A Trend Micro Research Paper

Concerns Regarding Flaws in the New DKIM Standard

Douglas Otis
(Forward-Looking Threat Research Team)

Contents

Introduction

IPv4 address reputation currently provides the primary basis for defending open Simple Mail Transfer Protocol (SMTP) services (acceptance without prior arrangement). The use of IP addresses in this role becomes impractical when dealing with IPv6 due to data requirements and the inability to defend detection of subscription violations.[1] 8,210,980,092,416,010 /64 equivalent IPv6 prefixes are currently routed.[2] In comparison, 2,644,737,232 IP addresses are routed for IPv4. While IPv4 is reaching its maximum, IPv6 has about 0.1% of the available /64 prefix routed and this continues to rapidly grow. Unlike IPv4, there is no practical means to scan reverse Domain Name System (DNS) namespace within IPv6 since each /64 prefix may contain any number of pointer (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 four decimal numbers are often considered unacceptable, for example. Our processing of reverse DNS namespace in cooperation with network providers now excludes about 38% or 1,000,000,000 IPv4 addresses. A comparison of IPv6 /64 prefixes with the remainder of routable IPv4 addresses shows that there are 11.3 million times more IPv6 /64 prefixes that need to be categorized. 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 risks. Tracking currently routed IPv6 /64 prefixes using a single bit requires 6 million billion bytes or 5,650 terabytes 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 deal 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.

---

1 The Internet Society. (1998). "Internet Protocol, Version 6 (IPv6) Specification." Last accessed September 11, 2013, http://www.ietf.org/rfc/rfc2460.txt.

2 Geoff Huston. (September 11, 2013). "AS6447 IPv6 BGP Table Data." Last accessed September 11, 2013, http://bgp.potaroo.net/v6/as6447/.

Members within organizations such as the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) are suggesting SMTP error response schemes to establish DomainKeys Identified Mail (DKIM) or the Sender Policy Framework (SPF) as acceptance requirements to better ensure a domain offers a basis for acceptance to replace that of the IP address used by SMTP clients. Due to IPv6 reputation services' understandable inability to scale, domain-based alternatives are being sought. Some at least understand DKIM is unable to support negative reputation schemes. However, reliance on a mechanism unable to sustain close scrutiny of negative assertions makes sustained differentiation of positive and negative views less tenable.

In the April 2013 Rocky Mountain IPv6 Task Force Summit in Denver, the second day government track sessions raised concerns about the lack of methods available to defend SMTP over IPv6. Some proposals within the Internet Engineering Task Force (IETF) aim to establish DKIM as a basis for reputation schemes in the Repute WG, which introduces the use of DKIM domains along with SMTP client IP addresses and rfc5321.helo also identifying the SMTP client.[3] 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.

Safe Incremental Deployment?

RFC5863's introduction states that "DKIM allows an organization to claim responsibility for transmitting a message, in a way that can be validated by a recipient."[4] Based on actual use of DKIM, Trend Micro published a blog entry entitled, "Possible Phishing with DKIM."[5] Dave Crocker dismissed DKIM's phishing role by stating:

[3] Nathaniel Borenstein and Murray S. Kucherawy. (January 2012). "A Reputation Vocabulary for Email Identifiers: draft-ietf-repute-email-identifiers-02." Last accessed September 11, 2013, http://tools.ietf.org/html/draft-ietf-repute-email-identifiers-02.

[4] Tony Hansen, Ellen Siegel, and Dave Crocker. (May 2010). "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations." Last accessed September 11, 2013, http://tools.ietf.org/html/rfc5863.

[5] Douglas Otis. (June 14, 2011). *TrendLabs Security Intelligence Blog.* "Possible Phishing with DKIM." Last accessed September 11, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/possible-phishing-with-dkim/.

