SPF classic

Przemek Jaroszewski

CERT Polska / NASK

The 17th TF-CSIRT and FIRST joint Event, Amsterdam, 23-25 January 2006

ZMYSŁ TELEKOMUNIKACJI

NASK

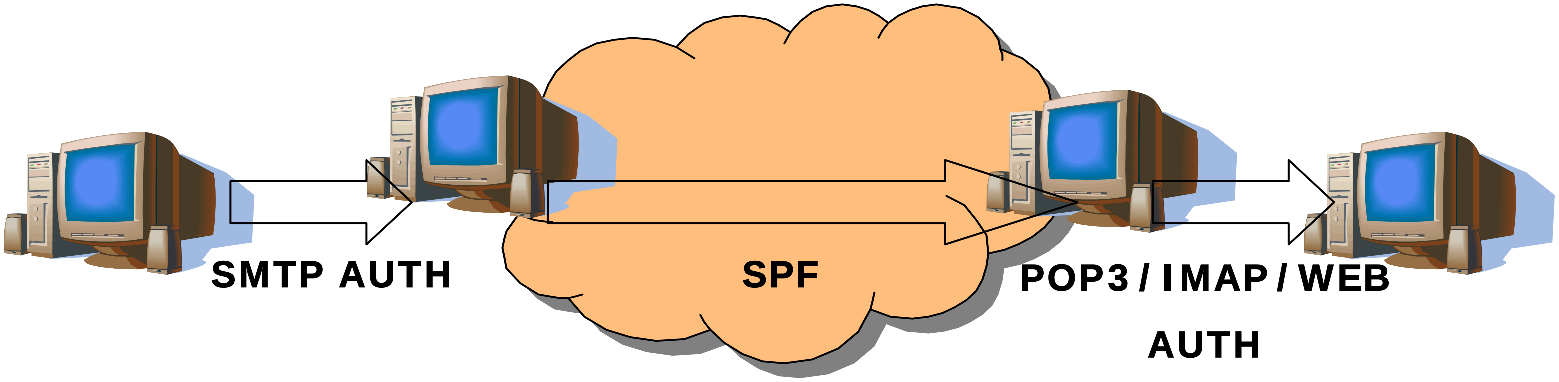
CERT POLSKA

Agenda

- What is SPF and how does it work?
- History and current status
- Mitigations and limitations
- Implementation guidelines
- Implementation examples
- Security considerations

Basic facts about SPF

- SPF stands for "Sender Policy Framework" (originally "Sender Permitted From")
- It is an anti-forgery, and not, as sometimes misunderstood, an anti-spam mechanism
- Allows mail servers/MUAs to determine whether a connecting host is authorised to speak on behalf of a given domain
- Uses DNS, working tranparently over SMTP
- Requires implementation on both sending and receiving side to be fully usable, but nothing is broken when either is missing



History and current status

- In **June 2003** the RMX (Reverse-MX) and DMP specifications were merged along with various programmers' suggestions. Large number of changes were made afterwards. The outcome of this work was SPF, now sometimes called SPF classic.
- In **early 2004**, the IETF created the **MARID** (MTA Authentication Records in DNS) working group and used SPF and Microsoft's CallerID proposal as the basis for the **Sender ID** protocol. Ultimately, Sender ID was primarily SPF with many incompatible changes. What remained of CallerID, as well as other disputed issues, caused the working group to be closed without advancing any standards. After the MARID working group was closed, **the SPF community returned to the original "classic" version of the specification**.
- In **July 2005** SPF specification was accepted by the IETF as an **experimental protocol** and will likely become an RFC in 2006.
- **Wide acceptance** and deployment of SPF in 2005, especially by major players (e.g. AOL, Hotmail, Google, EBay, Amazon.com) made it already a **de-facto standard**.

How does it work?

