# Anti-Spam Policy Instruction/Distribution Operation

A new Internet Draft to MARF - "draft-cai-marf-policy-instruction-operation-00.txt"

Yigang Cai (yigang.cai@alcatel-lucent.com)

03/29/11

# Overview of Policy Instruction/Distribution

- **Spam report server or client can instruct and distribute anti-spam policies to one or multiple clients which actually conduct spam filtering and detection, to**

  - **have latest spam filtering criteria and policies instructed by the network;**

  - **receive spam filtering and detection algorithms and rules from other spam reporting clients via the centralized spam reporting server**

  - **update and enhance existing local filtering algorithms and rules;**

  - **prevent in advance from upcoming spam with new abuse contents and/or from new sources**

  - **optionally, further distribute the received policies to other spam reporting clients in its network.**

- **Spam Reporting Server**

  - **receiving spam reports**

  - **conducting spam analysis**

  - **summarizing anti-spam criteria/policies/rules, and distributing to clients**

- **Spam Reporting Client (SMSC, MMSC, email server, IM server, etc.)**

  - **detecting spam messages using local spam filtering criteria/rules**

  - **reporting spam messages to server**

  - **receiving the instruction of anti-spam policies/rules from server**

  - **optionally receiving/forwarding the anti-spam policies/rules from/to other clients.**

Alcatel·Lucent

# Procedures of Policy Instruction/Distribution

- **Unsolicited model (push model)**

  - Server or client sends policy instruction/distribution request to clients

  - Clients can send notification to subscribe/unsubscribe policy instruction/distribution

- **Solicited or on-demand model**

  - Client sends a request to server requesting provide policy instruction/distribution

  - Server can send anti-spam policies in a response (synchronous)

  - Server can send anti-spam policies in a new request to demanding client (asynchronous)

# Policy Instruction/Distribution Operations

**Unsolicited Request:**

Request ID
Request timestamp
Originating node address
Terminating node address
* Policy Body
 {
    Policy ID
    Network types
  * Protocol ID
  * Message Types
    Message attributes
  * Suspicious network domain
  * Suspicious address
  * Suspicious address type
    Spam type
    Language indicator
    Detection information
    {
    * Algorithm ID
    * Rule ID
    * Spam Keyword
    * Spam Pattern
    }
    Action information
    {
       Block with notification
       Block without notification
       Unblock and deliver
       Hold and quarantine
    }
    Privacy shield information
    Affective filtering start timestamp
    Affective filtering stop timestamp
 }

**Unsolicited Response:**

Request ID
Request received timestamp
Response timestamp
Originating node address
Terminating node address
Result Code
* Policy Specific Result Code
  {
     Policy ID
     Result Code
  }

**Subscriber/Unsubscribe Request:**

Request ID
Request  timestamp
Originating node address
Terminating node address
Anti-Spam Policy Instruction Control
 {
    InstructionAction
 * Existing Policy IDs
 }

**Subscriber/Unsubscribe Response:**

Request ID
Request received timestamp
Response timestamp
Originating node address
Terminating node address
Result code

**On-demand Request:**

Request ID
Request timestamp
Originating node address
Terminating node address
Anti-Spam Policy Instruction Control
{
InstructionAction
*Existing Policy IDs
}