> "DKIM's sole job is to attach an identifier that can be believed, specifically a domain name that can be unrelated to any other identifier in the message. That domain name is used for associating the reputation of the domain owner with the message. … The DKIM specification mandates that input to DKIM must be valid according to RFC5322. In requiring this, it is placing a burden on the containing system to ensure that a message is well formed. It is not DKIM's job to do the basic message validation; it's the job of the requesting software."[6]

Refuting this, RFC6376 Section 3.8 use should not mandate compliance with RFC5322 nor will noncompliance affect the validity of a DKIM signature as it is currently defined.[7] His response also misconstrues the statement, "DKIM was intended to authenticate domain relationships with an email message bound at a minimum to that of the From header field," to mean, "DKIM verifies the From header field." This is erroneous, as is the assertion of the signature associating the reputation of the domain owner with the message instead of just a signed message fragment. Most will assume a reference to "message" implies the entire email. This conflation appears in several documents, including Section 5.4 of RFC5863.

In fact, dismissing the phishing concern overlooks operational strategies suggested in deployment documents where DKIM supplants often problematic message filtering. Such likely use makes it essential for DKIM validation to exclude messages containing invalidly repeated header fields. This generalization is also used in RFC5863, which suggests that messages that have valid signatures from trusted sources can be white-listed to avoid additional content processing. Here again, concerns related to the inclusion of prefixed header fields were not mentioned. Prefixed header field concerns were not mentioned until Section 8.15 was added to RFC6376. Even then, this section does not offer a mitigation strategy when DKIM signatures ensure delivery by bypassing additional filtering. Several email service providers, including Yahoo, have implemented exactly this strategy, delivering content straight to an inbox when a valid and trusted DKIM signature is present in a message.

Barry Leiba's response to the assertion that DKIM enables phishing suggests the attack is overstated due to the following reasons:

1. It relies on the sender's ability to get a DKIM signature onto a phishing message and assumes the message will be treated as credible by the delivery system.

---

[6] Dave Crocker. (June 21, 2011). *CircleID.* "Searching Under Lampposts with DKIM." Last accessed September 11, 2013, http://www.circleid.com/posts/searching_under_lampposts_with_dkim/.

[7] Dave Crocker and Tony Hansen. (September 2011). "DomainKeys Identified Mail (DKIM) Signatures." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6376; The IETF Trust. (2008). "Internet Message Format." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5322.

2. It ignores the fact that delivery systems use other factors to decide how to handle incoming messages and will downgrade the reputation score of a domain that has been seen to sign these sorts of things.

3. It ignores the fact that high-value domains with strong reputations will not allow the attackers to use them for signing.

4. The attack creates a message with two "From" lines and such messages are not valid. It ignores the fact that delivery systems will take that into account as they score the message and make their decisions.[8]

Assertions about the phishing concern being overstated are wrong and item 3 is irrelevant. As for item 1, sending yourself a message from a high-volume DKIM provider and prefixing some header field and relaying the modified message to any number of recipients is simple and has a high probability of being accepted. As for items 2 and 4, it is common for trust in a DKIM signature to cause message filtering to be bypassed as suggested in RFC5863. As such, this assumes DKIM validation checks for invalid header fields. Although such validation is possible, seldom is the double-listing of singleton header fields ever used, which also suggests that this will not affect a domain's signature rating. Making the detection of invalidly repeated header fields optional places all other domains at risk.

Leiba's response goes on to say, "Validity checking is an important part of the analysis of incoming email, but it is a separate function that's not a part of DKIM. All messages, whether DKIM is in use or not, should be checked for being well-formed, and deviations from 'correct' form should increase the spam score of a message. That has nothing to do with DKIM."

Leiba's response is also incorrect. Undetected introduction of prefixed header fields is not likely included in a signature by a trusted domain. However, this trusted domain signature is still likely to enable a message with prefixed header fields to bypass content filtering as described in RFC5863. Since DKIM must process the entire header field stack from top to bottom and then from bottom to top, failure to note when this stack does not meet DKIM's input requirements and declare associated signatures valid represents evidence of a negligent protocol that failed to validate its input.

[8] Barry Leiba. (June 21, 2011). *Staring at Empty Pages.* "Misconceptions About DKIM." Last accessed September 12, 2013, http://staringatemptypages.blogspot.com/2011/06/misconceptions-about-dkim.html.

Network architecture often assumes communication functions are organized into nested levels of abstraction called "protocol layers" with related metadata organized in the same fashion. Rigid layering is considered a desirable means to force compliance with existing standards. In practice, this requires careful review of overall protocol operation. Suggesting that layering is inadequate may call for an alternative organizational principle for protocol functionality, especially with respect to a store-and-forward transport. Passing metadata should not require needlessly repeating resource-intensive operations, as is the case with the current DKIM specification.

