Dmail: A Globally Authenticated Email Service

Michael Cheng Yi Cho, Pokai Chen, and Shiuhpyng Winston Shieh,
National Chiao Tung University

The global public-key authentication infrastructure standardized in the Domain Name System Security Extension (DNSSEC) paves the way for Dmail (DNSSEC-enabled email), a framework that allows secure email address authentication.

Despite its fundamental role as an infrastructure for locating Internet entities and devices worldwide, the Domain Name System (DNS) remains vulnerable to malicious attacks, such as pollution attacks and counterfeit DNS responses. DNS response records aren't immune to forging, nor can their authenticity be fully guaranteed. In 2005, the Internet Engineering Task Force (IETF) took steps to secure the DNS by standardizing the Domain Name System Security Extension (DNSSEC), the global deployment of which has done much to enhance Internet protocol and application security.

For most current email systems, however, security is still, at best, minimal; an email sender field is easily forged and receivers have no way to authenticate an email's origin. This problem is due in large part to the lack of a global public-key infrastructure (PKI). While DNSSEC was designed primarily to authenticate DNS response records, it also offers a vehicle for global public-key exchange. Thus, a DNSSEC-based system for email authentication on various types of devices is now feasible.

Here, we introduce a framework that incorporates DNSSEC to secure email. Called Dmail (for DNSSEC-enabled email), this service has been deployed in both the campus network of the National Chiao Tung University (NCTU) and the Taiwan Ministry of Education network. To our knowledge, Dmail is the first attempt to build such a large-scale email service using DNSSEC.

BACKGROUND

Experts have long been aware that the most widely used email protocols—the Internet Access Message protocol (IMAP), the Post Office Protocol (POP), and the Simple Mail Transfer Protocol (SMTP)—aren't secure, that receipt of counterfeit emails is common, and that unscrupulous users can find ways to eavesdrop over communication channels to spy on email content.

To secure emails, encryption options such as Open Pretty Good Privacy (OpenPGP)[1] and Secure/Multipurpose Internet Mail Extensions (S/MIME)[2] have been proposed. These proposals' primary mechanism for ensuring email confidentiality and integrity, whether sent or received, is through some sort of PKI, which though effective, comes at a considerable cost because it requires a certificate authority (CA) to certify the public keys. Service costs for any trustworthy CA are expensive, and deployment is difficult to scale. Moreover, cross-domain authentication isn't easy due to the current lack of any global PKI: digitally signed emails can't be authenticated across domains.

Because of its existing global infrastructure, the DNSSEC—which the IETF has standardized as the security extension of DNS in three Requests for Comment (RFC 4033,[3] RFC 4034,[4] and RFC 4035[5])—can fill this gap. To summarize the RFCs, DNS records are signed with the private key of a DNSSEC authoritative

