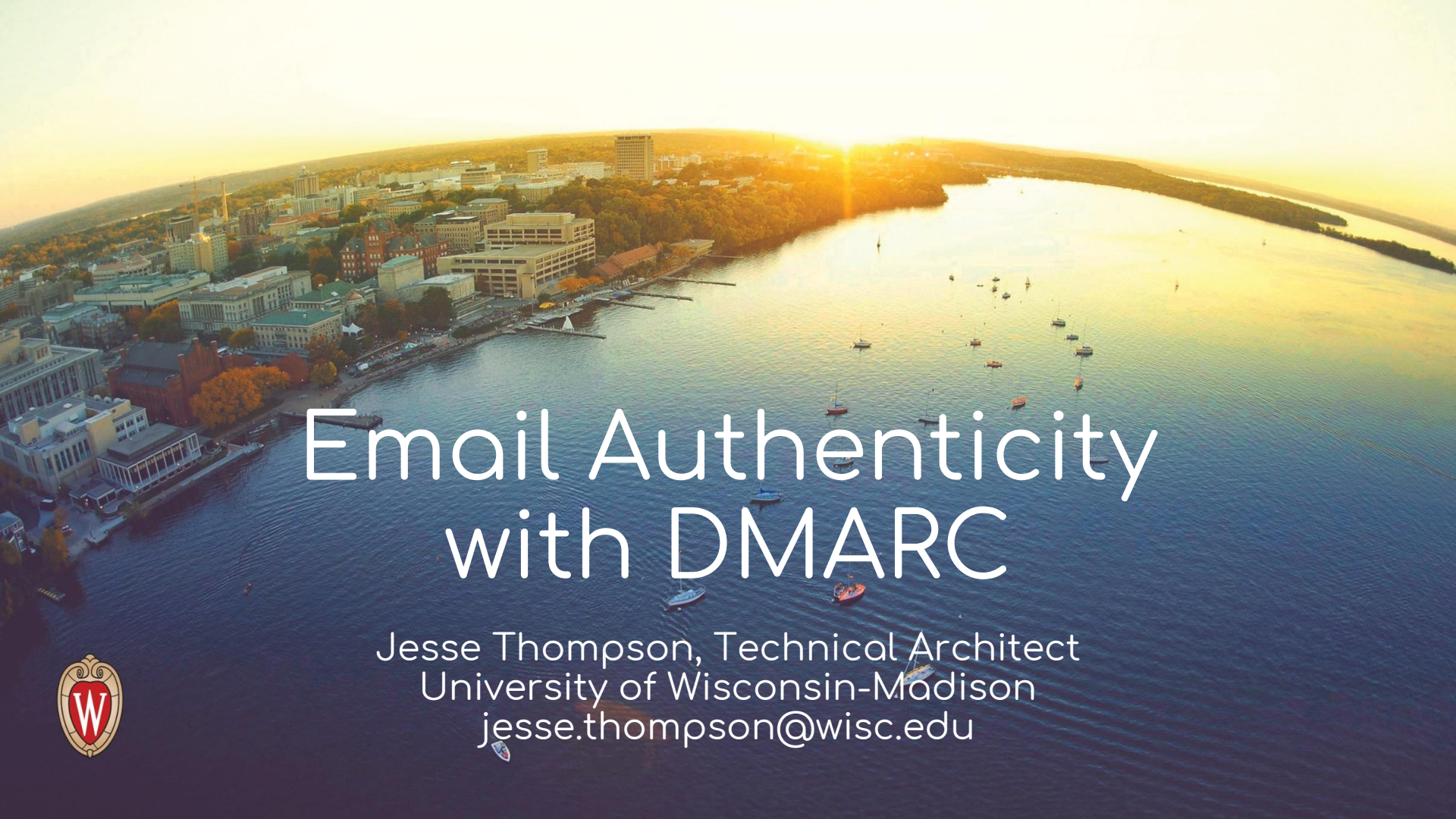


Email Authenticity with DMARC

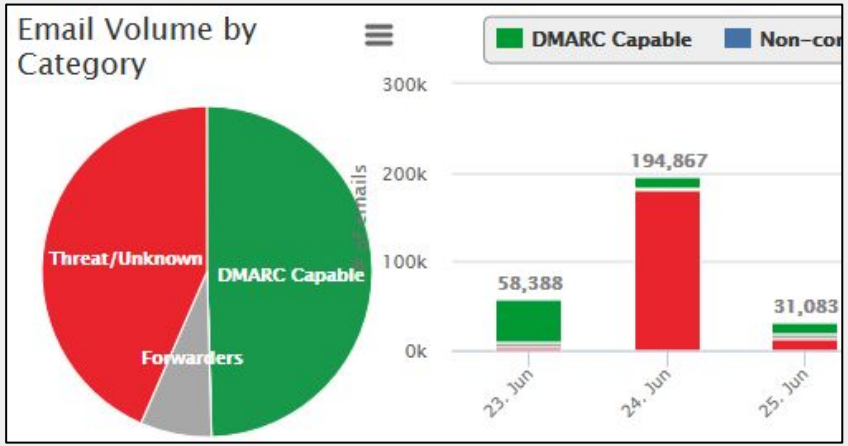
Jesse Thompson, Technical Architect
University of Wisconsin-Madison
jesse.thompson@wisc.edu

