JP AAWG

7 November 2022

M³AAWG Growth and Development

Severin Walker, Co-Chair
Dennis Dayman, Co-Chair

Introductions – Keynote Speakers

- Severin Walker
  - **Vade** Director of ISP Products and Tech Services
  - **M³AAWG** Growth and Development Chair, Open Roundtables Chair, Former Board of Directors Chairman

- Dennis Dayman
  - **Proofpoint** Resident Chief Information Security Officer
  - **M³AAWG** Growth and Development Chair, Program Committee Chair

Introductions – M³AAWG Chairs at JP-AAWG

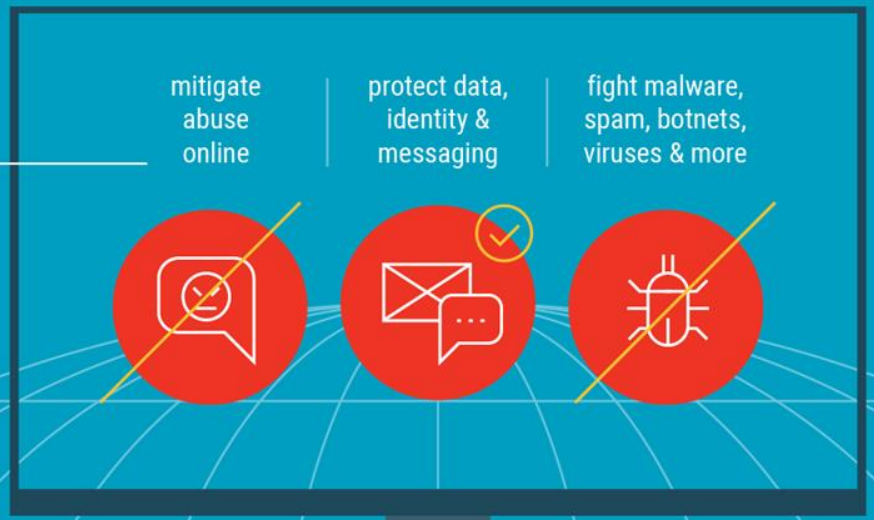
- Tom Bartel
  - **Validity** Senior Vice President, Data
  - **M³AAWG** Growth and Development Chair, Awards Chair

- Mariska Calabrese
  - **Outreach.io** Security Engineer, Platform Email Governance and Anti-Abuse
  - **M³AAWG** Brand SIG Vice-Chair, Open Roundtables Chair

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

The Messaging, Malware, and Mobile Anti-Abuse Working Group provides a collaborative global trusted forum that brings industry together to help fight and prevent internet online abuse.

M3AAWG publishes best practices, position statements, training/educational videos and other materials to



