



INFORMATION SECURITY DECISIONS


Hosted by  SearchSecurity.com

Steps to Safeguard Enterprise Email

Joel M Snyder
Senior Partner
Opus One, Inc.
jms@opus1.com

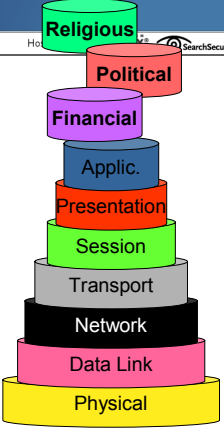


INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com


Our Strategy: Peeling the Onion

- Looking below RFC2821
 - Things that happen at TCP/IP layer and below
- Looking at the MTA
 - Concerns within RFC2821, the message envelope
- Looking at the body
 - RFC2822, the message body
- Looking within MIME
 - All that rich content, viruses, spam, malware and policy problems

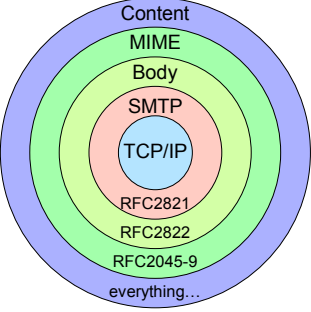


2

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

Security concerns are at every layer



3

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Before we start: We need a methodology

The Holy Trinity of Security

Evaluate each layer against constant criteria using a model.

4

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

E-mail sits on top of IP

- A wide variety of IP and TCP problems exist
- IP datagram source IP address easily forgeable
- IP fragmentation can fool simple firewalls and IDS sensors
- IP not generally encrypted
- TCP state machine allows attacker/initiator to consume resources on responder trivially
- TCP connection can be spoofed in some cases
- TCP connection easy to reset (third party DoS attack)
- DNS information not generally authenticated, yet must be trusted
- TCP and IP options can be used as a covert channel or to evade detection or pervert routing
- Distributed denial-of-service attack can consume all resources and open process slots on servers, yet be indistinguishable from normal traffic
- DNS root servers must be operating, yet are out of corporate control
- Common routing devices (e.g., Cisco) can be locked up with relatively low packet rates using DoS techniques

However, solving these problems is not unique to e-mail, so we're going to skip them.

5

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

RFC 2821: The envelope

TCP Connection:
1.2.3.4,12345 → 4.5.6.7,25
(mail1.from.com) → (mx1.to.com)

SMTP Session:
EHLO from.com
MAIL FROM: joe@from.com
RCPT TO: user1@eng.to.com
RCPT TO: user2@to.com

Body Headers:
Received: from mail1.from.com (1.2...)
Subject: Hello
From: "Bob" <bob@from.com>
To: "User One" <user1@eng.to.com>

Message Body:
Hello,

The body after the first blank line may contain many MIME parts. Second and following parts are often called "attachments"; first is often called "body" or "text." They are really all just "parts."

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Securing RFC2821: Integrity

- **Authentication**
 - Sender ID
 - Proper server configuration
- **Privacy**
 - Transport Layer Security
- **Integrity**
 - "Smart" MTAs
 - E-mail rate limiting
 - Resource conservation mode
 - SMTP ext. (SIZE)
 - LDAP & DNS rate limiting

```
smtp.acu.com ESMTP
EHLO Viola.Opus1.COM
250-SMTP.acu.com
250-SETIMEB
250 SIZE 1048576
MAIL FROM:<trumbo@Opus1.COM> SIZE=1024
250 sender <trumbo@Opus1.COM> ok
RCPT TO:<alan@acu.com>
452 Too many recipients received this hour
QUIT
```

10

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Security issues within RFC2822

TCP Connection:
1.2.3.4,12345 (mail1.from.com) → 4.5.6.7,25 (mx1.to.com)

SMTP Session:
EHLO from.com
MAIL FROM: joe@foofoo.com
RCPT TO: user3@mkkg.to.com
RCPT TO: user2@to.com

Body Headers:
Received: from mail1.from.com (1.2.3.4)
Subject: Hello
From: "Bob" <bob@barbar.com>
To: "User One" <user1@eng.to.com>

