

Individual
Internet-Draft
Intended status: Informational
Expires: December 6, 2013

D. Otis
D. Rand
Trend Micro
June 04, 2013

DKIM is Harmful as Specified
draft-otis-dkim-harmful-02

Abstract

Currently, email lacks conventions ensuring SMTP clients can be identified by an authenticated domain. Unfortunately many hope to use DKIM as an alternative, but it is independent of intended recipients and domains accountable for sending the message. This means DKIM is poorly suited for establishing abuse assessments for unsolicited messaging of commercial email otherwise known as SPAM, nor was this initially DKIM's intent. DKIM lacks message context essential to ensure fair assessment and to ensure this assessment is not poisoned (Who initiated the transaction and to whom).

DKIM was instead intended to establish increased levels of trust based upon valid DKIM signatures controlling acceptance and what a user sees within the FROM header field. But DKIM failed to guard against pre-pended header fields where any acceptance based on valid DKIM signatures is sure to exclude header field spoofing, especially that of the FROM. This weakness allows malefactors to exploit DKIM signature acceptance established by high-volume DKIM domains to spoof ANY other domain, even when prohibited within the Signer's network.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 6, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | | |
|-----------------------------|---|--------------------|
| 1. | Introduction | 4 |
| 2. | Exploiting Trust | 5 |
| 3. | Maintaining Trust | 6 |
| 4. | Responding to Defects and Exploitation | 6 |
| 5. | Conflating DKIM Fragments with Email Messages | 7 |
| 6. | SMTP Can't | 8 |
| 7. | DKIM Vulnerability | 9 |
| 8. | Barriers to an Authenticated Domain | 10 |
| 9. | Domains as a Basis for Managing Traffic | 10 |
| 10. | XMPP Shows the Way Forward | 11 |
| 11. | IANA Considerations | 11 |
| 12. | Security Considerations | 11 |
| 13. | Acknowledgements | 12 |
| 14. | References - Informative | 12 |
| Appendix A. | DKIM Examples | 14 |
| Appendix B. | Stats | 17 |
| | Authors' Addresses | 17 |

1. Introduction

Currently, IPv4 address reputation provides the primary basis for defending open SMTP services (acceptance without prior arrangement). Use of IP addresses in this role completely breaks down when dealing with IPv6 [[RFC2460](#)] due to data requirements and an inability to defend detection of subscription violations. There are currently 18,209,237,415,985,168 /64 equivalent IPv6 prefixes routed. [[v6-BGP-Rpts](#)]. In comparison, for IPv4 there are 2,614,654,096 IP addresses routed. While IPv4 is reaching its maximum, IPv6 has about 0.1% of the available /64 prefix routed and this continues to grow rapidly. Unlike IPv4, there is no practical means to scan reverse DNS namespace within IPv6 since each /64 prefix may contain any number of PTR records ranging up to 184,000,000,000,000,000,000.

A technique commonly employed to automate IPv4 address categorization of suitable hosts is to check whether reverse PTR records appear to represent valid hostnames. Those that represent 4 decimal numbers are often considered unacceptable, for example. Our processing of reverse DNS namespace in cooperation with network providers now excludes about 38%, or about 1,000,000,000 IPv4 addresses. Comparing IPv6 /64 prefixes with the remainder of routable IPv4 addresses shows there are 11.3 million times more IPv6 /64 prefixes needing categorization. In addition, there is no practical means to facilitate this effort.

IP address reputation requires logging associated connections to permit review. Whether describing reputations as only positive or only negative, errant exclusion or inclusion of either poses similar risk. Tracking currently routed IPv6 /64 prefixes using a single bit requires 6 million billion bytes or 5,650 Terra-bytes just to track simple use. Even feedback by IPv6 address prefix will expose mailboxes that detect subscription policy violations.

Some also suggest there will not be a significant increase in the number of servers running over IPv6 and since their overall number should be comparable, email should still be dealing with a similar number of IP addresses. Unlike IPv4, IPv6 does not constrain the number of IP addresses assigned to a network interface. This feature allows each connection from a server to originate from a different IP address, perhaps one for each user. The potential increase allowed by IPv6 may prove explosive, even those only from good actors.

