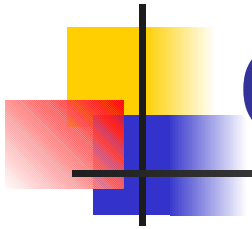
Signature des messages, un outil contre le spam ?

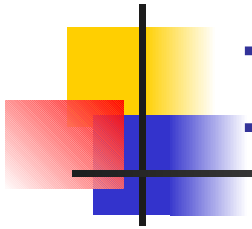
OSSIR groupe SUR 12/10/2004

François MORRIS : Francois.Morris@lmcp.jussieu.fr



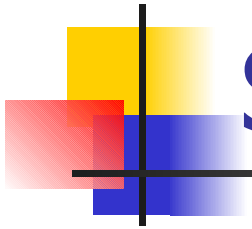
Constat

- Les spammeurs agissent masqués
  - Adresses usurpées
  - Adresses sans rapport avec le nom ou la raison sociale
- Mes amis ne m'envoient pas de spam



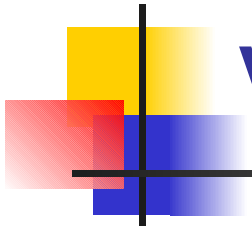
Idée

- Si je suis sûr de l'expéditeur, je peux plus facilement trier
- Techniques cryptographiques permettent d'authentifier l'émetteur d'un message
  - Empreinte (hash) : MD5, SHA-1
  - Chiffrement asymétrique (RSA)
    - Clé privée
    - Clé publique



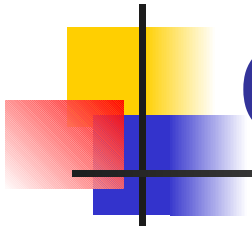
Signature d'un message

- Empreinte du message
- Chiffrement de l'empreinte à l'aide de la clé privée de l'expéditeur (signature)
- Envoi de la signature avec le message



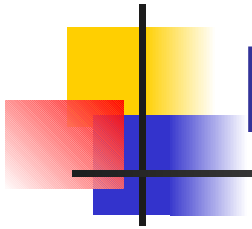
Vérification de la signature

- Déchiffrement de la signature avec la clé publique de l'expéditeur
- Calcul de l'empreinte du message
- Comparaison des deux



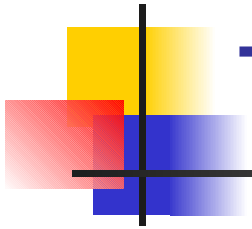
Ce que garantit la signature

- Celui qui a signé possédait bien la clé privée associée à la clé publique
  - Sinon déchiffrement impossible
- Mais pas nécessairement que le signataire en était le détenteur légitime
  - Il faut aussi une certification de la clé publique
- Intégrité du message



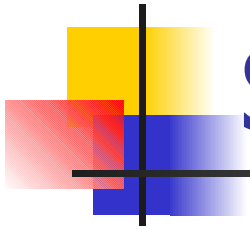
Les enjeux

- Distribution des clés publiques
- Comment être sûr que cette clé publique est bien celle de tel individu ?
- Même parfaitement identifié et authentifié l'expéditeur peut être un méchant



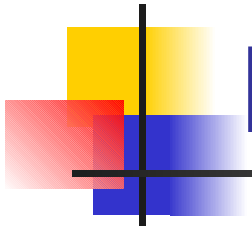
Terminologie

- MTA Message Transfer Agent
  - Transfert entre MTA : SMTP
- MUA Message User Agent
  - Lecture message
    - Fichiers
    - Serveur : IMAP, POP3
  - Envoi message
    - File d'attente du MTA
    - SMTP



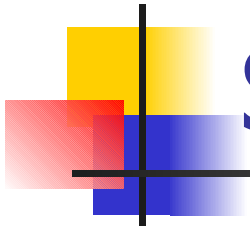
Structure d'un message

- Enveloppe
  - EHLO, MAIL FROM, RCPT TO
- En-têtes
  - From, To, Date, Subject, etc.
- Corps du message
  - Texte simple
  - MIME (Multipurpose Internet Mail Extensions) : structuration



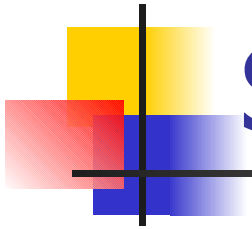
Les différentes techniques

- Sécurisation de bout en bout
  - S/MIME
  - PGP
- Sécurisation du canal
  - SMTPS, LMAP
- Signature par le MTA
  - DomainKeys
  - Identified Internet Mail
  - E-mail postmarks
  - MTA Signatures



