DMARC and Email Authentication

Steve Jones
Executive Director
DMARC.org

Cloud & Messaging Day 2016
Tokyo, Japan
November 28th, 2016

What is DMARC.org?

- DMARC.org is an independent, non-profit advocate for the use of email authentication
- Supported by global industry leaders:

Sponsors: AGARI COMCAST Google FARSIGHT SECURITY Return Path TDP Trusted Domain Project

Supporters: LinkedIn messagesystems PayPal ValiMail

What Does DMARC Do, Briefly?

- DMARC allows the domain owner to signal that fraudulent messages using that domain should be blocked
- Mailbox providers use DMARC to detect and block fraudulent messages from reaching your customers
- Organizations can use DMARC to perform this filtering on incoming messages – helps protect from some kinds of phishing and “wire transfer fraud” email, also known as Business Email Compromise (BEC)
- Encourage your partners/vendors to deploy inbound DMARC filtering for protection when receiving messages
- More information available at https://dmarc.org

Overview Of Presentation

- DMARC Adoption
- Case Study - Uber
- Technical Challenges
- Roadmap

DMARC Adoption

This section will provide an overview of DMARC adoption since it was introduced, globally and within particular country-specific top-level domains. It will also show how the DMARC policies published by top websites has evolved over the past two years.

Deployment & Adoption Highlights

2013:

- 60% of 3.3Bn global mailboxes, 80% consumers in US protected
- Outlook.com users submitted 50% fewer phishing reports
- PayPal: 70+% reduction in customers reporting fraudulent messages

2014:

- Twitter able to measure and block 110MM attacks per day, 2.5Bn over a 45 day period
- 600% increase in organizations using DMARC to filter incoming messages and sending reports to domain owners

Deployment & Adoption Highlights

2015:

- 35% of email received by top global MSPs protected by DMARC
- 70% of global mailboxes protected by DMARC
- .BANK/.INSURANCE require strong DMARC policy for all domains
- Blocket of Sweden adopts DMARC, blocks 99% of suspicious message, sees 70% reduction in customer phishing complaints

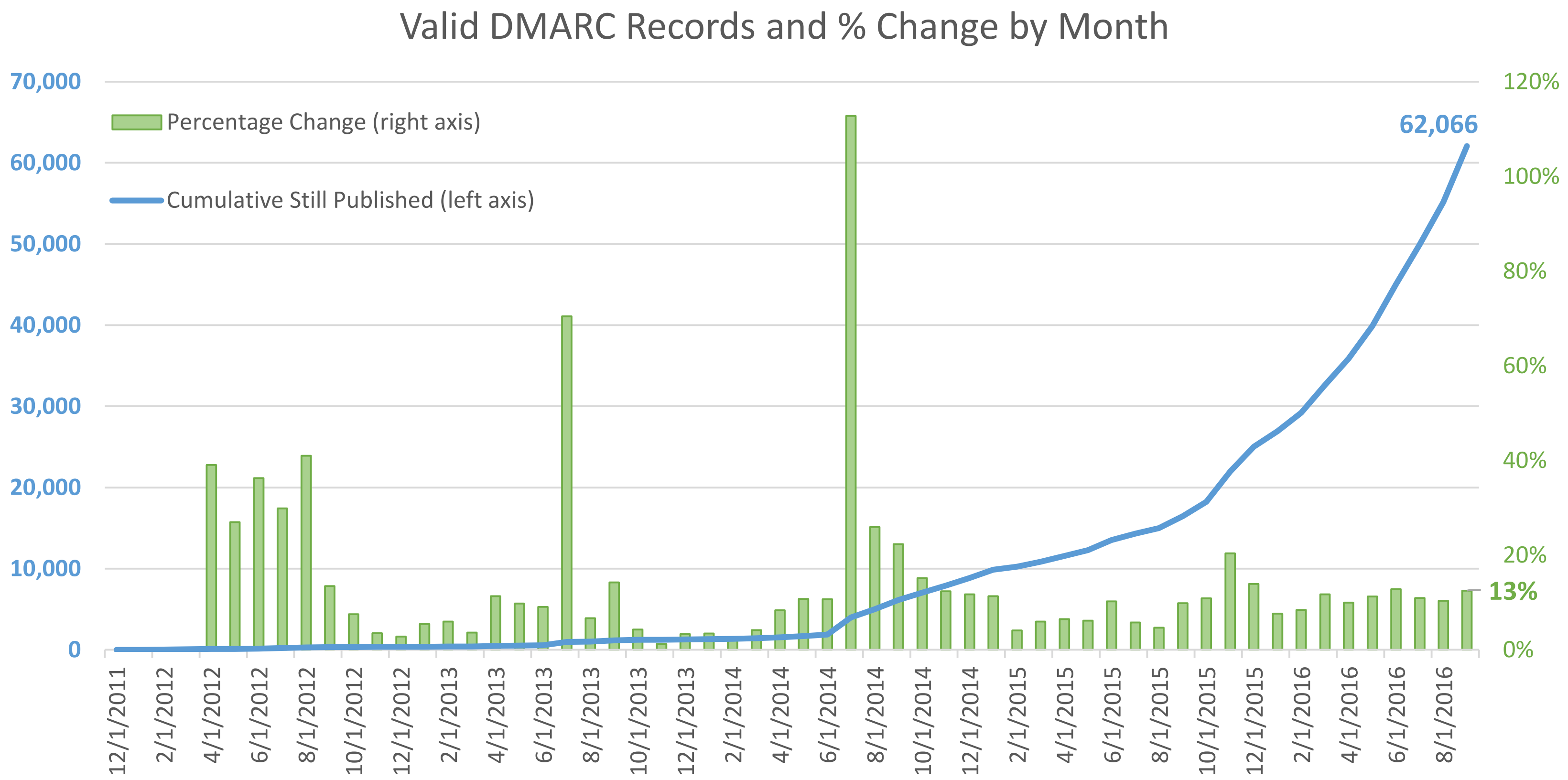
2016:

- 12 commercial email gateways offer DMARC filtering
- UK Cabinet Office requires DMARC for `service.gov.uk` domains
- NCSC deploys DMARC on `gov.uk` domain

