Introduction au courrier Internet

Présenté par

Alain Patrick AINA

Roger YERBANGA

RALL 2007
22 - 26 Novembre 2007
Rabat, Maroc

Agents de courrier

- MUA = Mail User Agent
- Interagit directement avec l'utilisateur final

  Pine, MH, Elm, mutt, mail, Eudora, Marcel, Mailstrom, Mulberry, Pegasus, Simeon, Netscape, Outlook, ...
- Les MUA sont nombreux sur un système – l'utilisateur final choisit

- MTA = Mail Transfer Agent
- Reçoit et délivre des messages

  Sendmail, Smail, PP, MMDF, Charon, Exim, qmail,Postfix
- Un MTA par système – Choix du sysadmin

Format de message (1)

From: Philip Hazel <ph10@cus.cam.ac.uk>
To: Julius Caesar <julius@ancient-rome.net>
Cc: Mark Anthony <MarkA@cleo.co.uk>
Subject: How Internet mail works
Julius,
I'm going to be running a course on ...

- Le format est à l'origine défini par RFC822 en 1982
- Remplacé par RFC 2822
- Le message se compose de :

  Des lignes d'en-tête
  Un interligne
  Des lignes du corps de message

Format de message(2)

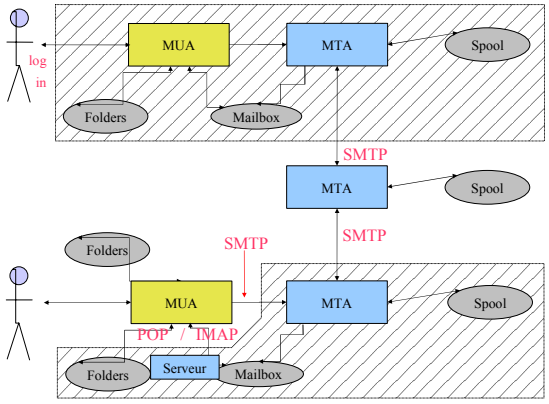
- Une adresse se compose d'une *partie locale* et d'un *domaine*

  aalain@*trstech.net*
- Un corps de message de base est non structuré

- D'autres RFC (MIME, 2045) ajoutent des entêtes additionnelles qui définissent la structure pour le corps

- MIME supportent des attachements de diverses sortes et dans divers codages

- Créer/décoder les attachements est le travail des MUA



Authentification des expéditeurs

- MUA incorporé utilise des appels inter-processus pour envoyer au MTA
  - -Il peut utiliser le pipe, le fichier, ou le SMTP interne au-dessus d'un pipe
  - -Le MTA connait l'identité de l'expéditeur
  - -Il insert l'entête *Sender :* si diffèrent du *From*:
- *MUA indépendant utilise SMTP pour envoyer*
  - *-MTA ne peut pas facilement distinguer les clients*
  - *-Aucune authentification dans le protocole de base*
  - *-Commande AUTH est dans l'extension SMTP*
  - *-Utilisation des sécurités additionnelles (TLS/SSL)*
  - *-Un MUA peut pointer vers n'importe quel MTA*
  - *- Besoin de contrôle du relayage (machine et le bloc IP)*

Un message en transit (1)

- Des en-têtes sont ajoutées par le MUA avant l'envoi

From: Philip Hazel <ph10@cus.cam.ac.uk>
To: Julius Caesar <julius@ancient-rome.net>
cc: Mark Anthony <MarkA@cleo.co.uk>
Subject: How Internet mail works

Date: Fri, 10 May 2002 11:29:24 +0100 (BST)
Message-ID: <Pine.SOL.3.96.990117111343.
19032A-100000@taurus.cus.cam.ac.uk>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII

Alain,
Je serai à l'heure au cours ...

