Email Authentication:

A common sense overview

IETF 87 – Berlin – 30 July 2013

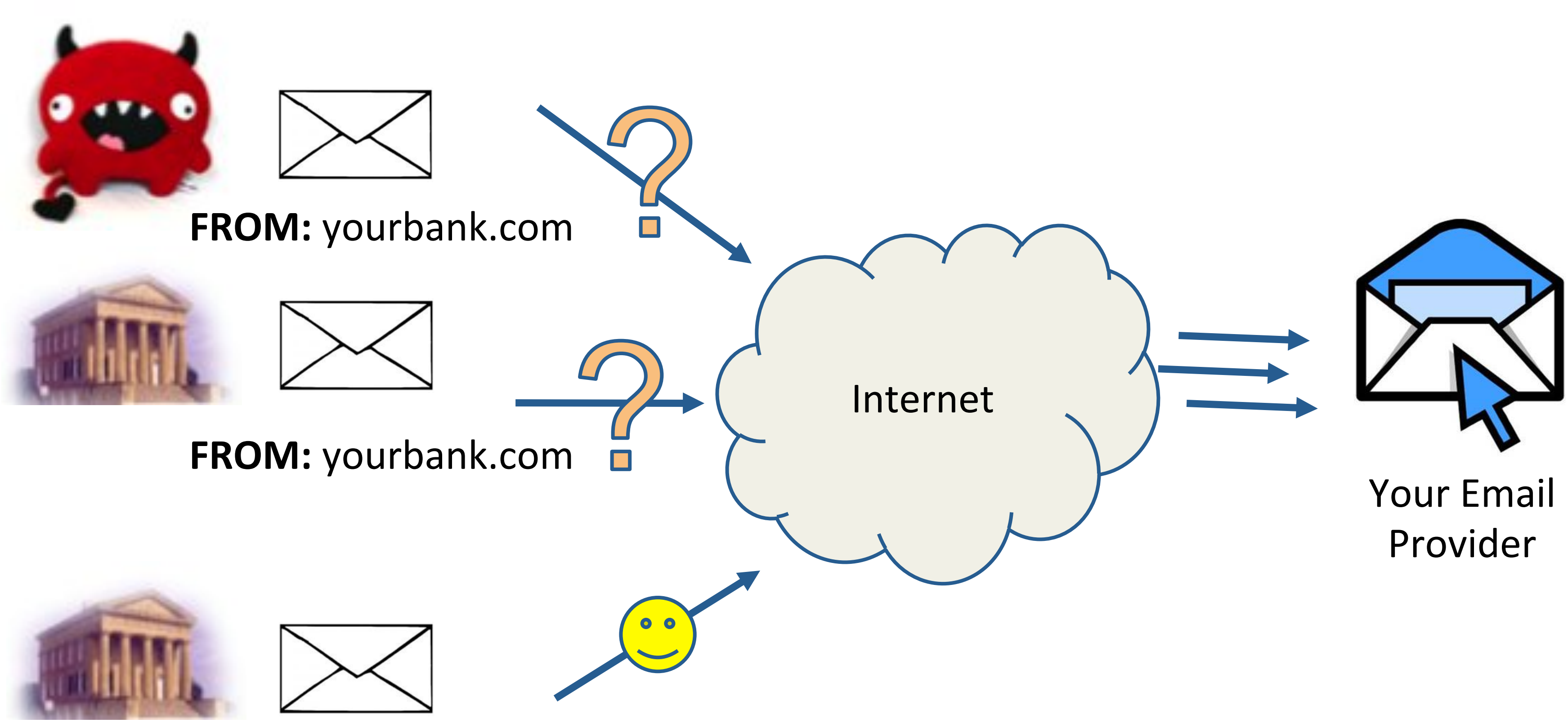
J. Trent Adams

(with Christine Runnegar)

Email Authentication

- **Introduction to Email Authentication**
  - What we mean by "authentication"
  - Authenticating the servers and mail envelope
  - Not about content-level inspection
  - Effective against spoofed-mail phishing
- **IETF Technologies in Place**
  - Authenticating the sending server (SPF)
  - Authenticating the message (DKIM)
  - Securing DNS (DNSSEC)
- **Adding Policy Declarations and Feedback Reports**
  - DMARC as an Example in Active Play
  - Building on SPF & DKIM, adding policy & reporting
  - Significant "running code" *(60% global coverage as of January 2013)*
  - An Individual Submission as a proposed Standard