Enforcing message structure compliance by a store-and-forward transport is impractical. DKIM aims to achieve more deterministic message acceptance through trust and less through Bayesian processes. Not all errant structures are malicious but DKIM use makes it imperative to ensure that invalidly repeated header fields do not produce valid signatures. This additional requirement that DKIM imposes is necessary to prevent abuse of the alternative processing it enables. Optional double-listing of header fields means other domains may not prohibit the inclusion of deceptive prefixed header fields. Having prefixed header field checks in DKIM being optionally included places all domains at risk since DKIM signatures themselves are not visible but nevertheless may influence inbox delivery. It is also unreasonable to assume that some other email protocol layer will ensure message structure compliance just to mitigate DKIM-related abuse. This is a problem that DKIM created and should be prepared to handle in order to support its safe incremental deployment.

Exploiting Trust

The trust established by a signing domain is being exploited to mislead recipients as to who authored messages. DKIM's trust-related function may be generalized as better ensuring delivery to inboxes as opposed to junk folder placement or silent discard. It is also apparent that receivers expect DKIM signature validation ensures that invalid header fields have not been prefixed. While it is possible for signing domains to support this expectation by including nonexistent header fields in a list of header fields added to the signature's hash, few implement this feature, which offers a poor alternative to the overlooked exclusion of invalidly repeated header fields.

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

Regardless of possible underlying motivations, it is clear that checks for valid header field message structure remains a general expectation of DKIM's validation process. Although a valid header field check is essential to ensure a safe result, it simply does not occur in most cases. Not every domain seeks to establish the same level of trust. Those that do not check for prefixed header fields and have greater latitude place all other domains at risk. Checking message structure should explicitly not be handled by the transport.[9] Modification to SMTP implementations such as Sendmail, Exim, or Postfix and the like are neither appropriate nor likely to be 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 inbox due to common use, exposing DKIM's vulnerability. DKIM's validation process does not explicitly ensure against invalidly repeated header fields due to optional hash inclusion. This hashing allowance permits the spoofing of other domains with prefixed header fields, making DKIM harmful by misleading recipients about who authored a message based on acceptance established by a DKIM signature. DKIM validation must be modified to ensure against invalidly repeated header fields in order to ensure that the trust established by a signing domain is not exploited to mislead recipients.

Maintaining Trust

Not every subsystem or protocol layer should be expected to repeat previous security checks to establish proper layering. However, important critical checks to enforce new relationships within a message should not be assumed, especially those that involve 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 cannot function if rigid message structures were enforced by the transport. Such enforcement does not scale and will impede necessary change when new authentication or presentation requirements involve small structural adjustments. For example, internationalization introduced a format negotiation not assured to survive beyond the next hop.

[9] Brian E. Carpenter. (June 1996). "Architectural Principles of the Internet." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc1958.txt; The Internet Society. (December 2002). "Internet Architectural Guidelines." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc3439.txt; John C. Klensin. (October 2008). "Simple Mail Transfer Protocol." Last accessed October 2, 2013, http://tools.ietf.org/html/rfc5321.

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, when discovered, should demand our attention and diligence to effect repair. Email has become an integral component in general commerce and maintaining security such as reporting system failures and break-in attempts and facilitating account access recovery.

Reporting or predicting failure should not be viewed as exhibiting lack of respect for accomplishments achieved. 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 increased the level of multiple From header field abuse seen to 21% of signed DKIM messages.

Conflating DKIM Fragments with Email Messages

DKIM signs only fragments of an email so it is more proper to refer to this as a "DKIM-signed fragments" and not a "DKIM-signed message." Normal DKIM signature validation offers a simple Pass/Fail response associated 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 such a case, the signed From header field fragment is likely invisible, as is the DKIM signature fragments that hide which other message fragments were encompassed by the DKIM signature process.