Organizations such as M3AAWG hope to use DKIM as a required acceptance requirement to better ensure a domain identity offers a basis for acceptance to replace that of the IP address used by SMTP clients. Due to the understandable IPv6 reputation services' inability to scale, domain based alternatives are being sought. Some

at least understand DKIM is unable to support negative reputation schemes. Reliance on a mechanism unable to sustain close scrutiny of negative assertions makes sustained differentiation of positive and negative views less tenable.

At this April's Rocky Mountain IPv6 Task Force summit in Denver, the second day government track sessions raised concerns about there being no means available to defend SMTP over IPv6. There are proposals within the IETF aimed at establishing DKIM as a basis for reputation schemes in the Repute WG (i.e. section 3.2 of [\[I-D.ietf-repute-email-identifiers\]](#) which introduces DKIM domains being used along with SMTP client IP addresses and [rfc5321.helo](#) also identifying the SMTP client. Identifying the SMTP client encompasses both "Who Initiated" and "To Whom" message elements to support fair negative assertions. However, DKIM does not encompass this essential information. In addition, DKIM's inability to detect invalid prefixed header fields also means any positive DKIM reputation assertion can prove highly harmful by increasing trust in possible deceptions.

2. Exploiting Trust

Trust established by a signing domain is being exploited to mislead recipients about who authored a message. DKIM's trust related function may be generalized as better ensuring delivery to in-boxes as opposed to junk folders or silent discard. It is also apparent receivers expect signature validation ensures invalid header fields have not been pre-fixed. While it is possible for signing domains to support this expectation by including non-existent header fields in a list of those added to the signature's hash, few implement this feature.

Perhaps signers consider such double listing wasteful of storage resources or they assume the validation process makes these checks without the non-intuitive double listing of header fields not permitted to repeat anyway. When a domain is very large, errant filtering is likely to entail costly customer support which affords them greater latitude and who are also likely sensitive to wasting their storage resources.

Regardless of possible underlying motivations, it is clear checks for valid message structure remains a general expectation of DKIM's validation process that simply does not occur. Not every domain is seeking to establish the same level of trust, where those not checking for pre-fixed header fields having greater latitude place all other domains at risk. Checking message structure is explicitly not to be handled by the transport. Modification to SMTP

implementations such as Sendmail, Exim, or Postfix and the like are neither appropriate, nor likely beneficial within a relevant time frame.

Larger domains often obtain their size by offering relatively easy access. These domains afford malefactors a simple method to have their deceptive messages reach their victim's in-box. DKIM's validation process not explicitly ensuring against invalid repeated header fields together with of limited hash inclusion permitting abuse of other domains makes DKIM harmful. DKIM validation MUST be modified to ensure against invalid repeated header fields so that trust established by a signing domain is not exploited to mislead recipients about who authored a message.

3. Maintaining Trust

Not every subsystem or protocol layer should be expected to repeat previous security checks to establish proper layering, however critical checks important for enforcing new relationships within a message should not be assumed, especially those involving a trivial effort. With high levels of abuse resulting from email's open nature, delegating checks in a structured manner better conserves essential resources. However, email's highly distributed store and forward protocol could not function if rigid message structures were enforced by the transport. Such enforcement does not scale, and may impede necessary change. New authentication or presentation requirements may involve small structural adjustments. For example, internationalization introduced a format negotiation not assured to survive beyond the next hop.

4. Responding to Defects and Exploitation

As with aviation, the success of email has risen to great heights. As within the world of aviation, faults threatening security, that when discovered, demand our attention and diligence to effect repair. Email has become an integral component in general commerce and the maintenance of security such as reporting system failures, break-in attempts, and facilitating account access recovery.

Reporting or predicting failure should not be viewed as exhibiting a lack of respect for achieved accomplishments. Noting and repairing faults only signify the importance of email's prominent role. As with most security related protocols, responding to noted defects is fairly common. Not responding to discovered defects in a security related protocol would be shocking. Simply publishing this draft appears to have already increase the level of multiple FROM header

field abuse seen where it is now at 21% of signed DKIM messages.