Adoption Data in Following Slides

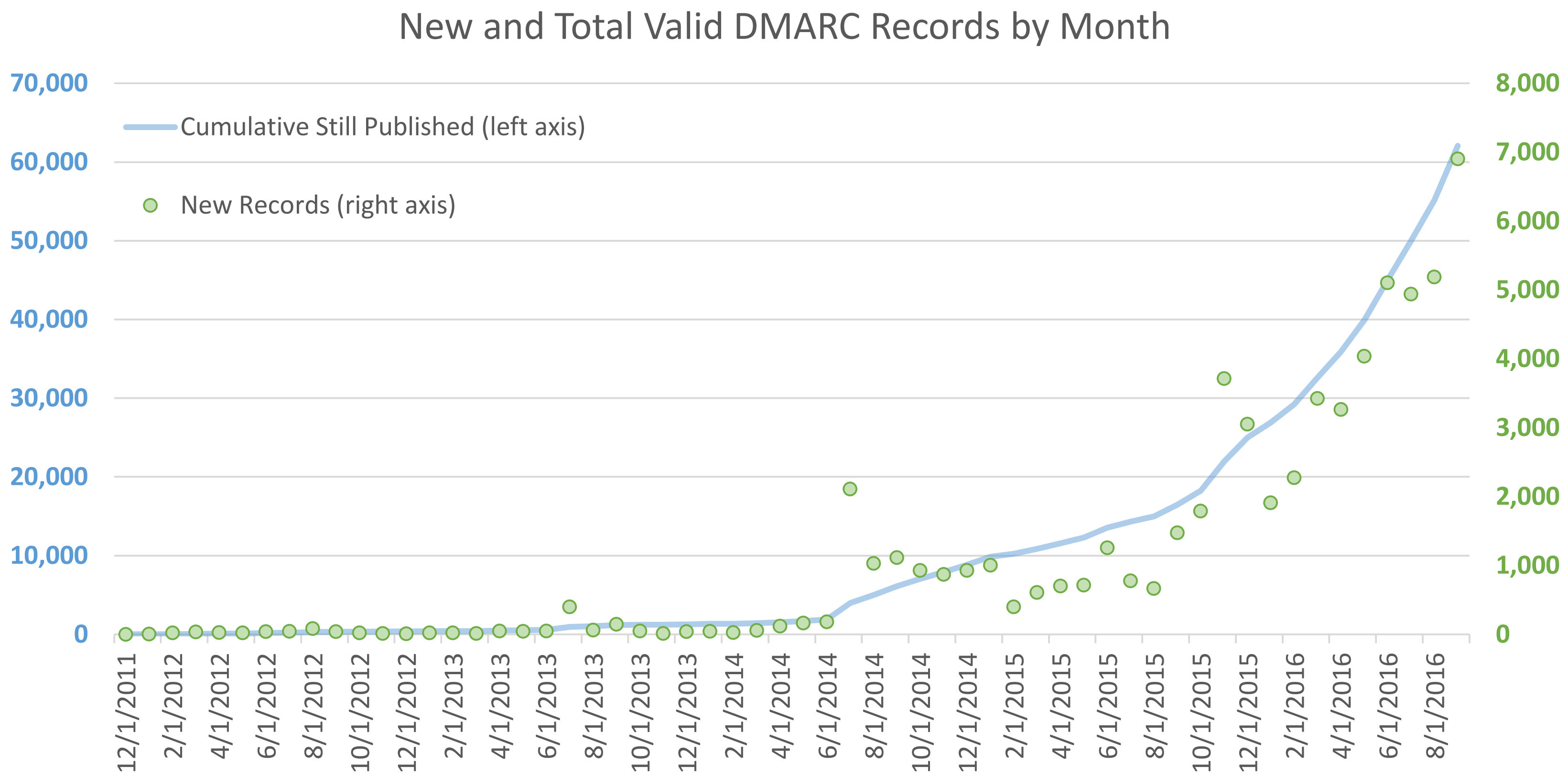
- Alexa data is based on DNS queries performed by DMARC.org
- Other data about DMARC records supplied by Farsight Security
- Farsight does not monitor the entire Internet – may miss records other organizations see and vice versa
- **But**, Farsight's data has been collected over the entire period DMARC has been deployed, providing a unique view of growth
- Only DMARC records that were still active/published at the time the graphs were created are included.
  - The global total would more than double including records no longer published

