TOMORROW starts here.

CISCO

Cisco *live!*

Don’t Be A Phish – Deep Dive Into E-mail Authentication Techniques

BRKSEC-3770

Hrvoje Dogan, Security Solutions Architect

Agenda

- Introduction to Phishing
- Hardening Your E-mail Infrastructure With Message Authentication:
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting & Conformance (DMARC)
- Q&A

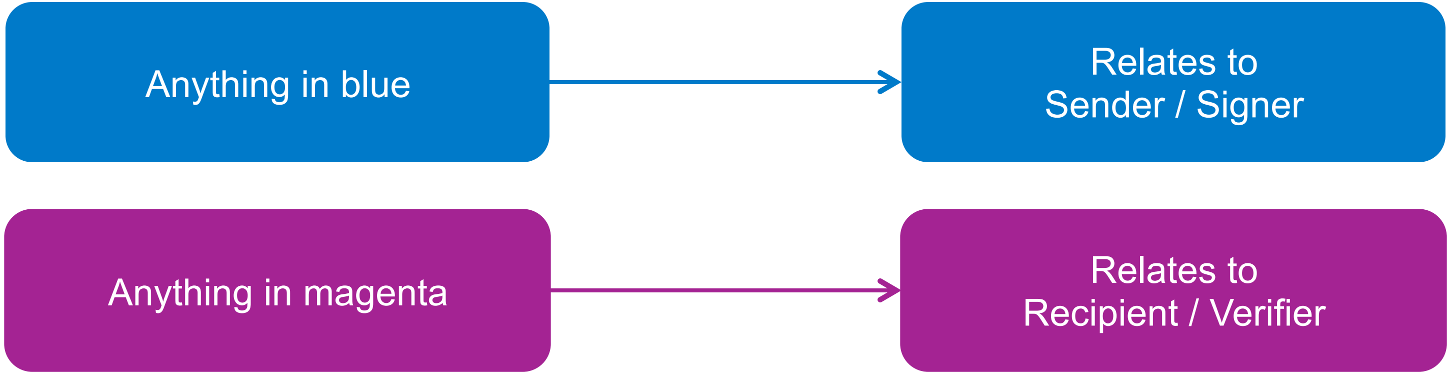
Abstract

Phishing is the plague of today's e-mail communication. With modern anti-spam rendering legacy spam almost non-existent, different variants of phishing attacks are becoming the primary threat to global e-mail systems. Several authentication methods have been around for a while, but their adoption was low and not properly encouraged, and they mostly solved just parts of the problem. However, recent developments upgrade on those legacy techniques, and make message authentication, reporting and visibility part of Internet standards.

This advanced session will provide an in-depth review of SPF, DKIM and DMARC, the prevalent message authentication techniques, and how Cisco E-mail Security products can utilize them.

We will architect a real-world message authentication architecture and show through examples how, once implemented by all parties, it makes phishing with your identity impossible. Proper implementation of e-mail authentication techniques not only prevents you from being phished, but also helps protect your identity and brand reputation, and keeps you a reliable, trustworthy communication and business partner.

Content Aids



Anything in blue → Relates to Sender / Signer

Anything in magenta → Relates to Recipient / Verifier

The curious fish that wants to know more
Adorns the slides that are For Your Reference

The caught fish is our Progress Indicator

Note: Some of the concepts laid out will be abstracted/simplified for easier delivery. I will make the best effort to point out when there is more happening “behind the scenes” but is not practical to deliver in this session.

Introduction to Phishing

Brodet

Dalmatian fish stew, usually served with polenta

- 1 kg of wild fish (scorpion fish, conger eel, angler… the more the merrier)
- 1-2 dl of olive oil
- 3 onions
- 6 cloves of garlic
- 500 gr of tomatoes, diced (canned or fresh)
- Salt, pepper, parsley leaves, bay leaf
- Some wine vinegar

Cut fish into large pieces. Dice onions and parsley, finely chop garlic.

In a medium to large pan, heat olive oil, fry onion until glassy. Add fish and fry shortly. Add tomatoes. Add the rest of the ingredients and enough water to completely cover the fish.

Cook on low to medium heat for about one hour, add water if it evaporates.

The key to a good brodet is finding out the right amount of wine vinegar to add, to give the tomato sweetness a nice twang. Just experiment!

“**phish·ing** *noun* \ˈfi-shiŋ\

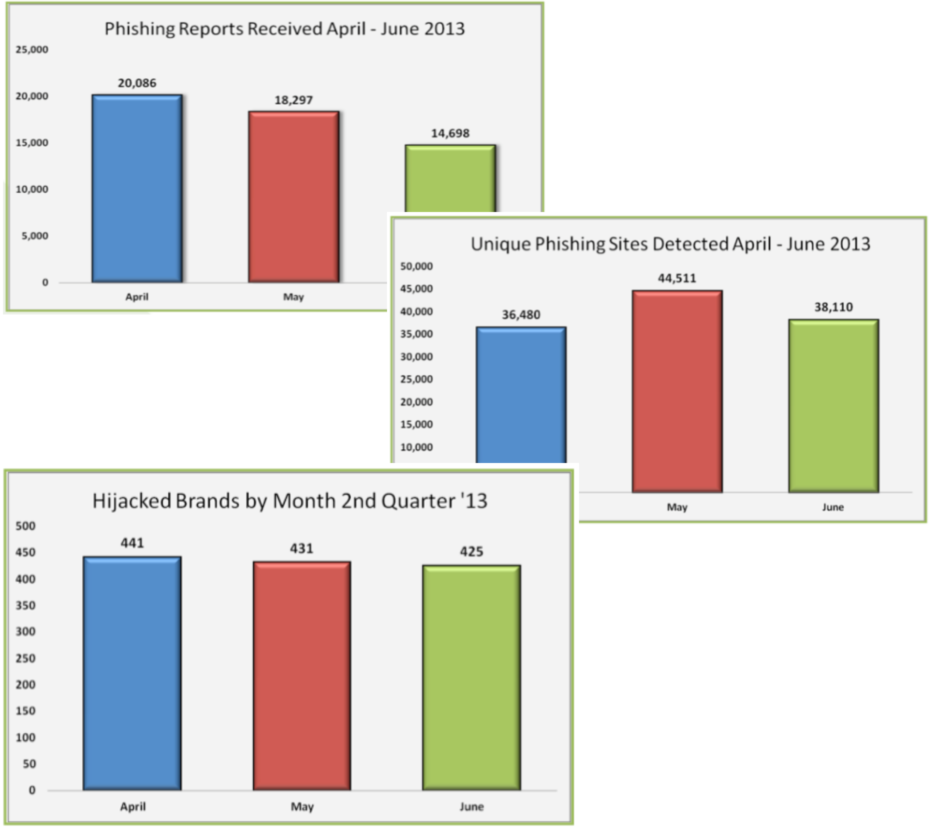
a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly”

Merriam-Webster Online Dictionary

A Short History of Phishing

- First use: 1996, alt.online-service.america-online
- 2001
  - Moved to wider Internet, targeting payment systems
  - Easy to spot messages, spelling errors…
- 2003
  - Legitimate site opens in the background, phisher runs a fake login window in front.
  - Gartner reports global cost of phishing in 2003 at 2.4 billion US$.
- 2004
  - Implemented data validation with real sites
  - Creating completely fake Websites of imaginary banks and financial firms.

