ASRG Status and Work Items

Paul Judge

ASRG status

- Announced 3 weeks ago
- ~450 mailing list members
- ~1800 mailing list messages
- 9 High-level work items

3 weeks X 450 people = 1722 messages = 9 work items

ASRG Work Items

- Inventory of problems*
- Characterization of the problems
  - Public Trace Data*
  - Spam Measurements
  - Spam Categorization
- Requirements for solutions*
- Taxonomy of solutions*
- Identification of need for interoperable systems*
  - Spam Test Message
  - Opt-out
  - Filtered Message Status
- Proposals of new solutions*
- Evaluation of proposals
- Best Practices documents
  - End-users
  - Mail administrators
  - Mass Mailers

Inventory of Problems

- Inconsistent definition of spam
  - One man's trash…
  - Gray area
  - Lack of system to capture the subjective definitions
  - Difficulty of implementing inconsistent policy close to source
- Evading accountability
  - forging envelope sender
  - forging From header
- Exploitation of weak systems
  - exploit open smtp relay
  - exploit insecure web services (cgi formmail)
  - exploit open proxies (HTTP CONNECT, HTTP)
- Efficient address gathering
  - directory harvesting (web, LDAP)
  - name guessing & probing
  - name guessing without probing [selling bogus data to others]
  - inappropriate database sharing/selling
- Inadequate opt-in
  - no actual opt-in
  - deceptive opt-in
  - single opt-in without confirmation

Inventory of Problems (cont.)

- Inadequate opt-out
  - opt-out not implemented
  - opt-out ineffective (pro forma removal from one list not all)
  - opt-out untimely
  - opt-out difficult to execute
  - opt-out hostile (used only for address verification & enrollment in even more databases)
- Evasion of automated filters
  - content randomization
  - eyespace transformation
  - inclusion of non-spam chaff (visible or invisible)
  - content in images, not text
  - content in other external links
- Evasion of human caution
  - fake DSN
  - fake content resembling common cgi-to-mail
  - "returned your call", "your account has a credit", etc
- Fraud & Crime
  - Chain Letter and Pyramid schemes
  - Nigerian 419
  - password/credit card theft

Requirements for anti-spam systems

1. must minimize unwanted messages to some acceptable level
2. must not affect delivery (latency, integrity, cost, reliability) of wanted messages to a point that would effect the normal use of email
3. must be easy to use
4. must be easy to deploy, incrementally
   - must provide incentives to deploy for those doing the deployment
5. must not depend on universal deployment to be effective
6. must not reduce privacy
7. must have minimal administration and implementation overhead
8. must have minimal computational and bandwidth overhead
9. must consider the threat and be robust in the face of such threats
   - (potential new work item: a spam threat model)
     - some properties of the threat:
       - adversary knows details of anti-spam systems
       - adversary is intelligent and well-funded
10. should consider how legal issues affect, support, or constrain the technical solution