International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Crypto Framed Data Protection for Trusted Aware Email System

Depuri Sandeep Kumar[1], Punugoti Pavan Kumar[2]

[1]Computer Science Engineering, Rise Krishna Sai Prakasam Group of Institutions, Ongole, India

Abstract: ***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 Security challenges have been raised by private and public sectors related to exchange digital data electronically. In the current state, protocols such as the simple mail transfer protocol (SMTP), post office protocol (POP), and internet message access protocol (IMAP) transfer and store email messages in plaintext. Therefore, the confidentiality of email messages cannot be assured. Email sent using these protocols and without using any other security tool, must be assumed to have been read and compromised, because its confidentiality and integrity cannot be assured. Thus in this paper a new approach as a tool for improvement of current popular email protocols is proposed. The novel proposed protocol will be manifested in the Email Security Protocol (ESP) which is designed to add a layer of security and confidentiality to email messages transmitted over unsecured public networks.***

Keywords: Electronic Email, Digital data, Protocol, Security Tool

1. Introduction

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.

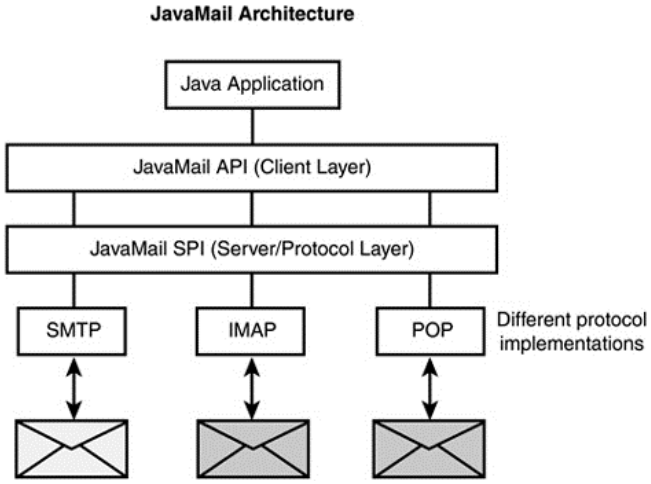
Email has become an integral part of today's digital life. Individual send and receive a vast mass of email messages every day. However, email is one of the most insecure types of communication media. Common configurations of email clients enable attackers to steal user names and passwords used to access email easily. The content of Web-based email not encrypted and is passed in the network in plain text. Messages deleted from an email server might still be retrievable from other servers halfway around the world without owner knowledge. This paper presents email security issues and proposes a new tool on how to improve email systems security.

2. 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 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.



Java Mail API

On the e-mail messaging front, higher level (consumer) developers can shop around for the implementation of the common API framework that best fits their needs -- or even support multiple implementations simultaneously. Lower level implementation providers can develop solutions that ensure efficient access to their mail server products.

One key to developing highly reusable and open API frameworks is to emphasize abstract interfaces in a way that supports existing standards but does not limit future enhancements or alternative implementations. The Java Mail API does just that! Furthermore, Sun is also rapidly developing -- or providing through third parties -- default implementations and utilities for the most commonly available protocols and standards. For example, default implementations such as POP3, SMTP, and IMAP protocol servers are currently available, so you can start developing that award-winning killer app now without having to reinvent the protocol wheel unless you want to (or really need to).

3. 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.

