iSATS: Leveraging Identity based Sender Authentication for Spam Mitigation

Sufian Hameed, Tobias Kloht and Xiaoming Fu
Computer Network Group, University of Göttingen, Göttingen, Germany

Keywords: Email Sender Authentication, Spam Prevention, Identity based Cryptography.

Abstract: A vast majority of spam emails today are sent from botnets with forged sender addresses. This has attracted researchers over the years to develop email sender authentication mechanism as a promising way to verify identity of the senders. In this paper we introduce *iSATS*, a new email sender authentication system based on Identity-based public key cryptography. *iSATS* leverages an identity based signature scheme to provide a reliable and easy way to bind the identity of legitimate sender to an email. Unlike the popular existing solutions like SPF and DKIM, it is hard for the spammer to adopt *iSATS*.

1 INTRODUCTION

Spam is still a largely unsolved problem that has outnumbered legitimate emails with big scores. Spam has already reached around 89.1% of total emails (Pingdom, 2011) i.e. 262 billion spam emails/day, increasing from 65% (MessageLabs, 2005) in 2005 and it is projected to cost $338 billion by 2013 (RedCondor, 2011). Email infrastructure was originally not designed to verify the authenticity of a sender address/identity. This weakness is greatly exploited by zombie networks or botnets to send spam/phishing messages with forged addresses. It is well-known fact that the majority of spam messages today - 88.2% (Symantec, 2010) of the total spam according to some estimates - are sent by botnets using forged addresses.

Email sender authentication mechanisms enable receivers to automatically distinguish forgeries from authentic messages. Over the years several sender authentication protocols have been proposed, out of which Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) are the most adopted ones.

SPF (Wong and Schlitt, 2006) is an IP-based sender authentication scheme that operates on SMTP envelope (*MAIL FROM*) to block forgeries at SMTP time. SPF allows the domain administrators to publish the IPs or range of IPs for their valid server(s) on DNS in simple text format referred to as SPF record. When the email exchange begins, the receiving side can query the DNS for sender's SPF record to validate if sender's IP is listed in the address range specified by the sender's domain. According to (Mori et al., 2011), SPF is the most adopted sender authentication scheme and over 60% of the prominent domains have published their SPF record as of July 2011. However, due to its simplicity, SPF is also easily adopted by spammers. According to (Mori et al., 2011) 20+% of spamming domains have already adopted SPF. If the majority of spamming domains will adopt SPF over time, SPF would become useless. (Mori et al., 2011) also show that significant amount of spams are successfully authenticated by SPF and on the other hand around 5+% of legitimate messages can potentially fail SPF tests. Message forwarding is also a limitation for IP-based SPF. Unless the return path is edited during forwarding, the receiver will treat the message as forgery for not coming directly from its listed sender.

DKIM (Allman et al., 2007) signs the email headers and body using public-key cryptography, and append the signature in a *DomainKey-Signature* header. The signature keys are bind to a domain name and the domain admins publish the public-key in the DNS. The receiver can query the DNS to extract the public-key of the sender and verify the signature. A successful verification implicates that the message content was not forged during the transmission and the message is actually from the sender responsible for it.

In DKIM, the signature can only be evaluated after the entire message content is received, thus, it is not possible to reject spam at earlier stages or during SMTP time. DKIM is prone to content munging and if the message content is altered during transit, DKIM will fail. DKIM cannot evaluate the trustworthiness

Hameed S., Kloht T. and Fu X..
iSATS: Leveraging Identity based Sender Authentication for Spam Mitigation.
DOI: 10.5220/0004078404080411
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 408-411
ISBN: 978-989-8565-24-2

of a sender and the spammers can also adopt it to sign their own messages. However, (Taylor, 2006) shows that only 2% of spam received are authenticated by DKIM, which is significantly less than the spam authenticated by SPF.

In *iSATS*, we introduce a new email sender authentication system that is based on identity based public key cryptography (IBC) (Shamir, 1985). With IBC a private key generator (PKG) or a trusted authority (TA) is responsible for generating a secret key (SK) against the identity of the domain used as public key i.e. the TA is also responsible to thoroughly verify the identity of a domain before issuing SK. This verification strongly binds the identity of the domain owner to its domain and makes it hard for the spammer to adopt *iSATS*, unless they are willing to give away their identity.

iSATS requires the sender's Mail Transfer Agent (MTA) to generate a signature using SK of the domain and append it along with SMTP envelop (*MAIL FROM*). This enables the recipient's MTA to quickly authenticate the sender by verifying the appended signature. Any invalid connection is terminated right away, saving valuable resources both at the MTA and in the network. Finally, email forwarding and munging of message along the transit is not a problem in *iSATS*.