DKIM's trust-related role is to better ensure message delivery to a user's inbox. Unless DKIM ensures that this trust is not used to perpetrate deception, no positive assertions regarding a DKIM domain is safe. As a result, DKIM cannot 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.[10] 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 will not preclude the occurrence of invalid messages and RFC5321 clearly states that it will not enforce RFC5322 message structure due to practical constraints.[11] Instead of relying on optional policies such as DMARC to make partial message structure checks that ignore Date or Subject header field spoofing that can still introduce malicious clickable links, these critical violations of message structure are sure to be mitigated only when DKIM considers any associated signature to be invalid. OpenDKIM offers this necessary albeit unspecified mode of operation by asserting the "conf→conf_reqhdrs" Lightweight Directory Access Protocol (LDAP) option, for example. Unlike DMARC, proper signature definition does not cross protocol layers, especially since no other layer enforces RFC5322 and no other layer determines the validity of a DKIM signature.

Since multiple DKIM signatures can occur, simple annotation of which fragments and domains are associated with a valid signature is precluded. The only message fragment ensured by a DKIM signature is the From header field. Just as DMARC concluded, recipients only closely observe the From header field. DKIM initially reached this conclusion as well. While no absolute assurance of header field validity is asserted, the domain together with its 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 overreaches when rejecting emails based on message format as with RFC6854. While DMARC is likely limited to domains that convey transactional messages, implementing the DMARC policy should not require reexamining messages to determine whether DKIM signatures are safely considered valid. A processing concern was also given as a reason why DMARC did not ensure a potentially dangerous Subject header field had not been prefixed. Such message reexamination that is necessary prior to employing a valid signature status represents poorly considered protocol layering. Such

[10] Murray S. Kucherawy. (October 2, 2013). "Domain-Based Message Authentication, Reporting, and Conformance (DMARC) draft-kucherawy-dmarc-base-00." Last accessed September 12, 2013, http://tools.ietf.org/html/draft-kucherawy-dmarc-base-00.

[11] The IETF Trust. (2008). "Simple Mail Transfer Protocol." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5321.

checks being made during the DKIM validation would likely reduce processing overhead with a minor risk of adding a few microseconds.

SMTP Can't

In keeping with the Architectural Principles of the Internet expressed in RFC1958 and RFC3439, RFC5321 recommends against rejecting messages based on perceived defects in the message structure. This liberal acceptance permits evolutionary change in message specifications starting with RFC0822, which was based on RFC0733, replaced by RFC2822 and again by RFC5322, RFC6152, RFC6532, and RFC6854.[12] The second to the 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 footnotes with the second referencing the latest version of RFC0822—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 Augmented Backus-Naur Form (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.

Many SMTP servers 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 if it has malformed header field stacks. To accomplish this, the DKIM specification must change.

[12] David H. Crocker. (August 13, 1982). "Standard for the Format of ARPA Internet Text Messages." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc0822.txt; David H. Crocker, John J. Vittal, Kenneth T. Pogran, and D. Austin Henderson, Jr. (November 21, 1977). "Standard for the Format of ARPA Network Text Messages (1)." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc733; John C. Klensin, Ned Freed, M. Rose, and D. Crocker. (March 2011). "SMTP Service Extension for 8-Bit MIME Transport." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6152; Abel Yang, Shawn Steele, and Ned Freed. (February 2012). "Internationalized Email Headers." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6532.

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 then up the header field stack while selecting the header fields to include in the hash process of the signature. The DKIM process will even ignore prefixed From header fields, which are the only header fields that are always included.

The workgroup concluded that "listing nonexistent header fields as signed" hacks added to non-normative language, together with opinions that checking for invalidly repeated header fields, should not 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 invalidly 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 it can best determine independent of other layers and is an option in the OpenDKIM implementation. That DKIM failed to make a robust effort to maintain the trust it is attempting to convey is likely to astonish most recipients. Three members of the workgroup authored proposed changes that specifically aim to address this issue.[13] 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., that violate RFC5322) and still 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 still also be in compliance with DKIM specifications. See the Appendix for examples of the possible abuse this permits.

[13] "Multiple-Header-Attack Alternative Proposal." Last accessed September 12, 2013, http://trac.tools.ietf.org/wg/dkim/trac/ticket/24.