Message Body:
Hello,

- **Authentication & Authorization**
 - Envelope != Body
- **Privacy**
 - Plaintext message
- **Integrity**
 - Confusing headers
 - Spam
 - Bodies that have viruses or other malicious foo

11

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

It may not be possible to resolve RFC2822 issues

- **Authentication and Authorization**
 - Some bad messages look this way
 - Some good messages look this way
- **Privacy**
 - S/MIME with PGP or PKI
 - This is already built into your e-mail system
- **Integrity**
 - "Cleaning up" headers and MIME formatting
 - Do this before you do spam filtering

12

INFORMATION SECURITY DECISIONS

Hosted by

The last layer is the one we work hardest to solve

- Spam
- Viruses
- Worms
- "Content Problems"
 - Whatever it is that you aren't supposed to send in e-mail

13

INFORMATION SECURITY DECISIONS

Hosted by

Solving content-based problems

- With...
- Antispam
- Antivirus/Antiworm
- Policy-based controls

14


INFORMATION SECURITY DECISIONS

Hosted by

The Usual Scary Numbers Apply Here...

15

INFORMATION SECURITY DECISIONS


Hosted by  SearchSecurity.com

Five Things To Remember in Designing a Large-scale Anti-Spam Strategy

- **Users need to be empowered and want control**
- **False positives are bad (m'kay?)**
- **Avoiding spam is better than filtering spam**
- **Every email is sacred**
- **Your spam filter wants to be empowered and wants control**

19

INFORMATION SECURITY DECISIONS


Hosted by  SearchSecurity.com

End-user control is critical to end-user satisfaction

- **Users need to be empowered and want control**
- **False positives are bad**
- **Avoiding spam is better than filtering spam**
- **Every email is sacred**
- **Your spam filter wants to be empowered and wants control**
- **Every anti-spam product will have false positives**
- **A "detected" false positive causes stress and frustration unless**
 - **Users have the opportunity to review and retrieve their false positives**
- **Users also want the ability to control their:**
 - **Whitelists**
 - **Blacklists (a waste of time)**
 - **Sensitivity settings**

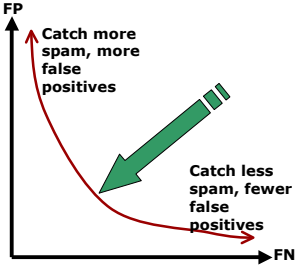
20

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

Every product has a tradeoff between false positives and false negatives

- **Users need to be empowered and want control**
- **False positives are bad**
- **Avoiding spam is better than filtering spam**
- **Every email is sacred**
- **Your spam filter wants to be empowered and wants control**




21

INFORMATION SECURITY DECISIONS


Hosted by SearchSecurity.com

If You Don't Accept the Mail, You Don't Have to Worry About It...

- Users need to be empowered and want control
- False positives are bad
- **Avoiding spam is better than filtering spam**
- **Every email is sacred**
- Your spam filter wants to be empowered and wants control



HOWEVER:
Accepting the Message Means You Accept Responsibility for the Message



... and You Leave a Great Audit Trail!



22

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Properly Placed Products Prevent Poor Performance

- Users need to be empowered and want control
- False positives are bad
- **Avoiding spam is better than filtering spam**
- **Every email is sacred**
- Your spam filter wants to be empowered and wants control

- Groupware Server
- Exchange™ Server
- Notes™ Server
- Open Source MTA

23

INFORMATION SECURITY DECISIONS



Hosted by SearchSecurity.com

Four Things To Remember When Deploying Large-scale Anti-Virus

- **Most mail with viruses in it is pure junk**
- **Cleaning viruses out of mail is a bad idea**
- **Telling people about viruses is a bad idea**
- **Every virus scanner is a three-state machine**

24

INFORMATION SECURITY DECISIONS

Hosted by  

Because Most Virus-laden Mail Is Pure Junk, Dealing With It Is a Waste of Time



- Virus scanners are generally too stupid to tell machine-generated virus-laden mail from human-generated virus-laden mail
- Opus One received 7616 viruses in February
 - Not one of them was in a human-generated message!