2 *iSATS* DESIGN

iSATS is a crypto-based email sender authentication system that operates on the SMTP envelop, in particular on *MAIL FROM* command, to perform domain level authentication during the SMTP time. *iSATS* leverages identity based signature (IBS) using identity-based public key cryptography (IBC) (Cocks, 2001; Boneh and Franklin, 2001) to authenticate the identity of an email sender. Compared to traditional public key cryptography, IBC saves the burden of managing and distributing the public keys, since publicly available unique identities are used as public keys. *iSATS* requires establishment of a trusted authority (TA) also known as private key generator (PKG), responsible for issuing secret key (SK) and system parameters. The TA is also responsible to verify the identity of a domain before issuing the SK.

2.1 Basic Requirement

At the outset, we seek a solution that works well with the current, entrenched system. This means that the system should:

- Work as an optional addition to standard mail clients or servers, and continue to support popular means of accessing mail (e.g. IMAP/POP/Webmail).
- Be incrementally deployable.
- Remains transparent to end users.

The functionality of *iSATS* can be divided into four steps: 1) setup, 2) identity verification and secret key extraction, 3) signature generation and 4) signature verification, discussed in the upcoming sections.

2.2 Setup

This step is executed once in the beginning and marks the creation of a whole IBC environment by a TA. The setup results in generation of Master Key and System Parameters. Master key is kept secret by the TA and it is used to generate SK for the domain based on their identity. System parameters are publicly available.

2.3 Identity Verification and Secret Key Extraction

This step is initiated when any domain wants to become part of *iSATS* and requests a SK (see Figure 1). *iSATS* represents a closed system, in a sense that domains are not automatically added to the system but the TA verifies their identity first. *iSATS* is envisioned to provide extended validation of the domain's identity. Identity verification with Extended Validation (EVC, 2009) provides high-security information to clearly identify a domain's organizational identity. This will help bind the owner's identity to the identity of the domain and will make misbehaving domains visible. Most well-known webmail providers and websites tend to have SSL certificates with extended verification, so this requirement is not excessive.

After identity verification, the TA will issue system parameters and a SK corresponding to the domain name which is also its identity. This meets the requirements of the system, as the domain name is a unique identity for the domain and is publicly available to all parties.

2.4 Signature Generation

This step is executed when a user wishes to send an email. The MTA will generate a signature on the sending user's email address (e.g. alice@example.com) using the SK and system parameters of the domain. After doing this, the signature is appended to *MAIL FROM* command as an additional

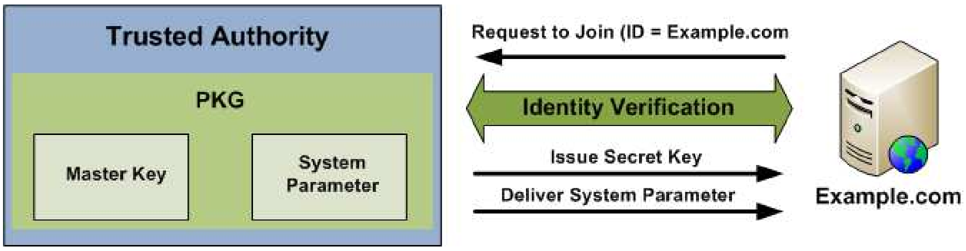

Figure 1: The process of domain joining iSATS.

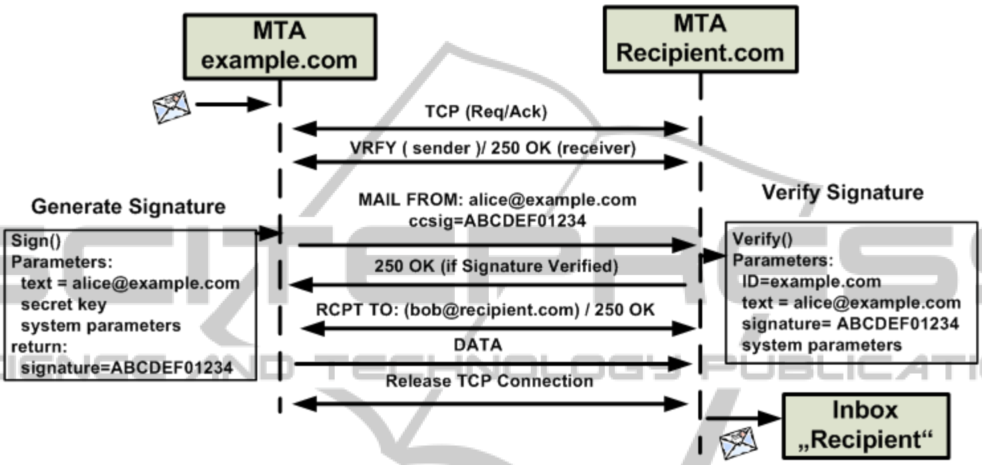

Figure 2: Email Processing with iSATS.

parameter (see Figure 2). The use of additional parameters in *MAIL FROM* is allowed and in line with the current SMTP specifications (Klensin, 2008).

