Authenticated
Received
Chain

Steven M Jones
DMARC.org

Email Service Provider Coalition
Tuesday, May 10th, 2016
Palo Alto, California

Introduction to DMARC.org

The mission of DMARC.org is to promote the use of DMARC and related email authentication technologies to reduce fraudulent email, in a way that can be sustained at Internet scale. This overall goal is met by educating individuals and organizations through a combination of articles, tutorials, and presentations.

For more information, please visit https://dmarc.org

DMARC.org is an initiative of the non-profit Trusted Domain Project (TDP).
For more about TDP, please visit http://trusteddomain.org

Introduction to DMARC.org

DMARC

The work of DMARC.org is made possible through the generous support of these companies:

Sponsors

AGARI COMCAST Google

FARSIGHT SECURITY Return Path TDP Trusted Domain Project

Supporters

messagesystems™ PayPal™ ValiMail

Background

Why Was ARC Created?

- Previous work had been done on a header to convey authentication results between ADMDs
- Original Authentication Results (OAR) was published as an Internet Draft in February 2012
- Assumes trust between ADMDs – not widely used
- Some large enterprises used it internally

Why Was ARC Created?

- Domains with strict DMARC policies (`p=reject`) may see legitimate messages blocked if they go through *indirect mailflows* such as mailing lists or forwarded mailboxes
- In 2014 AOL and Yahoo published `p=reject` for customer-use domains
- Working group formed to adapt OAR to address these *indirect mailflows*
- Significant changes required for a general solution, so a new name was chosen

Design Decisions for ARC

- Originator of message makes no changes
- Convey the `Authentication-Results`: content intact
- Allow for multiple “hops” in the indirect mailflow
- ARC headers can be verified at each hop
- Work at Internet scale
- Define ARC independently of DMARC if possible

Design Decisions for ARC

- Message recipient seeing an authentication failure may choose to check ARC headers
- If ARC headers are intact, they can see and validate `Authentication-Results`: content from first participant
- Depending on reputation of intermediary/-ies and results, they *may* use ARC information as basis for a "local override" of authentication checks

What Does ARC Do?

- Intact ARC chains give you:
  - DKIM, DMARC and SPF results as seen by first "hop"
  - Signatures showing these results were conveyed intact
  - Signatures from participating intermediaries can be reliably linked to their domain name
- Allows intermediaries to alter message with some attribution
- ARC can provide input to a reputation system that includes intermediaries

What Doesn’t ARC Do?

- Does not say anything about “trustworthiness”
- Says nothing about the content of the message
- Intermediaries might still inject bad content
- Intermediaries might remove some or all ARC headers

Implementation

Three New Header Fields

- `ARC-Authentication-Results:` (AAR)
  Archived copy of `Authentication-Results:`
- `ARC-Seal:` (AS)
  Includes some tags and a DKIM-style signature of any preceding ARC headers/sets
- `ARC-Message-Signature:` (AMS)
  A DKIM-style signature of the entire message except `ARC-Seal:` headers

ARC-Authentication-Results: (AAR)

- Copy of the contents of the locally generated `Authentication-Results`: header
- One addition – the **i=** tag is prepended, containing a sequence number for the current set of ARC headers

ARC-Message-Signature: (AMS)

- A modified DKIM signature – leverages existing libraries
- **i=** tag is different – under ARC, a sequence number for ARC header sets
- **v=** tag is missing in ARC
- Should not be usable as a DKIM signature in a replay attack

ARC-Seal: (AS)

- Populated with *key=value* pairs
- **b=** is a signature of all ARC headers
- **a=/d=/s=** fields match the corresponding DKIM tags
  - Same key format and DNS records as for DKIM
  - Can use your DKIM keys for ARC
  - *SMJ*: I recommend a separate key per best practices
- **cv=** indicates whether ARC chain validated as received by the reporting intermediary
- **i=** tag is a sequence number for ARC header sets

Order of Insertion

- `Authentication-Results`: content is copied into a new `ARC-Authentication-Results`: header, prefixed
- `ARC-Message-Signature`: is calculated for message, including newest AAR header, and prefixed
  - Must not include any `ARC-Seal`: headers
- `ARC-Seal`: is calculated and prefixed
- ARC headers prefixed per common practice, but order of appearance is not critical for validation