Phishing Today

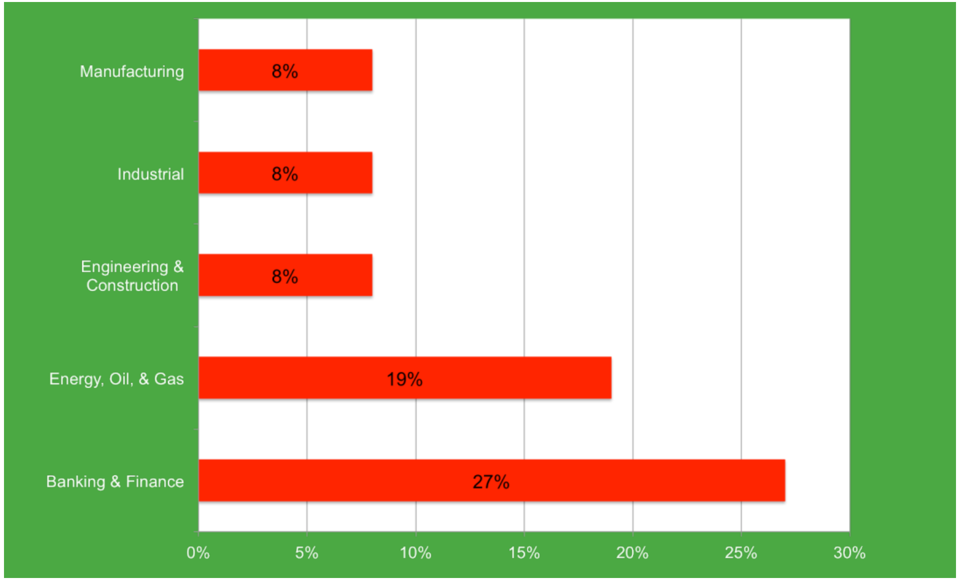


- Country hosting most target sites: USA
- Top 5 countries by attacked brands: USA, UK, India, Australia, France
- Most phishing attacks are launched on Fridays
- **Worldwide cost of Phishing in 2012: >1.5 billion US$**

Source: APWG Phishing Attack Trends Report 2Q2013, http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf

Source: RSA Online Fraud Report, http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012013.pdf

Who Is Attacked?



Source: Cisco TRAC Q1 2014 Quarterly Threat Briefing

- Energy sector targets in Q1:
  - An oil and gas exploration firm with operations in Africa, Morocco, and Brazil;
  - A company that owns multiple hydro electric plants throughout the Czech Republic and Bulgaria;
  - A natural gas power station in the UK;
  - A gas distributor located in France;
  - An industrial supplier to the energy, nuclear and aerospace industries;
  - Various investment and capital firms that specialize in the energy sector.

Hardening Your E-mail Infrastructure: SPF

Gregada

A quick fishermen’s hotpot

- 2 kg of fish (works best with angler fish, but even hake will do. Good with cod, too.)
- 1 kg of potatoes
- 1 onion
- 4-5 cloves of garlic
- 2 dl of white wine
- 2 dl of olive oil
- a splash of lemon juice
- fish stock
- a bunch of fresh parsley leaves
- a pinch of rosemary
- salt and pepper to taste

Cut fish into large pieces. Slice onions into rings, and potatoes into 1-2 cm thick slices. Dice parsley, garlic and rosemary.

In a large pot, fry onions on a little olive oil until glassy, add garlic and a little salt, and fry until onion is golden.

Add a layer of potatoes, then top with a layer of fish, and top the fish with more potatoes. Add the rest of the olive oil, white wine, and top off with fish stock just to barely cover the potatoes. Add a little bit of cold water. There should be no more than 1 cm of liquid over the potatoes.

Cook covered on **high** flame for 20 minutes. **DO NOT STIR!** Occasionally shake the pot instead. After 20 minutes, add lemon juice and parsley, and cook uncovered on low heat for a little while until the potatoes are soft.

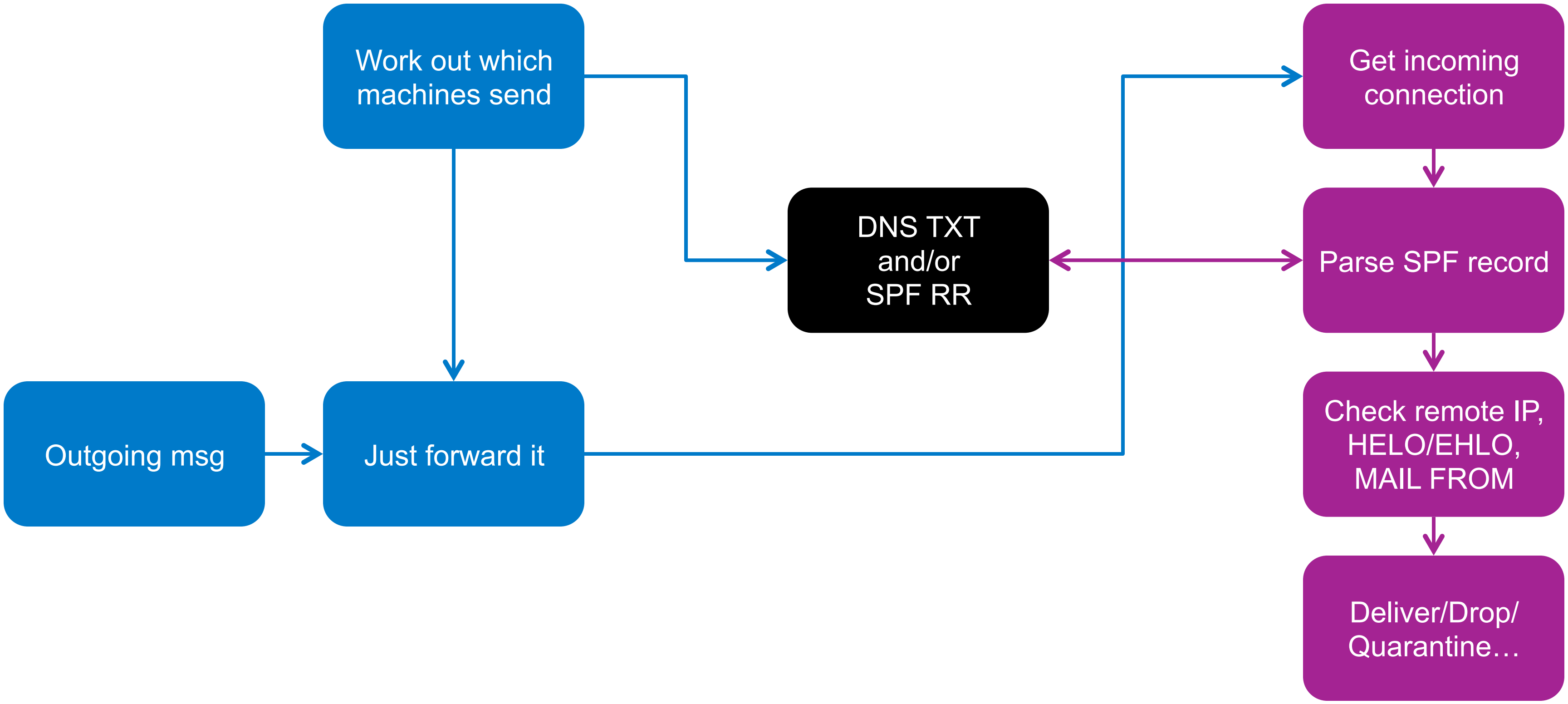
Before serving, let the pot rest for a while, so flavors even out. Sprinkle with olive oil in the plates.