Email Authentication - *Questions*



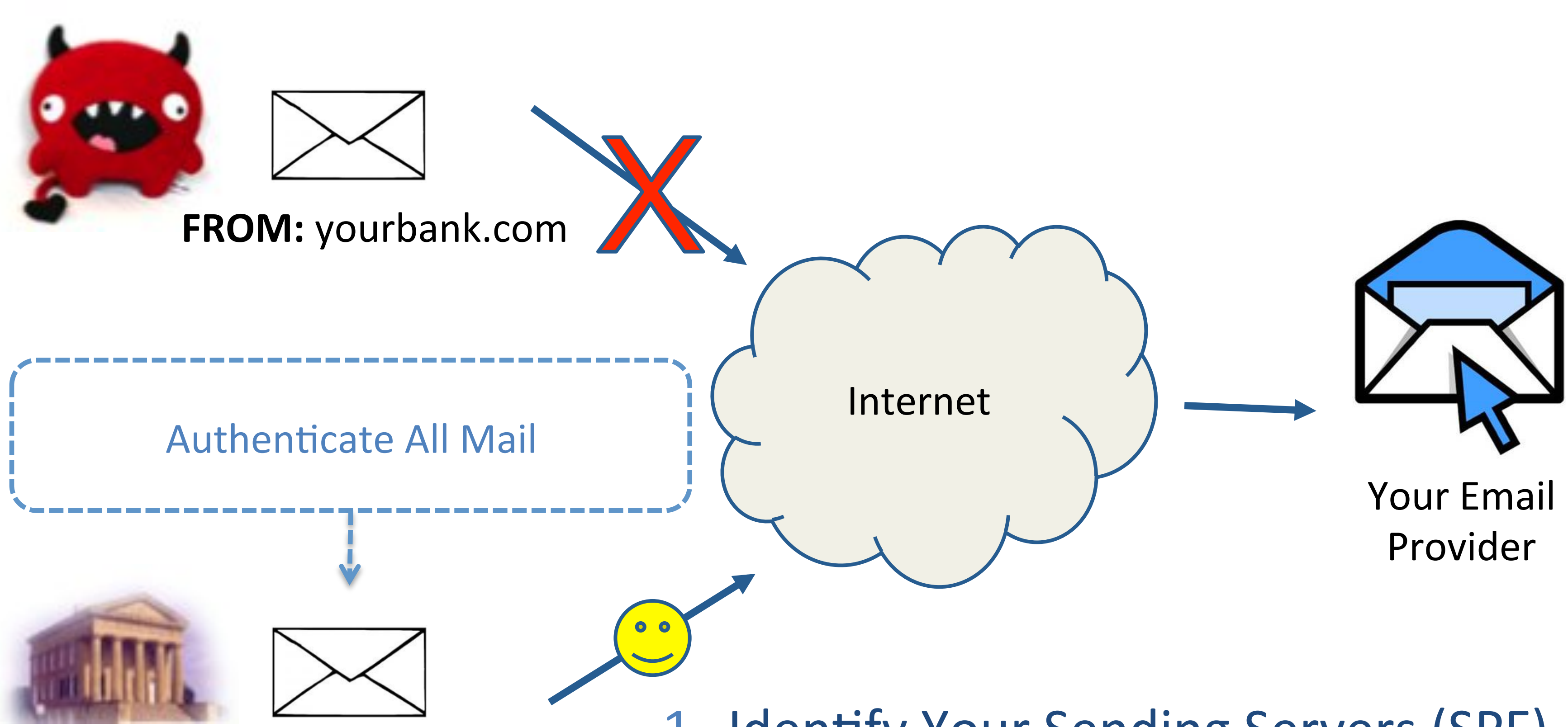
FROM: yourbank.com

FROM: yourbank.com

FROM: yourbank.com

How can a mailbox provider know if an email it receives is legitimate?

