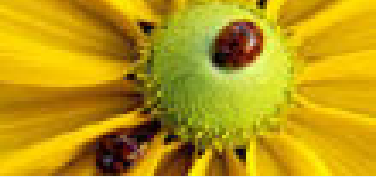


E-Mail Tools

David Hilley
davidhi@cc.gatech.edu



Roadmap

● Roadmap

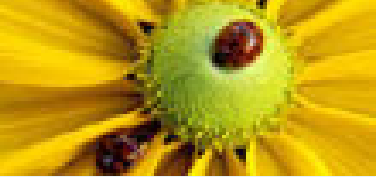
Introduction

Local Mail Utilities

Mail Server

Conclusion

- Introduction / Overview
- Local Mail Utilities & Configuration
- Running Your Own Mail Server?



- Roadmap

- Introduction

- Email Pipeline/Components?

- Lifecycle

Local Mail Utilities

Mail Server

Conclusion

Introduction



Email Pipeline/Components?

- MTA – Mail Transfer Agent (SMTP)
sendmail, qmail, Postfix, exim, Courier
- MDA – Mail Delivery Agent
procmail, maildrop (*or MTA*)
- Remote Access to delivered mail
POP3, IMAP, etc.
Dovecot, Courier, Cyrus IMAP, SquirrelMail
- MUA – Mail User Agent
Mutt, Gnus, Pine, etc.
- Mail tools
Fetchmail, SpamAssassin, BogoFilter, etc.

● Roadmap

Introduction

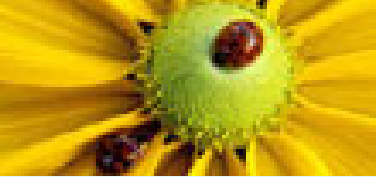
● Email Pipeline/Components?

● Lifecycle

Local Mail Utilities

Mail Server

Conclusion



Email Pipeline/Components?

- **MTA – Mail Transfer Agent (SMTP)**
sendmail, qmail, Postfix, exim, Courier
- **MDA – Mail Delivery Agent**
procmail, maildrop (*or MTA*)
- Remote Access to delivered mail
POP3, IMAP, etc.
Dovecot, Courier, Cyrus IMAP, SquirrelMail
- **MUA – Mail User Agent**
Mutt, Gnus, Pine, etc.
- **Mail tools**
Fetchmail, SpamAssassin, BogoFilter, etc.

● Roadmap

Introduction

● Email Pipeline/Components?