Sender Policy Framework

A Short Introduction

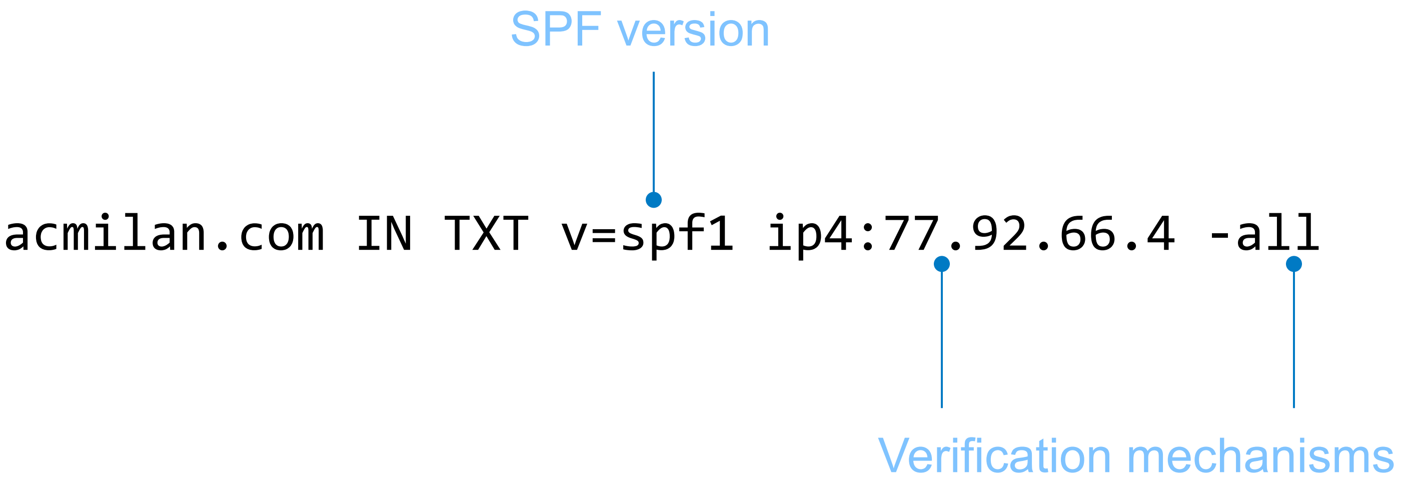
- Specified in RFC4408(bis)
- In a nutshell: Allows recipients to verify sender IP addresses by looking up DNS records listing authorized Mail Gateways for a particular domain
- Uses DNS TXT(16) or SPF (Type 99) Resource Records
  - SPF RR will be obsoleted due to low use
- Can verify HELO and MAIL FROM identity (FQDN)

SPF Operation



Work out which machines send
DNS TXT and/or SPF RR
Get incoming connection
Parse SPF record
Check remote IP, HELO/EHLO, MAIL FROM
Deliver/Drop/ Quarantine…
Outgoing msg
Just forward it

SPF Record Semantics



SPF version

```
acmilan.com IN TXT v=spf1 ip4:77.92.66.4 -all
```

Verification mechanisms

SPF Record Semantics

Mechanisms and Qualifiers

IP4

A

PTR

ALL

IP6

INCLUDE

EXISTS

MX

PASS (+)

NEUTRAL (?)

SOFTFAIL (~)

FAIL (-)

Cisco live!

SPF Record Examples

```
cisco.com IN TXT “v=spf1 ip4:173.37.147.224/27
ip4:173.37.142.64/26 ip4:173.38.212.128/27 ip4:173.38.203.0/24
ip4:64.100.0.0/14 ip4:72.163.7.160/27 ip4:72.163.197.0/24
ip4:144.254.0.0/16 ip4:66.187.208.0/20 ip4:173.37.86.0/24" "
ip4:64.104.206.0/24 ip4:64.104.15.96/27 ip4:64.102.19.192/26
ip4:144.254.15.96/27 ip4:173.36.137.128/26 ip4:173.36.130.0/24
mx:res.cisco.com ~all”
```

```
amazon.com IN TXT “v=spf1 include:spf1.amazon.com
include:spf2.amazon.com include:amazonses.com –all”
```

```
amazon.ses.com IN TXT “v=spf1 ip4:199.255.192.0/22
ip4:199.127.232.0/22 ip4:54.240.0.0/18 ~all”
```

```
openspf.org IN TXT “v=spf1 –all”
```

SPF Record Nesting

```
google.com IN TXT “v=spf1 include:_spf.google.com ip4:216.73.93.70/31
ip4:216.73.93.72/31 ~all”

_spf.google.com IN TXT “v=spf1 include:_netblocks.google.com
include:_netblocks2.google.com include:_netblocks3.google.com ~all”

_netblocks.google.com IN TXT “v=spf1 ip4:216.239.32.0/19 ip4:64.233.160.0/19
ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:209.85.128.0/17 ip4:66.102.0.0/20
ip4:74.125.0.0/16 ip4:64.18.0.0/20 ip4:207.126.144.0/20 ip4:173.194.0.0/16 ~all”

_netblocks2.google.com IN TXT “v=spf1 ip6:2001:4860:4000::/36
ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36
ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all”

_netblocks3.google.com IN TXT “v=spf1 ~all”
```

- Maximum of 10 mechanisms querying DNS (any other than IP4, IP6, ALL)!

What SPF Does NOT Address

- Primary purpose of SPF is to validate whether a message sender comes from a legitimate host
- Only checks Envelope From – headers can still be faked
  - Complementary technology, SenderID, checks purported sender (“Purported Responsible Address”) in the headers, but has many shortcomings
- Does not ensure message integrity
- Does not prevent intra-domain forgery

SPF Best Practices

- Plan to include “`-all`” in your SPF records
  - Consider all legitimate servers sending e-mail on your behalf
  - Make it part of security policy for roaming users to use authenticated SMTP on your gateways for sending outgoing mail
- Add your relay hosts’ HELO/EHLO identity to SPF records
- Create SPF records for all of your subdomains too
  - Publish null SPF records for domains/hosts that don’t send mail!

```
nomail.domain.com.      IN   TXT   "v=spf1 -all"
```

- Only include “`MX`” mechanism if your **incoming** mail servers also **send outgoing** mail
- (for now) Publish both TXT and SPF DNS Resource Records with your SPF record data.

Setting up SPF DNS Records and Configuring SPF Verification on Cisco ESA

Hardening Your E-mail Infrastructure: DKIM

(Musky) Octopus Salad

Musky Octopus is Octopus' smaller cousin, called "muzgavac" or "mrkač" in Croatian

- 2 kg of Musky Octopus (regular octopus will do too)
- 2 large-ish potatoes
- a bunch of fresh parsley
- 10 cloves of garlic
- 1 dl of olive oil
- juice of 1 lemon
- wine vinegar to taste
- salt and freshly ground pepper to taste

Deep freeze the (cleaned) octopus. This makes it softer and easier to cook. Dice potatoes in small cubes, and cook them.

