TXT "v=spf1 ip4:192.168.1.100"

Sender 192.168.1.100

Subject: ...

Intermediary 10.23.45.99

Subject: ...

Recipient

@
DMARC Forwarding challenge

All internet mailing lists need to rewrite the From
- Great opportunity to upgrade!
- Join: email-forwarders@g-groups.wisc.edu

Google Groups works better than O365
- If your list has non-UW members that can post

ARC (new standard supposed to fix forwarding problem)
- Doesn’t have a reputation component
- All mailing lists still need to rewrite the From header

We need to rethink how users forward their O365 email
DMARC inbound protection

Current:
- Subject is tagged & From header is rewritten
  - only wisc.edu is protected
- Some inbound spoofing is allowed (local policy)
- Spam scanning exemptions - using DMARC

Future:
- Reject or junk non-compliant messages
- Protect subdomains with similar controls
- Enforce published DMARC policies for non-UW domains
Sending email - existing

Office 365
- Authorizes user → email_address
- DKIM signs and passes SPF
- Can integrate via SMTP, Graph or EWS
- Supports OAuth integration (e.g. Salesforce)

SMTP Relay - plan to de-emphasize
- Does not DKIM
- Does not authorize user → email_address
- Does not prevent UW from spoofing other domains

SMTP Auth - phasing-out
- Duplicative of O365
Sending email - future

Rolling out: AWS Simple Email Service
- Requires SMTP+Auth+TLS
- Requires defined IAM policy
- New opportunities - metrics, feedback-loops

Future: Email API (Interop)

Potentially: 3rd party services
- Need integration of user→email_address data
- Need to reconcile UDS data feeds
  - difference between HR business address vs. the users’ primary address
- Need to build dynamic SPF

Strategy: Move away from IP-based auth
Moving beyond DMARC

DMARC only protects the domain in the From header...
Email Encryption

- **S/MIME - bearish**
  - Client support is getting worse
  - Lacks strong cert validation
  - Most people don’t use it for encryption anyway

- **Office 365 Message Encryption**
  - Available now in Outlook and web
  - Easy to use, strong encryption, strong authentication
  - Can be automatically enabled with data loss policies

- **SMTP+TLS**
  - Required for some domains
  - Others: opportunistic
  - Currently: Lacks any cert validation
  - EFF: STARTTLS Everywhere
  - IETF: MTA-STS, DANE, RequireTLS
Modern threats

Display name spoofing
- “Rebecca Blank” <chancellorblank@gmail.com>

Compromised credentials on the rise
- Attacks against non-MFA protocols
- DMARC makes credentials more valuable
- Credential stuffing

Bad industry practices
- List appending and ignoring unsubscribe rules
- Free tiers and no-hassle spoofing by email services
- Email address “verification” services
Strategic thoughts

Email will never die
- Need to secure it from abuse and enable more authentication and encryption
- Global identity system - e.g. Password reset emails
- People don’t want to trust Facebook / Twitter

New modes of communication and collaboration
- Chat and webhooks
- Supplement bulk email with SMS
- Use native “portal” communications within cloud services
Questions?

jesse.thompson@wisc.edu

go.wisc.edu/email-authenticity

https://www.ren-isac.net/events/techbursts/techburst_110118.html

Or find me on MS Teams and Google Chat