0018-9162/14/$31.00 © 2014 IEEE

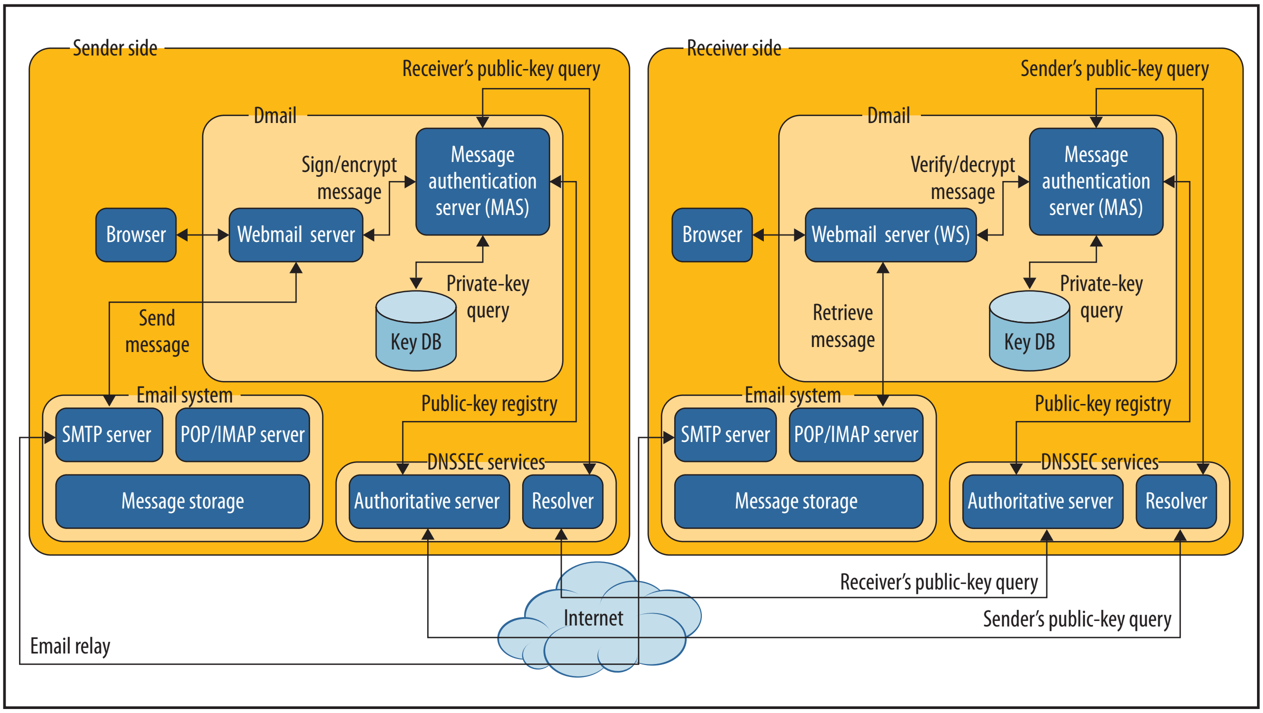

Figure 1. Flowchart of Dmail system interaction. The domain on the right represents the sending party and that on the left the receiving party.

server to ensure the records' authenticity and integrity. This authoritative server's public key is endorsed and signed by its parent server, creating a chain of trust. In the years since the RFCs' 2055 standardization, more than 40,000 domains, including the root and all top-tier domains, have been DNSSEC-enabled. Increasing use of the DNSSEC as a global PKI opens up opportunities for secure email applications to take the advantage of the service.

CHALLENGES FOR A DNSSEC-ENABLED EMAIL SYSTEM

It isn't a trivial matter to incorporate DNSSEC into an existing email service. Redesigning and inserting new code into each of the many different email systems available—such as Web-based Gmail and MS Outlook—to integrate them with DNSSEC requires expending considerable resources and time.

In designing and deploying Dmail, our new authenticated and encrypted email service, we faced several challenges:

- *Compatibility*. It's important that authentication, encryption, and DNSSEC functions be incorporated into existing email systems with minimal disruption and that the additional security functions be fully compatible and interoperable with the existing systems. The fact that an existing email system need not be replaced with a new one enhances the likelihood of user acceptance.
- *Robustness*. It's important to assure that any failure of a new security function doesn't affect conventional email operations. Users can still send and receive emails as usual.
- *Modulation*. All security functions must be modulated with DNSSEC query so that the security function modules can adapt to other email systems and thus reduce porting effects.

DMAIL OVERVIEW

Despite the number of email systems on the market with different user interfaces, they're all required to support the email protocol standards—IMAP, POP, and SMTP. To ensure interoperability with various types of email systems, we chose to design Dmail in compliance with these email protocol standards.

A webmail architecture is ideal for this purpose because it's decoupled from the email system. Failure of the webmail system won't affect email system availability, and a webmail interface is accessible from any type of device, which offers great options for Dmail implementation.

We designed and implemented Dmail as a webmail system operating between conventional email systems and their clients. In this way, Dmail's Web interface can coexist with the original user email interface; a user can choose either interface to access his or her emails. A user can also run any browser—Google Chrome, Internet Explorer, or Firefox, for example—to communicate with Dmail's webmail server. From a user's perspective, Dmail plays a "man-in-the-middle" role, allowing access to both the emails stored on the SMTP servers and the public keys stored on the DNSSEC server.

Users can generate and store their private keys either on the client side or on the Dmail server—a typical tradeoff between security and convenience. To alleviate any burden on naïve users, the second approach is preferred when the Dmail server generates user private/public-key pairs. The user private keys are stored in a domain's key database while the public keys are published in the DNSSEC authoritative server, as Figure 1 shows. The public keys will spread out quickly over the Internet through the DNSSEC trust chain. To access emails, the email client running the browser creates a secure HTTPS tunnel to the Dmail server, and the Dmail server forwards the user ID and password to the SMTP server for user authentication.

Dmail's message authentication server (MAS) encrypts and signs outgoing email and decrypts and verifies received email. To accomplish the twin goals of sending and receiving emails, Dmail relies on standardized email protocols for communicating with the corresponding SMTP server in conventional email systems. To encrypt or verify emails, Dmail's MAS may need to retrieve both the private key in its local key database and the public key in the DNSSEC resolver. If it can't find a public key, the DNSSEC resolver will retrieve it from a remote authoritative server through the DNSSEC trusted chain.

Figure 1 illustrates the sending and receiving processes as they run on Dmail's servers in two domains. In the preparation phase, the sending party (in the domain at the figure's left) must register a public key on the local DNSSEC authoritative server before using the Dmail email signing service. Upon successful registration, the sender can sign the email digest with his or her personal private key, and encrypt the email content along with the signature using a secret block cipher key which is also encrypted using the receiver's public key.

The encrypted email along with the encrypted secret key is then passed on to the local email system for email relay. Upon the email's receipt, the receiving party (shown in the domain at the figure's right) relies on the local email system to retrieve the email. If the received email is encrypted, the MAS on the receiver side will use the recipient's personal private key to decrypt the email content and verify the appended signature using the sender's public key, acquired through his or her local DNSSEC resolver.