Put octopus in cold water, and cook over low flame for 40-ish minutes from boiling. If there is skin on them, you will know it's done when the skin starts falling off. Drain them, let them cool down and peel the skin. Dice the octopus in 1 cm cubes. Finely chop garlic and parsley.

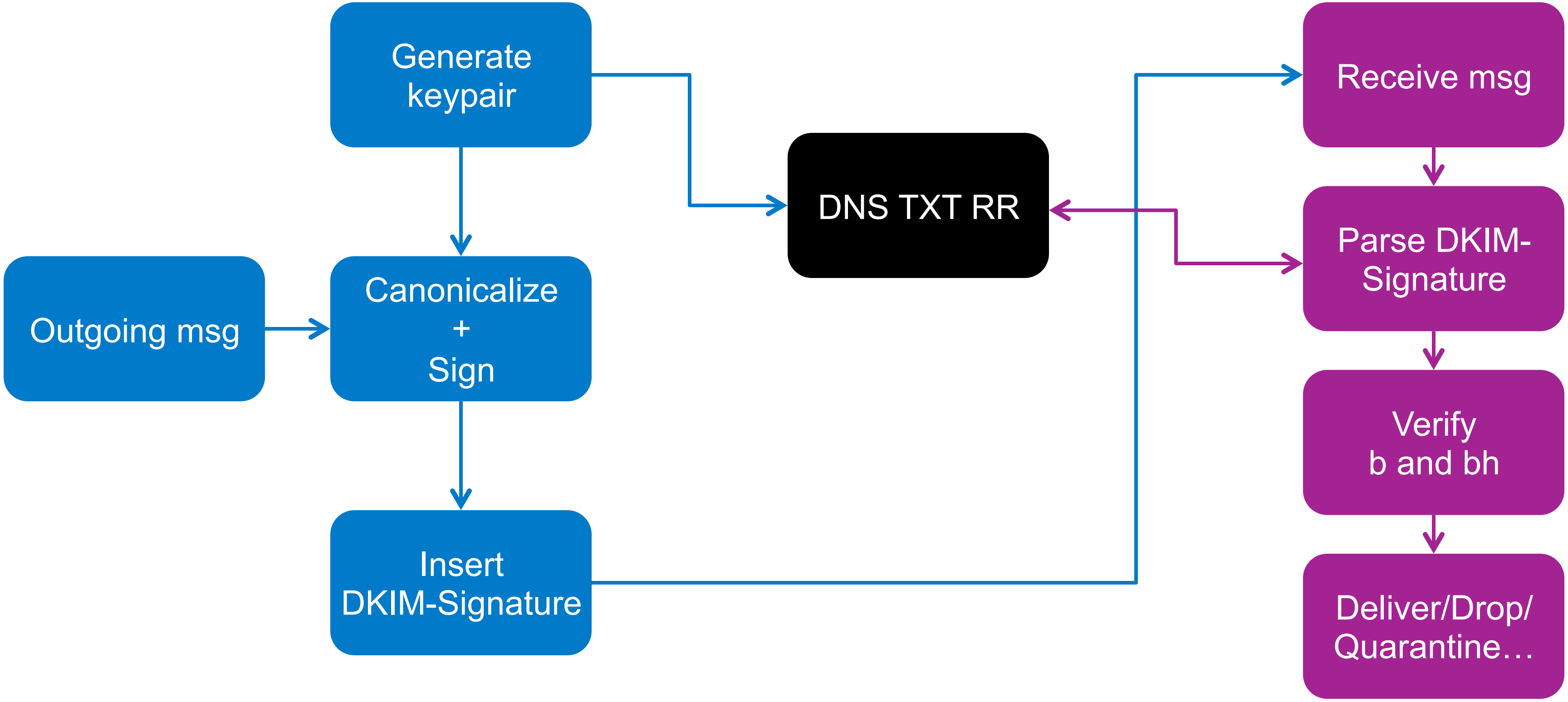
Add salt, pepper, lemon juice, 3 tbsp of wine vinegar, parsley, garlic and olive oil to diced octopus. Add potatoes. Mix well. Serve cold.

Domain Keys Identified Mail

A Short Introduction

- Specified in RFC5585
  - Additional RFCs: RFC6376 (DKIM Signatures), RFC5863 (DKIM Development, Deployment and Operation), RFC5617 (Author Domain Signing Practices (ADSP))
- In a nutshell: Specifies methods for gateway-based cryptographic signing of outgoing messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages
- Uses DNS TXT records to publish public keys

DKIM Operation



DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalization scheme

Selector

Signing Domain ID

Signed Headers

Header Hash

Body Hash

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+ADlVSR6I0zrYofA=;
        b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLh
        srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B
        JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh
        Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq
        ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ
        SyGhUFeuqwxJoCJcghGf7edZ0OIgZtEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Signature

Algorithms

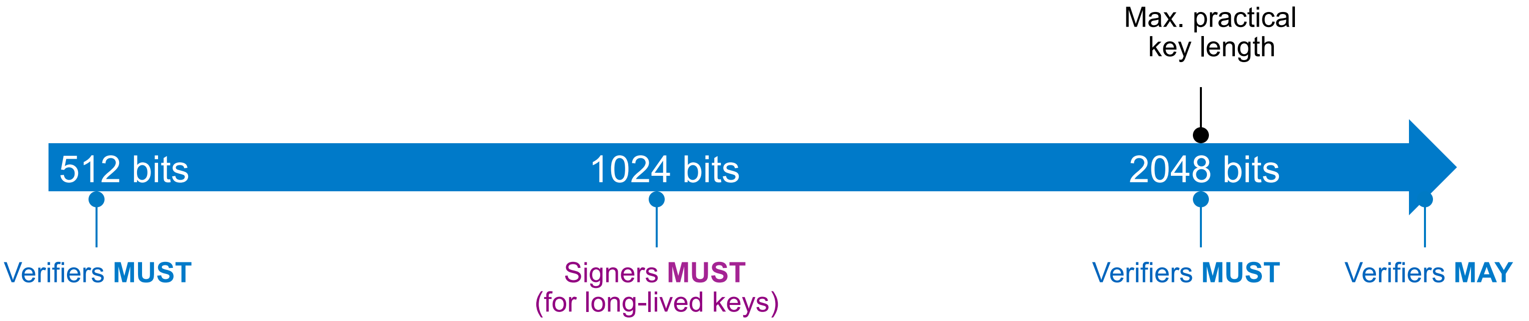
RSA-SHA1 or RSA-SHA256

Signers **MUST**

Verifiers **MUST**

Signers **SHOULD**

Verifiers **MUST**



Max. practical key length

DKIM Signature

Canonicalization

- Process of adapting the message content for signing to compensate for minor changes by MTAs in transit
- MUST NOT change the transmitted data in any way; just its presentation
- Two canonicalization schemes are supported for both headers and body:
  - Simple (almost no modification tolerated)
  - Relaxed (some modification, like header name case changes, line wrapping, whitespace replacement allowed)