High-Level Adoption of DMARC



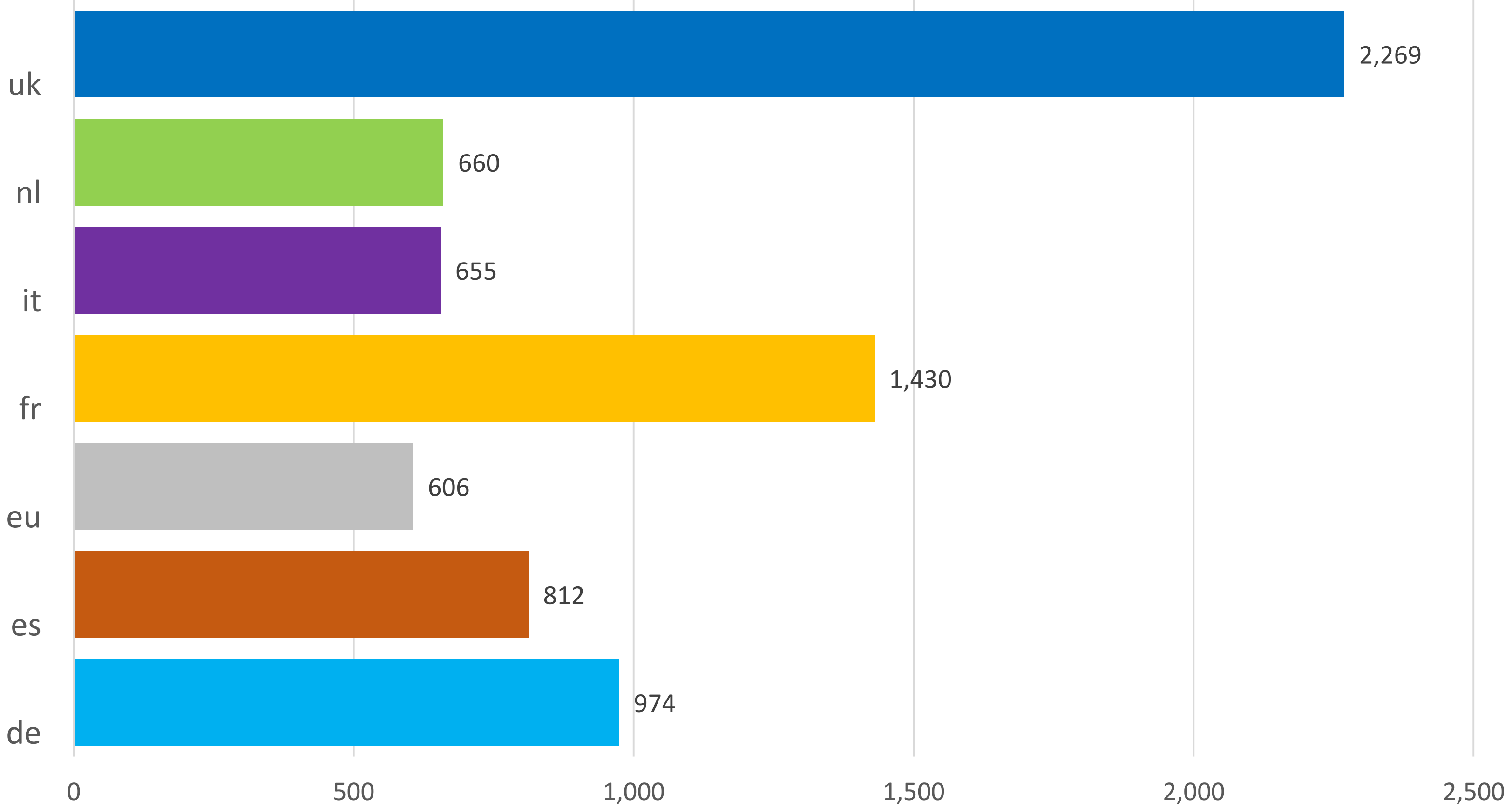
Data supplied by Farsight Security

New DMARC Records per Month



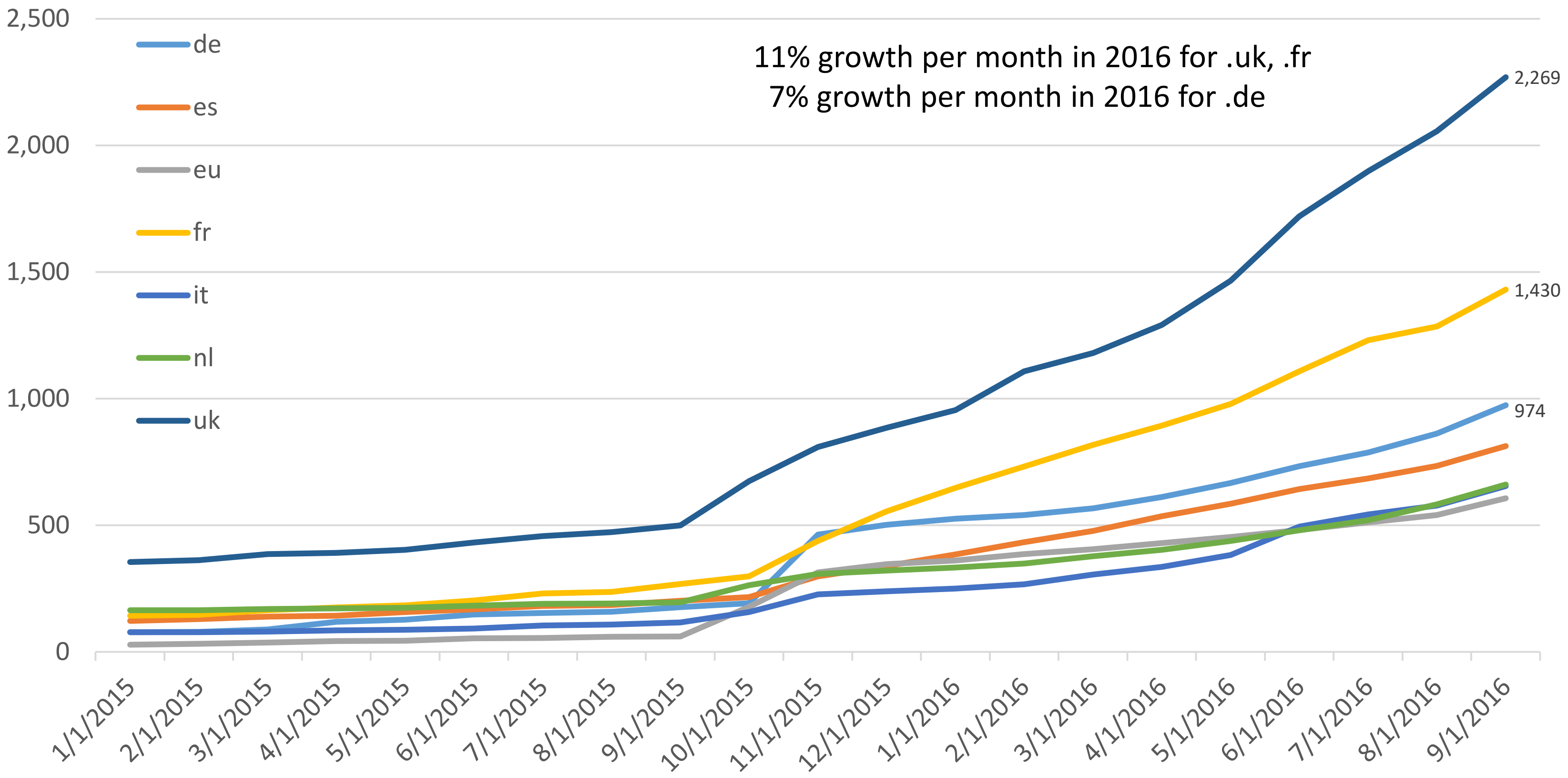
Data supplied by Farsight Security

Active DMARC Records in Euro ccTLDs



Data supplied by Farsight Security

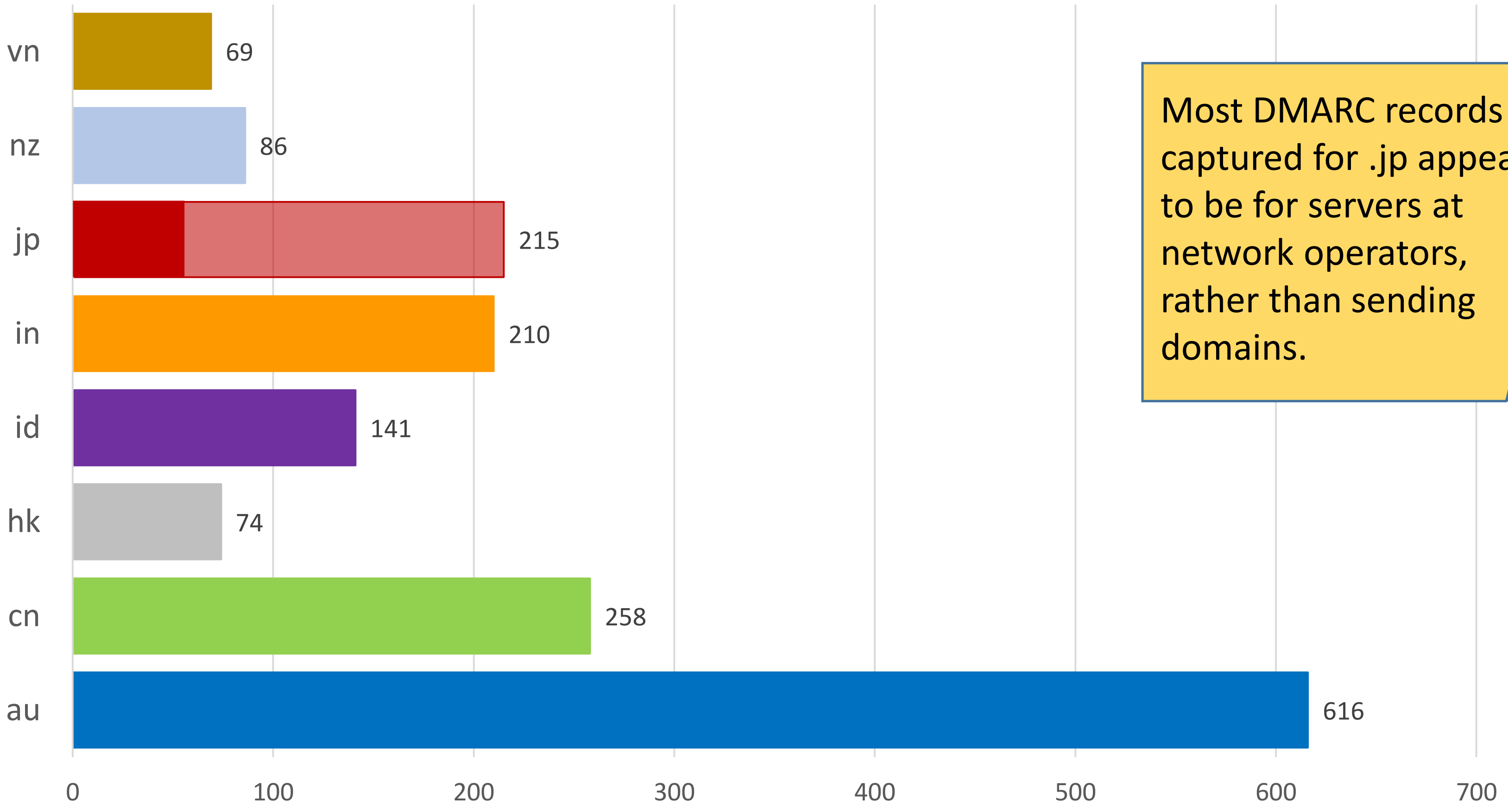
Active DMARC Records in Euro ccTLDs



11% growth per month in 2016 for .uk, .fr
7% growth per month in 2016 for .de

Data supplied by Farsight Security

