Email Authentication

Sana D. Coleman
Bureau of Consumer Protection
U.S. Federal Trade Commission
www.ftc.gov

The FTC's Role in the Fight Against Spam

- The FTC has played a significant and long standing role in the study of, and fight against, spam.
- The FTC has a threefold strategy to combat spam.

Threefold Strategy to Combat Spam

- Enforcement
- Education
- Research

Threefold Strategy to Combat Spam

- Enforcement
  - The FTC has brought 66 spam related cases against over 160 individuals and firms.

Threefold Strategy to Combat Spam

- **Enforcement (an International Perspective)**
  - **(2002) U.S./Canadian Sweep Targeting Deceptive Spam and Internet Fraud**
  - **(2004) The London Action Plan On International Spam Enforcement Cooperation**
  - **(2005) FTC and Spain's Agencia Española de Protección de Datos (AEPD) signed a bilateral MOU to promote enhanced cooperation and information-sharing on spam enforcement activities.**

Threefold Strategy to Combat Spam

- Education
  - Consumer education http://www.ftc.gov/spam/
  - Global education (e.g., "Operation Secure Your Server" (2004))

Threefold Strategy to Combat Spam

- Research
  - Spam Harvest Study (2002)
  - Spam Forum 2003
  - False Claims in Spam Report (2003)
  - Do Not Email Registry Report (2004)

Do Not Email Registry Report

- In the CAN-SPAM Act of 2003, Congress required the FTC to prepare a report about the possible creation of a Do Not Email Registry Report.

Do Not Email Registry Report

- Conclusion: Without a system in place to authenticate the origin of email messages, a Do Not Email Registry would:
  - fail to reduce the burdens of spam,
  - and, possibly, increase spam, as illegal marketers would use it as a DO Spam Registry.

The Underlying Problem Identified in the Report

- Solving the spam problem begins with recognizing that spammers are essentially anonymous.
- The current email system does not require accurate routing information, except for the intended recipient of the email.

The Resulting Problem

- A spammer can falsify:
  - portions of the header,
  - the entire header of an email, and
  - spoof the originating IP address.

What is the Solution?

- This is not a problem that lends itself well to governmental solution. The best hope is for the marketplace to develop and employ technological solutions to prevent spammers from hiding behind a technological veil.
- Domain-level email authentication is one promising technological tool, but it is not a silver bullet.

How Does Email Authentication Work?

- Private market proposals would verify the "ftc.gov" portion of the email address: abc@ftc.gov.
- but would not authenticate that the message came from the particular email address "abc" at this domain.

Email Authentication Summit

www.ftc.gov/bcp/workshops/e-authentication/index.htm

Email Authentication Summit

- Two-day Summit
  - **Day 1: Over 300 total attendees**
  - **Day 2: Over 250 total attendees**
  - **60 panelists, from the U.S. and abroad, including representatives from Microsoft, Yahoo!, Cisco Systems, Inc., America Online, and Earthlink.**

Summit Panels

- **Back to Basics –** an overview of email authentication and why it is important
- **Policy Framework-** policy considerations, including privacy, antitrust, and intellectual property considerations
- **The Proposals** - Cryptographic approaches, and Internet protocol/domain based approaches

Summit Panels

- **Testing -** the status of industry testing of various email authentication standards
- **Possible Loopholes** - a discussion of how spammers would be able to circumvent the various authentication methods (e.g., zombie drones)
- **Real World Effects -** how authentication will impact bulk email marketers and small ISPs

Summit Panels

- **Global Impact** - an overview of international considerations for the adoption of a domain-level email authentication standard
- **Moving Towards Implementation** - a candid discussion with the proponents of various standards about the next steps required to adopt an email authentication standard
- **The Role of Accreditation** - domain level email authentication alone is not a silver bullet. Other tools that would help to indicate whether a sender is reputable are also important.

Summary of our Concerns

- Low cost to implement
- Minimal technical requirements for operators and end users
- No interference with flow of global email traffic
- Low false positives
- Low false negatives
- No undue burden on small ISPs

Summit Success

- The proponents of the different proposals agreed to an open approach with respect to publicly sharing their testing data. As a result, the computer analyst community and others, in the U.S. and abroad, will have access to the testing data.

FTC's Future Role

- To continue to monitor and spur the development of a widely adopted email authentication standard or standards.
- To create and manage a publicly available website for the posting of certain email authentication testing data.
- To collect hard data (e.g., the FTC has recently used its compulsory process to obtain testing and implementation data from ISPs.)

The FTC's Future Role

- Next Steps
  - Additional possible measures are identified in the DNE Registry Report.
  - These measures are viewed as an "if all else fails" approach.

Contact Information

Sana D. Coleman
Bureau of Consumer Protection
Federal Trade Commission
(202) 326-2249