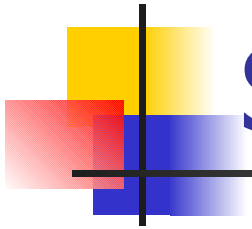
S/MIME, PGP

- De bout en bout
- Signé par l'expéditeur
- Signature ajoutée dans le corps du message
  - Attachement MIME pkcs#7 (S/MIME)
  - Séparateur ---- BEGIN PGP SIGNATURE ---
- Signé : contenu du message, pas les en-têtes
  - Subject : Free Viagra
  - From : Vérification au niveau du MUA
  - OK pour MTA qui modifient les en-têtes
  - Part: message/rfc822



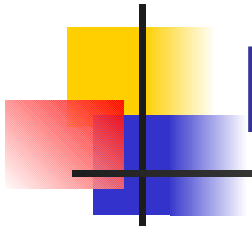
S/MIME, PGP

- Technologies éprouvées
  - Résiste bien au transit dans les différents MTA
    - Cependant certains sites refusent les messages signés
    - Impossibilité d'ajouter un texte (listes, avertissement)
  - Relativement bien géré par les MUA
    - Cependant certains MUA ne savent pas gérer les messages signés et envoient un avertissement dans ce cas
- Modèle de confiance
  - Association clé publique $\leftrightarrow$ individu
    - S/MIME
    - PGP



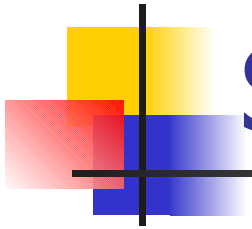
S/MIME

- Certificats X509
  - Complexe (ASN1)
- IGC
  - Lourd à mettre en œuvre
  - Un peu de technique et énormément d'organisation
- On fait confiance à des autorités de certification
- Analogie : document officiel (passeport)



PGP

- La clé publique d'un individu est certifiée par d'autres individus
- Modèle tribal
  - Les amis de mes amis sont mes amis
- En réalité le nombre moyen d'approbations reste faible
- Analogie : carte de membre du club de foot

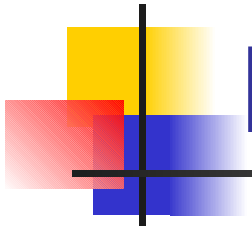


SMTPS

- Sécurise le canal de transmission entre 2 MTA
  - Authentification mutuelle (certificats)
  - Chiffrement
- Eprouvé
- Apporte peu dans la lutte contre le spam
  - Seul le MTA adjacent est authentifié
- Utile pour contrôler les émetteurs sur le réseau interne
  - Relais pour les nomades

Les technologies émergentes

- Pleine effervescence à l'IETF
  - Message Authentication Signature Standards (MASS)
    - BOF IETF (août 2004)
  - Entity-to-Entity S/MIME
  - DomainKeys
  - Identified Internet Mail
  - E-mail Postmarks
  - MTA Signatures

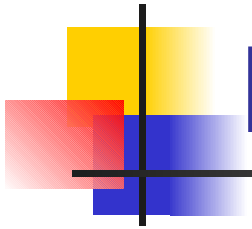


Entity-to-Entity S/MIME

- But : faciliter le déploiement de S/MIME
  - Pragmatique
  - Amélioration de la sécurité et non pas sécurité absolue
- Evolution du modèle S/MIME de bout en bout
  - Un MTA peut signer si le MUA de l'expéditeur n'a pas signé le message
  - Un MTA peut supprimer une signature si le MUA destinataire ne la supporte pas
  - Un MTA peut vérifier une signature et l'indiquer dans un en-tête

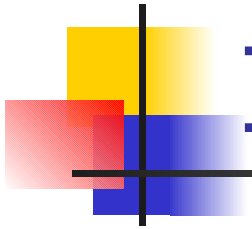
Entity-to-Entity S/MIME

- Verisign
- SMTP
  - Option SMIME en réponse EHLO
    - Le serveur saura traiter un MUA ne supportant pas S/MIME
- DNS
  - MTA Authorization Records un DNS (MARID)
    - Clé (domaine)
    - Certificat X509 (domaine)
- S/MIME
  - A définir