DMAIL IMPLEMENTATION AND DEPLOYMENT

Dmail is implemented based on Horde Groupware Webmail Edition, a free browser-based communication suite. We chose Horde because it's popular among users and offers a rich implementation of secure email modules that provide expandability. Horde's basic secure email scheme relies on a certificate database existing in the address book, which stores a list of email users' information as well as the corresponding public key. Whenever an authenticated email is sent or received, Horde queries the address book accordingly for the required public key. Therefore, a DNSSEC lookup function can be inserted whenever address book lookup occurs. This breaks up the operations into two parts:

1. If the user of the required public key *doesn't* exist in the address book, the Dmail module issues a DNSSEC query for the desired public key. If a valid public key is returned in response to the DNSSEC query, the public key is saved in the address book, and the corresponding public key is returned accordingly. Otherwise, no record is saved in the address book, and the Dmail module responds with an invalid public-key message. The user is notified when no public key is found.
2. If the user of the required public key *does* exist in the address book, the Dmail module will still issue a DNSSEC query to ensure the stored public key's freshness. If a valid public key is returned from the DNSSEC query, the Dmail module updates the address book and returns the corresponding public key. Otherwise, the Dmail module removes the public-key field and responds that no public key was found. Again, the user is notified when no public key is found.

As noted earlier, Dmail has been successfully deployed in the NCTU email network, accessing the campus's underlying Gmail service, and is also deployed in the Taiwan Ministry of Education. Future expansion is planned within the Taiwan Academic Network (TANet) consortium.

This year, the IETF began working on enhancements to S/MIME[6] and OpenPGP.[7,8] The mission is to assist email systems in accessing the digital certificates/public keys stored in a DNSSEC server. Once the drafts become standards and the software implementation of the DNSSEC system is updated with the new standards, our DNSSEC-based authenticated email service Dmail can become an official Horde feature available to the Internet community.

Dmail is the first attempt to integrate DNSSEC with conventional email systems to provide email authentication. However, privacy leakage shortcomings are still possible due to poor key management where a key pair or a linked node of the DNSSEC trust chain is compromised. This risk can be reduced if the DNSSEC server is well managed. Despite the possibility of privacy leakage, Dmail significantly improves the security of conventional email systems, and provides a globally authenticated email service to end users.

Acknowledgments

This work is supported in part by the Taiwan Ministry of Education, the National Science Council, TWISC, ITRI, III, iCAST, HTC, D-Link, Trend Micro, Promise, the Chungshan Institute of Science and Technology, the Bureau of Investigation, and Chunghwa Telecomm. We also thank Scott Rose for comments and suggestions that enhanced the content of this article.

References

1. J. Callas et al., “OpenPGP Message Format,” IETF RFC 4880, Nov. 2007; www.ietf.org/rfc/rfc4880.txt.
2. B. Ramsdell and S. Turner, “Secure/Multipurpose Internet Mail Extension (S/MIME) Version 3.2 Message Specification,” IETF RFC 5751, Jan. 2010; http://tools.ietf.org/rfc/rfc5751.txt.
3. R Arends et al., “DNS Security Introduction and Requirements,” IETF RFC 4033, Mar. 2005; www.ietf.org/rfc/rfc4033.txt.
4. R. Arends et al., “Resource Records for the DNS Security Extensions,” IETF RFC 4034, Mar. 2005; www.ietf.org/rfc/rfc4034.txt.
5. R. Arends et al., “Protocol Modifications for the DNS Security Extensions,” IETF RFC 4035, Mar. 2005; www.ietf.org/rfc/rfc4035.txt.
6. P. Hoffman, “Using Secure DNS to Associate Certificates with Domain Names For S/MIME,” IETF Internet draft, work in progress, Feb. 2014; www.ietf.org/id/draft-ietf-dane-smime-06.txt.
7. P. Wouters, “Using DANE to Associate OpenPGP Public Keys with Email Addresses,” IETF Internet draft, work in progress, Feb. 2014; www.ietf.org/id/draft-wouters-dane-openpgp-02.txt.
8. P. Wouters, “Best Common Practice for Using OpenPGPKEY Records,” IETF Internet draft, work in progress, Feb. 2014; www.ietf.org/id/draft-wouters-dane-openpgpkey-usage-00.txt.

***Michael Cheng Yi Cho** is a PhD candidate in the Department of Computer Science at National Chiao Tung University, Hsinchu, Taiwan. Contact him at michcho@ dsns.cs.nctu.edu.tw.*

***Pokai Chen** is a PhD candidate in the Department of Computer Science at National Chiao Tung University, Hsinchu, Taiwan. Contact him at pokai@ dsns.cs.nctu.edu.tw.*

***Shiuhpyng Winston Shieh** is a distinguished professor and past chair of the Department of Computer Science at National Chiao Tung University (NCTU), and director of the Taiwan Information Security Center at NCTU. He is an IEEE Fellow. Contact Shieh at ssp@cs.nctu.edu.tw.*

Editor: Jeffrey Voas, National Institute of Standards and Technology; j.voas@ieee.org