DKIM Signature

Header Canonicalization

- Simple Header Canonicalization
  - No changes to headers
  - Retains order, case and whitespacing
- Relaxed Header Canonicalization
  - Header names -> lowercase
  - Unfolds all multiline headers
  - Replaces sequences of WSP characters with a single WSP
  - Deletes WSP characters at EOL
  - Deletes WSP before and after the colon separating the field name from the value

DKIM Signature

Header Canonicalization in Action

```
Return-Path: v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
X-Original-To: hdogan@dir.hr
Delivered-To: hdogan@dir.hr
Received: from mx1.hc4-93.c3s2.smtpi.com (esa1.hc4-93.c3s2.smtpi.com [68.232.136.98])
            by rotkvica.dir.hr (Postfix) with ESMTP id B08562ABC01E
            for <hdogan@dir.hr>; Thu, 26 Dec 2013 12:03:32 +0100 (CET) Received-SPF: Pass
(mx1.hc4-93.c3s2.smtpi.com: domain of
            v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
            designates 208.95.132.58 as permitted sender)
            identity=mailfrom; client-ip=208.95.132.58;
            receiver=mx1.hc4-93.c3s2.smtpi.com;
            envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
            x-sender=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
            x-conformance=sidf_compatible; x-record-type="v=spf1”
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
            postmaster@mail2112.eckler.mkt1970.com designates
            208.95.132.58 as permitted sender) identity=helo;
            client-ip=208.95.132.58; receiver=mx1.hc4-93.c3s2.smtpi.com;
            envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
            x-sender="postmaster@mail2112.eckler.mkt1970.com";
            x-conformance=sidf_compatible; x-record-type="v=spf1”
Authentication-Results: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (signature verified)
header.i=email@ecklers.messages1.com
X-IronPort-Anti-Spam-Filtered: true
```

DKIM Signature

Header Canonicalization in Action

```
return-path:v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
x-original-to:hdogan@dir.hr
delivered-to:hdogan@dir.hr
received:from mx1.hc4-93.c3s2.smtpi.com (esa1.hc4-93.c3s2.smtpi.com [68.232.136.98]) by rotkvica.dir.hr (Postfix)
with ESMTP id B08562ABC01E for <hdogan@dir.hr>; Thu, 26 Dec 2013 12:03:32 +0100 (CET)
received-spf:Pass (mx1.hc4-93.c3s2.smtpi.com: domain of v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
designates 208.95.132.58 as permitted sender) identity=mailfrom; client-ip=208.95.132.58;
receiver=mx1.hc4-93.c3s2.smtpi.com; envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-
sender=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-conformance=sidf_compatible; x-record-
type="v=spf1”
received-spf:Pass (mx1.hc4-93.c3s2.smtpi.com: domain of postmaster@mail2112.eckler.mkt1970.com designates
208.95.132.58 as permitted sender) identity=helo; client-ip=208.95.132.58; receiver=mx1.hc4-93.c3s2.smtpi.com;
envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-
sender=postmaster@mail2112.eckler.mkt1970.com; x-conformance=sidf_compatible; x-record-type="v=spf1”
authentication-results:mx1.hc4-93.c3s2.smtpi.com; dkim=pass (signature verified)
header.i=email@ecklers.messages1.com
x-ironport-anti-spam-filtered:true
```

DKIM Signature

Body Canonicalization

- Simple Body Canonicalization
  - No changes to the message, except:
    - removes any empty lines at the end of the message body
    - adds CRLF at the end of the message body, if not already there
- Relaxed Body Canonicalization
  - Simple Canonicalization, plus:
    - Ignores all WSP characters at EOL
    - Replaces sequences of WSP characters in a line into a single WSP

DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalization scheme

Signing Domain ID

Selector

Signed Headers

Header Hash

Body Hash

```
      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
          d=gmail.com; s=20120113;
          h=mime-version:date:message-id:subject:from:to:content-type;
          bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+ADlVSR6I0zrYofA=;
          b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLh
          srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B
          JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh
          Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq
          ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ
          SyGhUFeuqwxJoCJcghGf7edZ0OIgZtEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Signature

Signing Domain ID and Selector

- Signing Domain ID (SDID)
  - Identifies the entity claiming responsibility for the signed message
  - Must correspond to a valid DNS name under which a DKIM key is published
- Selector
  - Enables publishing of multiple keys per signing domain
  - Use cases:
    - Periodic key rotations
    - Delegating/splitting signing authority for different OUs
    - Delegating signing authority to 3rd parties
    - Allowing roaming users to sign their own messages

DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalization scheme

Selector

Signing Domain ID

Signed Headers

Header Hash

Body Hash

```
        DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
                d=gmail.com; s=20120113;
                h=mime-version:date:message-id:subject:from:to:content-type;
                bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+ADlVSR6I0zrYofA=;
                b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLh
                srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B
                JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh
                Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq
                ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ
                SyGhUFeuqwxJoCJcghGf7edZ0OIgZtEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Public Key Retrieval

- DNS query:

<selector>._domainkey.<SDID>

- For our example:

```
20120113._domainkey.gmail.com IN TXT “k=rsa\;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabg
bFwh+eBCsSTrqmwIYYvywlbhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyo
xcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD0" "7y2+07wlNWwIt
8svnxgdxGkVbbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIh
kx4xYSIc9oSwVmAl5OctMEeWUwg8Istjqz8BZeTWbf41fbNhte7Y+YqZOwq1S
d0DbvYAD9NOZK9vlfuac0598HY+vtSBczUiKERHv1yRbcaQtZFh5wtiRrN04B
LUTD21MycBX5jYchHjPY/wIDAQAB”
```

DKIM Signature

Anatomy of the DKIM-Signature Header

Mandatory tags

V	A	D	S	H	B	BH

Optional tags

C	I	L	Z

Recommended tags

T	X

DKIM Signature Tags

Expanded View

- Required signature tags:
  - v, a, d, s, h, b, bh
- Optional signature tags:
  - c – defaults to simple/simple
  - i – Agent or User ID – usually corresponds to sender's e-mail address
  - l – Body length
  - z – Copied header fields, separated by "|" – used for diagnostics
- Recommended signature tags:
  - t – Signature timestamp in Unix Epoch time, GMT
  - x – Signature expiration in Unix Epoch time, GMT. Must be greater than "t" time

DKIM Public Key

Anatomy of the DKIM DNS Record

Mandatory tags

P

Optional tags

H=SHA1 | K=RSA | S=EMAIL | T=Y | T=S | G | N

Recommended tags

V=DKIM1

DKIM Public Key

Expanded Tags

- Only “p” tag is required
- Optional tags:
  - h – acceptable hash algorithms
  - k – key type
  - n – notes (for human interpretation)
  - s – service type
  - g – key granularity; local part of the “i” tag of the signature must be equal to it
  - t – flags
    - y – This domain is testing DKIM
    - s – if “i” tag is used in signature, domain part of the “i” tag must be equal to “d” tag. Recommended to be present if no subdomains are used.
- Recommended tags:
  - v – Version of the DKIM key record. If present, must be “DKIM1”.