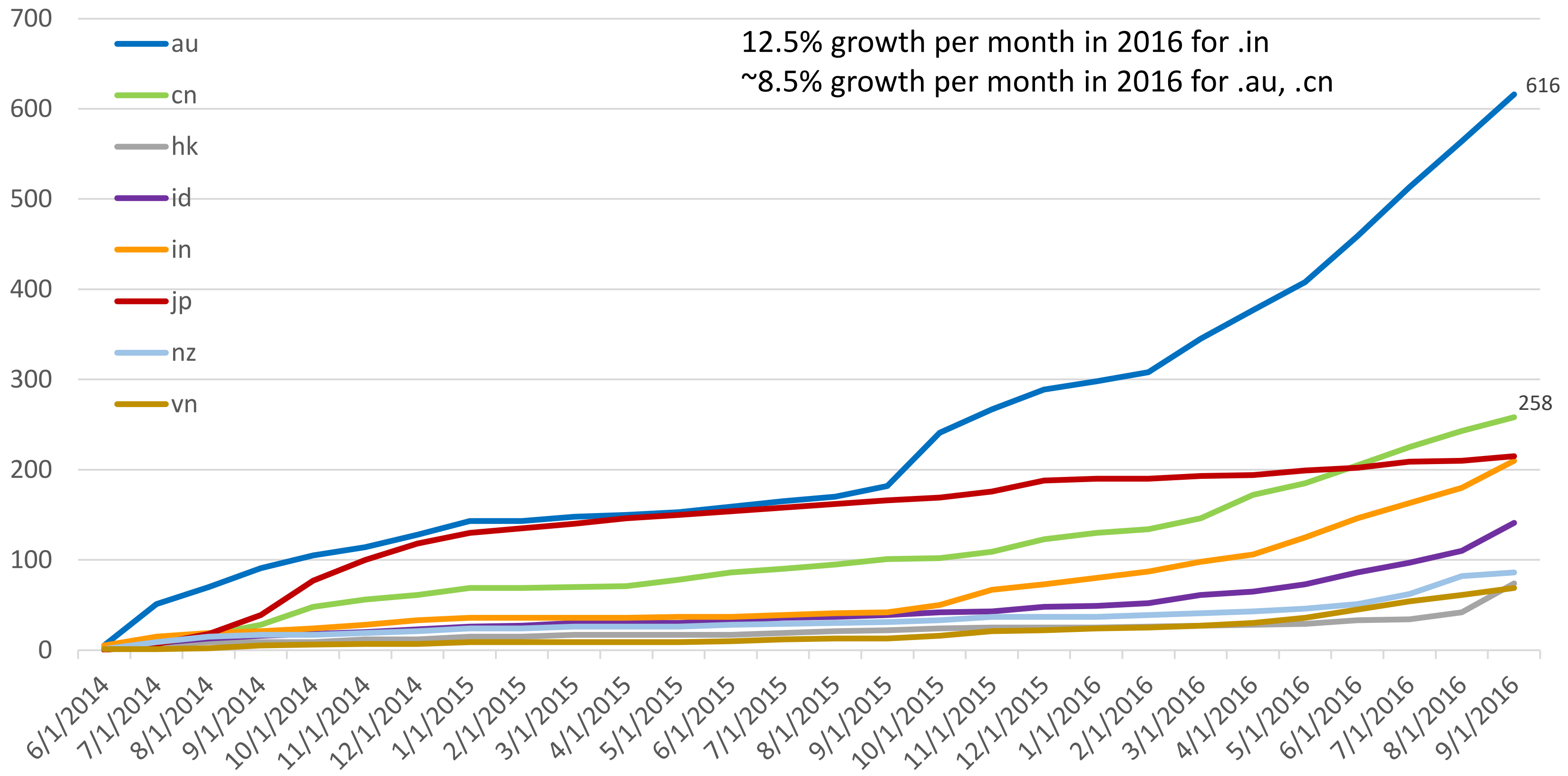
Active DMARC Records in Asia ccTLDs



Most DMARC records captured for .jp appear to be for servers at network operators, rather than sending domains.

Data supplied by Farsight Security

Active DMARC Records in Asia ccTLDs



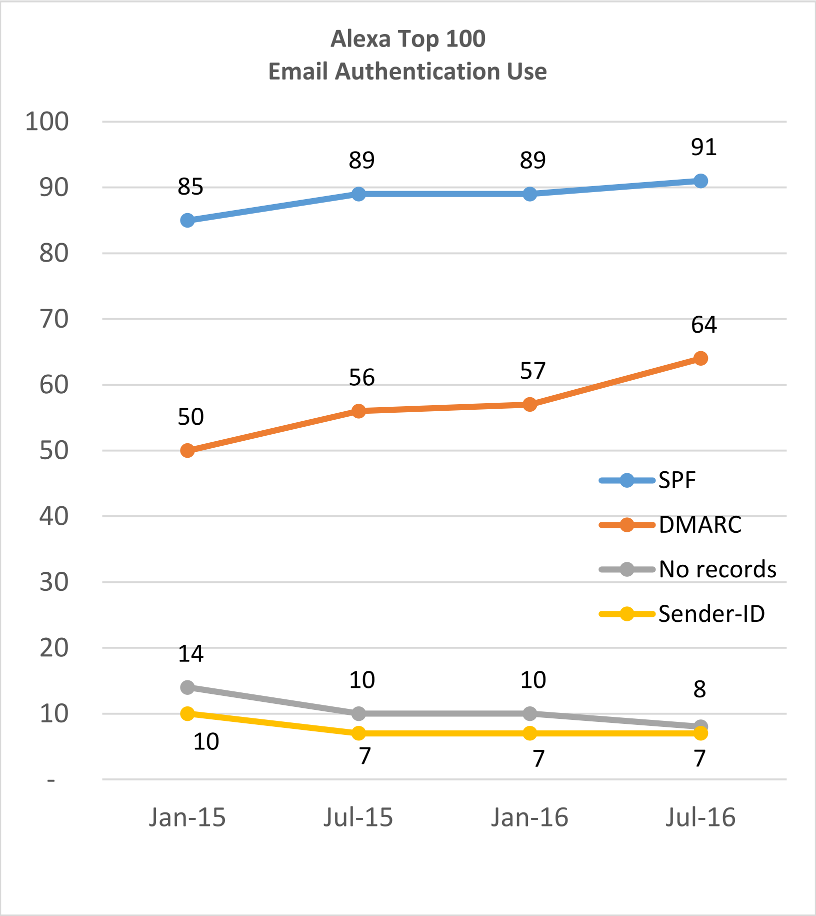
12.5% growth per month in 2016 for .in
~8.5% growth per month in 2016 for .au, .cn

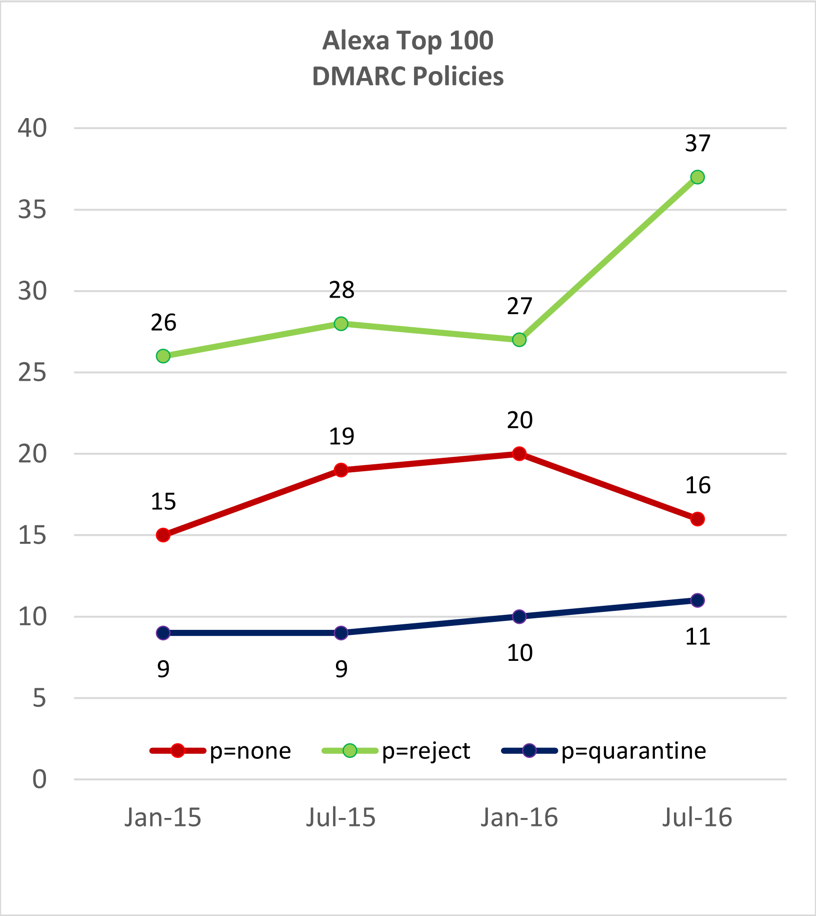
Data supplied by Farsight Security

Who Publishes DMARC in Japan?

