April 09, 2015

Discovering Public Key of Recipient By Email

Weihaw Chuang

Brian Goodman

Nicolas Lidzborski

Jakub Vrana

Discovering Public Key of Recipient By Email

Abstract: Requests and responses to obtain public keys may be sent and received via email. Before sending an email to be encrypted, a requestor may send a request email to the recipient requesting the recipient's public key. The recipient may send a response email to the requestor, with the response email including the public key. The requester may then encrypt subsequent emails according to the received public key and send encrypted emails to the recipient. The recipient may automatically respond to the request for the public key, without need for a user to approve the request.

Information sent via email may be encrypted to protect the contents of the email. One example of encryption is encrypting the information using public keys, such as those associated with X.509 certificate Public-Key Infrastructure (PKI) public keys, which are meant to be publicly distributed and associated with particular recipients, and which can be decrypted only with a corresponding private key that is known only to the recipient. The public keys may be stored in public directory services, and persons or computers desiring to send encrypted information to a particular recipient may retrieve the recipient's public key from the public directory.

However, maintaining a public key in a public directory may notify spammers that an account and/or email address associated with the public key is a "good" or "active" account, assisting spammers in sending spam emails to the good accounts. Spammers may also impose resource burdens on the public directories by repeatedly requesting public keys for possible email addresses to harvest email addresses that do have associated public keys.

To address these drawbacks of maintaining public keys in public directories, it is proposed to use email, such as Simple Mail Transport Protocol (SMTP) email, as a transport mechanism for requests and responses to obtain public keys. A client or server that is about to send an email to a recipient may, before sending the email, send a request email to the recipient requesting the recipient's public key, the recipient may send a response email to the requestor

with the public key, and the client or server may encrypt the email according to the received public key and send the encrypted email to the recipient. The recipient may automatically respond to the request for the public key, without need for a user to approve the request. The recipient may employ safeguards to prevent abuse, such as DomainKeys Identified Mail (DKIM) to ensure that the request email is coming from a trusted domain, and/or one or more spam filters may be used when processing emails on the recipient side.

FIG. 1 is a timing diagram showing actions performed by, and messages sent between, a requester 102 and a responder 104 to enable the requestor 102 to obtain a public key from the responder 104 to encrypt and send an email to the responder 104. The requester 102 may include a computing system such as a client and/or server associated with a first user who wants to send an email to second user associated with the responder 104. The responder 104 may include a computing system such as a client and/or server associated with the second user to whom the first user wants to send the email.

The first user may begin typing an email (106) into the requester 102. The first user may begin typing the email (106) into a web browser-based email program, or an email program locally installed onto the requester 102. During the typing of the email, the first user may type a recipient address (108). The recipient address may include an email address of the second user.

After the first user has typed the recipient address (108), the requester 102 may determine that a key is needed (110) to send an encrypted email to the recipient address. The key that the requester 102 may determine is needed may be a public key, such as an X.509 public key. The requester 102 may determine that the key is needed (110) based, for example, on a policy of sending emails only after encrypting the emails and determining that the requester 102 does not already have the key associated with the recipient address, based on a domain name of the

recipient address, and/or based on a setting of sending only encrypted emails associated with the recipient address.

Based on determining that the key is needed (110), the requester 102 may send a request email 112 to the responder 104. The requester 102 may send the request email 112 to the responder 104 via, for example, SMTP. The request email 112 may request the responder 104 to send the public key associated with the second user to the requester 102 via email, such as via SMTP email.

FIG. 2 is a diagram of the request email 112. The request email 112 may include a header 202 and a body 204. The header 202 may be an SMTP Request for Comments (RFC) 5322 X-header (also known as an experimental header). The X-header may declare the request email 112 as a request to look up information in the responder's 104 service, and/or may enable a fast path with the automated response from the responder 104 by allowing a differentiated automated response service.

The header 202 may include a from field 206 with an email address of the first user, a to field 208 with an email address of the second user, and a request field 210 identifying the request email 112 as a generic request. The request field 210 may include an action subfield 212 identifying the specific action requested by the request email 112, namely the request for the responder 104 to send the public key to the requester 102, an identifier subfield 214 including a number that identifies a thread of the email, and one or more parameter subfields 216 including parameters of the request. The identifier field 214 may be included only if the parameters 214 do not request the response email 214 to be sent to the requester 102 synchronously with the request email 112. The parameters 216 may include, for example, a time by which the requester 102 requests the responder 104 to send a response email 116 (described below) with the public key

before doing some other action, whether the responder 104 should send the response email 116 synchronously or asynchronously, how the responder 104 should encode the response email 116 such as by the American Standard Code for Information Interchange (ASCII), Unicode, or any other encoding format, or other parameters. The body 204 may be empty, may include padding, or may include parameters if the parameters exceed a maximum allowed size of the header 202.