The **i=** Sequence Number

The **i=** sequence tag is used to order the ARC headers for various operations

- Allows multiple headers to be grouped correctly
- Eliminates reliance on the order of headers being inserted – or not being altered
- Compare with order of insertion of various authentication, content scanning, or `Received:` headers

What A Valid ARC Chain Looks Like

Method used by each participant to determine the **cv=** value in their `ARC-Seal`:

- All `ARC-Seal`: headers must validate
- The **cv=** value for those AS headers must be Pass
- The most recent `ARC-Message-Signature`: (highest **i=** value) must validate

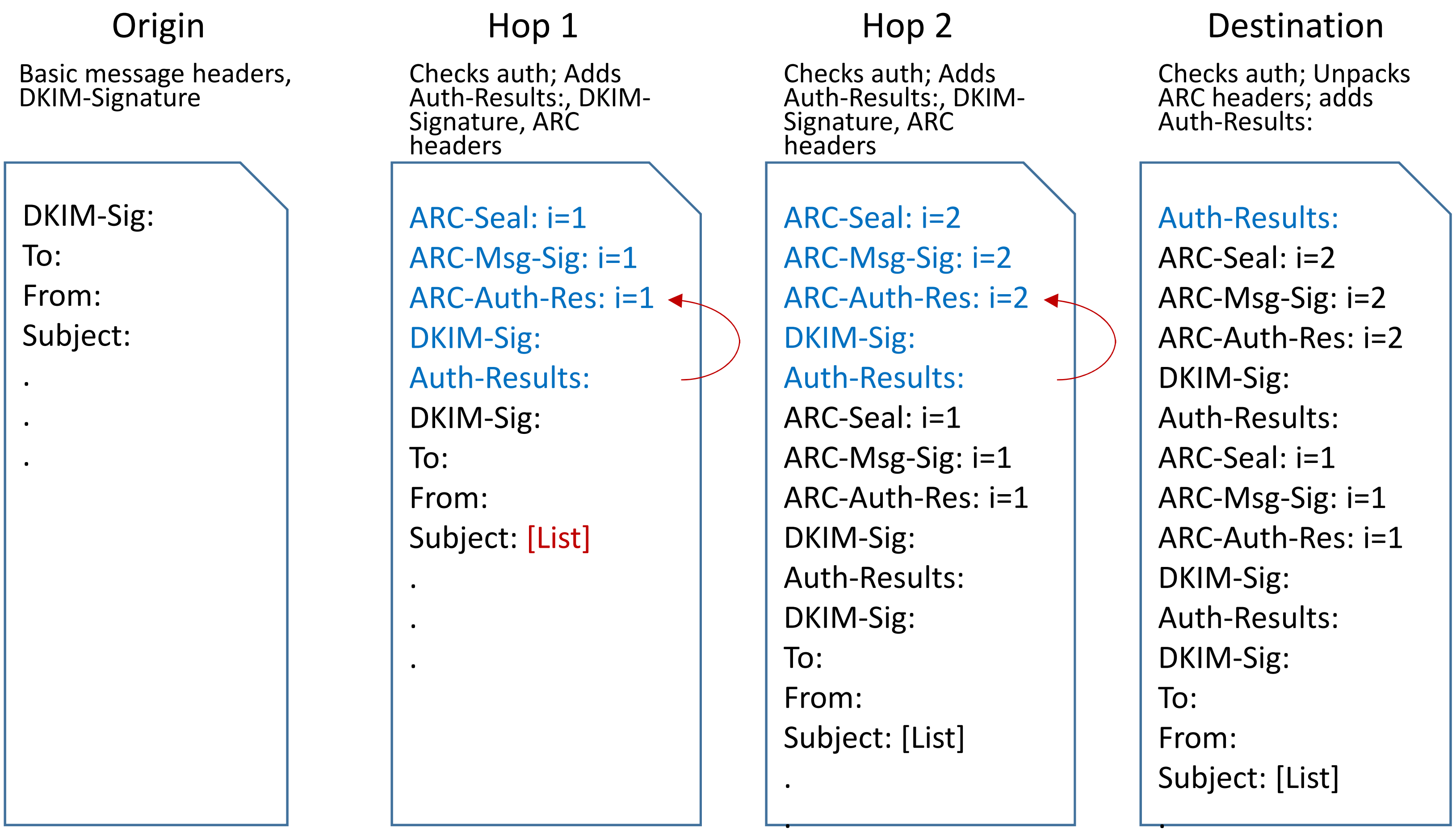
When Would I Insert ARC Headers?