5. Conflating DKIM Fragments with Email Messages

DKIM signs only fragments of an email message, so it is more proper to refer to "DKIM Signed Fragments", and not "DKIM Signed Messages". Normal DKIM signature validation offers a simple PASS/FAIL associating it with a specific domain. When a recipient receives a PASS status, only the last FROM header field message fragment is ensured to have been included in the DKIM signature process. Other message fragments, including the message body, are optional and may not have been included. The FROM header field is normally visible UNLESS there are multiple FROM header fields. In which case, the signed FROM header field fragment is likely invisible, as is the DKIM signature fragments that hide which other message fragments had been encompassed by the DKIM signature process.

DKIM's trust related role is to better ensure message delivery to a user's in-box. Unless DKIM ensures this trust is not used to perpetrate deception, no positive assertions regarding a DKIM domain is safe. As a result, DKIM can not be used with either positive or negative reputation assertions in its current form.

The FROM header field is the Author identifier in section 11.1 of [[I-D.kucherawy-dmarc-base](#)]. The DMARC specification offers normative language that a message SHOULD be rejected when multiple FROM header fields are detected. This requirement would not be necessary or impose protocol layer violations if DKIM did not offer valid signature results when repeated header fields violate [[RFC5322](#)]. [[RFC5322](#)] declaring a message structure invalid does not preclude the occurrence of invalid messages, and [[RFC5321](#)] clearly states it will not enforce [[RFC5322](#)] message structure due to practical constraints. Instead of relying on optional policies such as DMARC that make partial guesses that ignore DATE or SUBJECT spoofing for example, critical violations of the message structure that pertain to enhancing trust can be enforced by DKIM simply defining the associated signatures invalid. Unlike DMARC, proper signature definition does not cross protocol layers, especially since no other layer enforces [[RFC5322](#)].

Since multiple DKIM signatures can occur, simple annotation of which fragments and domains associate with a valid signature is precluded. The ONLY message fragment ensured by a DKIM signature is the FROM header field. Just as DMARC concluded only the FROM header field is closely observed by recipients, DKIM initially reached this conclusion as well. While no absolute assurance of header field validity is asserted, the domain together with it's reputation

permits recipients to increase their trust in what is observed in the FROM header field. This trust further increases when the DKIM domain is authoritative for the FROM header field domain.

When acceptance is predicated on the DKIM signature, as occurs with DMARC, preserving trust associated with the FROM header field in conjunction with the DKIM domain is destroyed whenever multiple FROM header fields are permitted by not invalidating these DKIM signatures. DMARC over reaches when rejecting email based upon message format as with [\[RFC6854\]](#) group syntax in the FROM header field. DMARC should not be required to second guess whether a DKIM signature is valid.

6. SMTP Can't

SMTP [\[RFC5321\]](#) recommends against rejecting messages based upon perceived defects in the message structure. This liberal acceptance permits evolutionary change in message specifications starting at [\[RFC0822\]](#) that was based on [\[RFC0733\]](#) replaced by [\[RFC2822\]](#) and again by [\[RFC5322\]](#), [\[RFC6152\]](#), [\[RFC6532\]](#), and [\[RFC6854\]](#); the second to last paragraph in [section 3 of \[RFC5321\]](#) provides a definitive statement messages should not be rejected due to perceived defects in the [\[RFC0822\]](#) message structure. The initial reference to [\[RFC0822\]](#) in this paragraph offers two foot notes with the second referencing the latest version of [\[RFC0822\]](#) which is [\[RFC5322\]](#) which itself has recently been updated. The impact of initially removing text specifically indicating which header fields are not to repeat is unknown. This information was implied within the then-new ABNF notation. Clarifying text for this requirement did not return until the [\[RFC0822\]](#) revision 19 years later which also indicates this specification's success at providing a foundation that allowed email to flourish.

There are many SMTP servers that have been in operation for decades with years passing between security patches. Such an accomplishment is most remarkable considering the volume of traffic being handled, often from highly malicious sources. This amazing stability and scalability with high levels of security would not have been possible if SMTP had been expected to validate message formats.

Expecting SMTP to validate message formats to protect against vulnerabilities pertaining to protocols such as DKIM does not scale. The general use of DKIM permits signature checks subsequent to acceptance where only the status of signatures determines internal placement. As such, it becomes critical to ensure a DKIM signature is never declared valid having malformed header field stacks. To accomplish this, the DKIM specification must change.

