iSATS: Leveraging Identity Based Sender Authentication for Spam Mitigation

Sufian Hameed, Tobias Kloht, Xiaoming Fu
Computer Network Group, University of Göttingen, Göttingen, Germany
{sufian.hameed, fu}@cs.uni-goettingen.de, tobias.kloht@stud.uni-goettingen.de

Introduction

Spam
- In 2010, 89% of the emails were spam (262 billion spam messages daily) [1].
- Projections show that spam will incur a cost of $338 billion by 2013 [2].

Why Spam Works
- SMTP was originally not designed to verify authenticity of a sender address. Therefore, exploited MTAs (i.e., botnets) are used with forged From: addresses.
- 88.2% of the total spam are sent by botnets using forged addresses [3].
- Marginal or no infrastructural cost
- No ownership, spammer remains anonymous, hence no action legal action possible

Email Sender Authentication

- Email sender authentication mechanisms enable receivers to automatically distinguish from address forgeries from authentic messages.
- Several sender authentication protocols have been proposed, out of which Sender Policy Framework (SPF) [4] and Domain Key Identified Mail (DKIM) [5] are the most adopted ones.

Sender Policy Framework (SPF)
- SPF is an IP-based sender authentication
- Operates on SMTP Envelope
- Allows domain admins to publish IP(s) for their valid servers as SPF record.
- The receiving side can query the DNS to validate the sender’s IP.
- Most Adopted (60% of prominent domains)

Problems
- SPF is also easily adopted by Spammers
- 20% of Spamming domains already adopted SPF
- 5% of legitimate messages can potentially fail SPF test
- Message forwarding is also a limitation

Domain Key Identified Mail (DKIM)
- Header Based Approach (default work at SMTP time) RFC 4871
- Defines a new RFC5322 message header field
- Defines a domain level digital signature authentication
- MTAs sign all the outgoing mail (email header, body, etc)
- Use Public key cryptography
- DNS are used as key server technology (public keys are publish on the DNS)
- Receiver query the DNS for public key to verify the signature

DKIM-Signature: a=rsa-sha1; q=dns;
   d=dns.example.com;
   s=jam2005.eng;
c=relaxed/simple;
t=1171794938;
  h=From:;To:;subject:date; 
  b=daTvYfAKeCdxzJFoC9z29QuLiXS8rk118b
   av=yu04szEr0012zEvO48HHHyrsR

Problem
- Spam Transmission: signature can only be validated after the entire message content is received.
- Prone to content mangling (common problem with lists)
- Spammer can also adopt it to sign their messages.

Goal of iSATS
- Email Sender Authentication at the SMTP time
- Bind the identity of the domain owner to its domain and make it hard for the spammer to adopt iSATS.

iSATS
- Crypto based sender authentication
- Leverages Identity-based signature (IBS) under Identity-based cryptography (IBC)
- IBC saves the burden of PKI required for managing and distributing public keys.
- Require establishment of Trusted Authority (TA) also called Public Key Generator (PKG)
- PKG issues Secret Key (SK) and System Parameters
- TA is responsible for verifying the identity of a domain before issuing the SK.

ISATS: Four Functional Steps

1. Setup
- Executed once in the beginning by TA/PKG
- Generate Master Key and System Parameters

2. Identity Verification and SK Extraction
- ISATS is a closed system and domains are not added automatically.
- TA verifies the identity of the domain. TA is envisioned to provide extended validation (organizational identity) for domain’s identity.
- TA issues system parameters and SK

3. Signature Generation
- MTA generates Signature
- Append with MAILFROM

4. Signature Verification
- Extract Signature
- Verify Signature

Prototype

The basic prototype implementation includes:
- Server Implementation for TA
- System setup
- Extraction and distribution of SK
- iSATS based email processing
- Signature generation and verification

The prototype utilized
- Cha-Cheon IBS scheme [6]
- Mail Avenger (SMTP Daemon)
- Postfix (MTA)
- Mutt email client

Conclusion

- Introduced iSATS, a new crypto-based email sender authentication scheme.
- iSATS forms a closed system that provide reliable and easy ways to bind identity of a legitimate sender.
- On the other hand, it is hard for the spammer to adopt the system without getting noticed.

Selected References