RHODES UNIVERSITY

Grahamstown • 6140 • South Africa

Sender Policy Framework as a tool for SPAM reduction

Guy Antony Halse <G.Halse@ru.ac.za>

What is SPF

- The sender policy framework provides a way for the recipient of an e-mail to verify that the apparent sender of an e-mail is in fact genuine.
- It is a set of rules used when processing incoming e-mail.

Why should we care?

- You can prevent your domain (and thus your organisation’s name) from being used as the envelope sender of SPAM
- You can reduce the amount of SPAM you receive by honouring other people’s SPF rules

How does it work?

- `ru.ac.za. IN MX 10 a.mx.ru.ac.za.`
- `ru.ac.za. IN MX 20 b.mx.ru.ac.za.`
- `ru.ac.za. IN MX 30 c.mx.ru.ac.za.`
- `ru.ac.za. IN TXT "v=spf1 redirect=_spf.ru.ac.za"`

How does it work?

- `_spf.ru.ac.za. IN TXT`
  `"v=spf1`
  `mx:ru.ac.za`
  `ip4:146.231.128.0/23`
  `ip4:146.231.120.102`
  `ip4:146.231.115.0/24`
  `ip6:2001:4200:1010::/64`
  `~all“`

All mail exchangers

Bits of our network that might originate e-mail, in both IPv4 and IPv6 CIDR notation

Everything we haven’t explicitly covered

http://www.openspf.org/SPF_Record_Syntax

How does it work?

- You get e-mail apparently from somebody@ru.ac.za ….

- If it’s sent from 146.231.128.29 ip4:146.231.128.0/23
- If it’s sent from 2001:4200:101(ip6:2001:4200:1010::/64
- If it’s sent from 192.42.99.51 mx:ru.ac.za
- If it’s sent from 196.21.79.52 ~all
- If it’s sent from 172.16.0.22 ~all

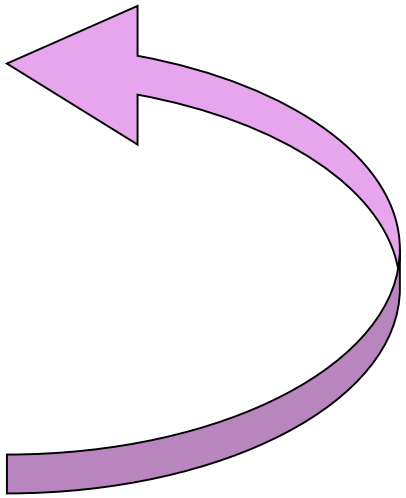
So what does “all” do anyway?

- +all – hard pass
- -all – hard fail
- ~all – soft fail
- ?all – neutral

- So in the example, “~all” is a soft fail

Where does this all fit in

- Real-time block lists
- Greylisting
- Local recipient checks
- **SPF rules**
- Protocol enforcement



- SpamAssassin
- Virus scanning

Who’s using SPF

- In ac.za …
  - che.ac.za, cput.ac.za, ctech.ac.za, cut.ac.za, edupark.ac.za, hartrao.ac.za, hmo.ac.za, nwu.ac.za, puk.ac.za, puknet.ac.za, rhodes.ac.za, ru.ac.za, tfs.ac.za, tofs.ac.za, ufh.ac.za, ufhel.ac.za, ufs.ac.za, ukzn.ac.za, uniwest.ac.za, uovs.ac.za, uv.ac.za
- Elsewhere …
  - Google Mail, Hotmail, Yahoo!, etc

Complementary Technologies

- SRS – Sender Rewriting Scheme
  - If you haven't implemented this, and you allow your users to forward their e-mail, do not publish a "-all" SPF rule!!
- Message submission (RFC 2476)
  - Reduces the number of places your mail can originate.
  - Allowed by most ISPs these days. Make sure you allow your users to use it to.
  - Not infallible