7. DKIM Vulnerability

DKIM permits a vulnerability by not checking the message header field stack for invalid repeats when signing or verifying a signature. The DKIM signature process must walk both down and then up the header field stack while selecting the header fields to be included in the hash process of the signature. The DKIM process will even ignore prefixed FROM header fields which is the only header field always included.

The WG concluded that "listing non-existent header fields as signed" hack added in non-normative language together with opinions that checking for invalid repeated header fields is not to be considered DKIM's problem. See [section 8.15 of \[RFC6376\]](#) where this issue was expressed as not an attack against the trust DKIM intends to convey, and thus not a concern for DKIM. Nevertheless, improperly formed messages may display only the first of multiple header fields that, as a result of erroneous assumptions of there being no invalid repeated header fields, the prefixed header fields are likely to be displayed in lieu of those signed while not impacting DKIM's signature validity.

DKIM incorrectly assumed the header field stack's starting condition, which DKIM itself is best able to determine, and is an option in the OpenDKIM implementation. This is likely to astonish most recipients that DKIM failed to make a robust effort to maintain the trust it is attempting to convey. Three members of the WG authored proposed changes aimed specifically at addressing this issue [[DKIM-MH-Attack](#)]. At the time, some expressed concerns about whether this might set back DKIM's standardization process. As such, DKIM Signers may sign malformed messages (e.g., violate [[RFC5322](#)]) and be in compliance with DKIM specifications. In addition, receivers may verify these messages as having valid signatures despite multiple instances of a header field only permitted to occur once and also be in compliance with DKIM specifications. See addendum for examples of the possible abuse permitted.

Use of DKIM on such messages exposes a vulnerability in the evaluation process. Rather than ensuring essential checks are made prior to producing a result, a wasteful hack was later suggested where extra non-existent header fields could be included in the list of signed header fields. Any pre-pended header field added after signing would thereby change resulting hashes and invalidate the signature. Not all domains are attempting to achieve the same level of trust and may be more sensitive to incurring incremental storage requirements. Some domains may even inadvertently sign invalid repeated header fields because this check had not been required in the DKIM process. These same DKIM domains are also likely to

establish themselves as being Too Big To Block. These TBTB domains can then be used to spoof other domains that may have otherwise established a high level of trust by implementing the hack where, due to this defect in DKIM, can still do nothing in their defense from the perspective of now deceived recipients.

This vulnerability in DKIM represents an exploit allowing serious attacks caused by erroneous assumptions made in DKIM's signature process. There is also a header field, which because of its label, may potentially mislead recipients into believing it contains valid "Authentication-Results" [[RFC5451](#)]. Common phrases such as "Authentication-Results", "pass", and "fail", rather than use of result codes belies introductory claims this header is not intended for direct human consumption.

8. Barriers to an Authenticated Domain

Some advocate use of DKIM as a means to obtain domain references based on the increased prevalence of this protocol. DKIM is independent of the domain actually sending the message and the recipient by design. Unfortunately, DKIM also does not attempt to protect against likely abuses that are also beyond the control of the signing domain in which DKIM signature validity conveys no assurance pre-fixed header fields have not changed what recipients see. As such, DKIM signing domains can not be held accountable for incidents of abuse appearing to violate subscription policies or that spoof other domains.

Because of DKIM's vulnerability to header field spoofing, it would not be safe to express positive reputations either. Any such assurance could be exploited by malefactors to deceive those trusting DKIM results. In short, a DKIM signed domain as currently defined, can not be safely used in any context, other than the most rigid exclusion of any unsigned content which is well beyond any existing implementation. DKIM can not be safely used for email reputation as currently defined.

9. Domains as a Basis for Managing Traffic

A manageable basis for assessments can leverage a smaller number of related domains, compared to IPv6 or even IPv4 addresses. Although technically the domain name space can be larger than the massively large IPv6 address space, in practice it is not. One hundred thousand domains control 90% of Internet traffic out of approximately 100 million domains active each month. The top 150 domains control 50% of the traffic, and the top 2,500 domains control 75%. This

level of domain consolidation permits effective fast-path white-listing. Improvements achieved using domains to consolidate the threat landscape can easily justify added cryptographic authentication burdens. Even APL resource records [[RFC3123](#)] can authenticate EHLO using a single DNS transaction, but this would not allow IPv6 email to be more easily managed when facing extensive use of transitional technologies such as ISATAP, Teredo, 6to4, NAT64, and DNS64, which cryptographic technology can offer.