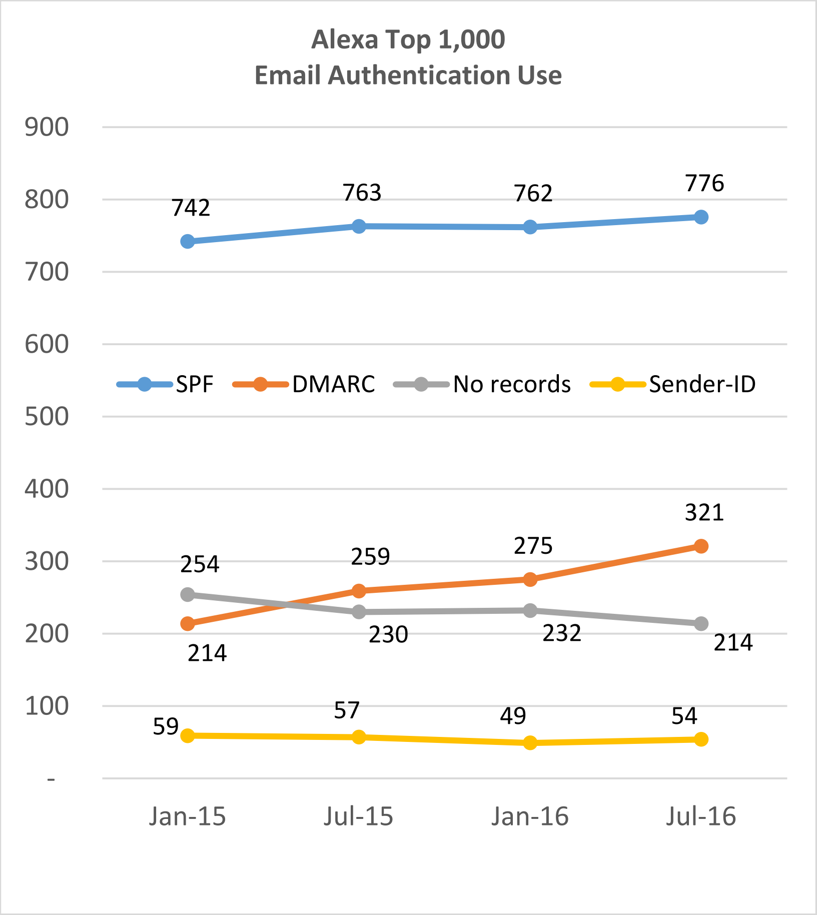
- Mostly network operators (ne.jp = 147)
  - 60 odn.ne.jp
  - 47 att.ne.jp
  - Most are 4-level (`_dmarc.xxx.yyy.ne.jp`)
- Domestic companies
  - 三井住友銀行 (SMBC Trust Bank)
  - 株式会社ローソン (Lawson)
  - 三菱UFJフィナンシャル･グループ (Mitsubishi UFJ Financial)
  - 楽天市場 (Rakuten)
  - 東芝 (Toshiba)
- Foreign companies (Amazon, AmEx, Apple, Citi, Google, PayPal)

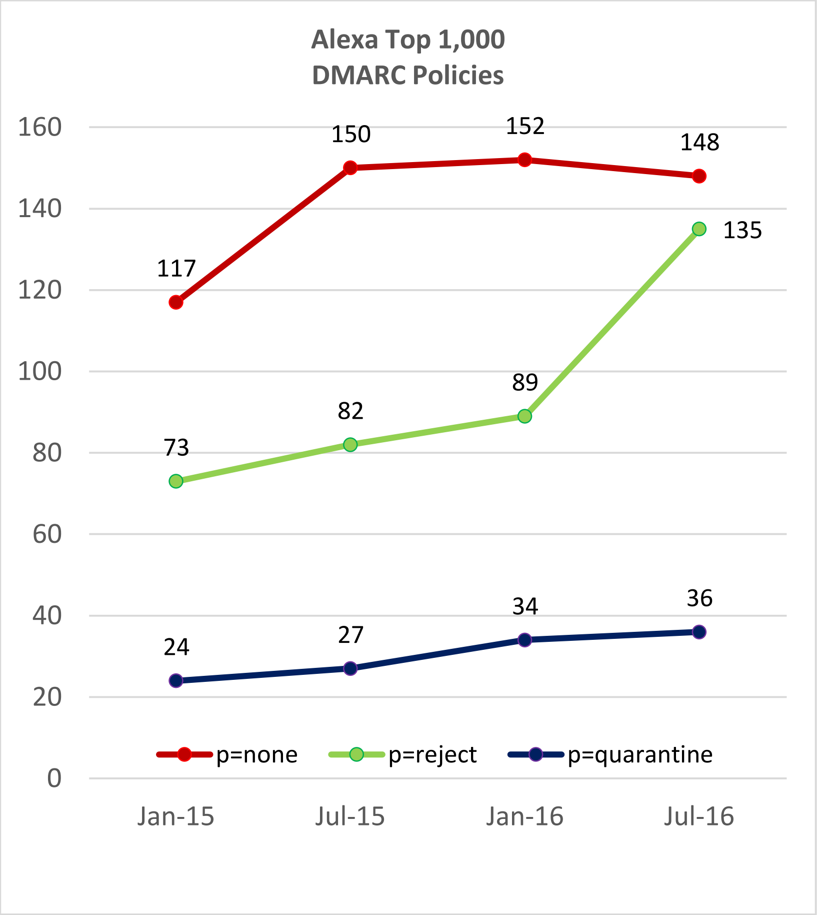
Alexa Top Sites and Email Auth





Alexa Top Sites and Email Auth





Case Study

Uber's Road to Email Authentication

Uber’s Road to Email Authentication

- We regret that we do not have permission to redistribute the slides from this section of the presentation.

- We thank Uber and ValiMail for making them available to our audience on November 28th

Technical Challenges

This section describes some technical challenges currently facing the email community.

Technical Challenges

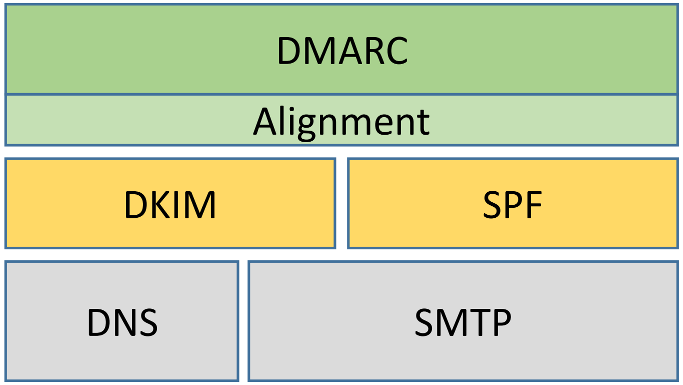
- Indirect Mail Flows And ARC
- DKIM Replay

Indirect Mailflows
And ARC

This section describes the problems indirect mailflows pose to email authentication, and how the Authenticated Received Chain (ARC) is designed to address these problem.