DKIM use on such messages exposes a vulnerability in the evaluation process. Rather than ensuring that essential checks are made prior to producing a result, a wasteful hack was later suggested where extra nonexistent header fields could be included in the list of signed header fields. Any prepended header field added after signing would thereby change resulting hashes and invalidate the signature. Not all domains attempt to achieve the same level of trust and may be more sensitive to incurring incremental storage requirements. Some domains may even inadvertently sign invalidly repeated header fields because this check was not required in the DKIM process. These same DKIM domains are also likely to establish themselves as being too big to block (TBTB). 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."[14] Common phrases such as "authentication-results," "pass," and "fail" rather than the use of result codes belies introductory claims that this header is not intended for direct human consumption.

Barriers to an Authenticated Domain

Some advocate DKIM use 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 does not also attempt to protect against likely abuses that are also beyond the control of the signing domain for which DKIM signature validity conveys no assurance that prefixed header fields have not changed what recipients see. As such, DKIM signing domains cannot be held accountable for incidents of abuse that appear to violate subscription policies or 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 who trust DKIM results. In short, a DKIM-signed domain as currently defined cannot be safely used in any context other than the most rigid exclusion of any unsigned content, which is well beyond any existing implementation. DKIM cannot be safely used for email reputation as currently defined.

[14] Murray S. Kucherawy. (April 2009). "Message Header Field for Indicating Message Authentication Status." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5451.

Domains as a Basis for Managing Traffic

A manageable basis for assessment can leverage a smaller number of related domains compared with 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 the 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 can authenticate EHLO using a single DNS transaction but this would not allow IPv6 emails to be more easily managed when facing extensive use of transitional technologies such as Intra-Site Automatic Tunnel Addressing protocol (ISATAP), Teredo, 6to4, NAT64, and DNS64, as well as the solutions offered by cryptographic technology.[15]

[15] Peter Koch. (June 2001). "A DNS RR Type for Lists of Address Prefixes (APL RR)." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc3123.

XMPP Shows the Way Forward

In addition to SMTP using STARTTLS, Extensible Messaging and Presence Protocol (XMPP) uses STARTTLS over a different port with many of the features used by web servers such as RFC2560 as one means to increase scalability.[16] In addition to SMTP using StartTLS, XMPP uses StartTLS over a different port with many of the features used by web servers such as the Online Status Certificate Protocol (OSCP) as one means to increase scalability. I-D.ietf-dane-smtp or I-D.dukhovni-smtp-opportunistic-tls offers several other interesting innovations. DNS-Based Authentication of Named Entities (DANE) offers greater transparency than that afforded by Certificate Authorities.[17] With general availability without added expense, StartTLS/DANE can also exchange client certificates. Client certificates offer a safe basis for acceptance or rejection without any need to examine email header field stacks. Header stack examination is needed with DKIM because only a fragment of the message is signed. In comparison, StartTLS encompasses the entire message stream that identifies both the sender and recipient that allows domain reputation to be effective at mitigating spam via negative reputations, which DKIM is unable to support.

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 the Transmission Control Protocol (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 that email is not being delivered or just see an ever-growing percentage of spam.

IANA Considerations

This document does not require Internet Assigned Numbers Authority (IANA) consideration.

---

[16] Paul Hoffman. (February 2002). "SMTP Service Extension for Secure SMTP over Transport Layer Security." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc3207.txt; Peter Saint-Andre. (March 2011). "Extensible Messaging and Presence Protocol (XMPP): Address Format." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6122; Peter Saint-Andre. (March 2011). "Extensible Messaging and Presence Protocol (XMPP): Core." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6120; Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. (June 1999). "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc2560.txt.

[17] Santosh Chokhani; Warwick Ford; Randy V. Sabett, J.D., CISSP; and Charles R. Merrill. (November 2003). "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc3647.txt; Viktor Dukhovni. (July 2013). "SMTP Security via Opportunistic DANE TLS." Last accessed October 1, 2013, http://www.ietf.org/id/draft-dukhovni-smtp-opportunistic-tls-01.txt; Paul Hoffman and Jakob Schlyter. (August 2012). "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA." Last accessed October 1, 2013, http://tools.ietf.org/html/rfc6698.

Security Considerations

This draft intends to describe serious security concerns that have been raised with regard to DKIM use exacerbated by IPv6 emails. The recommendations in it are expected to reduce these security concerns. To better ensure security, the DKIM specification must change.

