Using a Certificate Public Key to Protect DKIM Public Key Spoofing

Brett Krueger

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Krueger, Brett, "Using a Certificate Public Key to Protect DKIM Public Key Spoofing", Technical Disclosure Commons, (April 07, 2020)
https://www.tdcommons.org/dpubs_series/3103
Using a Certificate Public Key to Protect DKIM Public Key Spoofing

Brand Indicators for Message Identification (BIMI) is a standard that allows domain owners to coordinate with Mail User Agents (MUAs) (i.e., email clients) to display brand-specific indicators next to properly authenticated messages. The BIMI standard relies on the domain name system (DNS) to specify policies and to assist with authenticating email along with authentication protocols such as Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM). Brand Indicators for Message Identification describes to email services how to fetch and authenticate a brand indicator (e.g., a logo) to display to a user to identify the sender of the message. However, DNS is susceptible to several different spoofing attacks such as DNS cache poisoning, Border Gateway Protocol (BGP) attacks, etc.

A Verified Mark Certificate (VMC), which is validated by a third party Certificate Authority (CA), helps protect against spoofing attacks by including a proof mechanism to validate, using public-key cryptography, each organization with their associated logo. However, currently the entity certificate public key is not used as a signature. While DKIM (RFC6376) and SPF (RFC7208) authenticate the email sender, they are both still susceptible to DNS attacks and neither provides graphical logos to identify messages¹. Additionally, Secure/Multipurpose Internet Mail Extensions (S/MIME) (RFC5751) also authenticates email messages, but is not in common use and also does not provide graphical logos to identify messages. Various propriety solutions exist to provide logos, however these methods rely on the host company of the email

service to validate the logos which is problematic as it lacks scalability, lacks uniformity, and poses a significant burden on the host company.\(^2\)

This paper offers a profile that aligns the DKIM public key and the VMC end-entity public key with each other (i.e., make them equivalent). Thus, if the DKIM DNS policy record is spoofed or otherwise attacked, the email service may detect the attack and untrust the message published via the spoofed DNS record. While the proposed profile still uses DKIM to perform initial message validation, the profile also allows for DNS attacks to be exposed.

As illustrated in Figure 1 above, the CA validates and associates a logo with the email sender organization and issues the email sender organization a VMC. This VMC is associated with a public key created by the email sender organization (and to which the email sender organization maintains the associated private key). The email sender organization, when sending an email to a user, aligns the DKIM public key with the public key associated with the VMC. That is, the email sender organization ensures that the DKIM public key matches (i.e., is the

\(^{2}\) See, for example https://support.google.com/business/thread/1858263?hl=en and https://partner.microsoft.com/en-us/marketing/branding
same) as the VMC public key. The email sender organization indicates this alignment via, for example, a policy object identifier (OID).

The user’s email service receives the email from the email sender organization and, upon detecting the feature via the policy OID, verifies the alignment of the VMC public key and the DKIM public key. When the VMC public key and the DKIM public key are aligned (and the VMC is properly authenticated), the email service provides the email to the user with the logo displayed. When the VMC public key and the DKIM public key do not align (i.e., they are not equal), the email service rejects authentication and refuses to display the logo with the message. Additionally, the email service may impose additional penalties upon the message. For example, the email service displays a warning along with the message or hides the message from the user (e.g., places the message in a spam folder).

The solution described may be used for all messages sent using the BIMI standard. The solution provides a use for the currently unused public key associated with a VMC and thus requires minimal impact to current infrastructure. The use of a standard such as BIMI with the proposed solution allows all domain owners interested in ensuring that their logos are displayed correctly to publish brand logos for use with any participating MUA, thus offering more flexibility and scalability than current proprietary solutions.
ABSTRACT

Brand Indicators for Message Identification (BIMI) is a standard that allows domain owners to coordinate with Mail User Agents (MUAs) to display brand-specific indicators or logos next to properly authenticated messages. A Verified Mark Certificate allows an email service to authenticate a logo, but currently BIMI is susceptible to DNS spoofing attacks. In this work, BIMI messages are protected from DNS spoofing by aligning the message’s DomainKeys Identified Mail (DKIM) public key with the public key associated with the VMC. The email service may validate the alignment between the keys as part of the authentication of the message. When the keys match, the email service may display the indicator or logo along with the message. When the keys do not match, the email service may reject the authentication and not display the logo or indicator.