Returning to FIG. 1, the responder 104 may determine whether to respond to the request email 112 (114). The responder 104 may determine whether to respond (114) based, for example, on a domain of the request email 112 which may include authenticating the request email 112 based on a DKIM signature authenticating the domain of the request email, may determine whether to respond (114) based on spam filtering techniques performed on the request email 112, and/or may determine whether to respond (114) by requiring the second user to manually review and approve the first user's email address.

If the responder 104 determines to respond to the request email 112, then the responder 104 may generate and send the response email 116 to the requester 102. The responder 104 may send the response email 116 to the requester 102 via SMTP. The response email 116 may include the public key associated with the recipient address, and may be send in accordance with the parameters 216 included in the header 202 of the request email 112. The response email 116 may include the request email 112, such as in a body 304 (described below) of the response email 116 to include a digital signature of the request email 112. The responder 104 may send the response email 116 to the requester 102 synchronously or asynchronously, which may depend on the parameters 216 included in the request email.

FIG. 3 is a diagram of the response email 116. The response email 116 may include a header 302 and a body 304. The header 302 may include a from field with an email address of

the second user, a to field 308 with an email address of the first user, and a response field 310 identifying the response email 116 as a response to the request email 112 that includes the public key associated with the recipient address. the response field 310 may include an identifier subfield 312 including the same number included in the identifier field 214 of the header 202 of the request email 112 identifying the thread of the request email 112 and response email 116. The identifier field 312 may be included only if the response email 116 is sent asynchronously to the request email 112. The public key 314 associated with the recipient address may be included in the body 304 of the response email 116, or may be included in an attachment of the response email 116 or trailer of the response email 116. The body 304 may include other 316 information, such as a payload and/or padding, and may include the request email 112 including the digital signature of the request email 112.

After and/or while the requester 102 receives the response email 116, the first user may finish the email (118). The first user may finish the email (118) such as by typing the email to completion and clicking ‘send’ or enter another prompt for the requester 102 to send the email to the second user. After the first user finishes the email (118), the requester 102 may encrypt the email (120). The requester 102 may encrypt the email (120) using the public key 314 included in the response email 116 and received from the responder 104. The requester 102 may also store the public key 314 for future use so that the requester 102 does not need to request and/or retrieve the public key 314 again. After encrypting the email (120), the requester 102 may send the encrypted email 122 to the responder 104.