The recommendations rejected by the DKIM Workgroup aimed to repair this defect by simply requiring that the definition of a valid DKIM signature ensures no invalidly repeated header fields are present. It is also clear that the non-normative language describing the nonintuitive approach of listing nonexistent header fields has not been widely embraced, especially by domains sensitive to storage requirements. The overall storage requirement was one of the weighing factors in selecting between Identified Internet Mail (IIM) and DKIM. IIM's inclusion of the public key within the message was considered an unnecessary waste of storage. It seems that many also consider the prophylactic listing of nonexistent header fields an unnecessary waste. Based on current data, the present DKIM specification did not result in something that can retain trust and that leads to protocol-layer violations as seen with DMARC.

Section 8.15 of RFC6376 states that "it is up to the identity assessor or some other subsequent agent to act on such messages as needed such as degrading the trust of the message (or, indeed, of the signer), warning the recipient, or even refusing delivery." Despite DKIM ignoring critical aspects essential for retaining trust, it now suggests that this be fixed by some undefined process. Since virtually all DKIM domains will not employ prophylactic double-listing of signed header fields, an identity assessor is neither a timely nor reasonable remedy either. To be absolutely clear, the DKIM specification must change to ensure that valid signatures do not include invalidly repeated header fields.

References

- Abel Yang, Shawn Steele, and Ned Freed. (February 2012). "Internationalized Email Headers." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6532.
- Barry Leiba. (June 21, 2011). *Staring at Empty Pages.* "Misconceptions About DKIM." Last accessed September 12, 2013, http://staringatemptypages.blogspot.com/2011/06/misconceptions-about-dkim.html.
- Brian E. Carpenter. (June 1996). "Architectural Principles of the Internet." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc1958.txt.

- Dave Crocker and Tony Hansen. (September 2011). "DomainKeys Identified Mail (DKIM) Signatures." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6376.
- Dave Crocker. (June 21, 2011). *CircleID*. "Searching Under Lampposts with DKIM." Last accessed September 11, 2013, http://www.circleid.com/posts/searching_under_lampposts_with_dkim/.
- David H. Crocker. (August 13, 1982). "Standard for the Format of ARPA Internet Text Messages." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc0822.txt.
- David H. Crocker, John J. Vittal, Kenneth T. Pogran, and D. Austin Henderson, Jr. (November 21, 1977). "Standard for the Format of ARPA Network Text Messages (1)." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc733.
- Douglas Otis. (June 14, 2011). *TrendLabs Security Intelligence Blog*. "Possible Phishing with DKIM." Last accessed September 11, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/possible-phishing-with-dkim/.
- Geoff Huston. (September 11, 2013). "AS6447 IPv6 BGP Table Data." Last accessed September 11, 2013, http://bgp.potaroo.net/v6/as6447/.
- John C. Klensin, Ned Freed, M. Rose, and D. Crocker. (March 2011). "SMTP Service Extension for 8-Bit MIME Transport." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6152.
- Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. (June 1999). "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc2560.txt.
- "Multiple-Header-Attack Alternative Proposal." Last accessed September 12, 2013, http://trac.tools.ietf.org/wg/dkim/trac/ticket/24.
- Murray S. Kucherawy. (April 2009). "Message Header Field for Indicating Message Authentication Status." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5451.

- Murray S. Kucherawy. (October 2, 2013). "Domain-Based Message Authentication, Reporting, and Conformance (DMARC) draft-kucherawy-dmarc-base-00." Last accessed September 12, 2013, http://tools.ietf.org/html/draft-kucherawy-dmarc-base-00.
- Nathaniel Borenstein and Murray S. Kucherawy. (January 2012). "A Reputation Vocabulary for Email Identifiers: draft-ietf-repute-email-identifiers-02." Last accessed September 11, 2013, http://tools.ietf.org/html/draft-ietf-repute-email-identifiers-02.
- Paul Hoffman. (February 2002). "SMTP Service Extension for Secure SMTP over Transport Layer Security." Last accessed September 12, 2013, http://www.ietf.org/rfc/rfc3207.txt.
- Paul Hoffman and Jakob Schlyter. (August 2012). "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA." Last accessed October 1, 2013, http://tools.ietf.org/html/rfc6698.
- Peter Koch. (June 2001). "A DNS RR Type for Lists of Address Prefixes (APL RR)." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc3123.
- Peter Saint-Andre. (March 2011). "Extensible Messaging and Presence Protocol (XMPP): Address Format." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6122.
- Peter Saint-Andre. (March 2011). "Extensible Messaging and Presence Protocol (XMPP): Core." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc6120.
- Santosh Chokhani; Warwick Ford; Randy V. Sabett, J.D., CISSP; and Charles R. Merrill. (November 2003). "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc3647.txt.
- The IETF Trust. (2008). "Internet Message Format." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5322.
- The IETF Trust. (2008). "Simple Mail Transfer Protocol." Last accessed September 12, 2013, http://tools.ietf.org/html/rfc5321.
- The Internet Society. (1998). "Internet Protocol, Version 6 (IPv6) Specification." Last accessed September 11, 2013, http://www.ietf.org/rfc/rfc2460.txt.