● Lifecycle

Local Mail Utilities

Mail Server

Conclusion

Lifecycle



● Roadmap

Introduction

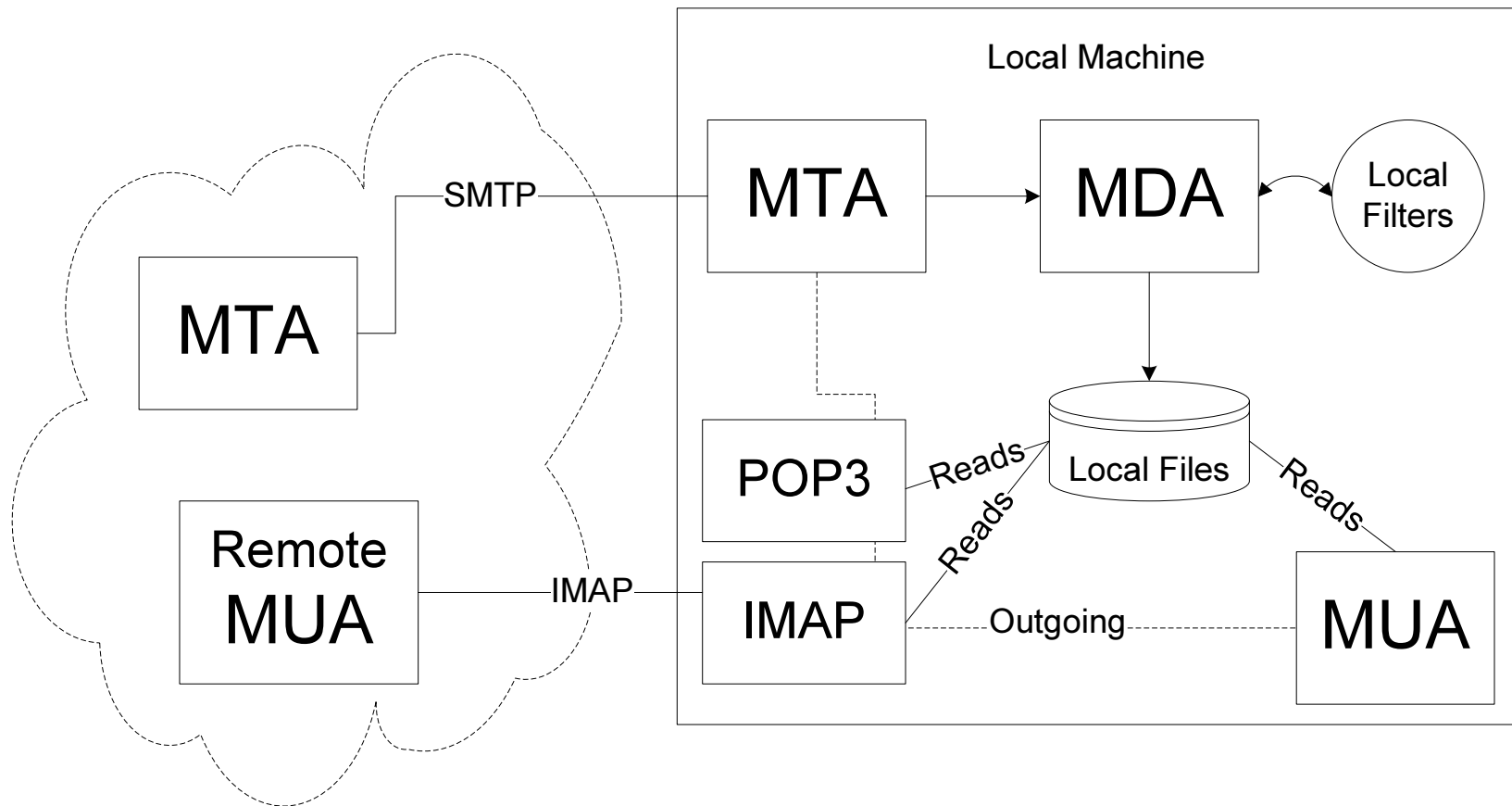
● Email Pipeline/Components?