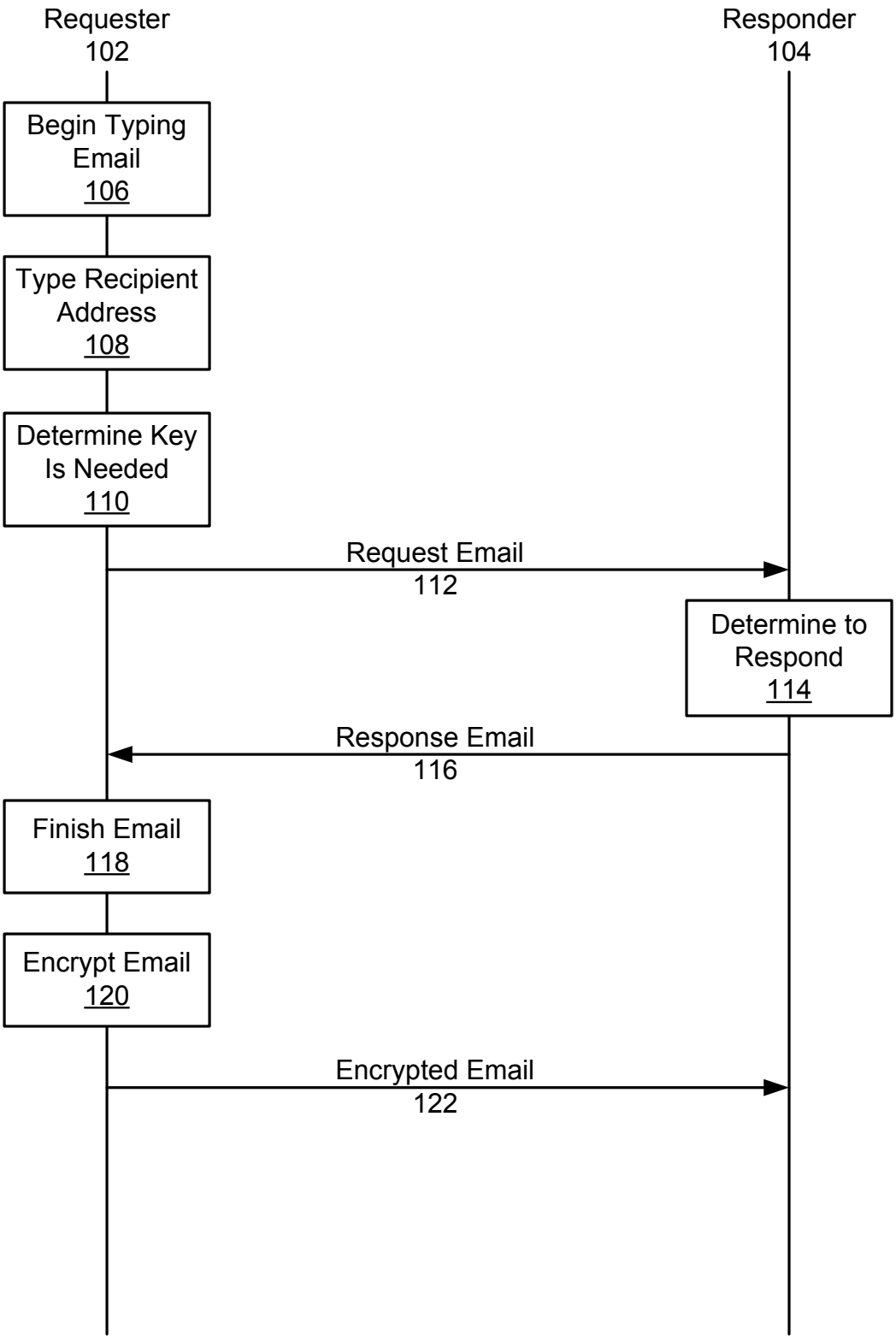
Requester
102
Responder
104
Begin Typing Email
106
Type Recipient Address
108
Determine Key Is Needed
110
Request Email
112
Determine to Respond
114
Response Email
116
Finish Email
118
Encrypt Email
120
Encrypted Email
122

FIG. 1

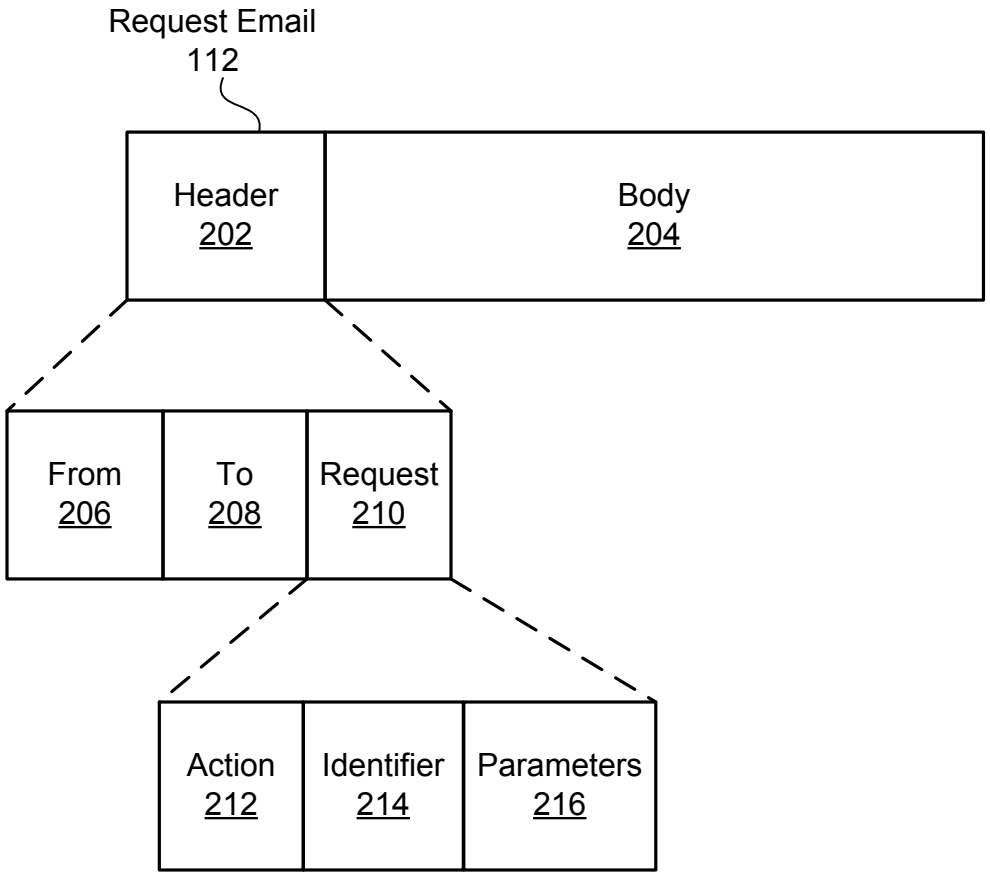
Request Email
112
Header
202
Body
204
From
206
To
208
Request
210
Action
212
Identifier
214
Parameters
216