Un message en transit (2)

- Des en-têtes sont ajoutées par les MTA

Received: from taurus.cus.cam.ac.uk
([192.168.34.54] ident=exim)
by mauve.csi.cam.ac.uk with esmtp
(Exim 4.00) id 101qxX-00011X-00;
Fri, 10 May 2002 11:50:39 +0100
Received: from ph10 (helo=localhost)
by taurus.cus.cam.ac.uk with local-smtp
(Exim 4.10) id 101qin-0005PB-00;
Fri, 10 May 2002 11:50:25 +0100
From: Philip Hazel <ph10@cus.cam.ac.uk>
To: Julius Caesar <julius@ancient-rome.net>
cc: Mark Anthony <MarkA@cleo.co.uk>

Un message en transit(3)

- Un message est transmis par une *enveloppe*

  MAIL FROM:<ph10@cus.cam.ac.uk>

  RCPT TO:<aalain@trstech.net>
- *L'enveloppe est séparée du message RFC 2822*
- *les champs de l'enveloppe (RFC 2821) n'ont pas besoin d'être identiques aux champs de l'en-tête (RFC 2822)*
- *Les MTA sont principalement concernés par des enveloppes (Juste comme la poste...)*
- *Les messages d'erreur ("rebond") ont un champ expéditeur nul*

  MAIL FROM:<>

Une session de SMTP (1)

telnet relay.ancient-rome.net 25

220 relay.ancient-rome.net ESMTP Exim ...

EHLO taurus.cus.cam.ac.uk

250-relay.ancient-rome.net ...

250-SIZE 10485760

250-PIPELINING

250 HELP

MAIL FROM:<ph10@cus.cam.ac.uk>

250 OK

RCPT TO:<julius@ancient-rome.net>

250 Accepted

DATA

354 Enter message, ending with "."

Received: from ...

Une session de SMTP(2)

From: ...

To: ...

etc...

.

250 OK id=10sPdr-00034H-00

quit

221 relay.ancient-rome.net closing conn...

Les codes retour de SMTP

2xx ok

3xx envoyez plus de données

4xx Echec temporaire

5xx Echec permanent

Contrefaçon du courrier

- Il est banal de forger un courrier non crypté et non signé
- C'est une conséquence inévitable quand les machines de l'expéditeur et du destinataire sont indépendantes
- Il est moins banal de forger vraiment bien!
- La plupart des SPAM contiennent habituellement certaines lignes d'en-tête forgée
- Être alerté par la contrefaçon au cours des investigations

Le Service de Nom de Domaine

- Le DNS est une base de données distribuée
- Les serveurs DNS s'appellent serveurs de nom
- Il y a plusieurs serveurs par zone
- Les serveurs secondaires sont de préférence en dehors du site
- Des enregistrements sont introduits par type et nom de domaine
- Les serveurs racines sont à la base de la hiérarchie
- Le cache sert à améliorer la performance
- Chaque enregistrement a une durée de vie(TTL)

Utilisation du DNS pour le courrier(1)

- Deux types d'enregistrement DNS sont utilisés pour le courrier
- *Mail Exchange (MX) fait correspondre les domaines à des serveurs, et fourni une liste de préférence:*

```
hermes.cam.ac.uk. MX 5 green.csi.cam.ac.uk.
                  MX 7 ppsw3.csi.cam.ac.uk.
                  MX 7 ppsw4.csi.cam.ac.uk.
```

- *Les enregistrements (A) font correspondre les noms aux adresses IP :*

```
green.csi.cam.ac.uk.  A  131.111.8.57
ppsw3.csi.cam.ac.uk.  A  131.111.8.38
ppsw4.csi.cam.ac.uk.  A  131.111.8.44
```

Utilisation du DNS pour le courrier (2)

- Les enregistrements MX ont été ajoutés au DNS après son déploiement initial
- Règle de compatibilité :

  "Si aucun enregistrement MX n'est pas trouvé, recherchez un enregistrement A, et si trouvé, traitez le comme un MX avec la préférence 0

- Les enregistrements MX ont été inventés pour des passages à d'autres systèmes de courrier, mais sont maintenant fortement utilisés pour manipuler des domaines génériques de courrier

Autres enregistrements DNS

- Le type d'enregistrement PTR fait correspondre les adresses aux noms

  57.8.111.131.in-addr.arpa. PTR green.csi.cam.ac.uk.

- Les enregistrements PTR et A n'ont pas besoin d'être un pour un

  ```
  ppsw4.cam.ac.uk.   A   131.111.8.33
  ```

  33.8.111.131.in-addr.arpa. PTR lilac.csi.cam.ac.uk.

- Les enregistrements CNAME fournissent une facilité d'alias

  pelican.cam.ac.uk. CNAME redshank.csx.cam.ac.uk.