10. XMPP Shows the Way Forward

In addition to SMTP [[RFC5321](#)] using StartTLS [[RFC3207](#)] XMPP [[RFC6122](#)] uses StartTLS [[RFC6120](#)] over a different port with many of the features used by web servers such as [[RFC2560](#)] as one means to increase scalability. It seems plausible that by defining SMTP access over a different port is where a new authentication and international requirements can be resolved together. Of course, port 25 can be used where it might require StartTLS in the case of IPv6 connections.

Many administrators overlook a serious problem made much worse by chatty protocols that impose processing delays. Examining server logs will not reveal any problem either, because the limited resource being consumed is the number of outstanding connections TCP is able to support. Reaching this limit will prevent new connections from being instantiated but this is not logged as an event. Over time administrators may hear complaints email is not being delivered or just see an ever growing percentage of spam.

11. IANA Considerations

This document requires no IANA consideration.

12. Security Considerations

This draft intends to describe serious security concerns raised with use of DKIM that is exacerbated with IPv6 email. The contained recommendations are expected to reduce these security concerns. To better ensure security, the DKIM specification must change.

Recommendations [[DKIM-MH-Attack](#)] rejected by the DKIM WG were aimed at repairing this defect by simply requiring the definition for a valid DKIM signature to ensure no invalid repeated header fields are present. It is also clear that the non-normative language describing the non-intuitive approach of listing non-existent header fields has

not been widely embraced, especially by the domains sensitive to storage requirements. The overall storage requirement was one of weighing factors in selecting between IIM and DKIM. IIM's inclusion of the public key within the message was considered an unnecessary waste of storage. It seems many also consider the prophylactic listing of non-existent header fields an unnecessary waste as well. Based upon the current data, the present DKIM specification did not result in something that can retain trust, and that ultimately leads to even greater protocol layer violations.

13. Acknowledgements

The authors wish to acknowledge valuable contributions from the following: Dave Crocker.

14. References - Informative

[DKIM-MH-Attack]

<http://trac.tools.ietf.org/wg/dkim/trac/ticket/24>,
"Multiple-header-attack alternative proposal", April 2011.

[I-D.ietf-repute-email-identifiers]

Borenstein, N. and M. Kucherawy, "A Reputation Response Set for Email Identifiers",
[draft-ietf-repute-email-identifiers-07](#) (work in progress),
May 2013.

[I-D.kucherawy-dmarc-base]

Kucherawy, M., "Domain-based Message Authentication, Reporting and Conformance (DMARC)",
[draft-kucherawy-dmarc-base-00](#) (work in progress),
March 2013.

[RFC0733] Crocker, D., Vittal, J., Pogran, K., and D. Henderson,
"Standard for the format of ARPA network text messages",
[RFC 733](#), November 1977.

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, [RFC 822](#), August 1982.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", [RFC 2560](#), June 1999.
- [RFC2822] Resnick, P., "Internet Message Format", [RFC 2822](#), April 2001.
- [RFC3123] Koch, P., "A DNS RR Type for Lists of Address Prefixes (APL RR)", [RFC 3123](#), June 2001.
- [RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", [RFC 3207](#), February 2002.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", [RFC 4408](#), April 2006.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), September 2007.
- [RFC4954] Siemborski, R. and A. Melnikov, "SMTP Service Extension for Authentication", [RFC 4954](#), July 2007.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), October 2008.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", [RFC 5322](#), October 2008.
- [RFC5451] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", [RFC 5451](#), April 2009.
- [RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", [RFC 6120](#), March 2011.
- [RFC6122] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Address Format", [RFC 6122](#), March 2011.
- [RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, "SMTP

Service Extension for 8-bit MIME Transport", STD 71,
[RFC 6152](#), March 2011.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys
Identified Mail (DKIM) Signatures", [RFC 6376](#),
September 2011.

[RFC6532] Yang, A., Steele, S., and N. Freed, "Internationalized
Email Headers", [RFC 6532](#), February 2012.

[RFC6854] Leiba, B., "Update to Internet Message Format to Allow
Group Syntax in the "From:" and "Sender:" Header Fields",
[RFC 6854](#), March 2013.