DKIM Public Key Examples

```
iport._domainkey.cisco.com IN TXT “v=DKIM1\; s=email\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCctxGhJnvNpdcQLJM6a/
0otvdpzFIJuo73OYFuw6/8bXcf8/p5JG/iME1r9fUlrNZs3kMn9ZdPYvTyRbyZ0
UyMrsM3ZN2JAIop3M7sitqHgp8pbORFgQyZxq+L23I2cELq+qwtbanjWJzEPpV
vrvbuz9QL8CUtS+V5N5ldq8L/lwIDAQAB\;”
```

```
lufthansa3._domainkey.lufthansa.com IN TXT “g=*\; k=rsa\; t=y\;
n="Contact postmaster@responsys.com with any questions concerning
this signing"\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA7e
WF9kW/HY6ppS6g3U6Be0JRfu59Iv3oYgW+ztDJK1HsLf/hmah4buPBtVaGb
CagDNN7wK12uhs6ko6f4SulZpwqVdtp1R6jujvW56hcNhx4RJ0E17mefniciwYfQx
DhQmE8lkUzJR4BXWuKsPSSSy/pT3rM+LusuTAbFWKsMQIDAQAB\;”
```

Choosing Your DKIM Parameters

- Make the best use of selectors
  - Periodic key rotation
  - Delegation of signing authority
- Sacrificing security for performance
  - If you must, consider “weakening” your signatures in the following order:
    - Reduce the signing key size (and combine with selector rotation)
    - Use “simple” for body canonicalization
    - Use “simple” for headers canonicalization
    - Change signing algorithm to sha-1

      However, RFC6376 says: “`Signers MUST implement and SHOULD sign using rsa-sha256`”

Configuring DKIM Signing and Verification Using Cisco ESA

DKIM Advertisement Problem and ADSP

- The biggest problem of DKIM is that there is no straightforward advertising
  - Unsigned messages can come in unverified
- ADSP (Author Domain Signing Practices, RFC5617) is an extension to DKIM
  - A DNS-based method for sender domains to advertise that they are signing messages
  - A simple TXT record at _adsp._domainkey.<domain>, containing just:

    `dkim=unknown|all|discardable`
- ADSP is obsoleted as of November 2013 due to lack of deployment

```
_adsp._domainkey.yahoo.com IN TXT “dkim=unknown”
```

Hardening Your E-mail Infrastructure: DMARC

Sardines on a spit

Traditional dish of fishermen from the island of Vis

- 1 kg of fresh sardines
- coarse-grain sea salt
- a branch of fresh rosemary
- olive oil

This extremely simple dish is a secret specialty of fishermen from Croatia’s most remote island, Vis. Do google it.

The recipe includes a bit of DIY: You need to make (well, or buy) a thin spit out of non-tanin-releasing wood. Bay leaf branches work best. The spit should be up to 1 cm wide, as thin as possible, and sharp at one end.

Dip the branch of rosemary in little olive oil.

Wipe the sardines with a rough cloth to remove the scales, and let them covered in sea salt for about half an hour, to make the fish firmer.

Slide the fish on the spit so the spit is always **under** the spine. Place the spit over burning coal, with spine facing **up**. This is critical, because if you miss sides, fish will fall off as you turn it. Grill it for a few minutes, then turn **once**, grill for another few minutes, and set aside in a pot, cover, and let them sit for a few more minutes. Never turn the fish more than once.

Sprinkle with rosemary-infused olive oil, and serve with potato salad, or freshly baked bread. This is probably the crudest, and best way to cook sardines. Enjoy!

> "DMARC is designed to prevent bad actors from sending mail which claims to come from legitimate senders, particularly senders of transactional email. One of the primary uses of this kind of spoofed mail is phishing"

draft-kucherawy-dmarc-base-02

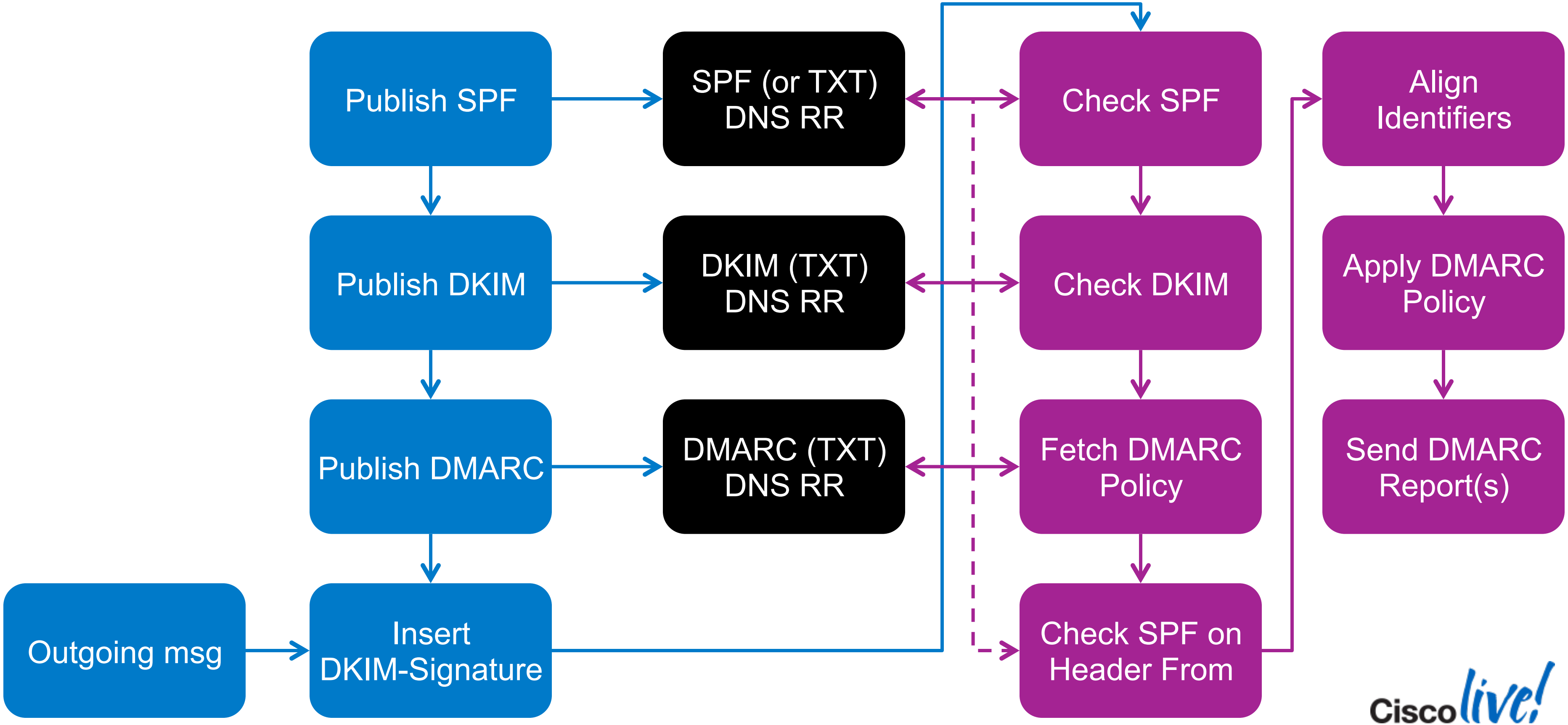
IETF Network Working Group

Moving Towards DMARC

- Both DKIM and SPF have shortcomings, not because of bad design, but because of different nature of each technology
- DKIM policy advertising was addressed by ADSP, but:
  - There was no visibility by spoofed parties into offending traffic
  - Even though a receiver implemented both SPF and DKIM verification, there was no requirement of the two technologies being in sync
    - A smart attacker might make use of this to push illegitimate messages through
- SPF checks HELO/MAILFROM identity, but no verification or alignment of Header From is ensured

