M^{3}AAWG Liaison Summary

IETF 120 – IABOPEN session
Barry Leiba, IETF Liaison to M3AAWG
2024-07-25

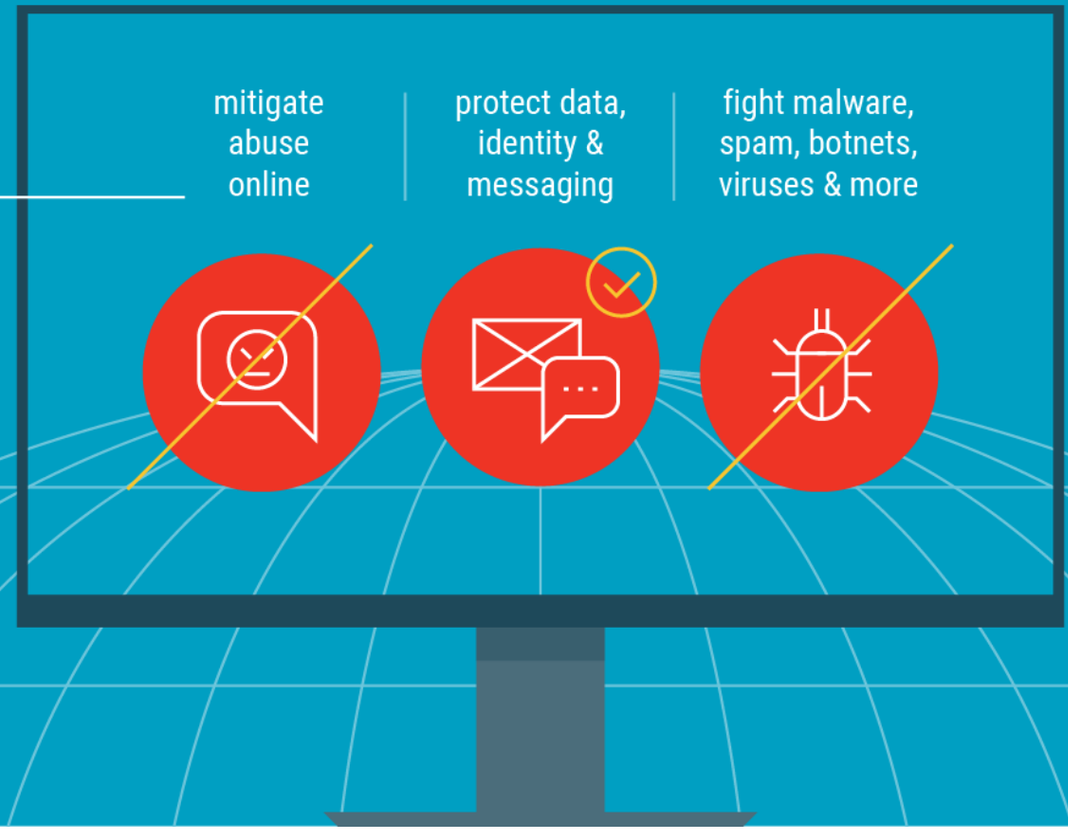
M^3AAWG

- Messaging, Mobile, Malware Anti-Abuse Working Group
  - Originally MAAWG: ”Messaging” is the “original M”
  - Formed in 2004, 20 years ago as a place to discuss messaging abuse and defense/mitigation thereof
  - Mobile and Malware added later; the “3” is silent

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

M^{3}AAWG is a worldwide, technology-neutral, non-political working body

Who are M^{3}AAWGs 250+ 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

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

M3AAWG's relation to the IETF

- M3AAWG's output includes best practices documents, information sharing, education & outreach, **technology transfer**
- M3AAWG has been heavily involved in DKIM, SPF, DMARC – collectively, "email authentication"
- M3AAWG has brought work into the IETF in working groups such as DMARC, SPFbis, UTA, MARF, REPUTE, in addition to BoFs
- IETF work is important to M3AAWG, and liaison work involves information and work flow in both directions
- M3AAWG participants have participated in and chaired IETF working groups, and edited working group documents

Relevant/Interesting M3AAWG Committees

- New: AI Committee, focuses on anti-abuse topics related to AI
  - abuse facilitated by AI systems
  - abuse of AI systems
  - using AI to counter abuse
- Data and Identity Protection Committee, covers issues of authentication, authorization, password practices & MFA, etc
- Names and Numbers Committee, identify and collaboratively address risks and threats against the identifier systems of the Internet
  - Connects with ICANN

Relevant/Interesting M3AAWG Committees

- 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
- Technical Sub-Committee: DDoS SIG, helps ISPs, hosting companies, and 3rd party DDoS service providers understand existing and emerging attack types, prevention methods, monitoring and mitigation architectures and strategies
- Technical Sub-Committee: IoT SIG, coordinates efforts of M3AAWG members in resolving abuse issues driven by compromised IoT devices

Some Recent M3AAWG Publications

- M3AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries
- Best Common Practices for Managing Port 25 for IP Networks (update)
- Ransomware Active Attack Response Best Common Practices
- Protecting Parked Domains Best Common Practices (update)
- Email Authentication Recommended Best Practices
- Sending Domains Best Common Practices
- Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic

- See all here: https://www.m3aawg.org/published-documents

Examples of Potential M3AAWG Work

- Best Current Practice for Enterprise Mobile Messaging
- Best Current Practice: Forbid “Open Web Proxies”
- Password Recommendations for Account Providers
- MFA/2FA
- Privacy/Security/Anti-Abuse by Design Principles
- Routing Security

Thank you