Abbreviations, Jargon and Selected Terms of Art Commonly Used in M³AAWG

Please send updates to this listing to yadira@m3aawg.org

BCP (Best Current Practice or Best Common Practice)

"BCPs and white papers represent the cooperative efforts of M³AAWG members to provide the industry with recommendations and background information to improve messaging security and protect users. M³AAWG best practices are updated as needed and new documents are added as they become available." (Source: M³AAWG website "Best Practices" – https://www.m3aawg.org/published-documents)

BoF (Birds of a Feather) Session

A new subject matter area at M³AAWG often begins as a "Birds of a Feather" (BoF) session. A BoF session is scheduled with the goal of exploring what kind of work the group may do, whether the work is feasible, who is interested in it, whether M³AAWG should or should not pursue it, and other general discussion areas.

A BoF is often modestly sized, may be of limited duration, and may or may not have a firm expectation to produce an immediate work item or a productive deliverable. A BoF session is generally held over lunch during a M³AAWG General Meeting. Any M³AAWG member usually can participate.

DKIM (DomainKeys Identified Mail, http://www.dkim.org/)

DomainKeys Identified Mail (DKIM) lets an organization take responsibility for a message that is in transit. The organization is a handler of the message, either as its originator or as an intermediary. Their reputation is the basis for evaluating whether to trust the message for further handling, such as delivery. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication. (Source: http://www.dkim.org/)

DDoS (Distributed Denial of Service Attack)

A "denial of service" refers to an attack that overwhelms a system with data (most commonly a flood of simultaneous requests sent to a website to view its pages), causing the web server to crash or simply become inoperable as it struggles to respond to more requests than it can handle.

A simple DoS attack performed from a single machine is uncommon today. Instead, they have been supplanted by DDoS (distributed denial-of-service) attacks that come from many computers distributed across the web – sometimes hundreds or thousands of systems at once. (Source: https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/)

Perpetrators seek to make a machine or network resource unavailable to its intended users by disrupting services. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests overloading systems and preventing legitimate requests from being fulfilled.
"A denial of service (DoS) attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations." (Source: https://en.wikipedia.org/wiki/Denial-of-service_attack)

DMARC (Domain Message Authentication Reporting & Conformance)

"DMARC, which stands for 'Domain-based Message Authentication, Reporting & Conformance' is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email." (Source: https://dmarc.org/)

DNS (Domain Name System)

"The Domain Name System (DNS) is a hierarchical naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for the purpose of locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality of the Internet that has been in use since the 1980s." (Source: https://en.wikipedia.org/wiki/Domain_Name_System)

DNSSEC

"The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. [...]" (Source: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions)

End-to-End Encryption

"End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation. The systems are designed to defeat any attempts at surveillance and/or tampering because no third parties can decipher the data being communicated or stored. For example, companies that use end-to-end encryption are unable to hand over texts of their customers' messages to the authorities. [...]" (Source: https://en.wikipedia.org/wiki/End-to-end_encryption)

Identity Management

"In computer security, identity and access management (IAM) is the security and business discipline that 'enables the right individuals to access the right resources at the right times and for the right reasons'. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. [...] IdM covers issues such as how users gain an identity, the protection of that identity and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.)." (Source: https://en.wikipedia.org/wiki/Identity_management)

IoT (Internet of Things)

The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society."

"The IoT allows objects to be sensed" and/or controlled "remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. . .

"Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

"Experts estimate that the IoT will consist of almost 50 billion objects by 2020."

(Source: https://en.wikipedia.org/wiki/Internet_of_things)

M³AAWG Ambassador

Ambassadors design and implement collaborative relationships and programs with the groups and communities that M³AAWG would like to establish deeper relationships - and ultimately partnerships - with. A M³AAWG Ambassador's primary responsibility is to represent M³AAWG and the anti-abuse regime in a way that is relevant to the targeted community, highlighting the benefits of the anti-abuse regime and how to best implement and apply anti-abuse best practices.

M³AAWG Champion

M³AAWG Champions are experienced M³AAWG members who look for opportunities to introduce M³AAWG to new organizations that would both benefit from, and contribute to, the M³AAWG community.