- **During SMTP dialog, SPF-aware server asks sender's domain for an SPF record (via DNS query).**
- **Data received from the host is checked against the SPF record**
  - MAIL FROM identity (→ Reverse-Path) is a MUST
  - checking HELO indentity is recommended in addition
  - From: header is outside the scope of the protocol
- **Depending on the record's content and the address of the host which is trying to send a message, one of the following results is achieved:**
  - Pass – the host is authorised by the domain to send its e-mail
  - Fail – the domain forbids the host to send its e-mail
  - SoftFail – the domain believes the host isn't authorized but isn't willing to make that strong of a statement
  - Neutral – the domain owner explicitely states that they cannot or do not want to assert whether the IP is authorised or not
  - None – no SPF record found or no checkable sender's domain found
  - TempError – a transient error while verifying the SPF record
  - PermError – the SPF record could not be correctly interpreted
- **It is up to receiving software to determine what action should be taken, depending on the result.**
- **SPF describes standard Received-SPF email header.**

What is fixed?

- **Worm / Virus propagation** – malware with own SMTP engine cannot work from individual workstations
- **Spam** (in some way) – sender’s address forgery is much harder (yet not impossible)
- **Phishing** – limited mitigation since users will rely on From headers anyway
- **Forgery backscatter** – no NDRs from SPF-aware networks (major free e-mail account providers are included ☺)

What is not fixed (or gets broken)?

- **SPF is not a user authentication mechanism (a feature, not a bug)**
- **Multi-domain hosting**
  - Imposes risk of cross-domain spoofing
- **Mailing lists**
  - Required by RFC to change Reverse-Path appropriately
- **Forwarding services and aliases**
  - Will break stuff in most cases, since usually the Reverse-Path does not get updated – this can be mitigated in some ways
    - on sender’s side: by using advanced macros and some work on the DNS server
    - in the middle: it can get messy, but several strategies exist
    - on recipient’s side: by using whitelists / ignoring SPF from known (verified?) forwarding services

Implementation – Sender’s side

- Just a TXT RR in DNS

- A designated RR (99, SPF) was reserved by IANA in April 2005 but it will take some time until software makes use of it.

- Syntax (simplified):

```
"v=spf1 *([qualifier]mechanism)"
```

- Qualifiers

+	Pass
-	Fail
?	Neutral
~	Softfail

The qualifier is optional and defaults to "+"

- It might be a good idea to start publishing records with "~" or even "?" qualifiers and change to "-" when everything looks promising enough.

Implementation – Sender's side

- **Mechanisms**

A	Match if sending host's IP address matches a given A record (example: a:mailers.domain.org/28)
MX	Match if sending host is specified as domain's MX
PTR	Match if sending host's IP re-resolves to the domain (example: ptr:nask.waw.pl)
IP4	Match if sending host is within specified IPv4 range (example: ip4:192.168.0.1/24)
IP6	Match if sending host is within specified IPv6 range
EXISTS	Match if a specified domain exists. This can be used with SPF macro language to construct complicated queries
INCLUDE	Match if check for included domain would pass
ALL	Always match

Implementation – Sender’s side (examples)

```
google.com text "v=spf1 ptr ?all"

gmail.com text "v=spf1 a:mproxy.gmail.com
   a:rproxy.gmail.com a:wproxy.gmail.com
   a:zproxy.gmail.com a:nproxy.gmail.com
   a:uproxy.gmail.com a:xproxy.gmail.com
   a:qproxy.gmail.com ?all"

aol.com text "v=spf1 ip4:152.163.225.0/24
   ip4:205.188.139.0/24 ip4:205.188.144.0/24
   ip4:205.188.156.0/23 ip4:205.188.159.0/24
   ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com
   ?all”

cert.pl text "v=spf1 ip4:195.187.245.33/25
   ip4:195.187.7.66/29 ip4:195.187.243.229 -all"

ibm.com text "v=spf1 -all"
```