Email Authentication - *Answered*



FROM: yourbank.com

Authenticate All Mail

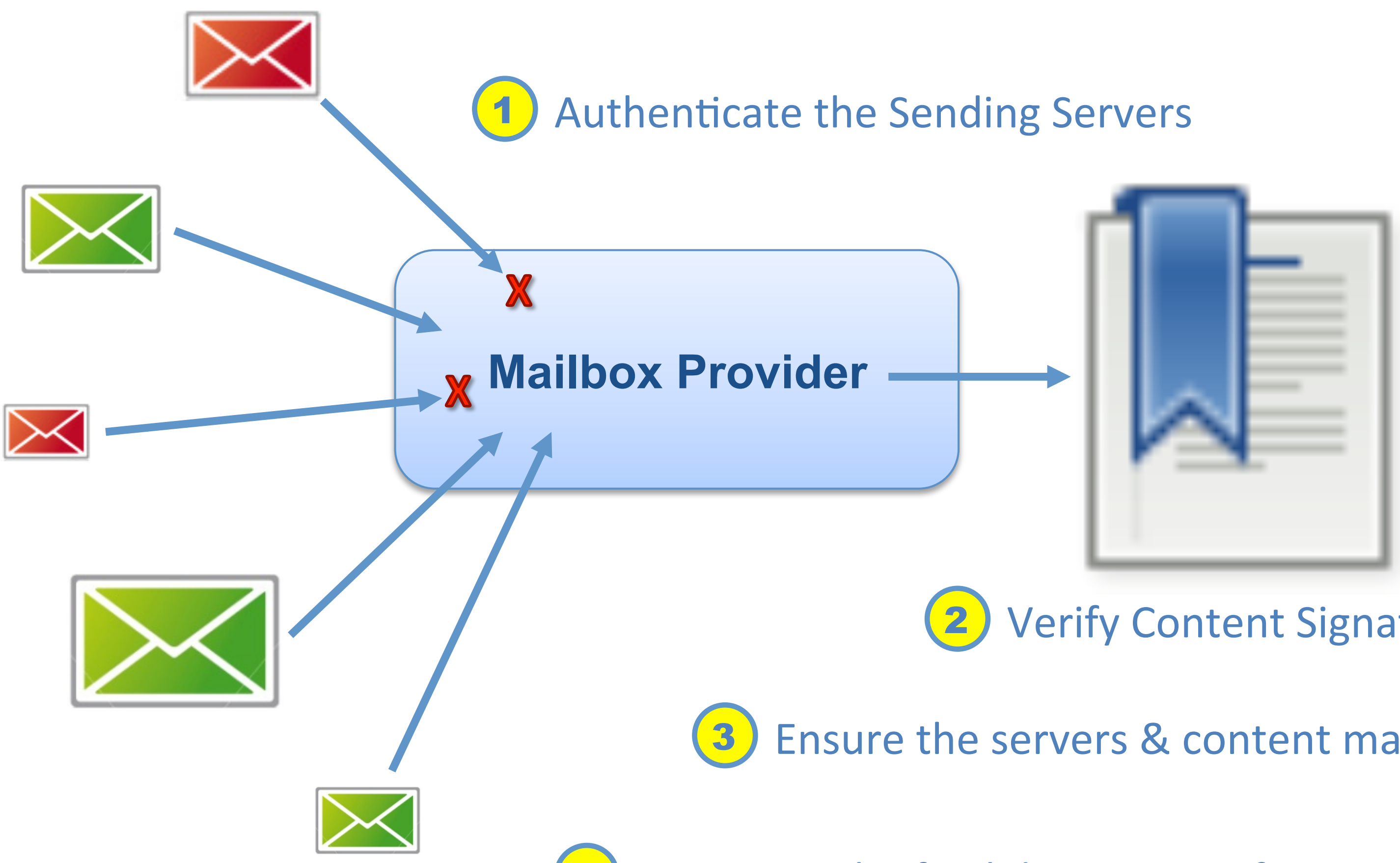
Internet

Your Email Provider

FROM: yourbank.com

1. Identify Your Sending Servers (SPF)
2. Sign the Content (DKIM)
3. Apply Authentication Policies (DMARC)

Email Authentication - *Receiving*



1 Authenticate the Sending Servers

2 Verify Content Signatures

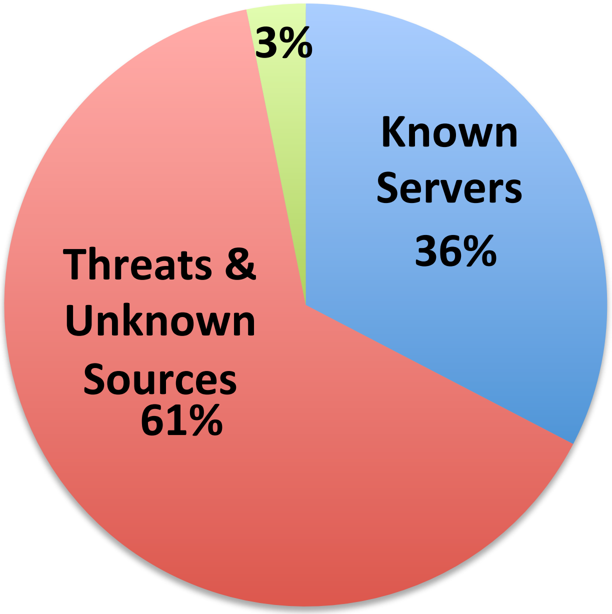
3 Ensure the servers & content match

4 Report on the final disposition of messages

Email Authentication - *Reports*

- A large international conglomerate didn't know if they had a spoofing problem or not.
- They published a DMARC "monitor" record (i.e. "p=none") to receive reports.
- They quickly determined they had a problem, and now knew how bad it was.

Actual Email Threat Profile



36% - Known Servers:
Messages sent from servers that were identified as belonging to the organization

3% - Forwarders:
Messages determined to be forwarded by third parties (e.g. discussion lists)

61% - Threats & Unknown Sources:
Messages sent by unknown and/or potentially malicious senders

Source: *Case study provided by Message Bus. More case studies can be found on DMARC.org*

Thanks! *Questions?*