4. ESP Proposed Protocol

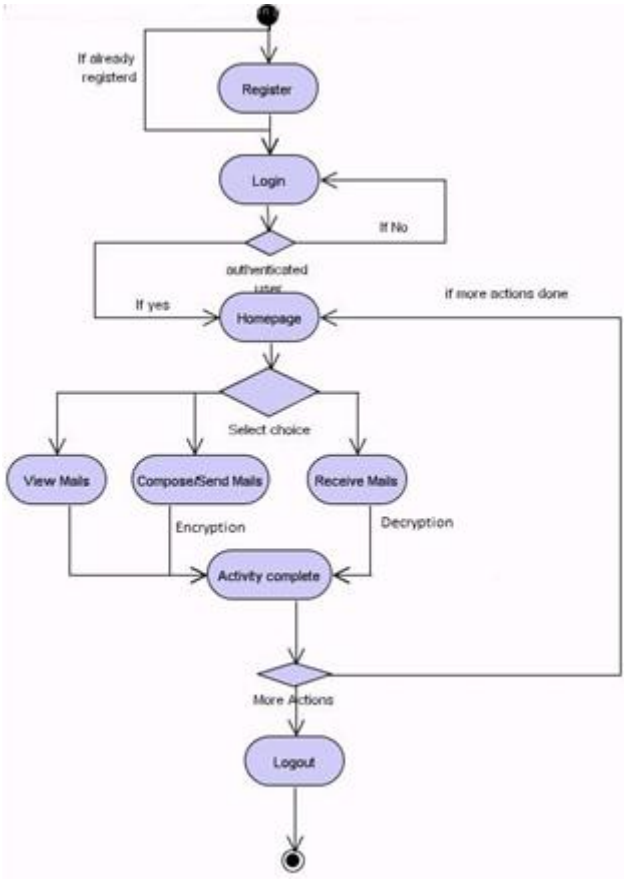
The security problems associated with the SMTP, POP, and IMAP protocols warrants the consideration of a new protocol that would eliminate some of the security risks associated with using these protocols. This protocol would be used for the secure transmission of email from one person to another through a public network (i.e., internet). Furthermore, this protocol is shown to protect the confidentiality of email that travels from one SMTP server to another while on its way to its intended recipient.

The proposed name for this protocol is the email security protocol (ESP). Its purpose is to add a layer of security and confidentiality to email in which it is used. The ESP is configured and implemented in an email program so that its functions are carried out automatically with minimal interaction with the user being required.

4.1. ESP Architecture

The Email Security Protocol (ESP) is designed in three models to allow efficient and effective implementation upon various information system architectures. Model I is designed based on a single server architecture which will process the encryption and the decryption procedures. It would be good on a network system isolated from the internet. The main feature of this model is that the email would stay encrypted on the server until the recipient decided to retrieve them. The email would thus be secure while being stored on the server. This model could also be used in a simulation in a computer laboratory; especially if the number of available servers for research is limited.

An advantage of the ESP is the ease of use for the end users. For example, in an organization that has a local area network (LAN) administered by information technology (IT) personnel, the IT staff can install and configure the ESP as needed, depending on the model used (I, II, or III), on the required computers, workstations, and servers that make up the LAN. Once the ESP is properly configured, users can send and receive email as they normally would and have the assurance that their email will be (1) securely (encrypted) stored on the server until retrieved by the intended recipient, (2) securely transmitted from one ESP configured server to another (e.g., one corporate office to another), or (3) securely transmitted from one ESP configured computer to another.



5. Conclusion and Future Research

It has been shown that the new proposed protocol (ESP) would be an enhancement and great email security tool to preserve the confidentiality of email messages in transit over the internet. Furthermore, it is evident that it provides a high degree of security which includes email securely stored on a server. Our future research is to investigate the ESP in depth using a large scale of data and advance it to eliminate any drawback.

References

[1] A 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.

Author Profile

Depuri. Sandeep Kumar Obtained the B.Tech. degree in Information Technology(IT) from Prakasam Engineering College, Kandukur. At present persuing the M.Tech in Computer Science and Engineering (CSE) Department at Rise Krishna Sai Prakasam Group Of Institutions,Valluru.

Punugoti. Pavan Kumar obtained the B.Tech Degree in Computer Science and Engineering from Prakasam Engineering College, Kandukur in 2006 and M.Tech from Acharya Najarjuna University in 2010..He has 5 years of Teaching Experience and working in Computer Science and Engineering(CSE) Department at Rise Krishna Sai Gandhi Group Of Institutions, Valluru.