- The Internet Society. (December 2002). "Internet Architectural Guidelines." Last accessed October 1, 2013, http://www.ietf.org/rfc/rfc3439.txt.
- Tony Hansen, Ellen Siegel, and Dave Crocker. (May 2010). "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations." Last accessed September 11, 2013, http://tools.ietf.org/html/rfc5863.
- Viktor Dukhovni. (July 2013). "SMTP Security via Opportunistic DANE TLS." Last accessed October 1, 2013, http://www.ietf.org/id/draft-dukhovni-smtp-opportunistic-tls-01.txt.

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_tChc7OagZYPBIscsK7APx8FMj835hEXclyJxoQr6Ojy40ccEugqmkym_ayJu65fKm.
KJY73k6aprxb9s7Bj6P32lpml6yGzxWFYdNXCwcxHtFGdhKe3v7Tjh8x051jkxjIqfuS0vo8J5rZOr.Z__6vD4
wiGFDUwFHNUWAwuz_pwp7pZ5HCivuuuyszYVvH0eIFsrQ9crR.rrk_3EQU2Xkv_fInlGDFR8fafFPMO
gQ7QOrHhy0zQUbptDEFGdh1QVOyLwIpjwEC7264k4MqxUH7zz_M5JOQzj6dJslH0.iz5y9Sgp6y6kTU
HAVP2f_t1hMeRvf3F7WJ61yY2rZJALIME1CtiNKQJoDctzgGFRnh_5mo415MvUcEIH7qqS5RFgWtXE
QpdJIpyYlECDXVUcuASoLmzbuGSiCEVLq7f4EiBTAsaMwXJ07OgXBR.QYDw3VfAZ0AcfnFrUVHNL
ZtLaFukQKzdk9c6SpHFHSuCAsvLPuZeRy4Ij5ndXd7viyCSIkAHsnhG_u3.nZr3zUDFOrqw8sEKphobj6Z
J8KEXtuhr_tx.94abE1JRJYi5fukj2h8y9s.K10ZxoTClaw41_DD8fxESbyfyTRPytiEXUdK1WEjgS3rAZ0TA
WPJPDr063xLYk20UY0V.N5J15lBCtqZcde_9pdXwxVySyXo1KEQOaH3TNRBZAKMFuCC7NF56aklki
Ugk2EWm8iYoHsFez5_HtOz1zmc1dv4mNFOPTaNrXF2XqjFiwfdUipupIlAEc6pIdv0_le.xvz1jnaewEOyx
o4dKd2XLVvybLfsLY16UFzLS9MJJ1wC0Cmf3G2SbOmT4ZiAvPjyv8QnHzbSDDDy3hqg8F0uEE03sJ5d
mon5FxOHZZ1wCH7DL1QAXpZYxYWKV.h3q69dKQMl6HbnmfT_WZQY4X8uKXqkZo34v.YmvJxH
SRCSmhFpug1EstpJ4gHVitl_eJzT_n6xYQwhNAuMZ9uRjN2xE1Lf7NpgzRf9bFvOpJAlyLoK5Xvxbx711c
MgEUfGIha_JtL1P7hyfncRszHDvtxgUYzcsVvRyAyVvwDAM.TEBsFhAtqqwOibqo2l5xCBj2yXRbKJ0EO
C1JDMsHA--

