WhitelistingEverybody

I want to whitelist everyone at my site. How do I do that?

If you simply use 'whitelist_from', this is quite trivial for spammers to exploit, as it simply examines the From:, Return-Path, and related headers of the mail. All a spammer needs to do is forge your address in the From: line, and they've whitelisted themselves. Because this mistake is quite common, it is frequently used in spam.

One way is to use 'whitelist_from_rcvd', which requires a hostname appear in the headers as well. This is the generally recommended method.

Note: for whitelist_from_rcvd to work, you must have your trusted networks set properly. See TrustPath for more details. That said, trusted_networks is NOT a whitelist mechanism in itself.

Another way is to examine the Received: headers of locally-originating mail, identify a pattern than will work, then create a local rule for this.

Note: this example is not particularly good, as it is effectively implementing whitelist_from_rcvd the hard way. The only advantage to the rule-based method is if you must check IPs due to lack of RDNS names. If RDNS hostnames exist, and the trust path is configured correctly, whitelist_from_rcvd will offer strong security against forgery. It will only honor received: headers inserted by trusted hosts, so you don't need to go to all this work.

For example, if every local mail passes through your mailserver with a Received line like this:

```
  Received: from phobos.labs.example.com (phobos.labs.example.com
        [192.168.2.14]) by mandark.labs.example.com (8.11.6/8.11.6)
        with ESMTP id g7CCUQp30306 for <someaddr@example.com>;
        Mon, 12 Aug 2002 13:30:26 +0100
```

Then you can construct a rule like so:

```
  header LOCAL_RCVD   Received =~ /from \S+\.example\.com\s+\(\S+\.example\.com\s+\[192\.168\..
*\s+by\s+mandark\.labs\.example\.com/
  describe LOCAL_RCVD Received from a local machine
  score LOCAL_RCVD   -50
```

and that will subtract 50 points from the score for each local mail.

Note that dots, brackets, and other non-alphanumeric characters need protection with a backslash; and that whitespace should be represented using \s+ instead of spaces in case the text is broken onto multiple lines.

If many sites do this, and create their own independent rules, the spammers will have to anticipate each one – which is not so easy to forge 😉