[v6-BGP-Rpts]
<http://bgp.potaroo.net/v6/as6447/>, "BGP Routing Table
Analysis Reports/IPv6/AS6447 views", May 2013.

[Appendix A](#). DKIM Examples

From Random User Tue Mar 12 12:07:37 2013
X-Apparently-To: just4spamdlr@yahoo.com via 72.30.237.8; Tue, 12 Mar 2013
12:08:37 -0700
Return-Path: <Fake.user@gmail.com>
Received-SPF: neutral (192.83.249.65 is neither permitted nor denied by domain
of gmail.com)
A3RleHQvcGxhaW4DAzACA3RleHQvaHRtbAMDMQ--
X-YMailISG: Po8J_9cWLDuz5QIo_tChc70agZYPBIscsK7APx8FMj835hEX
clyJxoQr60jy40ccEugqmky_ayJu65fKm.KJY73k6aprb9s7Bj6P32lpm1
6yGzxWfYdNXCwcXhtFGdhKe3v7Tjh8x051jkxjIqfuS0vo8J5rZ0r.Z__6vD
4wiGFDUwFHNUAWawuz_pwp7pZ5HCivuuuyszYVvH0eIFsrQ9crR.rrk_3EQU2
Xkv_fInlGDFR8fafFPM0gQ7Q0rHhy0zQUbptDEFGdh1QV0yLwIpjwEC7264k
4MqxUH7zz_M5JOQzj6dJs1H0.iz5y9Sgp6y6kTUHAVP2f_t1hMeRvf3F7WJ6
1yY2rZJALIME1CtiNKQJoDctzgGFRnh_5mo415MvUcEIH7qqS5RFgWtXEQpd
JIpyYlECDXVUcuASoLmzbuGSiCEVLq7f4EiBTAsaMwXJ070gXBR.QYDw3VfA
Z0AcfnFrUVHNLZtLaFukQKzdk9c6SpHFHSuCAsvLPuZeRy4Ij5ndXd7viiCS
IkAHsnhG_u3.nZr3zUDF0rqw8sEKphobj6ZJ8KExtuhr_tx.94abE1JRJYi5
fukj2h8y9s.K10ZxoTClaw41_DD8fxESbyfyTRPytiEXUdK1WEjgS3rAZ0TA
WPJPDr063xLYk20UY0V.N5J15lBCtqZcde_9pdXwxVySyXo1KEQ0aH3TNRBZ
AKMFuCC7NF56aklkiUgk2EWm8iYoHsFez5_HtOz1zmc1dv4mNFOPTaNRXF2X
qjFiwfdUipupIlaEC6pIdv0_le.xvz1jnaewE0yxo4dKd2XLVvybLfsLY16U
FzLS9MJJ1wC0Cmf3G2Sb0mT4ZiAvPjyv8QnHzbSDDdy3hqq8F0uEE03sJ5dm
on5Fx0HZZ1wCH7DL1QAXpZYxYWKV.h3q69dKQML6Hbnmft_WZQY4X8uKXqkZ
o34v.YmvJxHSRCSmhFpug1EstpJ4gHVitl_eJzT_n6xYQwhNAuMZ9uRjN2xE
1Lf7NpgzRf9bFvOpJAlYLoK5Xvxbx711cMgEUFGIha_JtL1P7hyfncRszHDv
txgUYzcsVvRyAyVvWDAM.TEBsFhAtqqw0ibqo2l5xCBj2yXRbKJ0EOC1JDMs
HA - -

X-Originating-IP: [192.83.249.65]
Authentication-Results: mta1225.mail.bf1.yahoo.com from=gmail.com;
domainkeys=neutral (no sig);

