Abstract

Spammers have a tremendous financial incentive to compromise user Email accounts. Many approaches to curb spam have been developed. In the traditional DKIM signature approach no Certificate Authority is used. Survey tells that most of the DNS are exploited to DNS cache poisoning attack. Further smaller keys are exposed to Wiener attack. Also DKIM does not verify the author and does not provide security after signature generation/verification. An attacker can be able to trick the recipient by masquerading as a legitimate sender and insert malicious information and send as spam Mails to other recipients. Therefore this paper addresses the issues by allowing sender to indicate that their emails are signed and encrypted using ID based mediated RSAA technique based on user identity. This system use Certificate Authority and a key Mediator in its architecture. During decryption the Key mediator does partial decryption and the recipient does full decryption of message. If original message is recovered and verified the sender message is accepted else rejected or blocked as spam message.
Spam Control Mechanism using Identity based Message Admission

- Meng Wong and Wayne Schlitt. Rfc 4408 - sender policy framework (spf) for authorizing use of domains in e-mail, version 1, April 2006.
- D. Eastlake 3rd; Motorola; RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS); Request for Comments: 3110; May 2001;
- J. Jonsson, B. Kaliski; RSA Laboratories; Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1; Request for Comments: 3447; February 2003.
- Johannes Blomer, Alexander May; A Generalized Wiener Attack on RSA.
- Sooel Son and Vitaly Shmatikov, The Hitchhiker’s Guide to DNS Cache Poisoning,
- M. Kutylowski, P. Kubiak; M. Tabor, D. Wachnik; Mediated RSA cryptography specification for additive private key splitting (mRSAA); Internet Draft; November 14, 2011.
- Jean Claude Bajard, Heinrich Hördegen; Pseudo-Random Generator Based on Chinese
Remainder Theorem; Advanced Signal Processing Algorithms, Architectures, and Implementations XIX, San-Diego; 2009.

Index Terms

Computer Science  Communications

Keywords

Spam control  DKIM  Wiener attack  DNS cache poisoning  and Identity based mediated-RSAA