DMARC and Indirect Mailflows

- DMARC operates on DKIM and SPF results
- Both DKIM and SPF have issues with “indirect mailflows”
  - Messages that transit multiple organizations
  - Forwarding, aliasing, mailing lists, etc
- Indirect mailflows are very important to their users
- Applying DMARC in many cases requires the ability to accommodate indirect mailflows
- This gave rise to the ARC protocol



DMARC

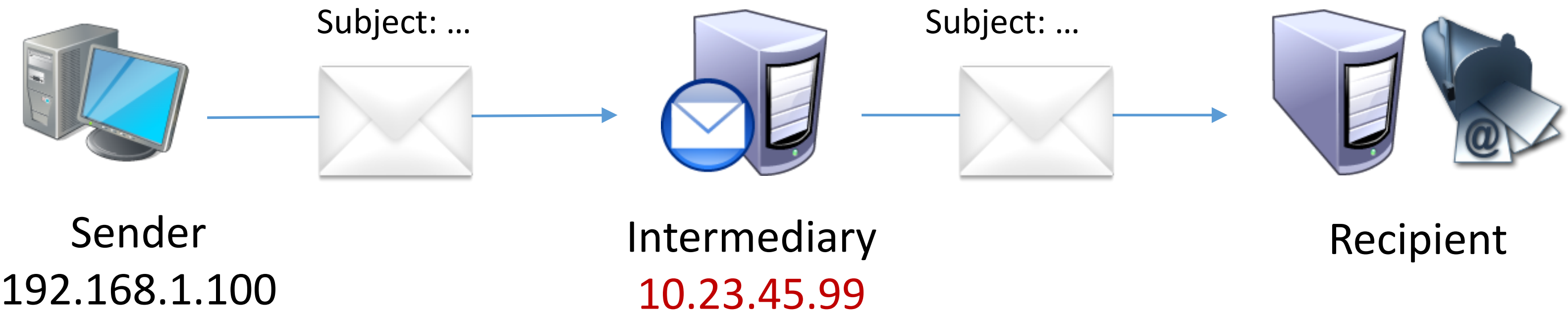
Alignment

DKIM SPF

DNS SMTP

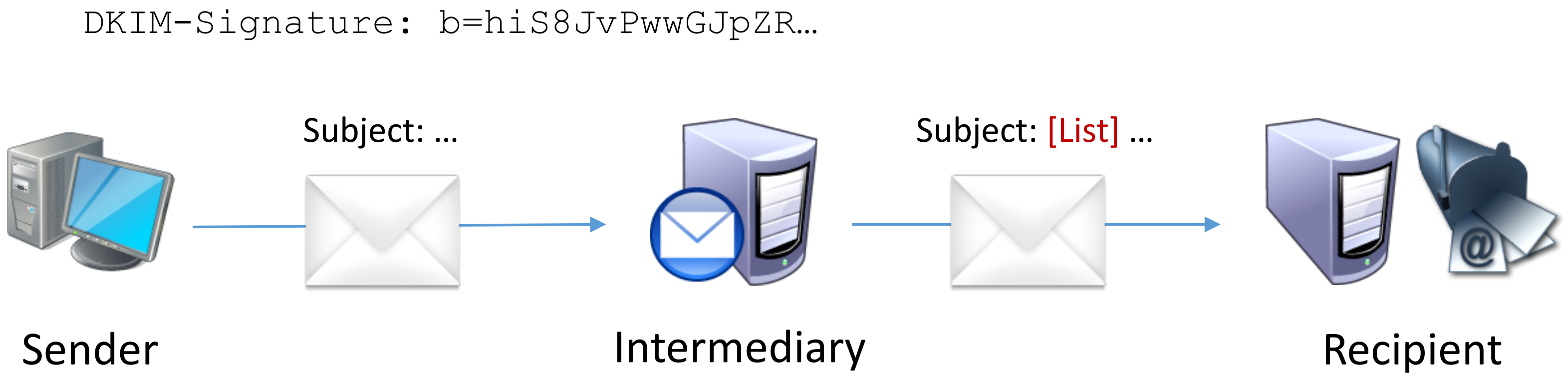
Example: Indirect Mailflows and SPF

```
example.com IN TXT “v=spf1 ip4:192.168.1.100”
```



- Intermediary verifies valid message from Sender
- Intermediary forwards the message from a different IP address
- SPF will fail to verify for Sender’s domain when checked at Recipient

Example: Indirect Mailflows and DKIM



- Intermediary verifies valid message from Sender
- Intermediary changes the message contents, for example Subject:
- Sender’s DKIM signature will fail to verify when checked at Recipient

Why Was ARC Created?

- Indirect mailflows always a challenge – not a new problem
- DMARC initially used for commercial domains – banking, marketing – where messages sent directly to consumer
- In Spring 2014 attackers start impersonating AOL and Yahoo addresses to attack their customers in great numbers
- AOL and Yahoo published a `p=reject` DMARC policy for their customer-use domains, `user@yahoo.com`
- Resolved the attack against their customers, but had very negative impact on ~1% of mail using indirect mailflows
- ARC working group formed

Design Decisions for ARC

- Originator of message makes no changes
- Convey the `Authentication-Results:` content intact from the first ARC intermediary forward
- Allow for multiple "hops" or systems/organizations handling messages
- ARC headers can be verified at each hop
- Work at Internet scale
- Define ARC independently of DMARC if possible

Design Decisions for ARC

- Message receiver seeing an authentication failure under DMARC can check for ARC headers in message
- If ARC headers are intact, they can see and validate `Authentication-Results:` content reported by the ARC participants
- Depending on reputation of intermediaries and results, message recipient may choose to use ARC information to make a "local override" of failed authentication checks like DMARC
  - ARC should be used with a reputation system

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 attribution
- ARC can provide data on intermediaries to a reputation system tracking their behavior
- Signed ARC headers are a more reliable trace header than unsigned Received: headers

What Doesn’t ARC Do?

- Does not say anything about “trustworthiness” of the message sender or intermediaries
- Says nothing about the contents of the message
- Intermediaries might still inject bad content
- Intermediaries might remove some or all ARC headers
- But the signed ARC headers help senders and receivers track down bad intermediaries

How Are ARC Headers Added?