Members

260

Founded

2004

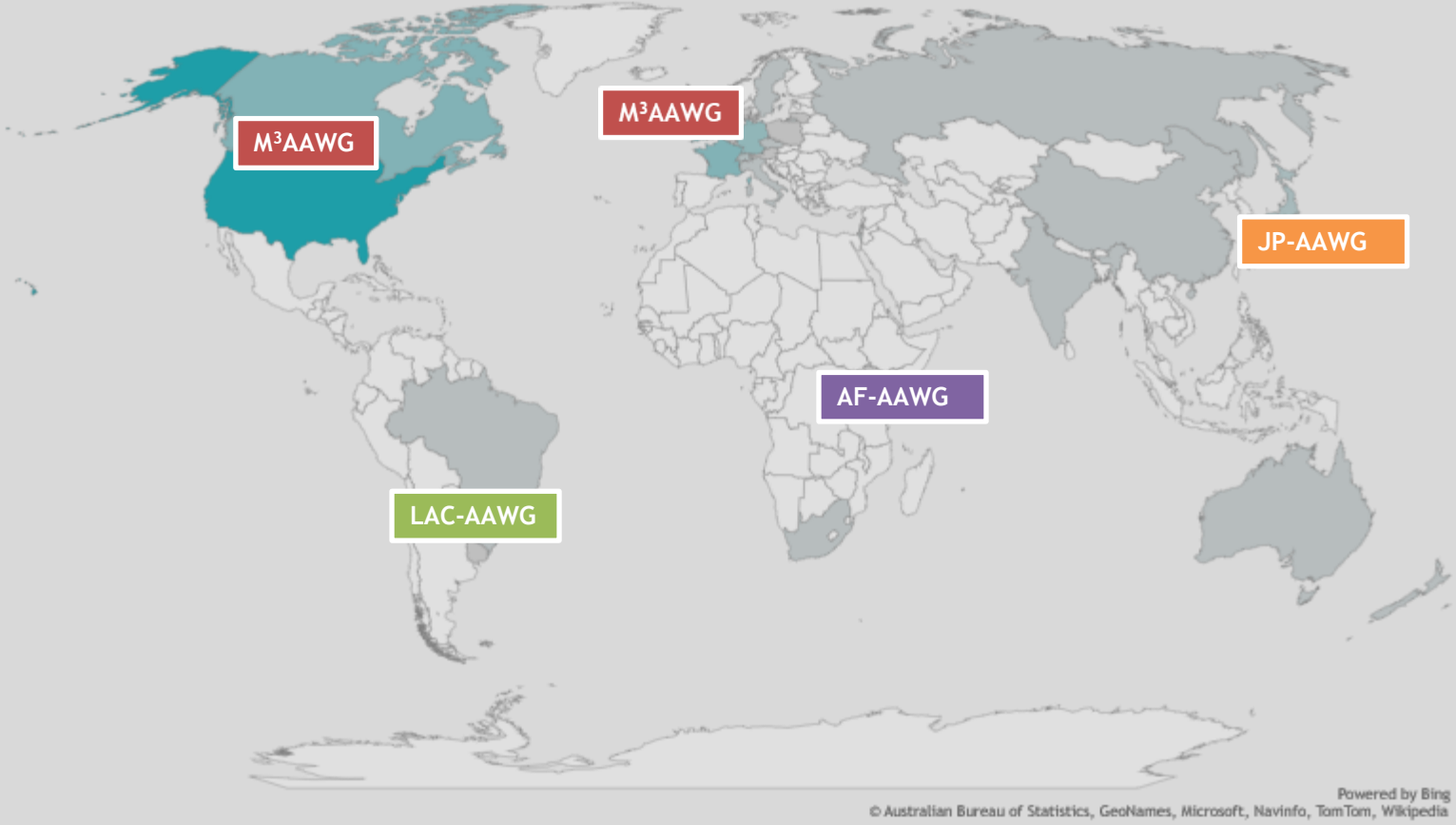
Peer working groups across the globe

Dozens of industry partnerships

Who are M³AAWGs 200+ Members?

- Academic/Researcher
- Cloud Service Providers
- Domain Registry
- Email Service Provider (ESP)
- Government
- Hardware & Software Vendors
- Hosting Provider
- Infrastructure Vendor
- Internet Service Provider (ISP)
- Major Brands Mobile Operator
- Network Operators
- Non-Profits
- Security Vendor
- Social Network Provider
- Standards Bodies

Regional AAWG Partners



Partner Organizations

This list is not all inclusive

Key Area: Organization

- Continue its efforts to strengthen and build the organization, which is largely comprised of volunteers
- Continue diversity and inclusion efforts
- Continue global outreach and working with partner organizations

KEY AREAS

As more advanced online abuse threats rapidly evolve, M3AAWG is proactively shifting its work to focus on 4 key areas, in addition to continuing to develop the organization, its partner ecosystem, while continuing to maintain a diverse and inclusive culture.

Data and Identity Protection

Protect online identity (ex. using multi-factor authentication), ensure data privacy and security through use of encryption/ encrypted protocols, adopt Zero Trust principles by verifying explicitly, using least privilege and assuming breach

Communications

Protect network, messaging, mobile, IoT communications/ systems/devices from malware, spam, phishing, DDoS, DNS attacks

Supply Chain

Understand downstream dependencies and risk, incorporate secure software development/ testing practices, proactively monitor, detect and manage vulnerabilities

Readiness

Shift to be proactive to identify emerging threats, focusing on prevention/ mitigation/detection, deprecating older technologies

Committees and Special Interest Groups - Sample

- Abuse Desk
- Brand
- Data & Identity Protection
- DDoS
- Diversity & Inclusion
- Dynamic Email Security
- Hosting
- Internet of Things
- Mobile
- Names & Numbers
- Public Policy
- Senders

Committee Work

Abuse Desk

Promotes communication among customer-facing security, operations and policy professionals on abuse prevention, detection and remediation, and facilitates industry best practices.

- Updating to the abuse desk training deck
- Building a business case for an abuse desk initiative in progress
- Reviving effort to come up with KPIs (measurables) for an abuse desk

Brand SIG

Provides a closed, trusted environment for addressing issues specific to an organization’s brand protection.

