Introduction to the Anti-Spam Research Group (ASRG)

Presented by Yakov Shafranovich, ASRG Co-chair

NIST Spam Technology Workshop

Gaithersburg, Maryland, February 17th, 2004

Internet Society

NIST National Institute of Standards and Technology

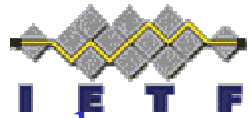
IRTF

Table of Contents

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1. IETF and IRTF

- **Internet Engineering Task Force (IETF)**



  - focuses on the ***short-term*** issues of engineering and standards making
  - Operates ***more formally***
  - Consists of 100+ working groups ***working on Internet standards***
- **Internet Research Task Force (IRTF)**

  - focuses on ***long-term*** research issues related to the Internet
  - Operates ***more informally***
  - Consists of 12 research groups ***doing research*** on Internet related issues

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2. Goals of the ASRG.

- **Research into Internet-wide solutions** to mitigate the sending and effects of spam
- **Pre-Standards work** for the IETF
- **Focus on technical** but may consider tools and techniques to aid the implementation of legal and other non-technical anti-spam measures

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3. Some Causes of Spam.

- **Social Causes:**
  - Same criminal and malicious behavior as regular society
  - Lack of sufficient funding for legal enforcement
- **Lack of Expertise Among End Users:**
  - Makes hijacking of computers easier
  - Users do not care about securing computers
- **Economic Nature of the Internet:**
  - Cheap communications medium
  - Low cost can be used for good and bad
- **Lack of Cooperation Among Network Operators:**
  - Inability to communicate blocking
  - Unwillingness to deal with abuse reports

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4. ASRG Research Agenda.

- **Problem Analysis**
- **Improving Existing Solutions**
- **Proposing New Solutions**

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4.1. ASRG Research Agenda.

- **Problem Analysis includes:**
  - **Inventory of Problems** - analysis of spam-related problems
  - **Analysis of Current Solutions** - inventory and analysis of current anti-spam solutions, their weaknesses and effectiveness
  - **Analysis of Spam** - analysis of persistent patterns in spam and spammer behavior that can be used to improve existing and propose new solutions

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4.2. ASRG Research Agenda.

- **Improving Existing Solutions includes:**
  - **Best Current Practices for Spam Control** - including email admins, end users, MTA developers, blacklist operators, etc..
  - **Filtering Standards** - dynamic updates, standard headers for MTAs, etc.
  - **Abuse Reporting Standards** - research into common standards for exchanging information about network and email abuse.

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4.3. ASRG Research Agenda.

- **Proposing New Solutions includes:**
  - **Requirements and Evaluation Model** - to be used for evaluation of proposed solutions
  - **SMTP Session Verification** - verification of the SMTP transaction (e.g. LMAP, etc.)
  - **Message Verification** - verification of both the message headers and content (e.g. DomainKeys, Project Lumos, TEOS, etc.)

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

5. Current Status of the ASRG.

- Seeking Volunteers:
  - Abuse Reporting Standards
  - Best Current Practices
  - Filtering
  - Problem Analysis
  - SMTP and message verification
- Coordinating with industry
- BOF at the next IETF meeting on DNS authentication

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6. Selected Proposals.

- Does Authentication Matter?
- Replacing SMTP?
- DNS-based Authentication Proposals

"Hostile armies may face each other for years, striving for the victory which is decided in a single day"

"Art of War", Sun Tzu

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6.1. Proposals - Does Authentication Matter?

- **Does Authentication Make a Difference?**
  - Do end users and ISPs care?
  - Spammers can hijack user's identity!
- **Better Authentication With Better Identity?**
  - Users and ISPs will care more about domains and email addresses being stolen?
  - Spammers will be more traceable
  - Narrows the playing field
  - "Quis custodiet ipsos custodes" – "Who will watch the watchers"?

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6.2. Proposals - Replacing SMTP?

- Several proposals have been submitted to both the IETF and the ASRG
- Seek to create an traceable email system
- ***Need for replacement has NOT been proven***
- Most discussions are taking placing outside the ASRG (www.imc.org/mail-ng/)

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6.3. Proposals - DNS-based Authentication Methods.

- **MTA Authorization Records in DNS:**
  - Seeks to eliminate forgery in SMTP transactions
  - Uses DNS for publication of domain authorization data
  - Significant issues remain to be addressed
  - Several competing proposals (RMX, DMP, SPF, etc.)
  - IETF BOF scheduled for March 4th, 2004 (Seoul)
- **MTA MARK**
  - Seeks to address the problem of hijacked computers
  - Uses rDNS records to mark specific IPs as MTA or non-MTAs

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Introduction to the Anti-Spam Research Group (ASRG)

Questions? Comments?

ASRG Website: asrg.sp.am

Copyright © 2004 ISOC
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.