Abuse Report Format

APPS Area Working Group Proposal
IETF 75 – Stockholm
Murray S. Kucherawy
<msk@cloudmark.com>
What ARF Is

• Abuse Report Format specification details a message format similar to DSN (RFC3464) that reports on abuse or potential abuse in a format suitable for machine parsing

• Machine parsing enables automated processing between operators
  – Demand for this is increasing in industry

• Specified in draft-shafranovich-feedback-report
Work To Date

• Originated within a messaging trade organization (MAAWG)
• Has undergone considerable evolution and deployment among its members, which include some large ISPs and senders
• Primary content used in many Feedback Loops (FBLs)
• Has now been stable for a couple of years
Current Installed Base

• Numerous internal-only implementations at various ISPs for generating and parsing ARF messages

• Some open source implementations such as mail filters that generate or parse ARF messages
  – And a few commercial ones that generate them

• Community interest in some open source tools for parsing standardized ARF messages
  – MAAWG considering sponsorship of such an effort
Purpose Of An ARF WG

• Refine the starting specification, considering additional features and taking advantage of the expertise in the IETF
  – Make necessary changes with a focus on compatibility
  – Maintaining compatibility with the existing installed base is key to success
• Propose tools to encourage further adoption
Purpose Of An ARF WG

• Consider several possible extensions proposed by the community
  – Means to relay the source AS of abuse activity
  – Attacks on specific services such as SSH, FTP, WWW servers
  – Mail to honeypots
  – DDoS reports
  – Botnet detection
  – “Drop boxes”
Purpose Of An ARF WG

• Specify integration of ARF into DKIM community
  – Using draft-kucherawy-dkim-reporting as basis
Goals and Milestones

- Nov ‘09 – Issue first WG-based ID defining ARF
- Jan ‘10 – Reach consensus on WG-based changes
- Feb ‘10 – Submit ARF ID to IESG for publication
- Apr ‘10 – Issue first WG-based ID about DKIM reporting extensions
- Jun ‘10 – Reach consensus on WG-based changes
- Jul ‘10 – Submit DKIM reporting ID to IESG for publication
Feedback?

• Volunteers?
  – Interested in a BoF?
  – Want to be a Co-chair?

• Suggestions on scope?

• Other topics?