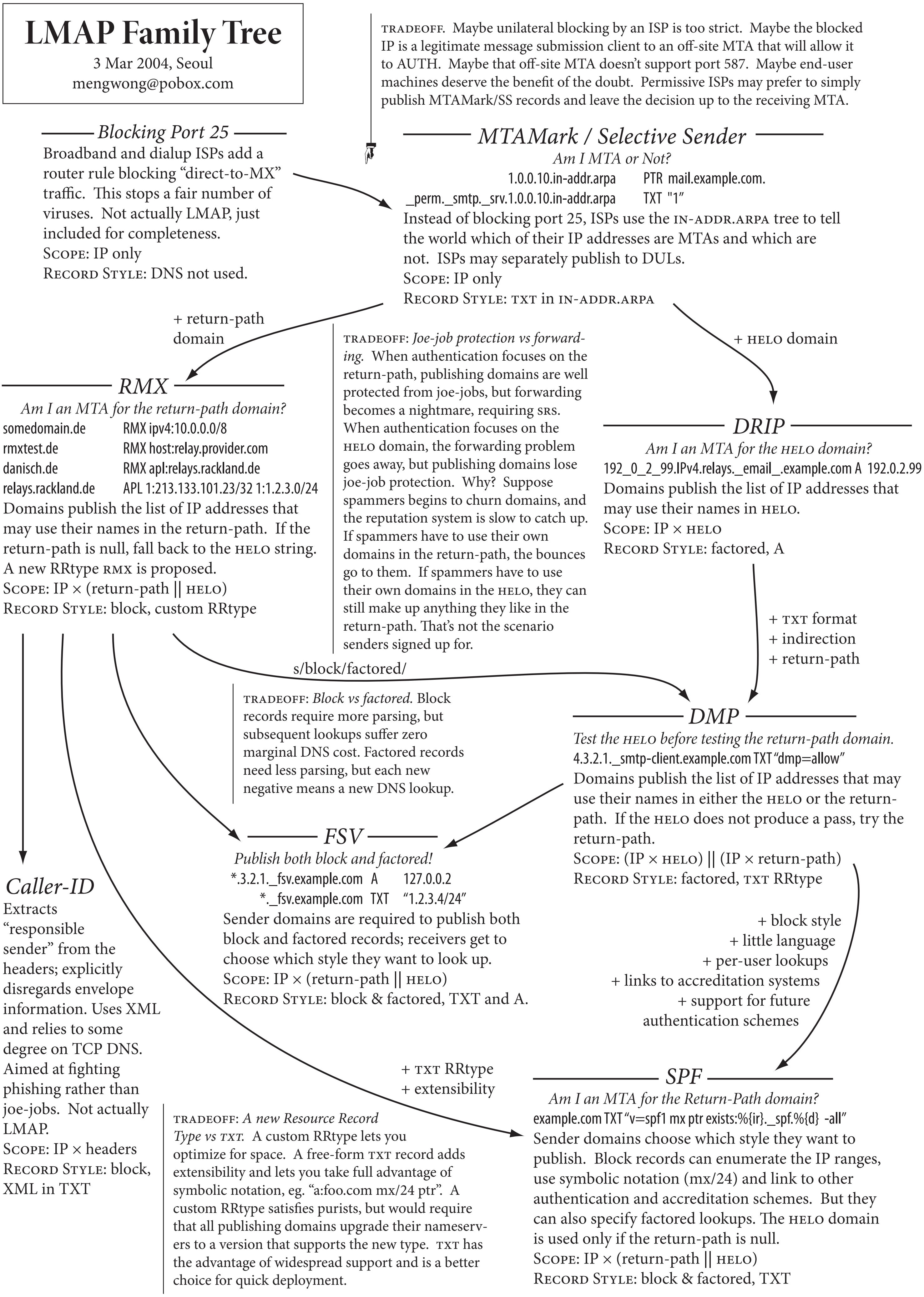
LMAP Family Tree

3 Mar 2004, Seoul
mengwong@pobox.com



TRADEOFF. Maybe unilateral blocking by an ISP is too strict. Maybe the blocked IP is a legitimate message submission client to an off-site MTA that will allow it to AUTH. Maybe that off-site MTA doesn't support port 587. Maybe end-user machines deserve the benefit of the doubt. Permissive ISPs may prefer to simply publish MTAMark/SS records and leave the decision up to the receiving MTA.

