DKIM Email Authentication Summit
February 13, 2006

Establishing Confidence in Email

Douglas Otis
Doug_Otis@trendmicro.com
Establishing Confidence

- DKIM:
  - Verifies Prefatory Domains
  - Can Ally Email-Addresses within Prefatory Domains
  - Policies Can Assure Alliances
  - Reduces False Positives Detecting Spoofs
DKIM is Independent of the Message Envelope

- Recipients are Not Verified
- Return-Path is Not Verified
- No Conventional Association with SMTP Clients
Ascribing Bad Behavior of Prefatory Domains

- Limited to Message Content
  - Malware
  - Misleading Links
  - Misleading Information
  - Invalid Encompassed Header Fields
- Evaluation is Resource Intensive
Safe Recipient Assurances

- Trust-Marks Can Overcome:
  - RFC 2047, 3490-3492 Unicode Character Repertoires
  - Unverified Display-Names
  - Confusing DNS Hierarchy
  - Visually Similar Characters or Ideograms
  - Non-Allied Email-Addresses

- Trust-Marks May Note Allied Email-Addresses
When Signing All Messages

• Use of Sub-Domains May Add Confusion
• Any Message Source Might Impact Trust
• Key or Message Tags Can:
  – Indicate Unvetted Sources
  – Reduce Evaluation Costs
  – Retain Prefatory Domain Trust
  – Condition Message Level Precautions