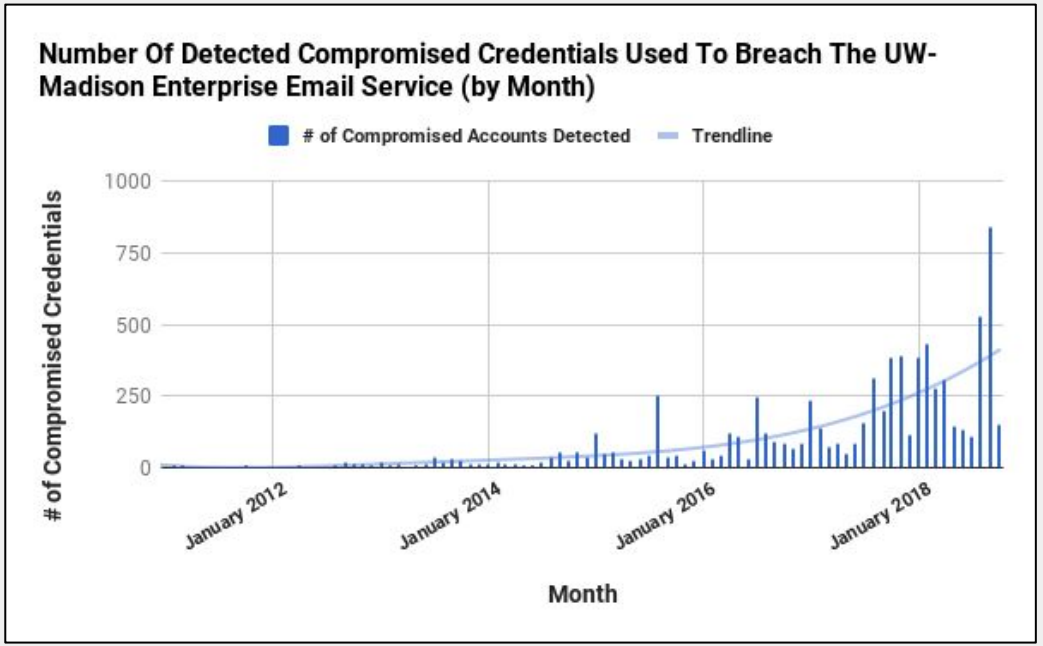
Motivation → Authenticity

- Mail your institution sends isn't accounted for
- Mail claiming to be your domain may be fraud
- Instead of filtering the bad...we start authenticating the good?

Functional Motivators for Email Authenticity

1. Deliverability: Google/MS/etc starting to require
2. Policies: [DHS Binding Operational Directive 18-01]
3. Security: Stop abuse





Build on SPF

SPF = Sender Policy Framework

Publish in DNS a list of servers authorized for MAIL FROM (SMTP envelope return path). Receivers consult list.

https://tools.wordtothewise.com/spf/check/wisc.edu

wisc.edu. 3600 IN TXT "v=spf1 ip4:144.92.197.128/25 ?all"

Build on DKIM

DKIM = Domain Keys Identified Mail

Attach signatures to email. Public key in DNS. Receivers verify signature.

https://tools.wordtothewise.com/dkim/check/wisc.edu/selector1

DKIM-Signature: v=1; a=rsa-sha256; d=wisc.edu; s=selector1; c=relaxed/relaxed; q=dns/txt; t=1126524832; x=1149015927; h=from:to:subject:date:keywords:keywords; bh=MHIzKDU2Nzf3MDEyNzR1Njc5OTAyMjM0MUY3ODlqBLP=; b=hyjCnOfAKDdLZdKIc9G1q7LoDWlEniSbzc+yuU2zGrtruF00ldcFVoG4WTHNiYwG

Build on SPF and DKIM

SPF Problems:

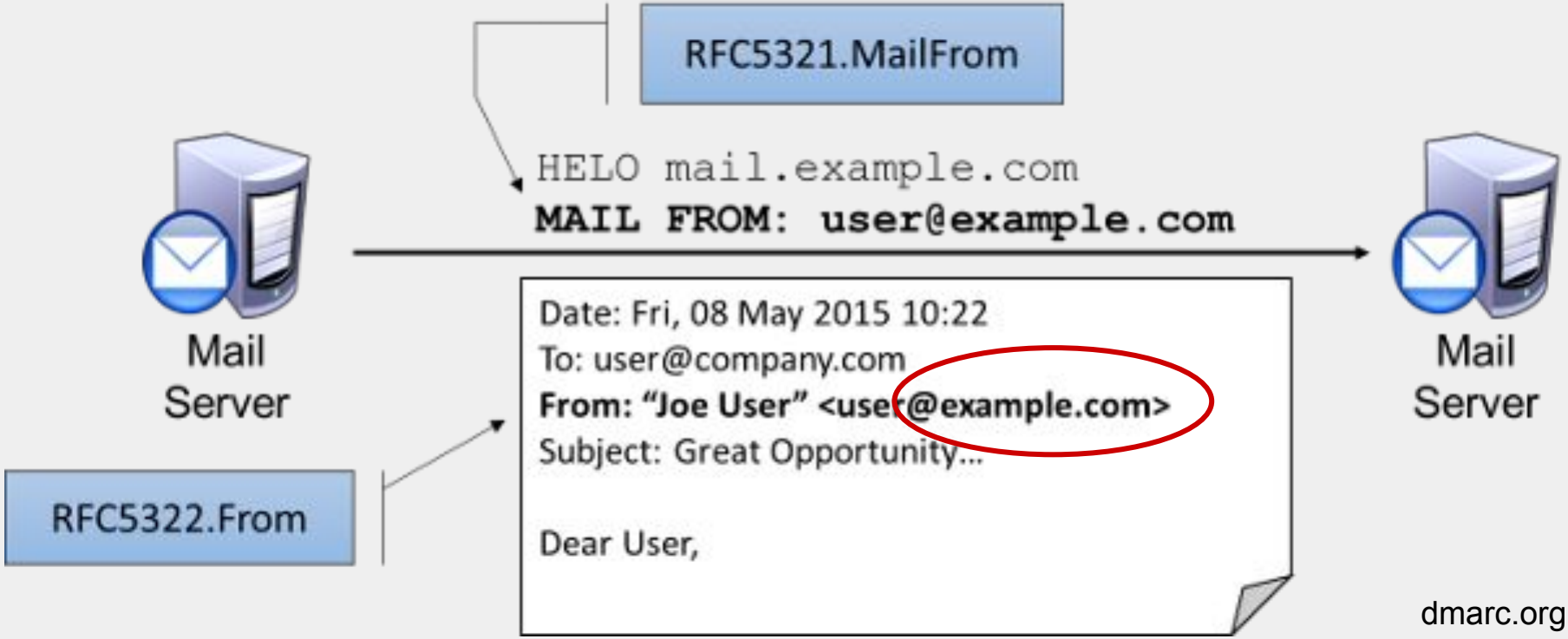
- Users can't see MAIL FROM / no alignment to Header From domain
- Forwarding / mailing lists
- DNS lookup limit of 10
- Inconsistent enforcement by receivers