Outils de consultation du DNS

- *host est facile à utiliser pour des requêtes simples*

  host demon.net

  host 192.168.34.135

  host -t mx demon.net

- *nslookup est plus largement disponible, mais est plus bavard*

  nslookup bt.net

  nslookup 192.168.34.135

  nslookup -querytype=mx bt.net

- *Dig est l'ultime outil*

  dig bt.net mx

  dig -x 192.158.34.135

Mystères du DNS

- Parfois les serveurs primaires et secondaires ne s'accordent pas

- Une fois mystifié, vérifiez le désaccord des serveurs

  host -t ns ioe.ac.uk

  ioe.ac.uk NS mentor.ioe.ac.uk

  ioe.ac.uk NS ns0.ja.net

  host mentor.ioe.ac.uk mentor.ioe.ac.uk

  mentor.ioe.ac.uk A 144.82.31.3

  host mentor.ioe.ac.uk ns0.ja.net

  mentor.ioe.ac.uk has no A record at ns0.ja.net (Authoritative answer)

Erreurs communes de DNS

- Points finaux manquant sur des noms dans les MX
- Les MX pointent vers des aliases au lieu des noms canoniques.

  -Ceci devrait fonctionner, mais est inefficace et déconseillé
- Les MX pointent vers des machines inexistantes
- Les MX pointent vers une IP au lieu d 'un nom

  -Malheureusement quelques MTA acceptent cela
- Les MX ne contiennent pas de préférence
- Certains serveurs de nom donnent une erreur de serveur pour des requêtes de MX inexistant

Routage d'un message

- Traiter les adresses locales

  Listes d'alias/Fichiers de transfert

- Reconnaitre les adresses distantes spéciales

  Exemple. Machines de clients locaux

- Recherchez les enregistrements MX pour les adresses distantes

- Si lui même dans la liste, ignorez tous les MX avec préférences >= à sa propre préférence

- Pour chaque MX, obtenez l'(es) adresse(s) IP

Livraison d'un message

- Effectuer la livraison locale
- Pour chaque livraison à distance
  - -Essayez de se connecter à chaque machine distante jusqu'au succès
  - -Elles acceptent ou rejettent de manière permanente le message
- Après des échecs provisoires, essayez plus tard
- Arrêt après trop de reports
- Les adresses sont souvent triées pour éviter d'envoyer des copies multiples

Vérification des expéditeurs entrants

- Beaucoup de messages sont envoyés avec de mauvaises enveloppes expéditeurs
  - Logiciel de courrier mal configuré
  - Domaines non enregistrés
  - Serveurs de nom mal configurés
  - Faussaires
- La contrefaçon semble être la plus grande catégorie
- Beaucoup de MTA vérifient le domaine de l'expéditeur
- Il est plus difficile de vérifier la partie locale
  - -Utilise beaucoup de ressources, et peut être assez lent
- Les messages de rebond n'ont pas enveloppe expéditeur

Vérification des destinataires

- Quelques MTA vérifient chaque destinataire local pendant la transaction SMTP
  - Les erreurs sont gérées par le MTA expéditeur
  - *Le MTA de réception évite des problèmes avec de mauvais expéditeurs*
- D'autres MTA acceptent des messages sans vérifier, et regarde les destinataires plus tard
  - Les erreurs sont gérées par le MTA de réception
  - Des messages d'erreur plus détaillés peuvent être générés
- La prolifération des expéditeurs forgés a rendu la première approche beaucoup plus populaire

Le contrôle de relais

- Incoming: De n'importe quel hôte aux domaines spécifiques
  - Par exemple : passerelle MTA entrant ou le MTA de sauvegarde
- Outgoing: Des machines spécifiques à n'importe où
  - Par exemple : passerelle sortante sur le réseau local
- Des machines authentifiées à n'importe où
  - Par exemple l'employé en déplacement ou le client d'un ISP connecté à un autre réseau
- Le chiffrage peut être utilisé pour la protection du mot de passe pendant l'authentification
- L'authentification peut également être faite en utilisant des certificats(SSL/TLS)

Les politiques de contrôles de courrier entrant

- Bloquez les réseaux et les machines malicieux connus

  Realtime Blackhole List (RBL), Dial-up list (DUL), etc.
  http://mail-abuse.org (payant maintenant) et autres

- Bloquez les expéditeurs malicieux connus
- Refusez les messages mal formés
- Reconnaissez les pourriels

  Détruire
  Enrichir ses bases de données