● Lifecycle

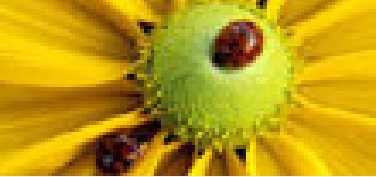
Local Mail Utilities

Mail Server

Conclusion



Lifecycle



● Roadmap

Introduction

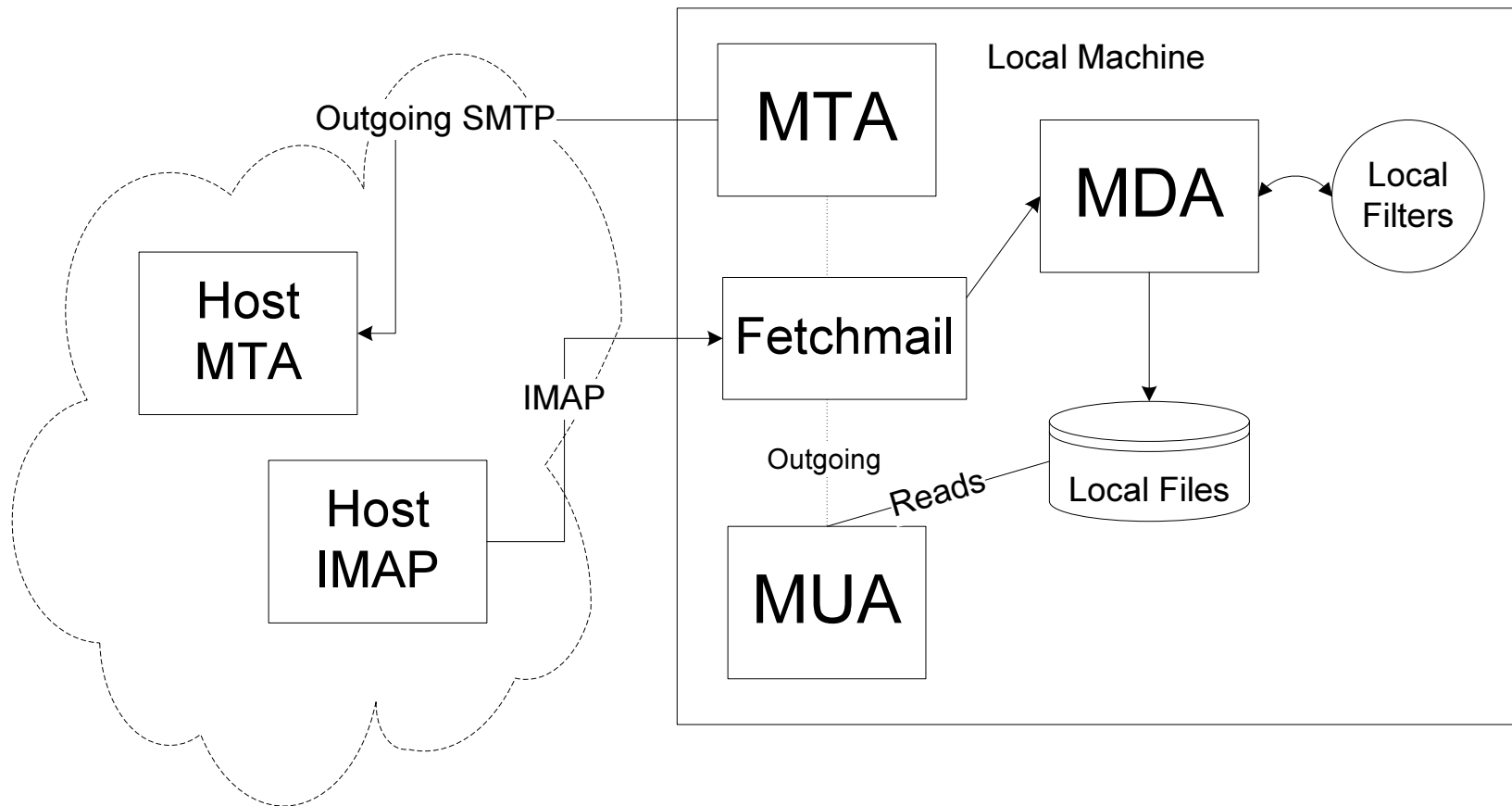
● Email Pipeline/Components?

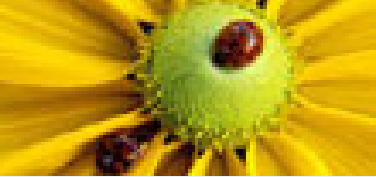
● Lifecycle

Local Mail Utilities

Mail Server

Conclusion





● Roadmap

Introduction

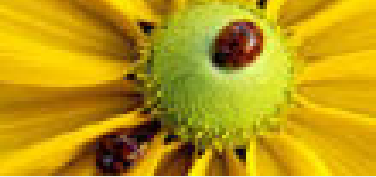
Local Mail Utilities

- One Possible Configuration
- Fetchmail
- Procmal
- SpamAssassin
- SpamAssassin Plugins

Mail Server

Conclusion

Local Mail Utilities



One Possible Configuration

- Remote server gets/sends mail
- Fetchmail – grabs mail to local machine
- Procmail – delivers mail on local machine
- SpamAssassin – filters spam
- Local MTA “smart-hosts” to remote server

This is a useful configuration even if you run your own mail server, because you may want to fetch and store/read your mail locally on a desktop.