Blocking Port 25

Broadband and dialup ISPs add a router rule blocking "direct-to-MX" traffic. This stops a fair number of viruses. Not actually LMAP, just included for completeness.
Scope: IP only
Record Style: DNS not used.

MTAMark / Selective Sender

Am I MTA or Not?

```
1.0.0.10.in-addr.arpa                PTR  mail.example.com.
_perm._smtp._srv.1.0.0.10.in-addr.arpa  TXT  "1"
```

Instead of blocking port 25, ISPs use the IN-ADDR.ARPA tree to tell the world which of their IP addresses are MTAs and which are not. ISPs may separately publish to DULs.
Scope: IP only
Record Style: TXT in IN-ADDR.ARPA

RMX

Am I an MTA for the return-path domain?

```
somedomain.de       RMX ipv4:10.0.0.0/8
rmxtest.de          RMX host:relay.provider.com
danisch.de          RMX apl:relays.rackland.de
relays.rackland.de  APL 1:213.133.101.23/32 1:1.2.3.0/24
```

Domains publish the list of IP addresses that may use their names in the return-path. If the return-path is null, fall back to the HELO string. A new RRtype RMX is proposed.
Scope: IP × (return-path || HELO)
Record Style: block, custom RRtype

TRADEOFF: *Joe-job protection vs forwarding.* When authentication focuses on the return-path, publishing domains are well protected from joe-jobs, but forwarding becomes a nightmare, requiring SRS. When authentication focuses on the HELO domain, the forwarding problem goes away, but publishing domains lose joe-job protection. Why? Suppose spammers begins to churn domains, and the reputation system is slow to catch up. If spammers have to use their own domains in the return-path, the bounces go to them. If spammers have to use their own domains in the HELO, they can still make up anything they like in the return-path. That's not the scenario senders signed up for.

DRIP

Am I an MTA for the HELO domain?

```
192_0_2_99.IPv4.relays._email_.example.com A  192.0.2.99
```

Domains publish the list of IP addresses that may use their names in HELO.
Scope: IP × HELO
Record Style: factored, A

TRADEOFF: *Block vs factored.* Block records require more parsing, but subsequent lookups suffer zero marginal DNS cost. Factored records need less parsing, but each new negative means a new DNS lookup.

DMP

Test the HELO before testing the return-path domain.

```
4.3.2.1._smtp-client.example.com TXT "dmp=allow"
```

Domains publish the list of IP addresses that may use their names in either the HELO or the return-path. If the HELO does not produce a pass, try the return-path.
Scope: (IP × HELO) || (IP × return-path)
Record Style: factored, TXT RRtype

FSV

Publish both block and factored!

```
*.3.2.1._fsv.example.com  A    127.0.0.2
      *._fsv.example.com  TXT  "1.2.3.4/24"
```

Sender domains are required to publish both block and factored records; receivers get to choose which style they want to look up.
Scope: IP × (return-path || HELO)
Record Style: block & factored, TXT and A.

Caller-ID

Extracts "responsible sender" from the headers; explicitly disregards envelope information. Uses XML and relies to some degree on TCP DNS. Aimed at fighting phishing rather than joe-jobs. Not actually LMAP.
Scope: IP × headers
Record Style: block, XML in TXT

SPF

Am I an MTA for the Return-Path domain?

```
example.com TXT "v=spf1 mx ptr exists:%{ir}._spf.%{d} -all"
```

Sender domains choose which style they want to publish. Block records can enumerate the IP ranges, use symbolic notation (mx/24) and link to other authentication and accreditation schemes. But they can also specify factored lookups. The HELO domain is used only if the return-path is null.
Scope: IP × (return-path || HELO)
Record Style: block & factored, TXT

TRADEOFF: *A new Resource Record Type vs TXT.* A custom RRtype lets you optimize for space. A free-form TXT record adds extensibility and lets you take full advantage of symbolic notation, eg. "a:foo.com mx/24 ptr". A custom RRtype satisfies purists, but would require that all publishing domains upgrade their nameservers to a version that supports the new type. TXT has the advantage of widespread support and is a better choice for quick deployment.