DKIM Problems:

- Users can't see key selector / no alignment to Header From domain
- Message modification in transit / mailing lists
- Key management / vendor support

Protagonist → Header From domain

Need to create a link between the domain and the message.



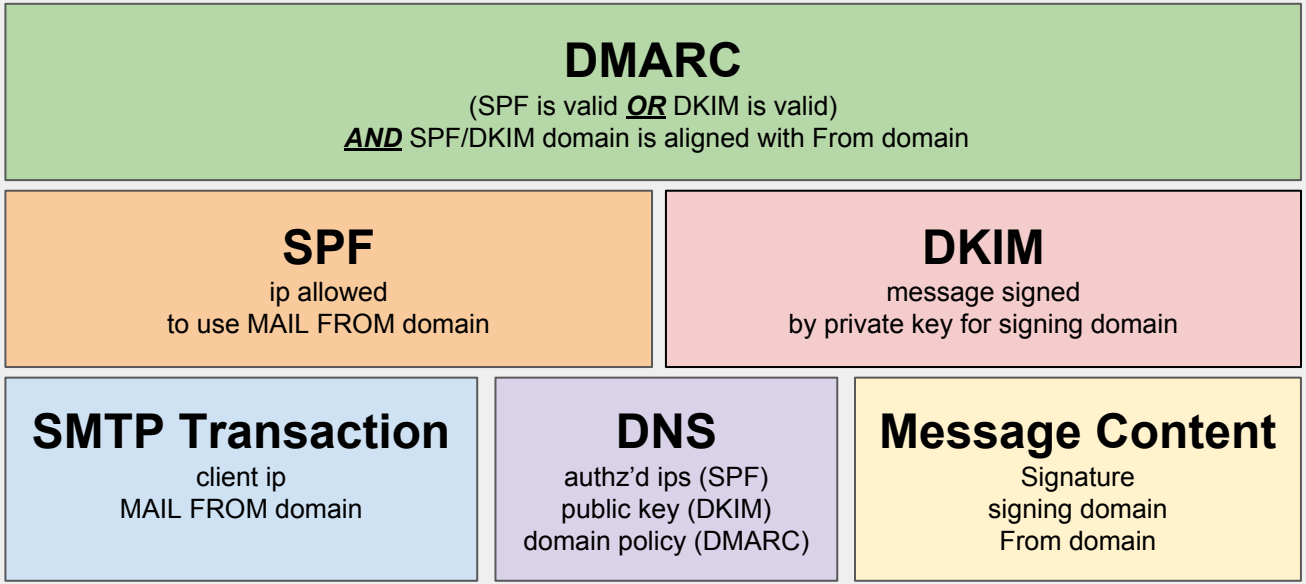
What is DMARC?

Domain-based Message Authentication Reporting and Conformance

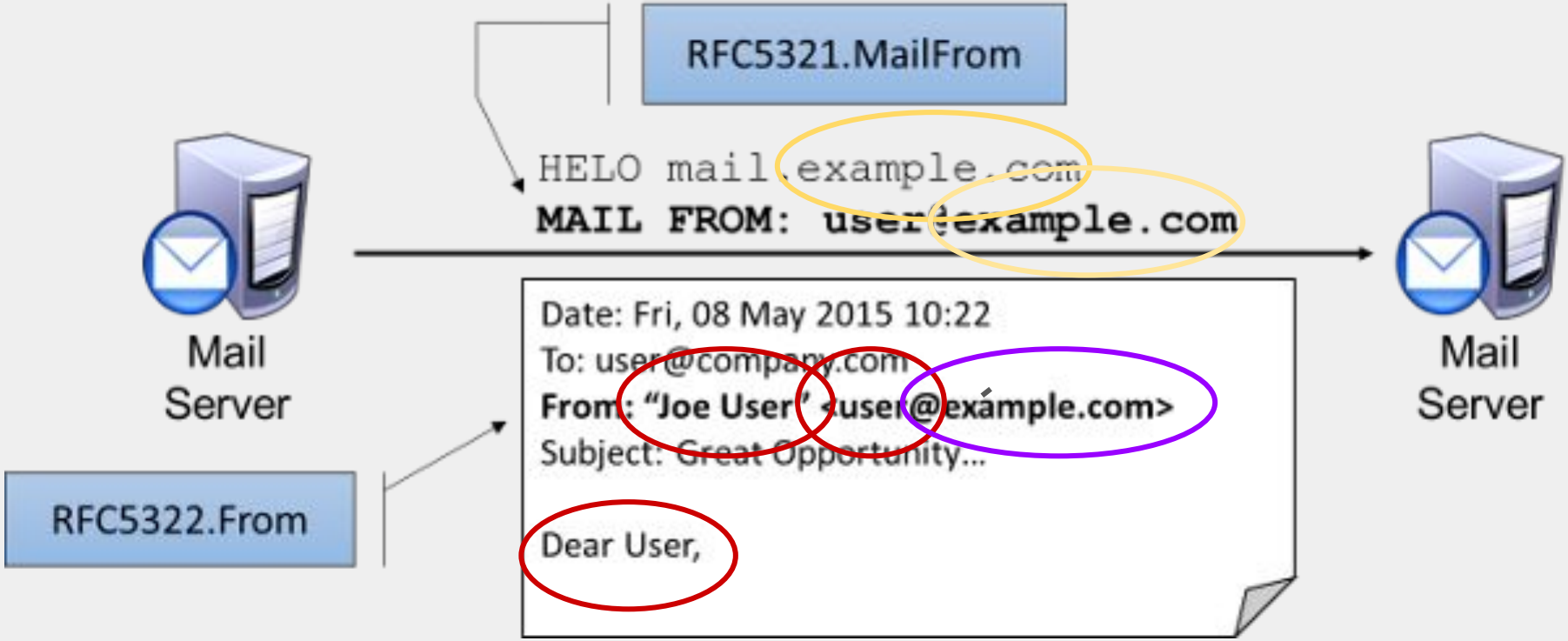
1. Authenticate Domain to Message
2. Reporting:
   - Visibility
   - Feedback
3. Conformance:
   - Protection
   - Governance