To support existing Brand Protection Kit*, we have a couple documents in the review process:

- Email Best Practices for Brand (very close to completion!)
- SMS Sending- Best Practices for Brands

*https://www.m3aawg.org/published-documents

Data and Identity Protection Committee

Provides technically sound yet approachable advice on these complex topics, striving for a balanced perspective and coordinating efforts with other organizations.

- Preparing a blog post to summarize some of the finding of the TLS 1.0/1.1 deprecation survey, with more to follow
- Planning sessions and initial recommendations around post-quantum cryptography
- Exploring options on a panel for increased support for modern authentication in email clients
- Continue working on zero trust material

Diversity and Inclusion

Works on shaping the group going forward. We provide mentorship to better integrate with the overall work of M3AAWG, and we provide a forum to give feedback and discuss challenges. This is an inclusive cross-membership effort.

- Blog content to be created to support keynote speaker on preventing online stalking and harassment

Names and Numbers Committee

Allows the M^{3}AAWG membership to identify and collaboratively address risks and threats against the identifier systems of the Internet, both seeking the public good as well as helping manage risks against the members' own infrastructures or customers.

- BGP hijacking and implementation of RPKI
- Trends in domain abuse (phishing, malware distribution, botnet command and control, others)
- Good registrar/registry practices to address malicious domains (point of creation + during lifetime)
- The Public Suffix List: Where is it headed?

Public Policy Committee

Interacts with government agencies and non-governmental support organizations globally and comments on operational issues that affect the industry's ability to protect end-users. Covered in this committee are information sharing, quantifying damages, abuse material takedown and WHOIS recommendations.

- Objective content takedown template* is complete with associated blog post published
- Beginning work on FCC NPRM with Tech-Mobile chairs

*https://www.m3aawg.org/published-documents

Senders Committee

Focuses on the views and concerns particular to large-scale email senders in preventing abuse from their own clients.Topics include bot sign-up abuse and tracking.

- Document "Help I hit a spamtrap" to be published October 2022
- Revisions to the Senders BCP document are well underway and we are hoping to push it for review soon
- Continuing ongoing discussions around the problems senders are facing while setting up an SMS product alongside email.
- Looking forward to taking on work around suppression lists and data transparency

Technical Committee

Focuses on technology-based issues, including denial of service issues, dynamic email security, the Internet of Things (IoT), malware, messaging, mobile tech, URL checking, open source and ransomware.

Technical Committee

Focuses on technology-based issues, including denial of service issues, dynamic email security, the Internet of Things (IoT), malware, messaging, mobile tech, URL checking, open source and ransomware.

- Ransomware BCP Document progressing after full committee review and expected for TRC and Board review shortly
- Mobile:
  - M³AAWG response to the FCC Notice proposed rulemaking
  - Best Practices for Mobile Text Spam Reporting
  - Requirements for a mobile text spam reporting format
  - Collaborative defense against conversational text spam

Tech Committee (Continued)

Messaging:

- Open co-chair position
- Follow-on work for in-progress items discussed during sessions here in Brooklyn
- Idea for new session in SF: Panel of young adult citizens to discuss their experiences with email.
- New idea suggested during MNO; Todd will be talking to ESPs to explore for further development.

Malware:

- Recruiting for a chair and vice-chair

2023 Meetings

57th General Meeting
February 20- 23, 2023 - San Francisco, CA USA

58th General Meeting
June 5-8, 2023 Dublin, Ireland

59th General Meeting
October 9-12, 2023 - Brooklyn, NY USA

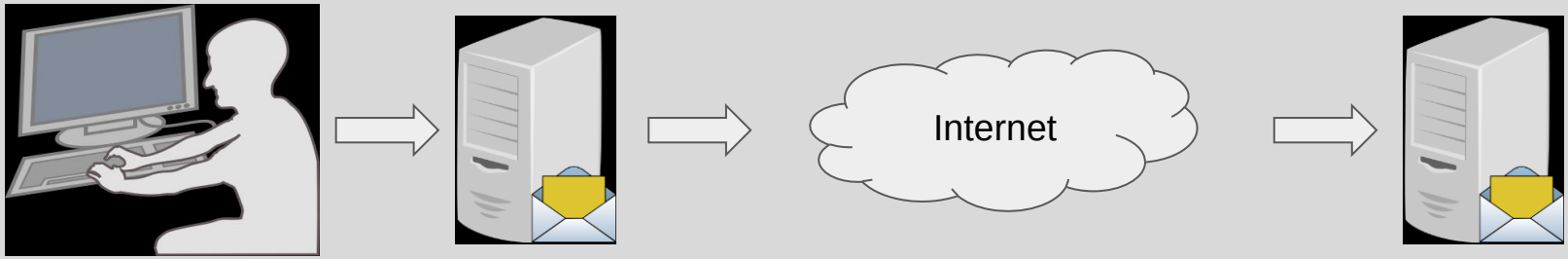
Details at https://www.m3aawg.org/upcoming-meetings

