M3AAWG
MESSAGING MALWARE MOBILE

M3AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012

M³AAWG DMARC Training Videos

(2.5 hours of training)

This is Segment 3 of 6

The complete series of DMARC training videos is available at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **What is DMARC?** **(about 20 minutes)**	**Segment 2** **DMARC Identifier Alignment** **(about 20 minutes)**	**Segment 3** **DMARC Policy Records** **(about 30 minutes)**
Segment 4 **DMARC Reporting** **(about 15 minutes)**	**Segment 5** **DMARC Information for Mailbox Providers** **(about 20 minutes)**	**Segment 6** **DMARC Information for Domain Owners and 3rd Parties** **(about 40 minutes)**

M3AAWG
MESSAGING MALWARE MOBILE

DMARC Policy Records

DMARC Segment 3 – about 30 minutes

Mike Adkins, Paul Midgen, DMARC.org

October 22, 2012

DMARC Spec – Policy Records

- TXT records in DNS
  - _dmarc.example.com
- Check for a record at the exact RFC5322.From
  - If no record is found, check for a record at the Organizational domain of the RFC5322.From
- Policy options:
  - “none” – simply monitor and supply feedback
  - “quarantine” – process email with high degree of suspicion
  - “reject” – do not accept email that fails DMARC check

DMARC Spec – Policy Records

Tag	Purpose	Example
v	Protocol Version	v=DMARC1
p	Policy for the domain	p=quarantine
sp	Policy for subdomains	sp=reject
pct	% of messages subject to policy	pct=20
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r
rua	Reporting URI for aggregate reports	rua=mailto:aggrep@example.com
ruf	Reporting URI of forensic reports	ruf=mailto:authfail@example.com
rf	Forensic reporting format	rf=afrf
ri	Aggregate reporting interval	ri=14400

DMARC Spec – Example Policy Records

M3AAWG
MESSAGING MALWARE MOBILE

Everyone's first DMARC record

```
v=DMARC1; p=none; rua=mailto:aggregate@example.com;
```

DMARC Spec – Example Policy Records

Dipping a toe in the pool

```
v=DMARC1; p=quarantine; pct=10; rua=mailto:agg@ex.com; ruf=mailto:fail@ex.com;
```

DMARC Spec – Example Policy Records

Very aggressive. 100% reject.

```
dig -t TXT _dmarc.facebookmail.com

v=DMARC1; p=reject; pct=100;
          rua=mailto:postmaster@facebook.com,mailto:d@rua.agari.com;
          ruf=mailto:d@ruf.agari.com;
```

DMARC Spec – Policy Record Exercises

Exercise 1
Is this a valid record?

```
p=none; pct=50; rua=postmaster@example.com;
```

DMARC Spec – Policy Record Exercises

Exercise 1
Is this a valid record?

```
p=none; pct=50; rua=postmaster@example.com;
```

Answer: No. The v= tag is required.

DMARC Spec – Policy Record Exercises

Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

DMARC Spec – Policy Record Exercises

Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

Answer: _dmarc.foo.example.com

If no record is found, what will happen?

DMARC Spec – Policy Record Exercises

Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

Answer: _dmarc.foo.example.com

If no record is found, what will happen?

Answer: _dmarc.example.com will be queried.

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 3
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com;
```

Is this email Aligned?

```
Return-Path:postmaster@foo.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
          designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@foo.example.com;
          dkim=pass header.i=@bar.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bar.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@bar.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

DMARC Spec – Policy Record Exercises

M3AAWG MESSAGING MALWARE MOBILE

Exercise 3
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com;
```

Is this email Aligned?

```
Return-Path:postmaster@foo.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
          designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@foo.example.com;
          dkim=pass header.i=@bar.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bar.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@bar.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Answer: Yes. Alignment is Relaxed by default.

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 4
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com
          does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
          dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 4
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com
          does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
          dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Answer: No. SPF did not pass. DKIM passed, but DKIM Alignment is in strict mode and the DKIM domain does not exactly match the From domain.

DMARC Spec – Policy Record Exercises

M3AAWG MESSAGING MALWARE MOBILE

Exercise 4
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com
          does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
          dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Then what will happen to the email?

DMARC Spec – Policy Record Exercises

M3AAWG MESSAGING MALWARE MOBILE

Exercise 4
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com
          does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
          dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Then what will happen to the email?

Answer: No policy action will be taken. The results will be included in the requested aggregate report and the message will be processed as normal.

DMARC Spec – Policy Record Exercises

M3AAWG MESSAGING MALWARE MOBILE

Exercise 5
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
        adkim=s; aspf=s; sp=reject;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
        does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
        dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
        q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
        Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
        b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
        +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
        LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@bar.example.com>
```

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 5
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
        adkim=s; aspf=s; sp=reject;
```

Is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
        does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
        dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
        q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
        Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
        b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
        +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
        LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@bar.example.com>
```

Answer: Trick question! It depends on whether or not there is a DMARC record at _dmarc.bar.example.com.

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 5
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
        adkim=s; aspf=s; sp=reject;
```

If there is no record at _dmarc.bar.example.com, is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
        does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
        dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
        q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
        Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
        b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
        +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
        LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 5
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
          adkim=s; aspf=s; sp=reject;
```

If there is no record at _dmarc.bar.example.com, is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
          does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
          dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

Answer: No. Both SPF and DKIM are in Strict Alignment mode and neither exactly match the From domain.

DMARC Spec – Policy Record Exercises

M3AAWG
MESSAGING MALWARE MOBILE

Exercise 5
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
        adkim=s; aspf=s; sp=reject;
```

If there is no record at _dmarc.bar.example.com, is this email Aligned?

```
Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
        does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
        dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
        q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-
        Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
        b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
        +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
        LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

Then what will happen to the email?
Answer: It will be rejected due to the subdomain policy action sp=reject. The results will be included in the requested aggregate report, and a forensic report will be sent.

This has been the third of six DMARC video segments

View the entire

M³AAWG DMARC Training Series

from the public training video pages on the M³AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org
for developing the material in this series
and allowing M³AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

For information about M3AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form