dmarc.org

RFC 7489



What DMARC does **not** protect



Teach me how to DMARC

https://tools.wordtothewise.com/dmarc/check/wisc.edu

v=DMARC1; p=quarantine; pct=0;
rua=mailto:dmarc-reports@wisc.edu;
ruf=mailto:dmarc-forensics@wisc.edu;
fo=1; sp=none;

v=DMARC1; p=none\; ...
v=DMARC1; p=reject\; ...

& SPF & DKIM

ROI Pillars

1. Security
    a. Anti-fraud (inbound), anti-spoofing (external)
    b. Brand erosion (sloppiness)
2. Deliverability
    a. Campus marketing/CRM,
    b. Gmail,etc will start requiring DMARC
    c. DMARC provides a foundation that receivers can build trust
3. Manageability
    a. Visibility, Compliance
    b. Shadow IT, BYOCloud
    c. Control (can be decentralized)

Get Reporting

Publish p=none and collect reports for all domains

Internal reporting / log analysis of internal mail

Implement systems to analyze the reports

Start having conversations with campus email senders and their vendors

Start Backfilling

Enable DKIM signing

Shore up SPF records

Encourage subdomains - Consultation to set up subdomain DMARC records

SMTP relay for internal senders

sp=quarantine - backstop the issue, prevent abuse on non-existent domains

SPF lookup limit

Flattening SPF records works

Be careful:

- You'll over-authorize and lose the DMARC ROI
- Harder to de-authorize later

Better to push people to use subdomains

Change Management

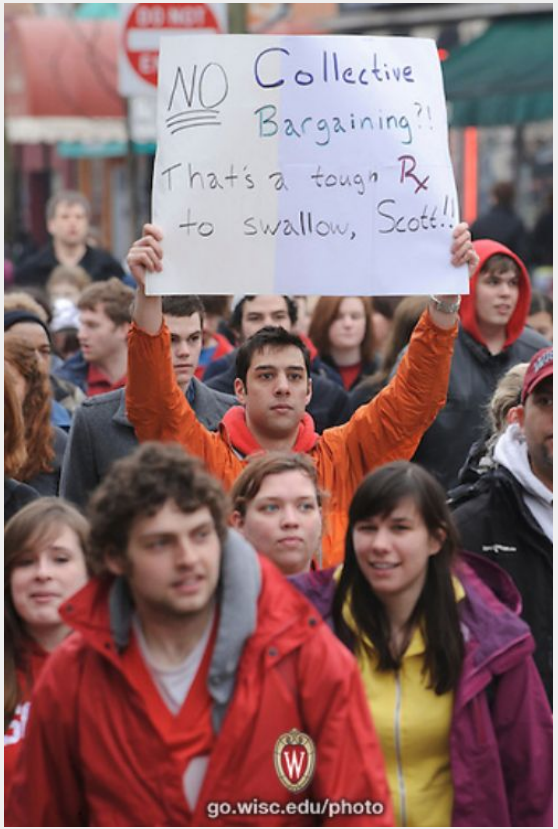
Documentation

Publish a plan

Make the incentives known

Publish metrics and measure progress

Guidance for procurement



Enact Change

From header rewriting (mailing lists)

p=quarantine pct=0

Self-service tools for subdomain owners

Tools for domains that are used for outbound email only

Hostmaster procedures/templates for new DNS domains

Tools / Services

Open source tools for DMARC reports
https://dmarc.org/resources/code-and-libraries/
(e.g. Yahoo's DMARC Report Processor)

Vendor types:

- Reporting value-add (e.g. Dmarcian)
- Managed services
- Delegated DNS hosting (e.g. ValiMail)

Integrating forensics reports into abuse desk operations (e.g. AbuseHQ)

Forwarding Challenge

Unpatched mailing list servers are everywhere in EDU

Resistance/unawareness - From header rewriting/wrapping is necessary

Highly variable problem due to original From domains having differing policies and receiving systems being inconsistent in enforcing (and it's a moving target)

Future → ARC? arc-spec.org

Convincing people is hard

People don't think spoofing is a problem

People don't feel comfortable changing DNS

People are afraid something will break

People think it's a power grab

Ultimately, it will be a leap of faith (not every receiver reports)