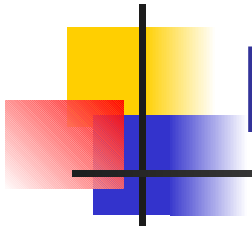
DomainKeys

- Yahoo
- Signature par le MTA
- En-têtes supplémentaires
  - Signature
  - Pointeur vers clé publique



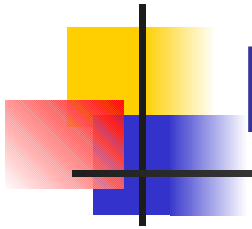
Identified Internet Mail

- Cisco
- Signature par le MTA
- En-têtes supplémentaires
  - Signature
  - Reproduit la structure d'un certificat dans l'en-tête



E-mail Postmarks

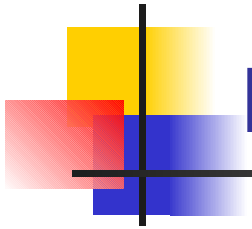
- Microsoft
- MIME PKC7 modifié
  - Signature
  - Certificats signataire



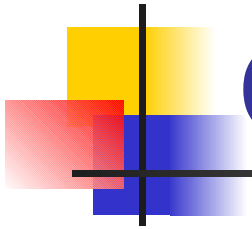
MTA Signatures

- En-tête supplémentaire
  - X-PostalTracking
- Une entité MIME (multipart/x-postal-data)
  - MIME header : attributs, comment vérifier
  - Fichier : pkcs7, signature

Comparaisons des différentes méthodes

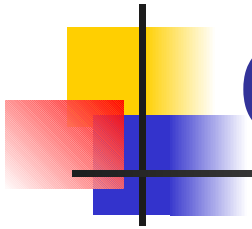


- Ce qui est signé
- Où est mis la signature
- Gestion de la clé publique



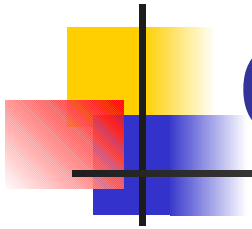
Ce qui est signé

- Corps du message
  - S/MIME, Entity-to-Entity S/MIME, E-Mail Postmarks
- Corps du message + tous les en-têtes
  - DomainKeys
- Corps du message + From + Subject + Date
  - Identified Mail
- Corps du message + From + Subject + Date + Received
  - MTA Signatures



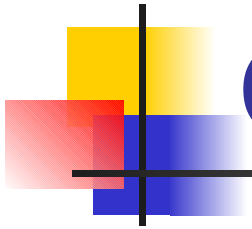
Que faut-il signer ?

- En-têtes sont importants
  - From, Subject, Date, etc.
  - Les MTA, gestionnaires de liste modifient, ajoutent, suppriment des en-têtes
- Question du From
  - Enveloppe
  - En-Tête
  - Autres : Sender, etc.



Où est mis la signature

- En-tête spécifique
  - DomainKeys, Identified Mail
- PKCS7
  - S/MIME, Entity-to-Entity S/MIME
- PKCS7 modifié (certificats additionnels)
  - E-Mail Postmarks
- PKCS7 dans postal-data (part supplémentaire)
  - MTA Signatures

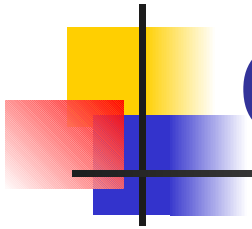


Gestion de la clé publique

- Certificat x509 + CA root
  - S/MIME, Entity-to-Entity S/MIME
  - E-Mail Postmarks (1)
  - MTA Signatures (1) : via http ou ftp
- DNS TXT
  - DomainKeys : référence dans en-tête
  - E-Mail Postmarks (2) : CN -> DNS TXT (_ep.domain) qui contient du XML

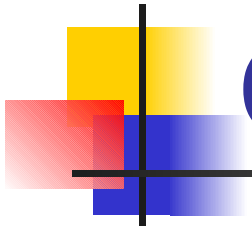
Gestion de la clé publique

- DNS KEY
  - MTA Signatures (2)
- En-tête + service de vérification
  - Identified Mail : référence vers un DNS SRV qui via http permet de vérifier la clé publique