- When a message is subject to handling that will knowingly break existing DKIM signatures
  - Inserting `Subject:` tags
  - Appending disclaimers and footers
  - Stripping attachments
  - Content-encoding changes
- When the message crosses a trust boundary, which might occur within a given ADMD
  - Multi-department or multi-entity enterprise

When Wouldn’t I Insert ARC Headers?

- ARC builds a verifiable chain of intermediate message handlers
- Anonymous remailers would not find this helpful
- *Other examples?*

What Does ARC Look Like?



Origin

Basic message headers, DKIM-Signature

DKIM-Sig:
To:
From:
Subject:
.
.
.

Hop 1

Checks auth; Adds Auth-Results:, DKIM-Signature, ARC headers

ARC-Seal: i=1
ARC-Msg-Sig: i=1
ARC-Auth-Res: i=1
DKIM-Sig:
Auth-Results:
DKIM-Sig:
To:
From:
Subject: [List]
.
.
.

Hop 2

Checks auth; Adds Auth-Results:, DKIM-Signature, ARC headers

ARC-Seal: i=2
ARC-Msg-Sig: i=2
ARC-Auth-Res: i=2
DKIM-Sig:
Auth-Results:
ARC-Seal: i=1
ARC-Msg-Sig: i=1
ARC-Auth-Res: i=1
DKIM-Sig:
Auth-Results:
DKIM-Sig:
To:
From:
Subject: [List]
.
.

Destination

Checks auth; Unpacks ARC headers; adds Auth-Results:

Auth-Results:
ARC-Seal: i=2
ARC-Msg-Sig: i=2
ARC-Auth-Res: i=2
DKIM-Sig:
Auth-Results:
ARC-Seal: i=1
ARC-Msg-Sig: i=1
ARC-Auth-Res: i=1
DKIM-Sig:
Auth-Results:
DKIM-Sig:
To:
From:
Subject: [List]
.

How Are ARC Verdicts Shown?

- `arc=pass` or `arc=fail` may be inserted into `Authentication-Results`: headers

- DMARC-aware receivers who incorporate ARC results should include ARC information in aggregate reports `local_policy` section:

```
<reason>
  <type>local_policy</type>
  <comment>arc=pass ams=d1.example d=d1.example,d1.example</comment>
</reason>
```

- `ams=` is the **d=** domain from the last AMS

- d= is the list of **d=** domains from validated `ARC-Seal`:

Summary

Benefits of ARC

Sender/Intermediary Benefits

- Allow more senders to adopt `p=reject` DMARC policies, block fraudulent messages
- Allow intermediaries to continue or resume traditional `From:` semantics, message modifications
- May improve deliverability

Receiver Benefits

- Allow more receivers to enforce DMARC policies
- Allow more mailbox providers to publish `p=reject` policies on their customer-facing domains
- More data for reputation systems

ARC Timeline

- October 2015:
  - Announcement at M^{3}AAWG 35 in Atlanta
  - Draft specification and usage doc published as IETF Internet-Drafts
- Fall 2015 – Winter 2016:
  - AOL, GMail, and OpenARC implementations developed
- February 2016
  - Interoperability event #1
- March-April 2016
  - Updates to the specification
- May 2016
  - Interoperability event #2
- June-July 2016
  - Interoperability event #3

ARC Resources

- Website for latest ARC news: http://arc-spec.org
- Mailing List for discussion of ARC: http://lists.dmarc.org/mailman/listinfo/arc-discuss
- Specification, current draft: https://tools.ietf.org/html/draft-andersen-arc-04
- Usage Guidelines, current draft: https://tools.ietf.org/html/draft-jones-arc-usage-01

Questions