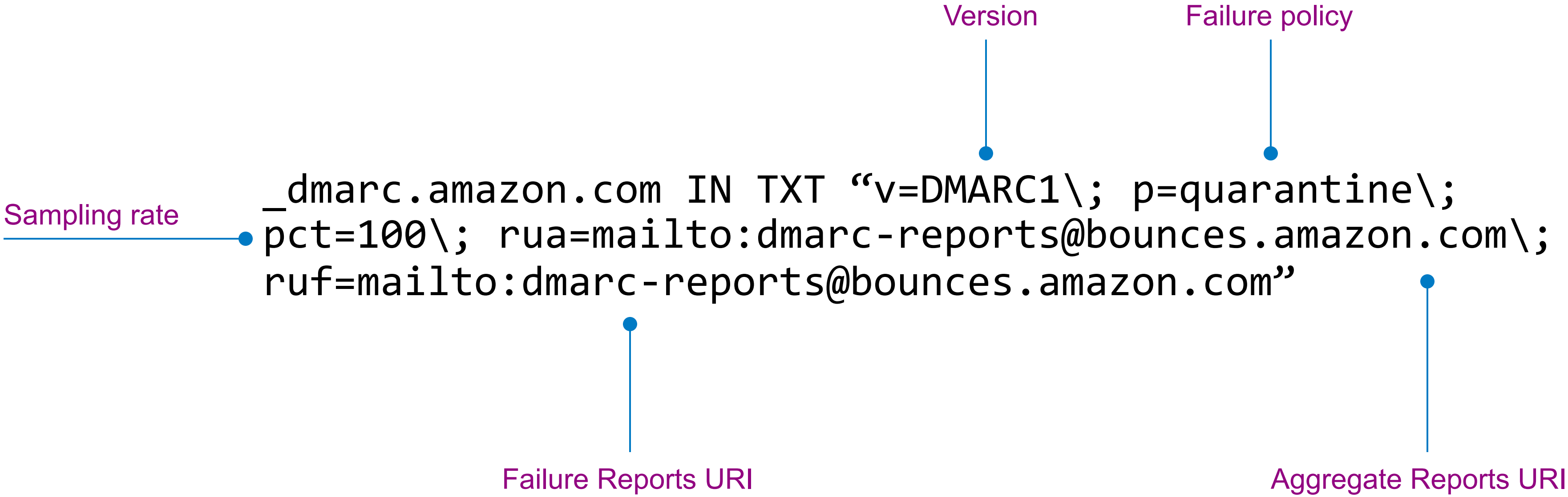
- Thus, DMARC was born:
  - Leveraging great existing technologies, providing a glue to keep them in sync, and allowing **senders** to mandate rejection policies and have visibility of offending traffic

DMARC Operation



DMARC Policy

Example of a DMARC DNS Record



```
_dmarc.amazon.com IN TXT “v=DMARC1\; p=quarantine\;
pct=100\; rua=mailto:dmarc-reports@bounces.amazon.com\;
ruf=mailto:dmarc-reports@bounces.amazon.com”
```

DMARC Policy

Policy Specification and “Slow Start”

- Policies requested by senders:
  - None
  - Quarantine
  - Reject
- Receivers MAY deviate from requested policies, but SHOULD inform the sender why (through Aggregate Report)
- Sampling rate (“p” tag) instructs the receiver to only apply policy to a fraction of messages

DMARC Policy

Reporting URIs

- mailto: and http:// URIs supported
- Two distinct report types:
  - Aggregate report
    - Sent on an interval
    - Summary of all incidents from a particular sender domain
  - Failure report
    - Sent on (every) failure
    - Detailed report on individual failures

DMARC Policy

Anatomy of the DMARC DNS Record

Mandatory tags

V=DMARC1	P

Optional tags

PCT	SP	ADKIM	ASPF	RI	RUA	RF	FO	RUF

DMARC Policy

Adherence to SPF/DKIM

- Sender can request Strict (“s”) or Relaxed (“r”, default) adherence to DKIM and SPF
- DKIM (“adkim”):
  - Relaxed: Header From FQDN can be a subdomain of “d” tag of DKIM signature
  - Strict: Header From FQDN must completely match the “d” tag of DKIM
- SPF (“aspf”):
  - Relaxed: Header From domain can be a subdomain of SPF-Authenticated (MAIL FROM) domain
  - Strict: Header From domain must match MAIL FROM domain

DMARC Policy

Failure Reporting

- Two supported Report Formats (“`rf`”):
  - `afrf`
    - Authentication Failure Reporting Format, defined in RFC6591, and extended by draft-kucherawy-dmarc-base (default)
  - `iodef`
    - Incident Object Description Exchange Format, defined in RFC5070
- Failure reporting options (“`fo`”), separated by colons in the Policy Record:
  - `0` : generate a report if **all** underlying mechanisms fail to align and pass (default)
  - `1` : generate a report if **any** underlying mechanisms fail to align and pass
  - `d` : generate a DKIM failure report if DKIM verification fails, regardless of alignment
  - `s` : generate an SPF failure report for failed SPF verification, regardless of alignment

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;
ruf=mailto:d@ruf.agari.com\;”
```

DMARC Reporting

Delegating Reporting Authority

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

ruf.agari.com

DMARC Reporting

Delegating Reporting Authority

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

facebook.com

ruf.agari.com

DMARC Reporting

Delegating Reporting Authority

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

```
facebook.com._report._dmarc.ruf.agari.com
```

DMARC Reporting

Delegating Reporting Authority

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

```
facebook.com._report._dmarc.ruf.agari.com IN TXT “v=DMARC1”
```

DMARC Record Examples

```
_dmarc.google.com IN TXT “v=DMARC1\; p=quarantine\;
rua=mailto:mailauth-reports@google.com”

_dmarc.cs.helsinki.fi IN TXT “v=DMARC1\; p=reject\; sp=reject\;
pct=100\; aspf=r\; rua=mailto:dmarc-reports@cs.helsinki.fi”

_dmarc.microsoft.com IN TXT “v=DMARC1\; p=none\; pct=100\;
rua=mailto:d@rua.agari.com\; ruf=mailto:d@ruf.agari.com\; fo=1”

_dmarc.dk-hostmaster.dk IN TXT “v=DMARC1\; p=none\;
rua=mailto:dmarc-report@dk-hostmaster.dk\; ruf=mailto:dmarc-
report@dk-hostmaster.dk\; adkim=r\; aspf=r\; rf=afrf”
```

DMARC Identifier Alignment

When Does A Message Pass?

- DMARC authenticates the domain from Header From
- DKIM authenticates the domain from DKIM-Signature (“d” tag)
- SPF authenticates domains from MAIL FROM or HELO identities
- **Identifier Alignment** is a concept of alignment between Header From and identifiers checked by DKIM and SPF
- Message **passes** DMARC check if **one or more** of the authentication mechanisms (DKIM **and/or** SPF) pass **with proper alignment**

DMARC Policy

Anatomy of the DMARC DNS Record

Mandatory tags

V=DMARC1	P

Optional tags

PCT	SP	ADKIM	ASPF	RI	RUA	RF	FO	RUF

DMARC Policy

Adherence to SPF/DKIM

- Sender can request Strict (“s”) or Relaxed (“r”, default) adherence to DKIM and SPF
- DKIM (“adkim”):
  - Relaxed: Header From FQDN can be a subdomain of “d” tag of DKIM signature
  - Strict: Header From FQDN must completely match the “d” tag of DKIM
- SPF (“aspf”):
  - Relaxed: Header From domain can be a subdomain of SPF-Authenticated (MAIL FROM) domain
  - Strict: Header From domain must match MAIL FROM domain

DMARC Identifier Alignment: SPF