FIG. 2

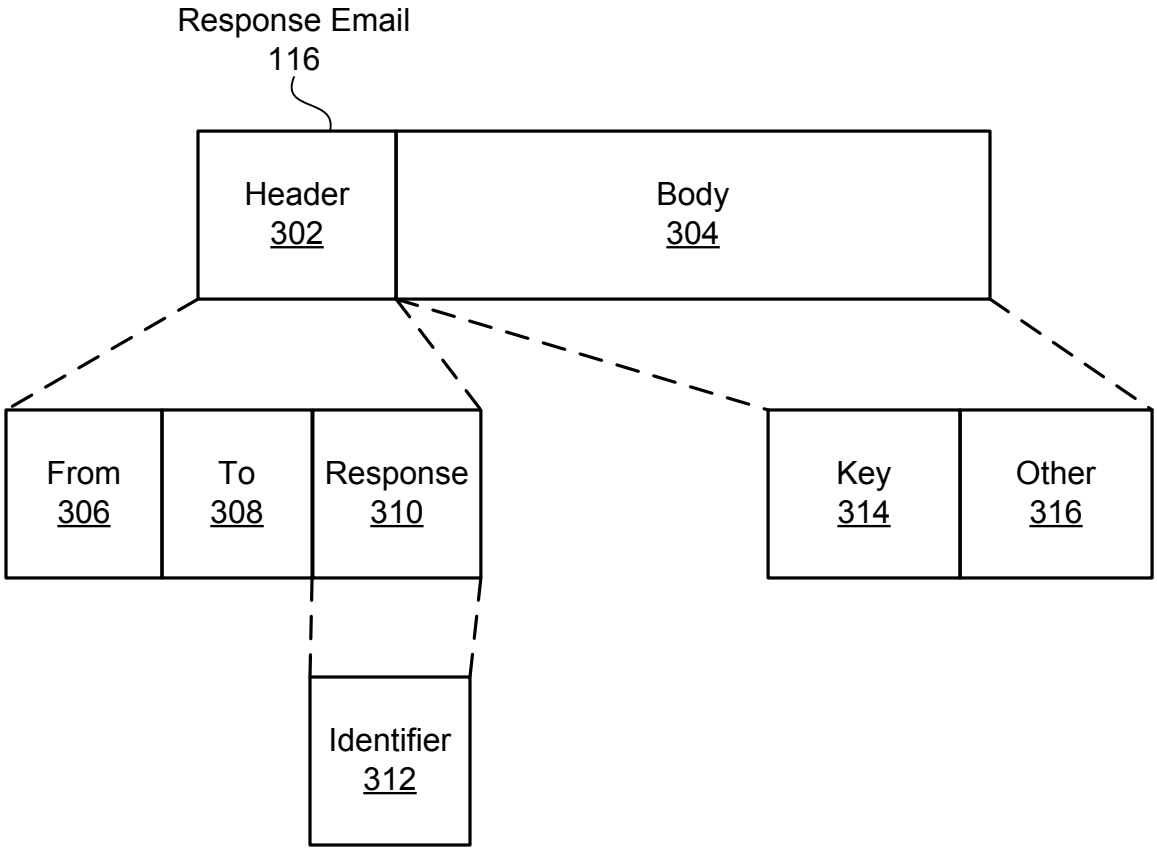
Response Email
116
Header
302
Body
304
From
306
To
308
Response
310
Key
314
Other
316
Identifier
312

FIG. 3