SENDMAIL®

THE FULL POWER OF EMAIL

FTC: Sender Authentication Testing

Larger Issues of Deployment

Sender Deployment

Deployment work for all solutions is very equivalent

- Biggest hurdle is auditing networks
  - *Outbound gateways, remote users, third party mailers*
  - *Must put in processes to keep all up to date*
- Be careful of signatures being broken because of improper mail client message encoding

Senders should provide multiple forms of authentication

- Senders can't detect which recipient addresses *might* break authentication
- Provide IP-based credentials as well as crypto

Performance

- CPU overhead for signing is small (5-7% max)
- Receiver DNS overhead for both approaches is comparable (5-7% delay)

Receiver Deployment

Interpreting Authentication Results

- Check multiple authentication methods (IP and crypto)
- Most authentication failures will be because of *receiver* requested action; receivers should use comparison of authentication results and traditional spam scanning to ferret out broken forwarders
- Be careful with handling of authentication failures
  - > *Either accept and process as un-trusted or reject at SMTP time*

End-user Experience

- Use authentication status in acceptance policies, be careful in presenting results to end users
  - > *Be wary of end-user interpretation of results*
  - > *Risk of conditioning users to accept broken authentication*