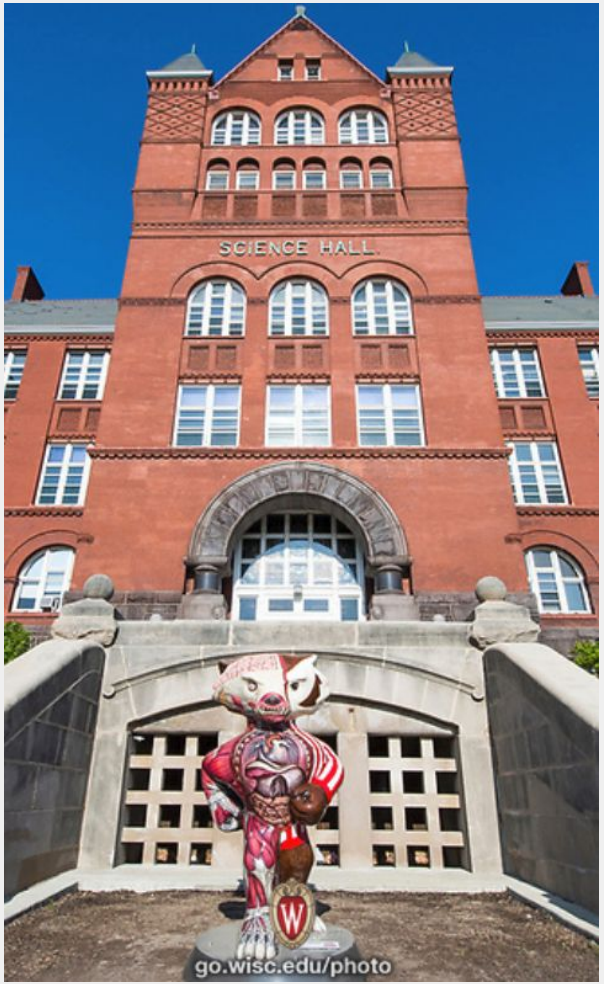
Delegated DNS

If you delegate DNS to campus units

Good luck

Resistance to change

Unaware local IT



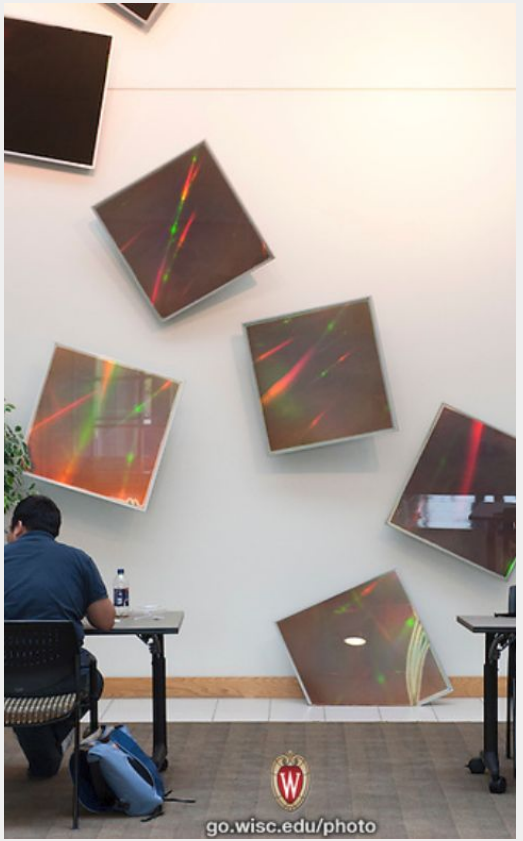
Baffling that it works

“I’m surprised DMARC is so successful because it does so little”

Most message recipients don’t even look at the From domain

Spammers adopt DMARC too

Does this mean that the sender management/compliance benefits of DMARC is the big win?