Otis & Rand

Expires December 6, 2013

[Page 14]

from=gmail.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO rdaver.bungi.com) (192.83.249.65)
by mta1225.mail.bf1.yahoo.com with SMTP; Tue, 12 Mar 2013 12:08:36 -0700
Received: by rdaver.bungi.com
via smail with stdio
id <m1UFUYr-00KeXPC@rdaver.bungi.com>
for Just4spamdlr@yahoo.com; Tue, 12 Mar 2013 12:08:33 -0700 (PDT)
(Smail-3.2.0.94 1997-Apr-22 #591 built 2011-Feb-5)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:x-received:date:message-id:subject:from:to
:content-type;
bh=PS9xMxYwwTGwWXbCd8bjBBm2rwb79wVOSDLhmp+k4b4=;
b=qnYVUccLSAi2DGJdUgDDIP9A3uPk3PaxgqhYLBn6xU382MsCi/ICFgKAoFPuwM7BvL
AuSuqL6P54cIJ3Pn36h2xmXy+ucNr5r50qIY63rtvj6Apjr4uW1PzG47J7BGEiP9iWZ
PLTz19ZLpZXvZZpTCJOXUQP2HF8q6aivCblyZiQcCdVRCftG+A4z0+dEyTHbxoAMx9U3
GFISRRHcZ7k7GAYmLrSr3fUTjvpa1YwONK+IcSALC2tKVS5FP1IQAT07f1e8+b0gHh
JleaQIw8b1Vj1zhs4hFKLdedmjQqjDJXVP/K3J+t/ggfYn4H547fu6Pb5syKZIiuPf1e
yJqA==

MIME-Version: 1.0
X-Received: by 10.220.221.143 with SMTP id ic15mr6773333vcb.32.1363115257152;
Tue, 12 Mar 2013 12:07:37 -0700 (PDT)
Received: by 10.52.70.169 with HTTP; Tue, 12 Mar 2013 12:07:37 -0700 (PDT)
Date: Tue, 12 Mar 2013 09:07:37 -1000
Message-ID: <CA+VnpPKv0s-
p2nKkAkNHS4V2SxZehw_6S9QF5p1p2ji+FMof=Q@mail.gmail.com>
Subject: An example signed message
From: Random User <random.j.user.994@gmail.com>
To: just4spamdlr@yahoo.com
Content-Type: multipart/alternative; boundary=14dae9cdc33bb0ff5204d7bf00ff
Content-Length: 280

reporting valid signature

From Fake User Tue Mar 12 12:07:37 2013
X-Apparently-To: just4spamdlr@yahoo.com via 72.30.237.8; Tue, 12 Mar 2013
12:09:01 -0700
Return-Path: <Fake.user@gmail.com>
Received-SPF: neutral (192.83.249.65 is neither permitted nor denied by domain
of gmail.com)
A3RleHQvcGxhaW4DAZACA3RleHQvaHRtbAMDMQ--
X-YMailISG: gFqc.ysWLDtqkdjDpSCH39uGwhgFfnsGdWobzNb5os6sP0We
_L38eAdX.VKZWQ2F75gFwoipcPyj4g0uKMm_vSayLjrnpS9lBxMGLvtTE8KT
XYxIw6vZb4aFZ_jEcPoRntvJDkZQl4XSGWGakfmJ5G2blTWZ_i1BVkBvj0Sv
jEymvhoIXZTb_l8C0Jh69ot3MgrNBvjhrBmhCK3sziUtDPpKQPJb_lxCnYKN
00SiArQ_TUXrCRFRNsyEiJxzVfSgJWIdsCV5BN3cp..NZ17X8fguB.YxNQjt

qjVcGMd4IjQioY.a4f1luQxuiCN1yWvYqiLpP6eOCQhMrHt9X0dk32HAXNuJ
GBraVtjrySTl9Db7PpRC46w1Ms3iIUHl3z0d4o6293sMA5qFmnbczGoLRGFs
RUVlBJuRoJCSYZh5L0wbj0RPQNX2Nmw.LHwF7SY3XcZWFUjvUQQ2sdX63m_J

Otis & Rand

Expires December 6, 2013

[Page 15]