Implementation – Sender’s side (examples, contd.)

```
hotmail.com text "v=spf1 include:spf-a.hotmail.com include:spf-
   b.hotmail.com include:spf-c.hotmail.com include:spf-
   d.hotmail.com ~all"

spf-a.hotmail.com text "v=spf1 ip4:209.240.192.0/19
   ip4:65.52.0.0/14 ip4:131.107.0.0/16 ip4:157.54.0.0/15
   ip4:157.56.0.0/14 ip4:157.60.0.0/16 ip4:167.220.0.0/16
   ip4:204.79.135.0/24 ip4:204.79.188.0/24 ip4:204.79.252.0/24
   ip4:207.46.0.0/16 ip4:199.2.137.0/24 ~all"

spf-b.hotmail.com text "v=spf1 ip4:199.103.90.0/23
   ip4:204.182.144.0/24 ip4:204.255.244.0/23
   ip4:206.138.168.0/21 ip4:64.4.0.0/18 ip4:65.54.128.0/17
   ip4:207.68.128.0/18 ip4:207.68.192.0/20 ip4:207.82.250.0/23
   ip4:207.82.252.0/23 ip4:209.1.112.0/23 ~all"

spf-c.hotmail.com text "v=spf1 ip4:209.185.128.0/23
   ip4:209.185.130.0/23 ip4:209.185.240.0/22 ip4:216.32.180.0/22
   ip4:216.32.240.0/22 ip4:216.33.148.0/22 ip4:216.33.151.0/24
   ip4:216.33.236.0/22 ip4:216.33.240.0/22 ip4:216.200.206.0/24
   ip4:204.95.96.0/20 ~all"

spf-d.hotmail.com text "v=spf1 ip4:65.59.232.0/23
   ip4:65.59.234.0/24 ip4:209.1.15.0/24 ip4:64.41.193.0/24
   ip4:216.34.51.0/24 ~all"
```

Implementation – Recipient's side

You may not be aware but...

- Most antispam software supports SPF for a long time.
- Many MTAs already speak SPF or have plugins/add-ons that allow them to do so – this includes Postix, Sendmail, Exim, Qmail
- Many ISPs and free e-mail providers are already using SPF
  - Adding Received-SPF headers
  - Filtering
- You may configure your reader to understand Received-SPF headers or look for existing plugins.

Implementation – Recipient's side

```
X-Gmail-Received: d07caab5c6cc18b775e66e5b6ddf7e5552fd184e
Delivered-To: przemj@gmail.com
Received: by 10.65.183.14 with SMTP id k14cs16216qbp; Fri, 20 Jan 2006
07:17:17 -0800 (PST)
Received: by 10.65.132.8 with SMTP id j8mr68400qbn; Fri, 20 Jan 2006 07:17:17
-0800 (PST)
Return-Path: lista@cert.pl
Received: from melkor1.nask.waw.pl (melkor1.nask.waw.pl [195.187.7.67]) by
mx.gmail.com with ESMTP id q13si1295973qbq.2006.01.20.07.17.11; Fri, 20 Jan
2006 07:17:17 -0800 (PST)
Received-SPF: pass (gmail.com: domain of lista@cert.pl designates 195.187.7.67
as permitted sender)
Received: from localhost.localdomain (localhost [127.0.0.1]) by
melkor1.nask.waw.pl (Postfix) with ESMTP id 30071AFB14; Fri, 20 Jan 2006
16:17:09 +0100 (CET)
```

Security considerations

- Possible DDoS attempts
  - Malicious SPF records pointing to a different domains could be used as amplifiers.
  - Malicious SPF records could force the client to make excessive DNS lookups (this should be easy to avoid if SPF check is implemented properly).
- SPF relies on DNS so DNS weaknesses affect the protocol.
- Cross-user forgeries are still possible – look for SMTP AUTH or, even better, cryptography to address that.
- Cross-domain forgeries are possible in some cases.
- Information about mail traffic is exchanged with DNS servers which may cause privacy issues.

Recommended reading

- **The RFC draft**

  http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt

- **SPF Homepage**

  http://www.openspf.org/

Questions?

Contact me:

Przemek Jaroszewski <przemek@cert.pl>

+48 22 380 83 77