Origin

Basic message headers, DKIM-Signature

Mailing List

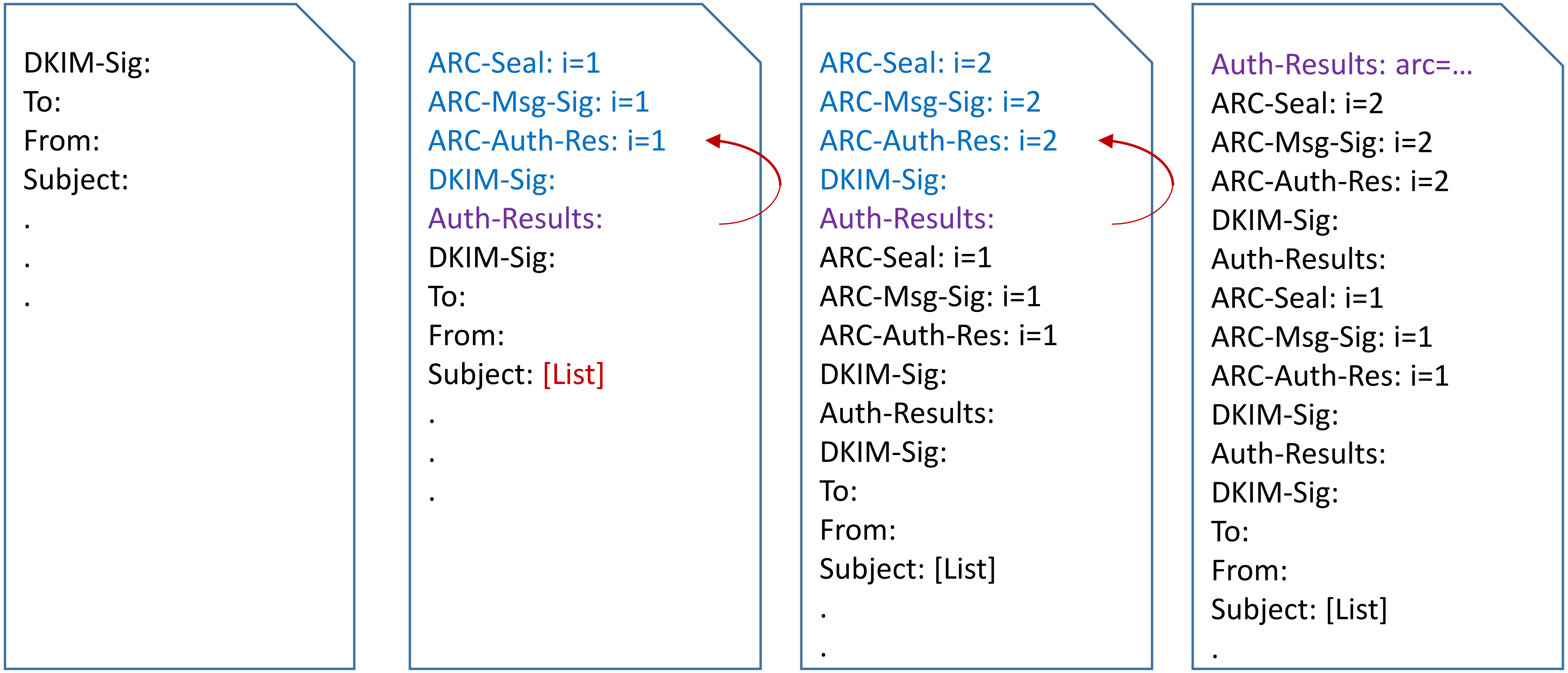
Checks auth; Adds Auth-Results:, DKIM-Signature, ARC headers, Subject tag

Alumni Mailbox

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

Destination

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



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

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

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]
.
.

Auth-Results: arc=…
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]
.

What Do ARC Headers Look Like?

```
X-Received: by 20.30.40.11 with SMTP id u204mr8130724ywa.51.1466170851933;
        Fri, 17 Jun 2016 06:40:51 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1466170851; cv=none; d=example.com; s=arctest;
        b=xe+jRquPNixNhesh5fostFt7OsrGic+UDHg9ZEnoM/lVyuT+vamXYq+ajRzeoHzkIQ
        qRqpka375Th/wZBCWPYyByFYT17kv/s/0w5TesTSYXxOtO2uGeGoyeg2ekXEdL2z3UxT
        cKIYtAmH7454+a/TVWB7tsm6LlvWSo8bwZMi0vN5YduhSTFOA8bLXq4hEAHkp2xm0xW+
        6fOHAcYIppRKAcF52WRdCKU5rGli+3bVj8mKaHFu+2TChaY9N6bubnR0LqmPkJ64KNhg
        3LvHA4fRSazTblTpdM3n0bEln/mhek1GwUTtsTi03viMbKBu58izA2oN+U2rz9HcAXC3
        Sneg==

ARC-Message-Signature: i=1; a=rsa-sha256; d=example.com; s=arctest;
        h=auto-submitted:subject:from:to:date:message-id:arc-authentication-results;
        bh=5BoDhYVbcbDAJ0VNngnjGAxJHFj24gqA3V1CMwjydl0=;
        b=2iotKbPydBaJ6yyAs3/2gcSJbumGYpN7GRH3lBs9NfU0FTmkikODOrg6KvIkHvUyzU
        7Baf3WoCoCDulCSp1AK/cCOxcyJ5xshuyOhS0e335/Xe8EzwH34w/W1iQsFjdI+CMDbN
        ww7GuCSTRv3SzHLlhVQK3ldLbAldrPsMSs6J8XtwovtJvkreWJWk+lOkQL7UhM8qHhQZ
        AsJ9plKBkzVhl+RCCc1qDXZxNraSVZZ48LYK8m7t9VQhQqJLnXb9OcrxrgMtzl3FQv0x
        qPddkAGzL8PwvFZo/U1Ga3Bw4q6eE6ZmdOIwCNj/9Bpy8ZLa3Ob2ra3YVx0NN3hvoJFg
        uT5Q==

ARC-Authentication-Results: i=1; mx.example.com;
        spf=pass (example.com: domain of kurta+arc@example.org designates
10:20:30:40::1 as permitted sender) smtp.mailfrom=kurta+arc@example.org;
        dmarc=pass (p=NONE dis=NONE) header.from=example.org;
        arc=none

Return-Path: <kurta+arc@example.org>
Received: from mango.example.org (mango.example.org. [10:20:30:40::1])
        by mx.example.com with ESMTP id f67si23622388wmf.85.2016.06.17.06.40.50
        for <arc-mod-subject@example.com>;
        Fri, 17 Jun 2016 06:40:50 -0700 (PDT)
```

Where Do ARC Results Appear?

- `arc=pass` or `arc=fail` may be inserted into `Authentication-Results:` headers
- DMARC-aware receivers who validate ARC results should include ARC information in DMARC aggregate report's `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 header
- `d=` is the list of **d=** domains from all validated `ARC-Seal:` headers, in other words a list of the ARC intermediaries

ARC Implementations

- Internal Implementations:
  - AOL
  - Google
- Commercial MTAs:
  - MailerQ
- Open Source MTAs:
  - OpenARC Milter – Adds ARC to Postfix or Sendmail
- Mailing List Managers:
  - Mailman
- Other Open Source Packages:
  - dkimpy – Python library

Interoperability Testing

- Previous tests between AOL, Google, and dkimpy successful
- OpenARC messages tested successfully with MailerQ verifier
  - See https://arc.mailerq.com
- Next testing event scheduled for Friday, December 16th
- For the latest information, visit http://arc-spec.org

DKIM Replay

This section describes an abuse of DKIM recently observed at scale by some of the largest global mailbox providers. It is a form of abuse described in the original DKIM standard, but recent successes in combatting email abuse have forced criminals to explore more time-consuming and expensive attacks like this one.