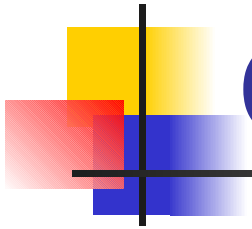
Gestion de la clé publique

- C'est le point délicat
- Grosses lacunes : drafts, discussions
- Comment initier la confiance ?
  - Clé publique par canal sûr (main à la main)
  - IGC, ramené au CA root
    - Acceptation de la politique de certification du CA
  - DNS ?
- Ne pas perdre de vu l'objectif
  - Lutte contre le spam
  - Pas signature de documents officiels



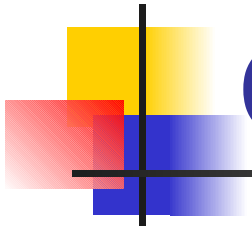
Questions

- Qui signe quoi ?
- Certificats et IGC
- Brevets et licences
- Ressources consommées
- Compatibilité avec l'existant
- Autres techniques que la signature



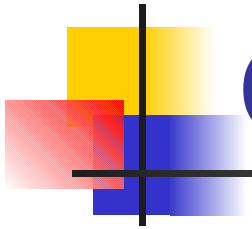
Qui signe quoi ?

- MUA
  - L'utilisateur qui a écrit son message
- MTA
  - Message reçu par le MTA
  - Contrôles de l'expéditeur
    - Machine émettrice (IP)
    - Données de connexion
    - Authentification SMTP, TLS
  - Virus qui envoie le message



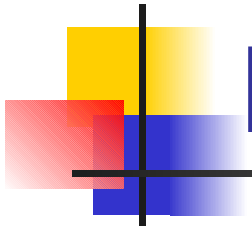
Certificats et IGC

- Réputation justifiée de complexité et de lourdeur
  - ASN1
  - Formalisme dans l'organisation
    - Politique de certification
    - Déclaration des pratiques de certification
- Complexité inhérente
  - Invention d'une usine à gaz pour remplacer les IGC



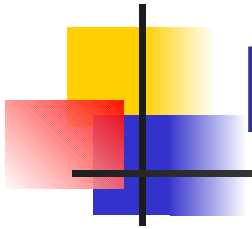
Certificats et IGC

- En-tête dont la complexité n'a rien à envier à un certificat
- Enregistrement DNS codé en XML
- Points délicats remis à plus tard dans les drafts
  - Révocation
  - Chaîne de confiance



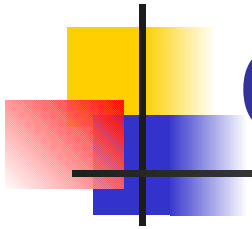
Brevets et licences

- Revendications
  - Yahoo, Microsoft, etc.
- Incompatibilités
  - Licence GNU
- Obstacles au développement



Ressources consommées

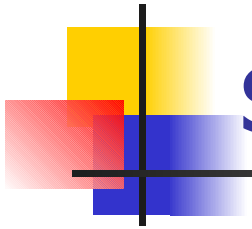
- Bande passante (signature augmente la taille des messages)
  - Si cela peut réduire le spam
  - Est-ce si grave ?
  - Les MUA ont besoin des en-têtes (IMAP)
- MTA
  - Générer, vérifier une signature
  - Récupération des clés publiques
  - Le prix à payer



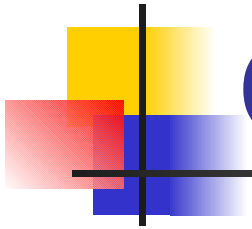
Compatibilité avec l'existant

- Plus facile d'agir sur les MTA que les MUA
  - Difficile (impensable ?) de changer les applications sur les postes utilisateurs
- Beaucoup de questions ouvertes
  - Liste de distribution
  - Forward
  - Bounces

Autres techniques que la signature

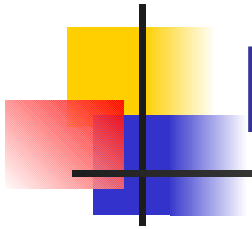


- Vérification de l'expéditeur au niveau de l'enveloppe
  - SPF
  - Sender-ID
- A considérer