Mgy7JHAWBTvH6ytULsbXvu38a5GIYHccfNnDKVjtsrIg9qBDpVASHrRkncL0
MFLy5FHLb_XBW1TPztCFtlRViKr_HFxmOb6aZite6T57AMqlV2YAHwVNObwX
WE8ZWtKKNWbXqJYytd3vyuyAHfuseBFP_Jfmj0zVtg52ExpILDiTANEOTamP
zeu23QbeRWJd_Gpz9bbGw_OorPdcV.WJOQ29DHpiYAQRgwJNLjkd8dI.vuM
vs1Fr7LOiE3wRpSU5AW_hrR4anvGrnwSP0QaFmpNE0pl8n.Vomrp.5NU8cgU
QYI1UCSPoE_HK5Som2HMPYZFQv0pJSu1NeitXLRM3DHkIMvW4aVYqrHSNVjl
gGCFfx77c25QW.XAGtySBYwcTzcULHP4fMa7Wli4u06C4N3pDPiQoXKOC10U
koXUMKFYmedaZYvEeQRP03_8xHwKyZ.QInDsnQRwPFwYKvcWCJu4c5zXDMG4
h1AsyT3CM80nZXk8.ZGhzfTgo810Xjn_OJVgUfkG1z3..ReN990deaWJY8F5
_j6lRWLZZRzCMwOGpJ6I.jgaN5mNk38Kj6.NYLFcPMTEIt28jIRHD85cfpa3
iOL3drg1TIKQwREhS9u3H29niQ_hjHbk7ys6uSJvowilRw08eB2s.Wz0
X-Originating-IP: [192.83.249.65]
Authentication-Results: mta1266.mail.bf1.yahoo.com
from=gmail.com; domainkeys=neutral (no sig);
from=gmail.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO rdaver.bungi.com) (192.83.249.65)
by mta1266.mail.bf1.yahoo.com with SMTP; Tue, 12 Mar 2013 12:09:00 -0700
Received: by rdaver.bungi.com
via smail with stdio
id <m1UFUZI-00KeXRC@rdaver.bungi.com>
for Just4spamdler@yahoo.com; Tue, 12 Mar 2013 12:09:00 -0700 (PDT)
(Smail-3.2.0.94 1997-Apr-22 #591 built 2011-Feb-5)
From: Fake User <fake.user@gmail.com>
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:x-received:date:message-id:subject:from:to
:content-type;
bh=PS9xMXywwTGwWxbCd8bjBBm2rwb79wVOSDLhmp+k4b4=;
b=qnyVUccLSAi2DGJdUgDDIP9A3uPk3PaxgqhYLBn6xU382MsCi/ICFgKAoFPuwM7BvL
AuSuqL6P54cIJ3Pn36h2xmXy+ucNr5r50qIY63rtvj6Apjr4uW1PzG47J7BGEiP9iWdZ
PLTz19ZLpZXvZZpTCJ0XUQP2HF8q6aivCb1YZIQcCdVRCftG+A4z0+dEyTHbxoAMx9U3
GFISRRHcZ7k7GAyYmLrSr3fUTjvpa1YWoNK+IcSALC2tKVSW5FP1IQAT07f1e8+b0gHh
JleaQIw8b1Vj1zhs4hFKLdedmjQqjDJXVP/K3J+t/ggfYn4H547fu6Pb5syKZIiuPf1e
yJqA==
MIME-Version: 1.0
X-Received: by 10.220.221.143 with SMTP id ic15mr6773333vcb.32.1363115257152;
Tue, 12 Mar 2013 12:07:37 -0700 (PDT)
Received: by 10.52.70.169 with HTTP; Tue, 12 Mar 2013 12:07:37 -0700 (PDT)
Date: Tue, 12 Mar 2013 09:07:37 -1000
Message-ID: <CA+VnpPKv0s-
p2nKkAkNHS4V2SxZehw_6S9QF5p1p2ji+FMof=Q@mail.gmail.com>
Subject: An example signed message
From: Random User <random.j.user.994@gmail.com>
To: just4spamdler@yahoo.com
Content-Type: multipart/alternative; boundary=14dae9cdc33bb0ff5204d7bf00ff
Content-Length: 280

spoofed DKIM with valid signature

Appendix B. Stats

DKIM total: 5063
DKIM pass: 4354
DKIM fail: 709
DKIM pass w/multiple from: 916 (about 21% on average)
An increase appears concurrent with the publication of this draft.

Looking at roughly a few hours of spam

Authors' Addresses

Douglas Otis
Trend Micro
10101 N. De Anza Blvd
Cupertino, CA 95014
USA

Phone: +1.408.257-1500
Email: doug_otis@trendmicro.com

Dave Rand
Trend Micro
10101 N. De Anza Blvd
Cupertino, CA 95014
USA

Phone: +1.408.257-1500
Email: dave_rand@trendmicro.com