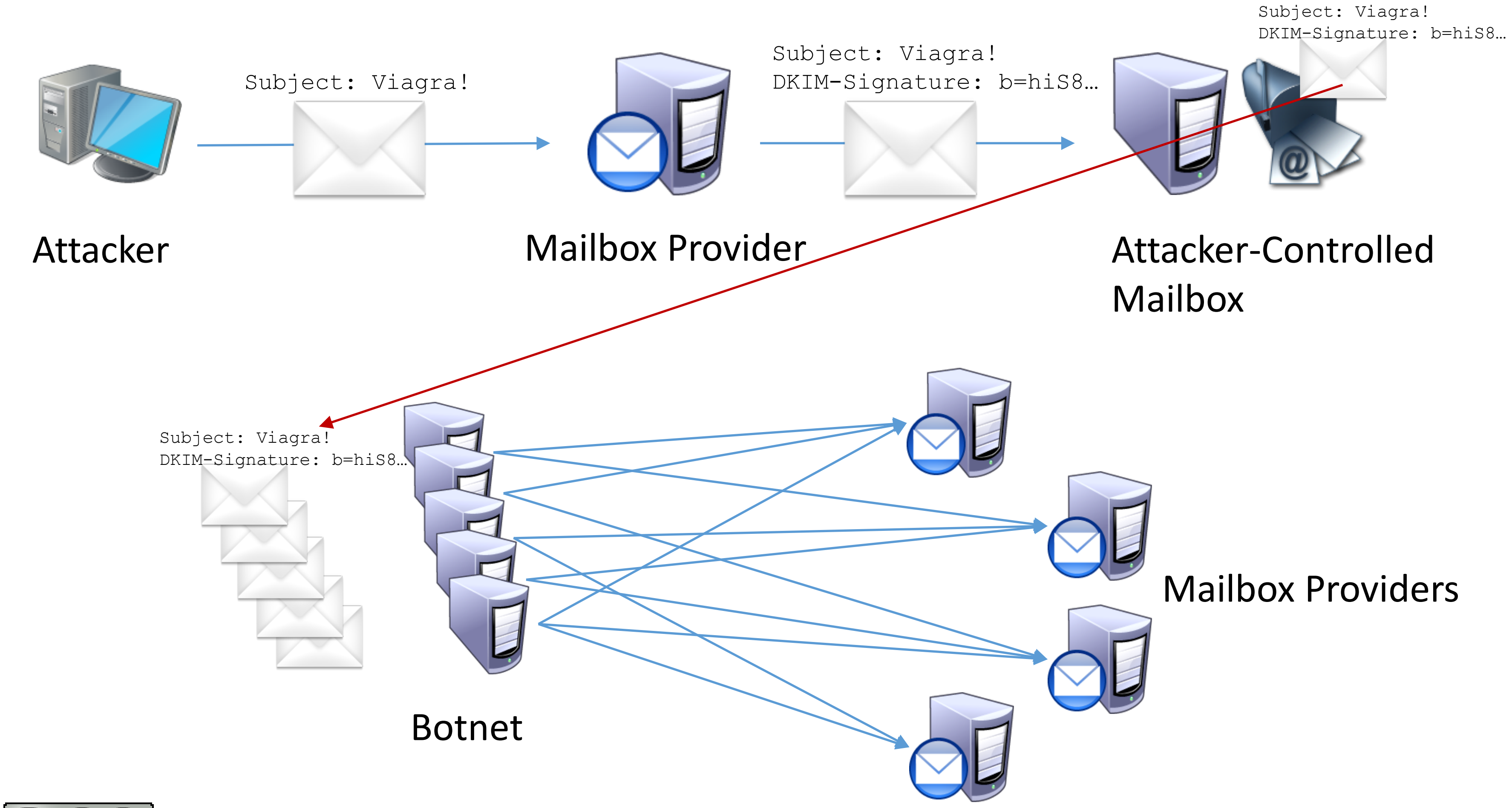
DKIM Replay Description 1

- An attack that was documented, but considered theoretical when DKIM was created
  - Described in RFC4871 and RFC6376
- One spam and/or malicious message is created or modified to get through a reputable service to a mailbox the attacker controls
  - May take the attacker many attempts, trying different changes each time
  - Message will get a DKIM signature from the reputable service

DKIM Replay Description 2

- Attacker takes signed message out of mailbox, loads into their own system, and sends it to many other recipients
  - RFC5322 message is unchanged – DKIM will still verify
  - List of RFC5321 (“envelope”) recipients set to whatever list attacker wants
  - Botnets are typically used to send messages as quickly as possible

DKIM Replay Illustration



Similar Behavior

- Mailing lists, “alias” forwarding can mimic behavior
  - Many copies of a message with the same DKIM signature
- Some ESPs, companies create a single DKIM signature for an entire mailing campaign
  - Millions of recipients, all get identical DKIM signature
- Result: Filtering cannot act solely on use of identical DKIM signature across many messages

Is DKIM Replay A Threat To You?

- Most reports have come from largest mailbox providers
- Not a threat for most companies and brands, unless they make mailboxes in their domain available to customers & partners

- Largest free mailbox providers often used to create messages
  - They also have more resources to detect and limit attacks
- ESPs and small mailbox providers very concerned about potential abuse of their reputation
  - High volume replay attacks may also overwhelm the feedback and abuse mailboxes of smaller companies

Proposed Solutions for DKIM Replay

There is no agreement on a solution for this threat so far.

Proposal 1:

- Include RFC5321.MailFrom addresses in DKIM signatures
- Breaks compatibility with existing DKIM signatures
- MTAs cannot change envelope addressing
- Forwarding of any kind will always break DKIM signatures
- Appears to limit messages to only one 5321 address each
- Internet Draft here: https://tools.ietf.org/html/draft-kucherawy-dkim-rcpts-01

Proposed Solutions for DKIM Replay

Proposal 2:

- Modify Proposal 1, provide a way for sending domains to advertise that they include 5321 addresses in DKIM signature via DNS records
- Allow end-users to provide list of forwarding services they use or allow to their mailbox provider
- Broken DKIM signatures from domains advertising that they include 5321 addresses in DKIM signatures can be checked against end-user’s list and allowed through
- Requires changes to end-user settings across Internet

Roadmap

This section describes the coming developments and next steps in several areas covered in this presentation.

Roadmap: Next Steps for DKIM Replay

- No broad agreement in technical community about how serious this threat is
- No agreement that either proposal described here is viable
- Technical community will continue to observe situation and try to develop viable countermeasures
- To contribute or monitor developments, consider joining relevant areas within M^{3}AAWG or the IETF

Roadmap: Next Steps for DMARC

- Some incremental changes to DMARC proposed
- IETF DMARC Working Group has accepted ARC protocol documents
- More changes to DMARC may be required based on experience with ARC
- Incorporating ARC *might* move DMARC to the “standards track” within the IETF

Roadmap: Next Steps for ARC

- First implementations arriving 2016 Q4
  - Open Source reference implementations (dkimpy, OpenARC)
  - Mailman mailing list package
- Some big players will announce 2016 Q4 / 2017 Q1
- Next stage will be refinements based on operational experience
- Watch for adoption by key organizations through 2017

Roadmap: Other Projects

- Several parties talking about giving the end-user some indication of message authentication results
- Open standard available to all interested parties
- Leverages DMARC to verify message authenticity
- Early/pilot work being done at GMail and Microsoft using proprietary data
  - GMail showing "?" for non-TLS, non-authenticated
- One group starting on protocols now
- Expect a proof-of-concept project in 2017

Resources and Information

The following slides include URLs for news articles, policy documents, and other materials that may be useful to those interested in the subjects described in this presentation.

Resources – ARC and DMARC

- DMARC.org website: https://dmarc.org
- IETF DMARC Working Group: https://datatracker.ietf.org/wg/dmarc/
- ARC general information: http://arc-spec.org
- ARC Protocol, current draft: https://tools.ietf.org/wg/dmarc/draft-ietf-dmarc-arc-protocol/
- ARC Usage Guidelines, current draft: https://tools.ietf.org/wg/dmarc/draft-ietf-dmarc-arc-usage/
- Mailing List for discussion of ARC: http://lists.dmarc.org/mailman/listinfo/arc-discuss

Resources – Dutch & German Policies

- Dutch government recommends and requires DKIM and DMARC
  https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uitopen-standaard/dkim

- German BSI recommends DMARC
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-098.html

- eco.de / Certified Senders Alliance: DMARC is compatible with Germany’s federal and state data privacy laws
  https://e-mail.eco.de/wp-content/blogs.dir/26/files/eco_dmarc_legal_report.pdf

- eco.de / Certified Senders Alliance: Members required to adopt strong authentication (DMARC)
  https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Directive.pdf

Resources – UK Policies

- November: £1.9 billion national cyber security strategy
  https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

- October: National Cyber Security Centre plans to create dashboard showing government department adoption of DMARC
  https://www.publictechnology.net/articles/news/national-cyber-security-centre-publish-rankings-departmental-email-security

- September: NCSC Chief outlines new, active approach
  https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

- June: Cabinet Office requires DMARC & HTTP STS by Oct 1st
  https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/