● Roadmap

Introduction

Local Mail Utilities

● One Possible Configuration

● Fetchmail

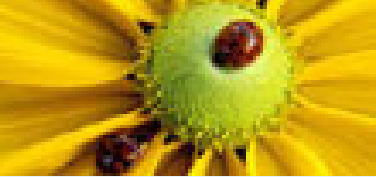
● Procmail

● SpamAssassin

● SpamAssassin Plugins

Mail Server

Conclusion



Fetchmail

- Two ways to run:
 - ◆ From crontab/mail client/manually
 - ◆ As daemon – supports IMAP IDLE

.fetchmailrc:

```
poll email2.cc.gatech.edu with proto imap:  
    user "davidhi" pass "12345678"  
    is "davidhi" here keep  
    mda "/usr/bin/procmail -d davidhi";  
    no rewrite ssl idle
```

```
poll mikkeli.cc.gatech.edu with proto imap preauth ssh:  
    plugin "ssh email 2> /dev/null";  
    user davidhi is davidhi here keep  
    mda "/usr/bin/procmail -d davidhi"
```

● Roadmap

Introduction

Local Mail Utilities

● One Possible Configuration

● Fetchmail

● Procmail

● SpamAssassin

● SpamAssassin Plugins

Mail Server

Conclusion



Procmail

- Filters/sorts/pipes mail, etc.
- Configure `.procmailrc` to specify mailboxes and rules

```
MAILDIR=$HOME/.incoming
```

```
DEFAULT=$HOME/.incoming/inbox
```

```
LOGFILE=$PMDIR/log
```

```
:0:
* < 256000
| spamc
:0:
* ^X-GT-Spam-Rating: #####
spam
```

```
:0:
* ^X-Spam-Status: Yes
spam
:0:
* ^Content-Transfer-Encoding: base64
* name=.*\.(exe|bat|scr|pif|com)
spam
```

● Roadmap

Introduction

Local Mail Utilities

● One Possible Configuration

● Fetchmail

● Procmail

● SpamAssassin

● SpamAssassin Plugins

Mail Server

Conclusion



SpamAssassin

● Roadmap

Introduction

Local Mail Utilities

● One Possible Configuration

● Fetchmail

● Procmal

● SpamAssassin

● SpamAssassin Plugins

Mail Server

Conclusion

■ Two ways to run:

◆ Per-invocation

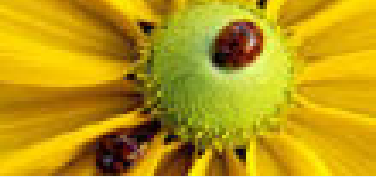
◆ `spamc client / spamd daemon`

■ system-wide config or

`~/ .spamassassin/user_prefs`

```
required_hits      5
whitelist_from     *@cc.gatech.edu
blacklist_from     *@microsoft.com

rewrite_subject    0
subject_tag        [SPAM]
```



SpamAssassin Plugins

● Roadmap

Introduction

Local Mail Utilities

● One Possible Configuration

● Fetchmail

● Procmail

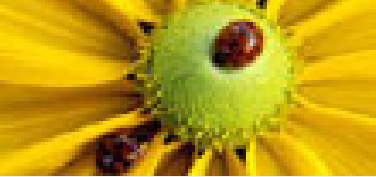
● SpamAssassin

● SpamAssassin Plugins

Mail Server

Conclusion

- ClamAV – detects malware attachments
- DNS-BL – blacklists like SORBS, Spamhaus
- DCC, Razor, Pyzor – distributed checksums
- Hashcash, SPF
- URI blacklists – SURBL.org
- Bayesian filtering: BogoFilter or built-in:
 - ◆ `sa-learn`
 - ◆ `use_bayes 1`
 - ◆ `bayes_auto_learn 1`



● Roadmap

Introduction

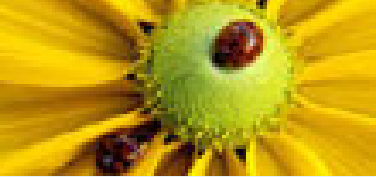
Local Mail Utilities

Mail Server

- Potential Issues
- Blueprint
- Sender Policy Framework
- DomainKeys

Conclusion

Mail Server



Potential Issues

- Different game today due to spam

- Caveats:

- ◆ Port 25 filtering

- ◆ Dynamic IP blacklists

- ◆ Reverse DNS doesn't match:

e.g. `c-69-180-23-68.hsd1.ga.comcast.net`

- ◆ Slightly used IP – already in DNSBL

● Roadmap

Introduction

Local Mail Utilities

Mail Server

● Potential Issues

● Blueprint

● Sender Policy Framework

● DomainKeys

Conclusion



Blueprint

● Roadmap

Introduction

Local Mail Utilities

Mail Server

● Potential Issues

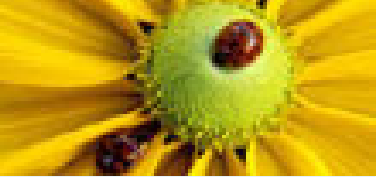
● **Blueprint**

● Sender Policy Framework

● DomainKeys

Conclusion

- Set up a mail server:
 - ◆ Postfix or exim
 - ◆ qmail
 - ◆ sendmail
- Make an MX record for your domain
- Set up SPF records
- Set up DomainKeys/DKIM
- Don't forget a backup MX



Sender Policy Framework

● Roadmap

Introduction

Local Mail Utilities

Mail Server

● Potential Issues

● Blueprint

● Sender Policy Framework

● DomainKeys

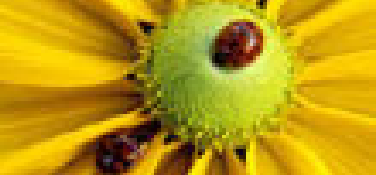
Conclusion

- Specifies who is allowed to send mail for a certain domain.

```
mit.edu.                60      IN      TXT
"v=spf1 ip4:18.7.7.0/24 ip4:18.7.21.0/24
      ip4:18.72.0.0/16 ~all"
```

```
ibm.com.                600     IN      TXT
"v=spf1 -all"
```

```
us.ibm.com.            600     IN      TXT
"v=spf1 ip4:32.97.182.0/24 ip4:32.97.110.0/24
      a:d25xlcore010.ca.ibm.com
      a:isource.boulder.ibm.com ~all"
```



DomainKeys

● Roadmap

Introduction

Local Mail Utilities

Mail Server

● Potential Issues

● Blueprint

● Sender Policy Framework

● DomainKeys

Conclusion

■ Cryptographic signatures

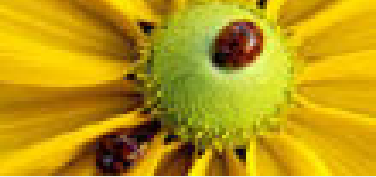
in email header:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
                d=gmail.com; s=gamma;  
                h=domainkey-signature:received:received:message-id:date:from:to:  
                bh=...;  
                b=...=
```

```
DomainKey-Signature: a=rsa-sha1; c=noFWS;  
                    d=gmail.com; s=gamma;  
                    h=message-id:date:from:to:subject:cc:in-reply-to:mime-version:co  
                    b=...=
```

lookup *selector._domainkey.domain*:

```
gamma._domainkey.gmail.com. 300 IN      TXT  
"k=rsa\; t=y\; p=MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQDIhyR3oItOy22ZOaB
```



- Roadmap

Introduction

Local Mail Utilities

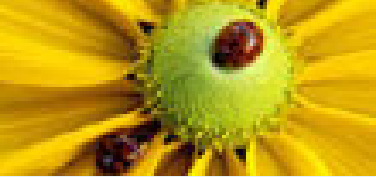
Mail Server

Conclusion

- Questions

- Resources

Conclusion



Questions

Questions?

● Roadmap

Introduction

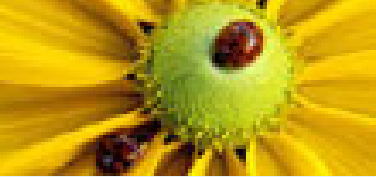
Local Mail Utilities

Mail Server

Conclusion

● Questions

● Resources



Resources

● Roadmap

Introduction

Local Mail Utilities

Mail Server

Conclusion

● Questions

● Resources

■ Fetchmail FAQ

<http://catb.org/~esr/fetchmail/fetchmail-FAQ.html>

■ Timo's procmail tips and recipes

<http://lipas.uwasa.fi/~ts/info/proctips.html>

■ Sender Policy Framework: Project Overview

http://www.openspf.org/Project_Overview

■ DomainKeys Identified Mail (DKIM)

<http://www.dkim.org>

■ Postfix

<http://www.postfix.org/>

■ exim Internet Mailer

<http://www.exim.org/>

■ qmail homepage

<http://www.qmail.org>

■ Sendmail FAQ

<http://www.sendmail.org/faq/>