2.5 Signature Verification

On receiving the *MAIL FROM* command, the MTA on the receiving side will verify the signature. For verification the MTA will use the public system parameters, signature (extracted from *MAIL FROM*), signed text i.e. sending users email address from *MAIL FROM* and the domain name of the sender as the public key (see Figure 2). The entire verification process is completed before replying to *MAIL FROM*, which give recipients the option to reject the message before its content is sent.

2.6 Discussion

2.6.1 Email Forwarding

In email forwarding, it is a common practice not to change the return path or *MAIL FROM* message envelop. This is an Achilles heel in IP-based SPF (Wong, 2005), but for *iSATS* message forwarding is not a problem as long as MAIL FROM command remains intact.

2.6.2 Message Munging

iSATS does not operate on the content of an email. If the content of the message is altered during transit by a mailing list (which is a common practice) it will have no effect on *iSATS*, unlike DKIM (Wong, 2005).

2.6.3 Security of TA

In *iSATS*, the security of the TA is very crucial and if an attacker is able to obtain the TA's master key, he would be able to issue SKs and generate valid signatures. It is synonymous to securing any Certification Authority (like VeriSign) for the legitimacy of the issued certificates. In order to secure central TA, Boneh and Franklin (Boneh and Franklin, 2001) introduce a concept for distributing the TA (PKG) in such a manner that the master key is distributed over a set of nodes, so that each node has no information over the key itself. Domains can extract their SK by obtaining partial keys from a subset of these nodes, where the subset must be bigger than a certain threshold. This kind of distribution will also help in minimizing the effect of DDoS attacks, which is still an open problem. Further discussion of the security of the TA is beyond the scope of this paper and we will consider it as part of future work.

2.6.4 Attack on Secret Key of Domain

Protection of SK is the responsibility of the MTA or Domain. Attacks related to key thefts are synonymous to hacking the domain and the corresponding defense mechanisms are beyond the scope of this paper. Hence we have left the discussion on key theft and revocation mechanisms as future work.

2.6.5 Signature Reuse or Misuse

In order to avoid reuse or misuse of signature by a potential attacker we recommend using a unique signature for each message. This can be done easily by using a nonce (a unique number used only once) and instead of just signing the sender's email id the MTA can sign email ID + nonce. The nonce can be composed of time stamp value, message ID or a combination of both. With this the new *MAIL FROM* will be something like this, *MAIL FROM*: <alice@example.com>, ccsig = Sign (alice@example.com + nonce), nonce.

2.6.6 Sender Reputation

Email sender authentication systems only authenticate the identity of the email senders at the domain level. For the legitimacy of the domain it is recommended that each domain maintain local reputation for the domains sending emails. As part of future work, sender reputation can also be centralized at the TA level, based on the feedback of individual legitimate domains.

Nowadays, it is also a common practice in legitimate domains, ISPs and major web-mail providers to run bot detectors against non-human automatic account creation and impose an email sending limit between 100 to 1000 recipients/day (EmailLimit, 2010).

3 CONCLUSIONS

We introduce *iSATS*, a new email sender authentication system that leverages identity based signatures for stronger sender authenticity than existing solutions. With the help of a trusted authority, *iSATS* forms a closed system that provides a reliable and easy way to bind the identity of a legitimate sender to an email. On the other hand, it is hard for the spammer to adopt the system without getting noticed. Further, *iSATS* operates on email envelope, specifically on *MAIL FROM* command, which makes it easy to reject spam before receiving the actual content.

REFERENCES

Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and Thomas, M. (2007). Domainkeys identified mail (dkim). RFC 4871.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO 2001*, Lecture Notes in Computer Science, pages 213–229. Springer Berlin / Heidelberg.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *Cryptography and Coding*, Lecture Notes in Computer Science, pages 360–363. Springer Berlin / Heidelberg.

EmailLimit (2010). Email address limit in webmail by providers. http://www.emailaddressmanager.com/tips/email-address-limit.html.

EVC (2009). Guidelines for the issuance and management of extended validation certificates. CA/Browser Forum Version 1.2.

Klensin, J. (2008). Simple mail transfer protocol. The Internet Society, RFC 5321.

MessageLabs (2005). Messagelabs intelligence report: Spam intercepts timeline. http://www.messagelabs.co.uk/.

Mori, T., Sato, K., Takahashi, Y., and Ishibashi, K. (2011). How is e-mail sender authentication used and misused? In Proceedings of CEAS '11.

Pingdom (2011). Internet 2010 in numbers. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

RedCondor (2011). Tracking the high cost of spam. http://www.redcondor.com/company/.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *Advances in cryptology*, pages 47–53. Springer.

Symantec (2010). 2010 annual security report.

Taylor, B. (2006). Sender reputation in a large webmail service. In *CEAS*.

Wong, M. and Schlitt, W. (2006). Sender policy framework (spf). RFC 4408.

Wong, M. W. (2005). Sender authentication: What to do. http://spf.pobox.com/whitepaper.pdf.