Inconsistent enforcement

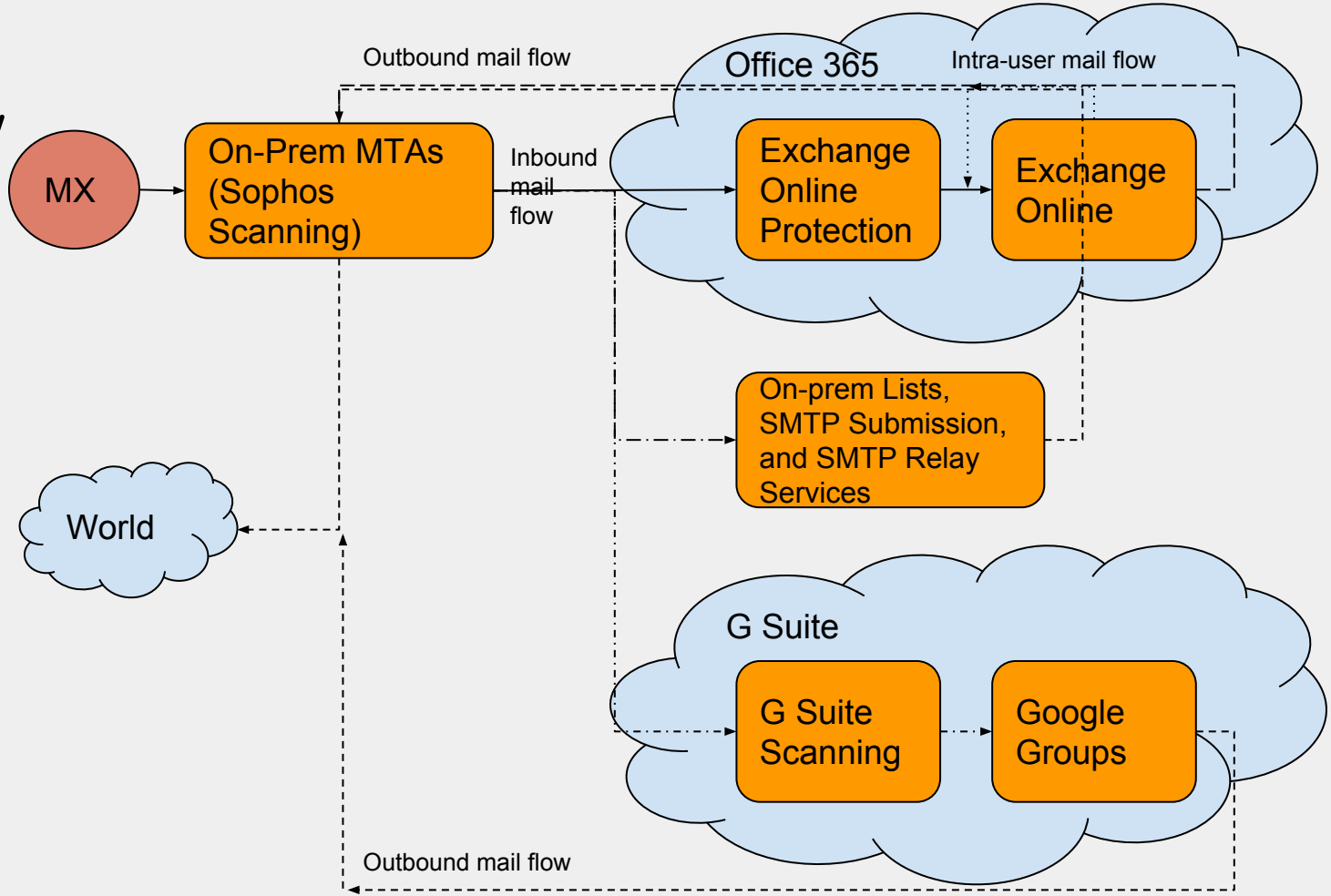
Not all receiving systems enforce DMARC

Not all receiving systems enforce DMARC to the standard

Exchange Online can only enforce DMARC if MX points at them (IP Skiplist coming soon?)

Mailing lists / forwarding MTAs are still a big hurdle

Complex Mail Flow



Email service sprawl

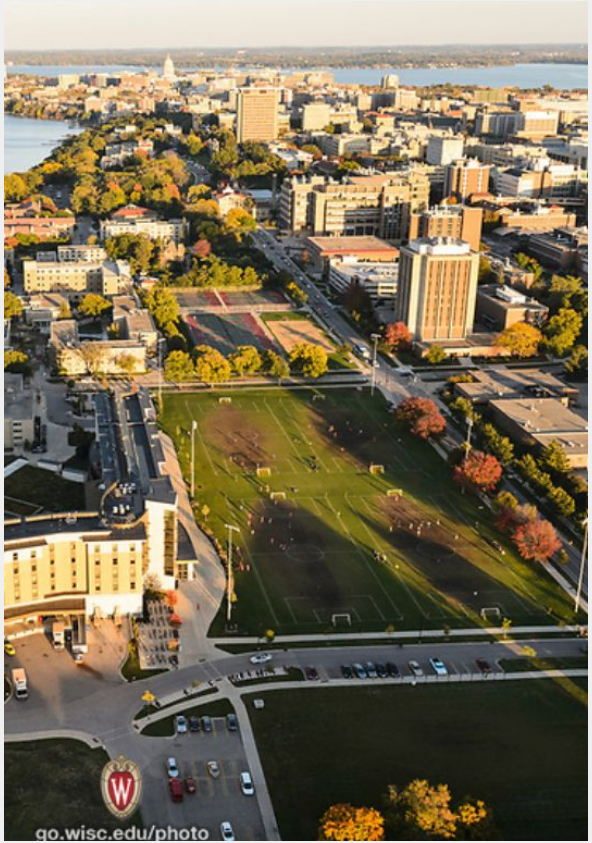
Email service sprawl is a form of Shadow IT / BYO Cloud

Embrace or restrict?

E.g. Constant Contact & Mailchimp

Authenticating with DMARC implies condonement?

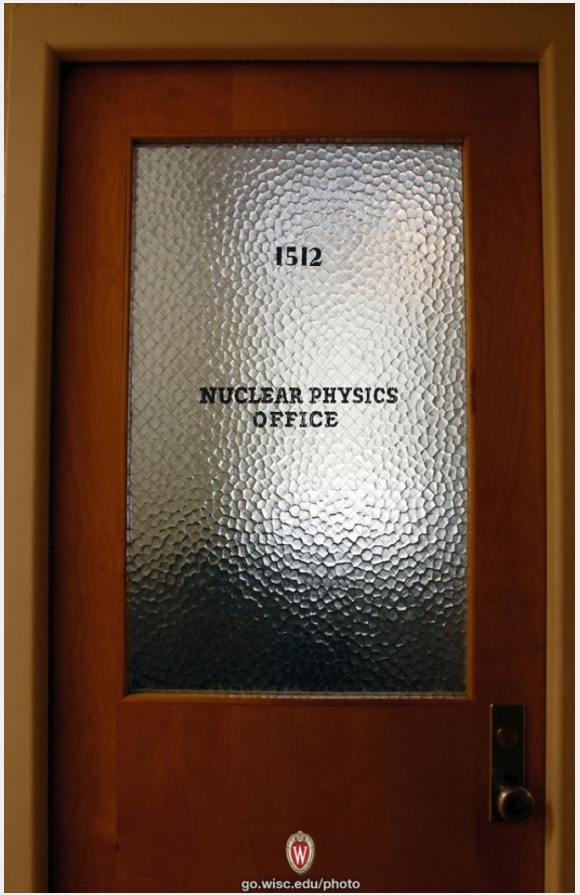
Attempts to centralize ESPs will undermine DMARC effort



Poor IAM by ESPs

Sending email to the user containing link (if even) is how email service providers implement authentication, directory synchronization, role based access controls, and deprovisioning.

