Софийски Университет
"Св. Климент Охридски"

Използване на DKIM при защита от SPAM

(DKIM - DomainKeys Identified Mail)

Веселин Колев

Софийски Университет
"Св. Климент Охридски"

Domain-Keys Identified Mail
като технология

Особености на DKIM:

- удостоверяват се предимно стойностите на стандартни полета в заглавната част на писмата, чрез подписването им;
- информацията за използваните подписващи ключове, източника на доверие, списъка на подписваните полета и електронния подпис върху тях и др., се прибавят като стойности на ново поле в заглавната част на писмата - "`DKIM-Signature`";
- прибавеното поле не е част от декларираните в SMTP полета и прочита и прибавянето му изискват съответна приставка.

Пример за DKIM подписана заглавна част на писмо

```
Return-Path: <test@vesselin.org>
Received: from test.host (test.host [192.168.12.1])
      by tls-smtp.lcpe.uni-sofia.bg (8.13.8/8.13.8) with ESMTP id n0CJekpU024592
      for <collector@vesselin.org>; Mon, 12 Jan 2009 21:40:47 +0200
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=vesselin.org; s=dec2008;
        h=domainkey-signature:received:message-id:date:from:to
         :subject:mime-version:content-type;
        bh=m5Ma89AFuXo6QapH/sdSPBa2+uH74jJgpIfdnIotXII=;
        b=KM9Lckxlah4Yi31mSJakGTCcw79+F/NuCENqL7DSslgcLl9IK7nHckr4ra6O8ylVdZ
         d7ZlcXcXfB41je6C409io3CAPIbgkizJRYCD0=
Received: from 192.168.100.1
        (SquirrelMail authenticated user test@vesselin.org)
        by vesselin.org with HTTP;
        Mon, 12 Jan 2009 21:40:45 +0200 (EET)
Message-ID: <46395.192.168.100.1.1232396440.squirrel@vesselin.org>
Date: Mon, 12 Jan 2009 21:40:44 +0200 (EET)
From: test@vesselin.org
To: collector@vesselin.org
Subject: Test Message
MIME-Version: 1.0
Content-Type: text/plain;charset=utf-8
```

Използвани криптографски алгоритми за подписване и хеш-функции:

- **подписващ алгоритъм: RSA с дължина на подписващия ключ от 512 до 2048 бита (възможно е използване и на 4096 битови ключове);**
- **хеш-фунцкии: SHA1, SHA256;**
- **използвани дължини на ключове и комбинации от алгоритъм за подписване и хеш-функция:**
  - **rsa-sha1** ***(непрепоръчително)***
  - **rsa-sha256** ***(препоръчително)***

Съхраняване на публичните RSA ключове в DNS зона

- всеки ключ се съхранява като TXT ресурсен запис с ресурсно име:

```
dec2008._domainkey.vesselin.org. 291 IN TXT "k=rsa\; t=y\;
                p=MIGfMA0DDSqGSIb3DQEBAQUAA4GNADCBiQKBgQ
                DihyR3oItOy22ZOaBrIVe9m/iME3RqOJeasANSpg
                2YTHTYV+XVA4xwf5gTjCmHQEMOs0qYu0FYiNQ35o
                gJ2t0Mfx934u06rfRBDjiIU9tpx2T+NGlWZ8qhbi
                Lo5By8apQuiMLyqTLavyPSrvsx0B3YzC63T4ge2CD
                qZYA+OwSMWQIDAQAB"
```

- в една зона на домейн може да има произволен брой ключове, с различни ресурсни имена.

Схема да действие на DKIM на ниво SMTP сървъри:

- изпращащият SMTP сървър, поставя електронен подпис върху тези полета на писмата, които са описания в политиката за използване на DKIM като подписваеми;
- приемащият писмото SMTP сървър извлича публичния ключ от зоната на домейна, отбелязана в “DKIM-Signature” полето и проверява електронния подпис над подписаните писма;
- при успешна проверка на подписа, приемащия SMTP сървър следва уточнената за такъв случай политика.

Софийски Университет
"Св. Климент Охридски"

Взаимодействие между DKIM и DNSSEC

Удостоверяване на DKIM ключове чрез DNSSEC

- подписването на TXT ресурсния запис, съдържащ DKIM публичния ключ, предотвратява подмяната му при пренос по мрежата и кеширане;
- ако използваната DNSSEC йерархия е удостоверена от всички участници в DKIM подписването и проверката, DKIM ключовете стават част от нея, ако SMTP сървърите използват резолвери с DNSSEC валидация;

Статус на DKIM при подписване на "." зоната:

- DNSSEC ще се превърне в DNS базирана PKI и ще делегира транзитивно доверие върху включени в зоните ключове;
- DKIM публичните ключове, съхранявани като TXT ресурсни записи, ще могат да се разглеждат като делегирани ключове (псевдосертификати – без мета информация);
- DKIM ще може да престане да бъде система използваща самоподписване без йерархична проверка и няма да бъде уязвима към подмяна на ключовете при пренос и кеширане.

Предимства и недостатъци на DKIM

(сравнение с други анти-SPAM технологии)

Предимства на DKIM

- DKIM полетата предоставят удостоверителна информация, използваема от филтри на съдържание, за извършването на възможно най-селективна “blacklist” и “whitelist” филтрация (напр. от SpamAssassin);
- DKIM е най-добрият начин за разкирване на “phishing”-атаки;
- позволява следване на антиспам политики в дълбочина – от SMTP сървър, през IMAP сървъри до пощенски клиенти (дори web базирани);
- Изпращачите получават стимул да използват DKIM.

Недостатъци на DKIM:

- подписването и проверката на електронния подпис са времеемки и енергоемки (относителен ефект – зависим от натоварване и хардуерна конфигурация) – възможност за DoS атака;
- не е възможно подписването на “return-path” полето в заглавната част, чиято стойност е важна (конструктивна особеност).

Софийски Университет
"Св. Климент Охридски"

Софтуер и документация, свързани с DKIM

(свободен софтуер и софтуер с отворен код)

- страница за координация на проекта (документация, презентации, връзки към софтуерни проекти):

  http://www.dkim.org/

- milter за Sendmail и Postfix:

  http://sourceforge.net/projects/dkim-milter/

Софийски Университет
"Св. Климент Охридски"

Възможности за сътрудничество и обмен на опит при внедряване и използване на DKIM в БИОМ

- **семинари за обучение за работа с DKIM и изграждане на DKIM базирани пощенски услуги – предаване на опит от страна на СУ;**
- **обмен на опит в рамките на уеб семинари и публикации между участниците в БИОМ, които вече са внедрили решението;**
- **създаване на trac система, за помощ при отстраняване на инциденти или технически проблеми, свързани с DKIM.**