COLDSPARK

FTC Email Authentication Summit

Email Authentication Methods:
Testing, Implementation, and Evaluation

November 2004

Overview

- **Email authentication**

- **SPF vs. cryptographic methods**

- **Implementation**

- **Testing**

- **Evaluation**

COLDSPARK

Email Authentication

- ❑ Effective reduction of a significant minority of unsolicited email

- ❑ Effective reduction of a potential majority of spoofed email

- ❑ Improved ability to accurately identify senders for classification (reputation, prioritization etc.)

- ❑ Marginal deterrence of fraud and spam through combined reduction in delivery performance of non-authenticated email and trace-ability of senders of authenticated email

COLDSPARK

SPF vs. Cryptographic Encryption

Drawbacks to SPF:

❑ Weaknesses in the Purported Sender Algorithms

❑ SPF can chain to a large number of DNS lookups, potentially creating continuous loops

❑ SPF can only tell us whether a server/IP is allowed to deliver mail for a domain

❑ Potential legal constraints

Added benefits of cryptographic approaches

❑ Crypto solutions provide a measure of validation/ transport integrity for the message which is not possible with SPF

❑ Crypto solutions add the ability to determine if the USER is allowed to send messages from that IP and that domain

www.coldspark.com

COLDSPARK

Implementation

Challenges

- CPU Intensive

- DNS Heavy

Development Requirements

- Low overhead

- Speed

- High speed DNS resolver

- Configurable outcomes

  - Block
  - Accept
  - Flag
  - Throttle

COLDSPARK

Testing - Real World

Evaluation Parameters

❑ CPU usage

❑ Speed

	Inbound		Outbound	
	CPU	Speed	CPU	Speed
Baseline	~30%	1MM per hour	~30%	1MM per hour
IIM	+55%	-16.3% 837k/hour	+55%	-15.5% 845k/hour
DomainKeys	+55%	-5.4% 946k/hour	+55%	-5.1% 949k/hour

Server spec:
- SparkEngine 4.1
- RedHat 8.0
- Dual Xeon (2.1 GHz)
- 2G Ram
- Mix of real world domains
- Msg size 10-200Kb
- Full DNS Lookups
- Java based solution

COLDSPARK

Testing - High Capacity

Evaluation Parameters

❑ CPU usage

❑ Speed

	Inbound		Outbound	
	CPU	Speed	CPU	Speed
Baseline	~44%	2.5MM per hour	~44%	2.5MM per hour
IIM	+50%	-66.1% 847k/hour	+50%	-65.4% 864k/hour
DomainKeys	+50%	-61.8% 956k/hour	+50%	-60.2% 996k/hour

Server spec:
•SparkEngine 4.1
•RedHat 8.0
•Dual Xeon (2.1 GHz)
•2G Ram
•Single domain
•Msg size 10-200Kb
•SMTP-SINK Relay
•Java based solution

www.coldspark.com

COLDSPARK

Evaluation

❑ Email authentication is practical and effective

❑ Cryptographic authentication is superior to SPF-type methods

❑ Performance impact can be minimized

❑ Adoption/roll-out can be gradual

COLDSPARK