```
MAIL FROM: <hrdogan@cisco.com>
```

```
From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

DMARC Identifier Alignment: SPF

```
MAIL FROM: <hrdogan@cisco.com>
```

```
From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

DMARC Identifier Alignment: SPF

```
MAIL FROM: <hrdogan@cisco.com>

From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

aspf="r"	aspf="s"
✓	✓

DMARC Identifier Alignment: SPF

	aspf="r"	aspf="s"
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>	✓	✓

```
MAIL FROM: <hrdogan@cisco.com>

From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

```
MAIL FROM: <hrdogan@cisco.com>

From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

DMARC Identifier Alignment: SPF

	aspf=“r”	aspf=“s”
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗

DMARC Identifier Alignment: SPF

	aspf="r"	aspf="s"
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗
MAIL FROM: <hdogan@linux.hr> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test		

DMARC Identifier Alignment: SPF

	aspf="r"	aspf="s"
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
MAIL FROM: <hrdogan@cisco.com> From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗
MAIL FROM: <hdogan@linux.hr> From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✗	✗

DMARC Identifier Alignment: DKIM

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

DMARC Identifier Alignment: DKIM

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

adkim=“r”	adkim=“s”
✓	✓

DMARC Identifier Alignment: DKIM

adkim=“r”	adkim=“s”
✓	✓

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com>
To: Hrvoje Dogan <hdogan@dir.hr>
Subject: DMARC test
```

DMARC Identifier Alignment: DKIM

	adkim=“r”	adkim=“s”
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗

DMARC Identifier Alignment: DKIM

	adkim=“r”	adkim=“s”
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗
DKIM-Signature: v=1; […] d=linux.hr;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test		

DMARC Identifier Alignment: DKIM

	adkim="r"	adkim="s"
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✓
DKIM-Signature: v=1; […] d=cisco.com;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@mail.cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✓	✗
DKIM-Signature: v=1; […] d=linux.hr;[…] From: Hrvoje Dogan (hrdogan) <hrdogan@cisco.com> To: Hrvoje Dogan <hdogan@dir.hr> Subject: DMARC test	✗	✗

Multiple DKIM signatures? **Any** must validate and align.

DMARC

How to start

1. Correctly deploy DKIM and SPF
2. Make sure that your identifiers will align
3. Publish a DMARC record with "`p=none`", gather `rua` and `ruf` reports for a while
4. Analyze the data and modify your mail streams (or DKIM/SPF parameters)
5. Apply "`reject`" or "`quarantine`" policy

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
  Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
  bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
  as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
  envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-conformance=sidf_compatible; x-record-type="v=spf1”
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
  h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
  i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
  +c8vp3q89JcMLPtRfO1OtRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
  Q/gNPFkJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
  Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
  bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
  as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
  envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-conformance=sidf_compatible; x-record-type="v=spf1”
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
  h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
  i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
  +c8vp3q89JcMLPtRfO1OtRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
  Q/gNPFkJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
  Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
  bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
  as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
  envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-conformance=sidf_compatible; x-record-type="v=spf1”
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
  h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
  i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
  +c8vp3q89JcMLPtRfO1OtRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
  Q/gNPFkJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
  Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
  bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
  as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
  envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
  x-conformance=sidf_compatible; x-record-type="v=spf1”
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
  h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
  i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
  +c8vp3q89JcMLPtRfO1OtRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
  Q/gNPFkJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC deployment using Cisco ESA

Don’t Be A Phish

Deploy DMARC!

- DMARC provides
  - Easy, simple and powerful existing-standards-based message authentication
  - Flexibility and gradual deployment
  - A chance to clean up your mail flows and tighten up messaging security
  - Easy protection from most phishing attacks – both as phish and as bait!
  - … and endless opportunities for corny fish jokes.

DON’T BE A PHISH.
IT’S SIMPLE.

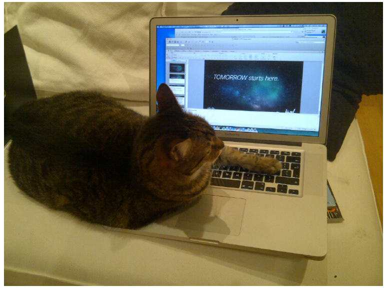
For More Information

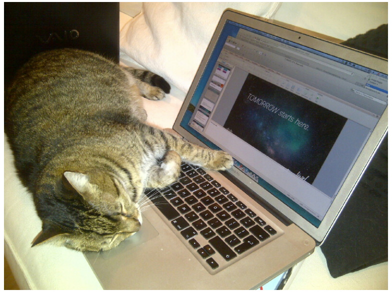
- http://www.openspf.org
- http://www.dkim.org
- http://blogs.cisco.com/security/big-data-in-security-part-v-anti-phishing-in-the-cloud/
- https://support.google.com/mail/answer/3070163?hl=en
- http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02
- http://dmarc.org
- http://dmarcian.com

- Presentation videos: http://bitly.com/bundles/hrvojedogan/1

Image credits

- Most photography on title slides courtesy of Novi List, http://www.novilist.hr, used with permission of the Editor of Photography. Authors of photography: Sergej Drechsler, Petar Fabijan, Marko Gracin, Roni Brmalj, Damir Škomrlj, Silvano Ježina, Livio Černjul
- Original artwork for icons and progress indicator done in ink on paper by Ivica Matić, http://www.medri.uniri.hr/~imatic/
- Special credits go to Helenka, for her relentless work on producing these slides





Call to Action…

Visit the World of Solutions:-

- **Cisco Campus**
  Cisco E-mail Security
- **Walk-in Labs**
- **Technical Solutions Clinics**
  Hrvoje Dogan, Dan Griffin, Tom Foucha, Scott Bower
- **Meet the Engineer**

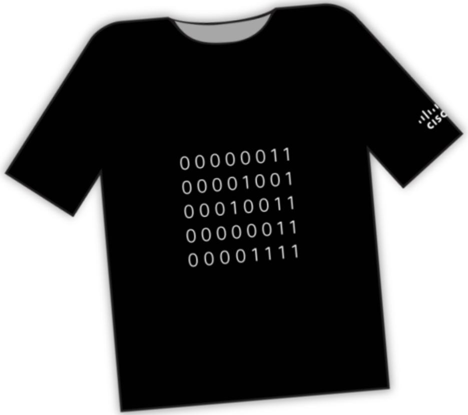
- **Lunch Time Table Topics**, held in the main Catering Hall

- **Recommended Reading**: For reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2014

Cisco live!

Complete Your Online Session Evaluation

- Complete your online session evaluation
- Complete four session evaluations and the overall conference evaluation to receive your Cisco Live T-shirt



cisco TM