X-Originating-IP: [192.83.249.65]

Authentication-Results: mta1225.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 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/ICFgKAoFPuwM7BvLAuSuqL6P54cIJ3Pn36h2xmXy+ucNr5r5OqIY63rtvj6Apjr4uW1PzG47J7BGEiP9iwDZPLTzl9ZLpZXvZZpTCJOXUQP2HF8q6aivCblYZIQcCdVRCftG+A4z0+dEyTHbxoAMx9U3GFISRRHcZ7k7GAyYmLrSr3fUTjvpa1YWoNK+IcSALC2tKVSW5FP1IQAT07f1e8+bOgHhJleaQIw8b1Vjlzhs4hFKLdedmjQqjDJXVP/K3J+t/ggfYn4H547fu6Pb5syKZIiuPf1eyJqA==

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_vSayLjrnps9lBxMGLvtTE8kTXYxIw6vZb4aFZ_jEcpoRntvJDkZQl4XSGWGakfmJ5G2blTWZ_i1BVkBvj0SvjEymvhoIXZTb_l8C0Jh69ot3MgrNBvjhrBmhCK3sziUtDPpKQPJb_lxCnYKNO0SiArQ_TUXrC

RFRNsyEiJxzVfSgJWIdsCV5BN3cp..NZ17X8fguB.YxNQjtqjVcGMd4IjQioY.a4f1luQxuiCN1yWvYqiLpP6eOCQhMrHt9XOdk32HAXNuJGBraVtjrySTl9Db7PpRC46wlMs3iIUHl3z0d4o6293sMA5qFmnbczGoLRGFsRUVlBJuRoJCSYZh5LOwbj0RPQNX2Nmw.LHwF7SY3XcZWFUjvUQQ2sdx63m_JMgy7JHAwBTVH6ytULsbXvu38a5GIYHccfNnDKVjtsrIg9qBDpVASHrRkncL0MFLy5FHLb_XBW1TPztCFtlRViKr_HFxMob6aZIte6T57AMqlV2YAHwVNObwxWE8ZWTkKNWbXqJYytd3vyuyAHfuseBFP_Jfmj0zVtg52EXpIlDiTANEOTamPzeu23QbeRWJd_Gpz9bbGw_OorPdcV.WJOQ29DHpiYAQRgWjJNLjkd8dI.vuMvs1Fr7LOiE3wRpSU5AW_hrR4anvGrnwSPOQaFmpNE0pl8n.Vomrp.5NU8cgUQYI1UCSPoE_HK5Som2HMPYZFQv0pJSu1NeitXlRM3DHkIMvW4aVYqrHSNVjlgGCFFx77c25QW.XAGtySBYWcTzcUlHP4fMa7Wli4u06C4N3pDPiQoXKOC10UkoXUMKFYmedaZYvEeQRPO3_8xHwKyZ.QInDsnQRwPFWYKvcWCJu4c5zxDMG4h1AsyT3CM80nZXk8.ZGhzfTgo810Xjn_OJVgUfkG1z3..ReN990deaWJY8F5_j6lRWLZZRzCMwOGpJ6I.jgaN5mNk38Kj6.NYLFCpMTEIt28jIRHD85cfpa3iOL3drg1TIKQWrEhS9u3H29niQ_hjHbk7ys6uSJvowilRwO8eB2s.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 Just4spamdlr@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/ICFgKAoFPuwM7BvLAuSuqL6P54cIJ3Pn36h2xmXy+ucNr5r5OqIY63rtvj6Apjr4uW1PzG47J7BGEiP9iwDZPLTzl9ZLpZXvZZpTCJOXUQP2HF8q6aivCblYZIQcCdVRCftG+A4z0+dEyTHbxoAMx9U3GFISRRHcZ7k7GAyYmLrSr3fUTjvpa1YWoNK+IcSALC2tKVSW5FP1IQAT07f1e8+bOgHhJleaQIw8b1Vjlzhs4hFKLdedmjQqjDJXVP/K3J+t/ggfYn4H547fu6Pb5syKZIiuPf1eyJqA==

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

spoofed DKIM with valid signature

Appendix B: Statistics

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. More data will be made available subsequently.

Looking at roughly a few hours of spam

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003