Have a high standard for authorizing use of your 2ld.edu



DKIM key management

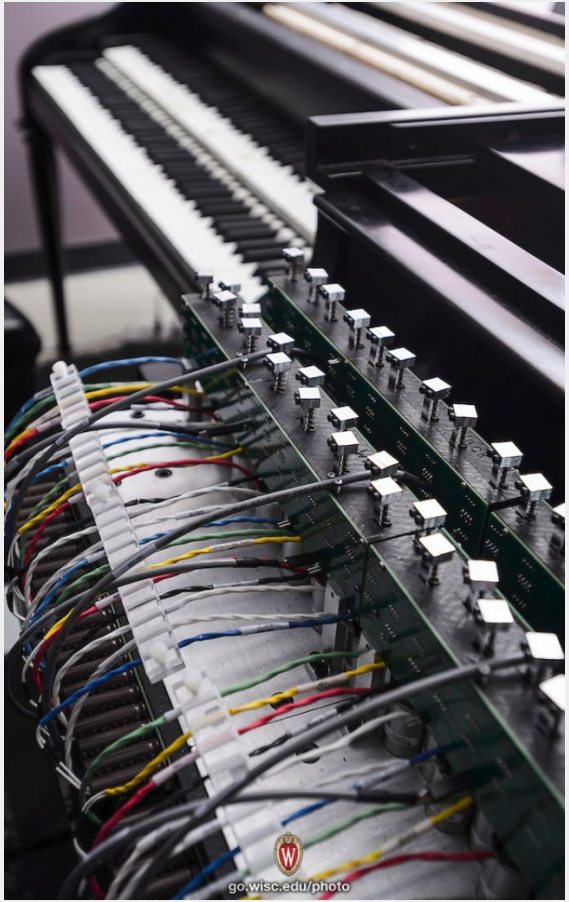
DKIM replay attacks are possible

Keys should be rotated

ESP key management are usually poor

CNAME records makes it easier

Don’t forget to ensure vendors practice good DKIM key management



Squeezes the balloon

DMARC success will shift abuse to other areas

- Compromised accounts
- Cousin domains
- Display name spoofing

Don’t use the word “Policy”

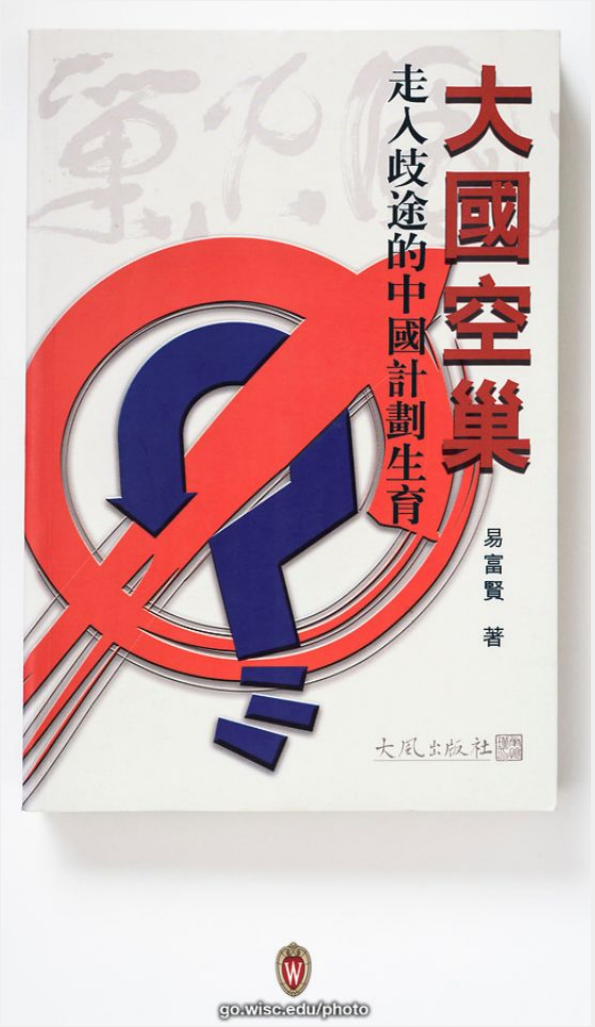
It’s off-putting

People hear big-P Policy

Use a positive term instead

“DMARC will protect your domain”

“DMARC will improve deliverability”



People just don't get email

Campus email senders don't pay attention, or they become paralyzed by uncertainty

Bouncing / messing with their mail may be the only way to get their attention

DMARC 'pct' mechanism is crude

Alternative strategy: rewrite From or Subject-tag inbound non-authenticated email

Engagement strategies

Direct engagement - proactive or immediately reactive - is most successful

If they don't see an immediate benefit after engagement, their interest plummets and they get distracted by other work

Website + consultation form → very little interest

DMARC "test" address → seems helpful

Shoutout to uncg.edu for being a trailblazer

Future

ARC - Authenticated Relay Chain

- Fixes complex/hybrid mail flow issues
- Fixes forwarding/mailing list issues
- Lacks: reputation system

Other:

- DMARC for TLDs
- BIMI
- Calendar Organizer

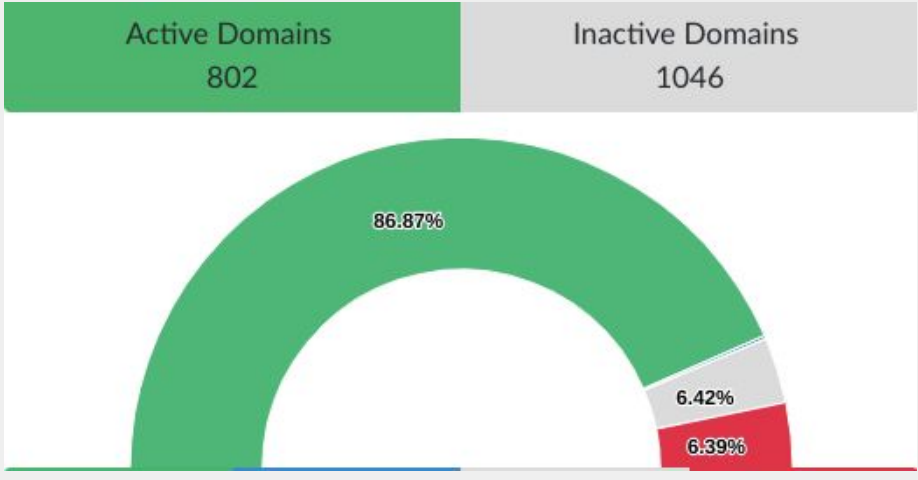
Next steps - UW-Madison

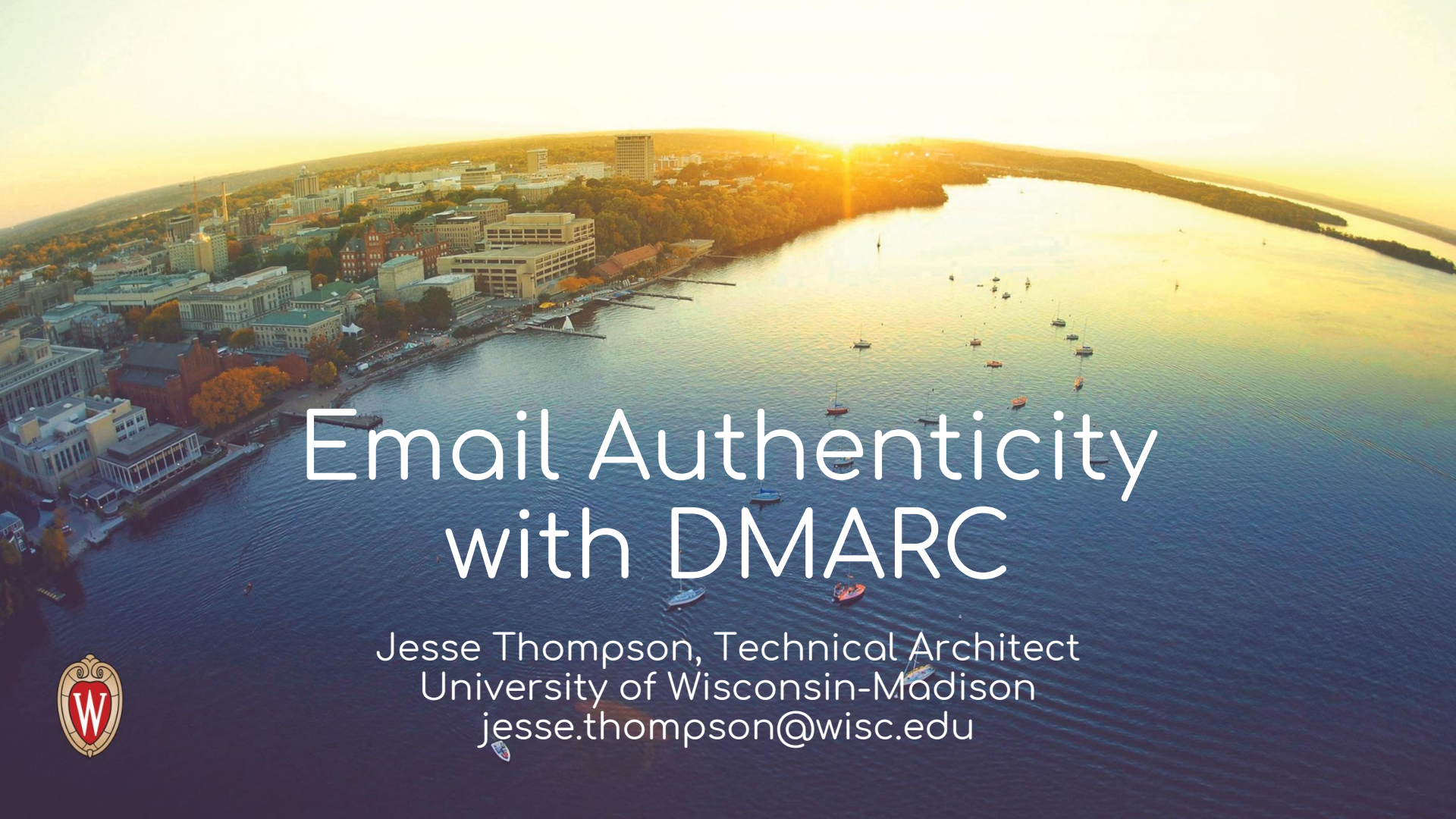
1. all subdomains → backfill p=none, and wisc.edu → sp=quarantine
2. nuanced enforcement of inbound spoofing
3. assist more subdomains and campus emailers with DMARC protection
4. assist mailing list operators and other forwarders
5. publish wisc.edu p=quarantine pct=100

Sources

Source	DMARC	SPF	DKIM
SPF-Identified Servers	94%	93%	43%
Constant Contact, Inc.	0%	0%	0%
MailChimp	0.06%	0%	0.06%
Related Servers	0.5%	0%	0.5%
MessageGears	0%	0%	0%

and 23 more





Email Authenticity with DMARC

Jesse Thompson, Technical Architect
University of Wisconsin-Madison
jesse.thompson@wisc.edu