M³AAWG Guide

The M³AAWG Guide Program welcomes new attendees to M³AAWG meetings, the organization and the community. The program aims to remove barriers to participation, help new attendees gain the most out of their meeting attendance, emphasize and foster the M³AAWG mission as a collaborative working group, and explain how to participate for newly represented organizations. A M³AAWG Guide is an experienced M³AAWG member who is partnered with new attendees at each meeting.

Pervasive Monitoring

"Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large scale, rather than by introducing new types of technical compromise.

The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organizations. The IETF community has expressed strong agreement that PM is an attack that needs to be mitigated where possible."

(Source: https://tools.ietf.org/html/rfc7258)

Phishing

"Phishing is an attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, [indirectly,] money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. According to the 3rd Microsoft Computing Safer Index Report released in February 2014, the annual worldwide impact of phishing could be as high as $5 billion.

"Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.

"Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security."

(Source: https://en.wikipedia.org/wiki/Phishing)

Ransomware

Ransomware is computer malware that installs covertly on a victim's device (e.g., computer, smartphone, wearable device) and that either mounts the cryptoviral extortion attack from cryptovirology that holds the victim's data hostage, or mounts a cryptovirology leakware attack that threatens to publish the victim's data, until a ransom is paid. (Source: https://en.wikipedia.org/wiki/Ransomware)

RPZ (Response Policy Zones)

"In computing, a response policy zone (RPZ) is a mechanism for use by Domain Name System recursive resolvers to allow customised handling of the resolution of collections of domain name information (zones). . .

"RPZ allows a DNS recursive resolver to choose specific actions to be performed for a number of collections of domain name data (zones).

For each zone, the DNS service may choose to perform full resolution (normal behavior), or other actions, including declaring that the requested domain does not exist (technically, NXDOMAIN), or that the user should visit a different domain (technically, CNAME), amongst other potential actions."

Their website is https://dnsrpz.info/ (Source: https://en.wikipedia.org/wiki/Response_policy_zone)

SIG (Special Interest Group)

Ranking between a M³AAWG BoF and a M³AAWG committee, a M³AAWG Special Interest Group (SIG) typically works on best common practices (BCPs) and other formal deliverables, has periodic SIG conference calls, and usually meets face-to-face during M³AAWG General Meetings.

A SIG normally has the expectation of continued existence and activity - unlike a BOF, which may be ad hoc and of short duration. Normally any M³AAWG member can join and participate in a SIG.

SPF (Sender Policy Framework)

"The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address [cf the rfc5321.MailFrom (return address) field] forgery. More precisely, the current version of SPF (SPFv1 or SPF Classic) protects the envelope sender address, which is used for the delivery of messages. . .

"Even more precisely, SPFv1 allows the owner of a domain to specify their mail sending policy, e.g., which mail servers they use to send mail from their domain. The technology requires two sides to play together: (1) the domain owner publishes this information in an SPF record in the domain's DNS zone, and when someone else's mail server receives a message claiming to come from that domain, then (2) the receiving server can check whether the message complies with the domain's stated policy. If, e.g., the message comes from an unknown server, it can be considered a fake."

Their website is http://www.openspf.org/
(Source: http://www.openspf.org/Introduction)

X-ARF (Network Abuse Reporting Format 2.0)

"x-arf is network abuse reporting 2.0 - it is an email format to report different types of network abuse incidents to network owners. [...]The main intention of x-arf is to extend the so far known Abuse Reporting Format which is defined in RFC 5965 and itself is caught in its strict limitation to reporting abuse with messaging services only. Unfortunately, there is no possibility to report - for example - ssh attacks or phishing websites with it. . . .

"In order to stop the increasing number of homegrown and self-invented reporting formats and offer an easy way to handle incoming complaints more effectively the x-arf format was designed."

Their website is http://x-arf.org/
(Source: http://xarf.org/)

Partner Organizations - See https://www.m3aawg.org/our-partners for the most current list:

- APWG.org (Anti-Phishing Working Group)
- CalConnect
- DMARC.org
- DNS-OARC (DNS Operations, Analysis, and Research Center)
- Global Cyber Alliance
- i2Coalition (Internet Infrastructure Coalition)
- ISOC (The Internet Society)
- LACNIC (Latin America and Caribbean Network Information Center)
- LAP/UCENet (London Action Plan; now called the Unsolicited Communications Enforcement Network)
- WorldHostingDays (WHD)
- Formal liaisons with IETF, ICANN and other organizations and a member of ISOC (The Internet Society), UCENet and DNS-OARC