MTA-STS and DANE

Email Encryption Work at M^{3}AAWG

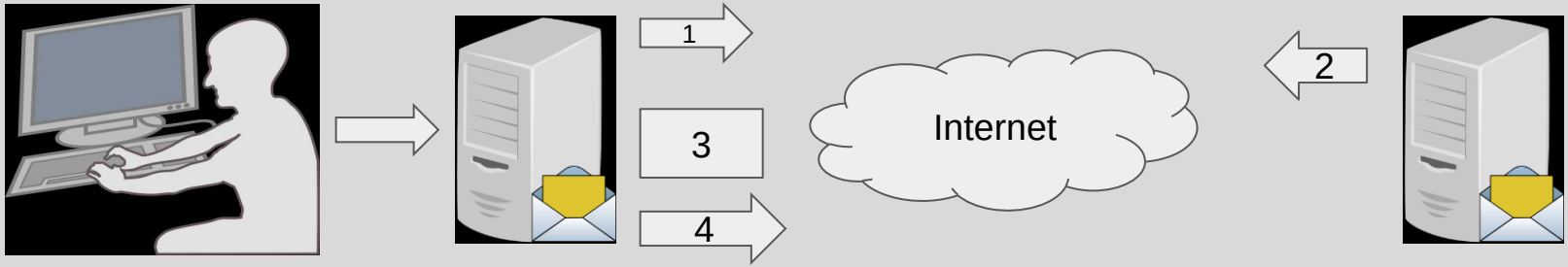
Basic Email Encryption

- Best effort to encrypt the channel for communication
  - Opportunistic Encryption - RFC7435 (https://datatracker.ietf.org/doc/rfc7435/)
  - Normally zero validation is performed
  - The certificate presented may be correct, malformed, expired, nonexistent, or a complete lie



MTA-STS

- Validate the presented certificate via the CA hierarchy
  - RFC8461 (https://datatracker.ietf.org/doc/rfc8461/)
  - Three modes: “none”, “testing”, “enforced”
  - Allows receiving site to require senders who understand MTA-STS to use TLS when delivering messages
  - But perhaps more important, verifies the destination is correct
  - Failure to validate during “enforced” results in a “tempfail”, will try again later



1) Initiate Session 2) Respond with Certificate information 3) Validate Certificate via CA 4) If valid, deliver message

Why is MTA-STS (or DANE) important

- Unencrypted messages can be sniffed/stolen on the wire
  - It may seem harmless, but why not protect it …
  - No one knows what stored information may be used for in the future
- Ensures messages are transmitted securely
  - At this point, all traffic should be transmitted using secure channels
  - But … We also need to ensure it's going to the correct destination
- MTA-STS (and DANE) ensure that the sender is talking to the correct destination (potential for PPAP solution)
  - Financial documents, medical records, legal agreements, receipts, private conversations
- MTA-STS is "Trust On First Use", and easier to deploy in most scenarios
- DANE is more robust, though uses DNSSEC

Stats

- In use since roughly September 2018
  - Supported by a number of commercial MTAs
  - Not aware of any OSS with core support (yet?)
- Well over 1,500 domains using MTA-STS today
- 90% of messages are protected by “enforce” in a user-to-user system
- Greater than 40% of destination domains are “enforce”
- Most large MBPs support MTA-STS
  - Gmail/Outlook at “enforce”, Yahoo/Facebook at “testing”

Thank you!

Questions?

To learn more

Contact us via https://www.m3aawg.org/contact-us

M3AAWG Website https://www.m3aawg.org

Find us on Social Media

Facebook: www.facebook.com/m3aawg
Twitter: www.twitter.com/m3aawg - @m3aawg
YouTube M³AAWG Channel: www.youtube.com/maawg
LinkedIn: https://www.linkedin.com/company/m3aawg