Recommended Solution:

- If you identify a virus in a message, log the results and drop the message

25

INFORMATION SECURITY DECISIONS

Hosted by  

Because No One Sent It, No One Needs To Know About It



- Sending mail to the recipient of a virus is a bad idea
 - They will be overwhelmed by junk
- Sending mail to the sender of a virus is a bad idea
 - They didn't send it
- Sending mail to anyone else when you get one is a bad idea
 - They don't want to know about it

Recommended Solution:

- If you identify a virus in a message, log the results and drop the message
- ...
- and that's all

26

INFORMATION SECURITY DECISIONS

Hosted by  

Every Virus Scanner Has Three Answers

- Yes: it is a virus (*false positives very uncommon*)
- No: it is not a virus (*false negatives expected*)
- I don't know: ???
 - The message was encrypted
 - The archive is protected
 - I crashed
 - Took too long
 - Ran out of disk or memory

Options

- Dropping unscannable messages is never the best answer
- Per-user (or per-group) policies help immensely

27

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

What are Policy Based Controls?

- **Controls on Email**
 - Flow
 - Content
 - Disposition

Based on Enterprise Policy

28

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Policy-based controls can have many different forms

- **Filters on messages or Actions on messages**
- **Typically based on policy outside of normal e-mail requirements**

- Drop all attachments of type MP3 or audio/mpeg.
- Stamp a footer disclaiming all responsibility for everything possible under the sun at the bottom of each outgoing message.
- Send a copy to Legal of anything with the codenames "snakebite" or "squeamish ossifrage" going to Internet.
- Send a copy of any pictures of Britney Spears to HR (big B.S. fans over in HR).
- Make an archive of anything from John Q. Suspicious just in case he's a secret agent.

29

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Products support almost any mangling you might want to do

- **Anti-spam and Anti-virus represent policy**
- **Message Prioritization (mailing lists, etc.)**
- **Content Scanning**
- **Content Modification**
- **Encryption/Decryption**
- **Destination Redirection**
- **Content Cloning**

30

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Policy Controls Can Be Anywhere

For example...

The diagram illustrates various points where policy controls can be implemented in an email system. It shows a flow from the Internet through a firewall, an appliance, a message store, and finally to the client. Callouts indicate where specific controls are applied: rate limiting at the external router, content filtering at the firewall, anti-spam and anti-virus at the appliance, archiving and cloning at the message store, and all of the above at the client.

31

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Why would you want Policy Controls?

- **Obvious and you have to do them:**
 - Anti-spam
 - Anti-virus
- **NON-obvious but you still have to do them**
 - Regulatory Things
- **Management wants it**
 - Message Cloning
 - Message Monitoring
- **Mail works better**
 - Queue Management
 - Rate Limiting

32

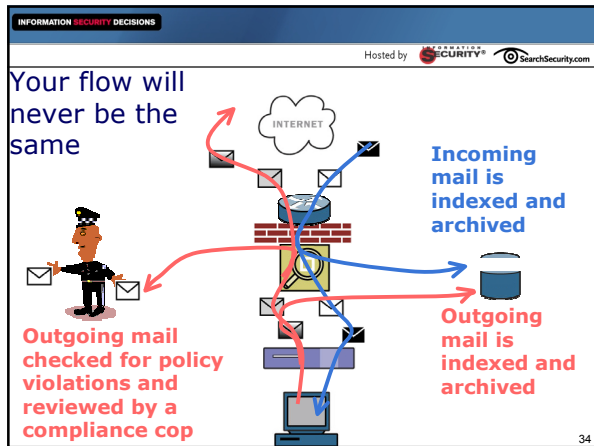
INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com


Regulatory Foo trumps Four Aces

● Sarbanes-Oxley Act of 2002	● Public companies must save email relevant to the audit process for 7 years
● SEC Rule 17A-4	● Brokerages must save email for 2 years
● Health Insurance Portability and Accountability Act	● Privacy rules limit what you can/cannot send via email and how you must protect it

33



- INFORMATION SECURITY DECISIONS
- Hosted by  SearchSecurity.com
- ### Top Six Policy Controls
- Footer Stamping
 - Compliance Checking
 - Message Archiving
 - Keyword Searching
 - Employee Monitoring
 - Encryption
- Every enterprise is going to do one, two, or all of these**
- 35

- INFORMATION SECURITY DECISIONS
- Hosted by  SearchSecurity.com
- ### Audience Response
- Questions?
- 36
