DKIM Threat Analysis
draft-ietf-dkim-threats-01

Jim Fenton <fenton@cisco.com>

20 March 2006

DKIM Threat Analysis
Current Status

- **draft-ietf-dkim-threats-01.txt posted March 7, 2006**
- **In WG Last Call as of March 9 (through March 24)**
- **Added since dkim-threats-00:**
  - **Description of key publication by higher level domain attack**
  - **Description of falsification of SSP replies**
  - **Section on other threats and description of packet amplification attacks via DNS**

Accepted changes since -01

- **Reworded “Document Structure” introduction from Stephen Farrell**
- **Less normative wording for mitigation of:**
  - **Theft of delegated private key**
  - **Body length limit abuse**
- **Description of reply variant of chosen message replay**
- **Numerous minor edits and clarifications**

Open issues

- **1171: Clarification of the DKIM mechanism in introduction**
- **1172: Impact of signed message replay**
- **1222: ABNF: Sender = Originator / Operator**

  (is this really a threats issue?)