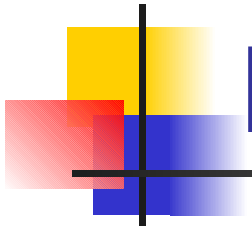
Quelques expériences

- Messages signés S/MIME
- DomainKeys + sendmail



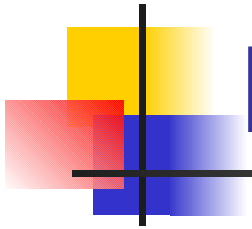
Messages signés S/MIME

- Situation
  - Le MUA vérifie bien la signature
  - Impossibilité de classer automatiquement les messages ayant une signature valide
    - Trop complexe pour les filtres intégrés
      - MUA (Mozilla)
      - Distribution des messages (sieve)
    - Règle possible pour message signé mais sans vérification : un peu juste



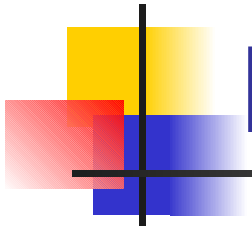
Messages signés S/MIME

- Ajout par le MTA final d'un en-tête
  - Signature valide ou non
    - Facile à utiliser dans un filtre
  - Plus exactement au niveau de l'antivirus et marquage de spam
    - amavisd-new
      - Patch
      - Commandes openssl
      - Configuration des CA root autorisés



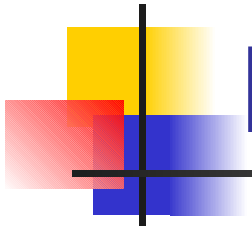
Messages signés S/MIME

- Retour d'expérience
  - Cela fonctionne
  - Assez limité
    - Peu de messages signés
      - Quelques interlocuteurs
      - Avis de sécurité
    - Dossier de messages fiables à consulter en priorité



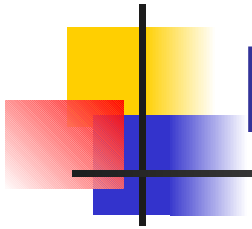
DomainKeys + sendmail

- Jose Marcio Martins da Cruz
  - jose-marcio.martins@ensmp.fr
  - j-chkmail
- Filtre milter
  - 1000-2000 lignes de C
  - Openssl
- Fichier config
  - Les MTA que l'on signe
  - On vérifie les autres
- Fiable, peu gourmand en ressource (~10%)



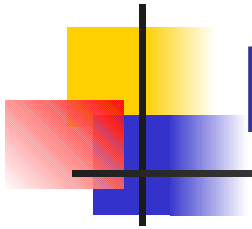
DomainKeys + sendmail

- MTA bordure entrée
  - 1 er filtre DomainKey
    - Signature invalide $\rightarrow$ poubelle
    - Non signé $\rightarrow$ filtrage normal
    - Signature valide
      - $\in$ liste blanche $\rightarrow$ filtrage allégé
      - $\notin$ liste blanche $\rightarrow$ filtrage normal
- MTA bordure sortie
  - DomainKey dernier filtre



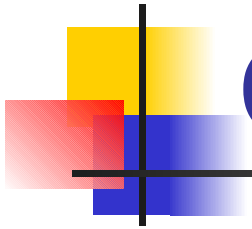
DomainKeys + sendmail

- Problèmes rencontrés
  - Canonisation
    - Espaces dans les en-têtes
  - En-têtes signés
    - Indication de la liste et de l'ordre
  - Modification du draft
- Prometteur
  - Vaut vraiment le coup de poursuivre



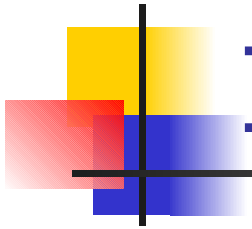
Du bon usage de la signature

- Le spam pourra être signé
  - Création d'un domaine, de clés, envoi de spam puis disparition
- Dans un domaine, du bon et du moins bon
  - ibm.com : des échanges et de la pub
  - hotmail : des connus et des inconnus
- White list
  - Domaine
  - Individu



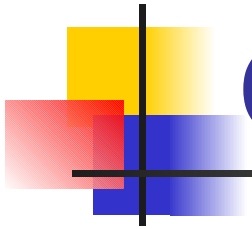
Condition sine qua non

- Opérateurs, FAI
  - Signent
  - Vérifient auparavant l'expéditeur
- Doutes
  - Actuellement quel opérateur interdit l'envoi de message dont l'adresse de l'expéditeur est manifestement usurpée ?
  - La signature entraînera-t-elle un surcroît de civisme ?
- Différents degrés de confiance



Illusions de la technique

- Ne surtout pas croire que la technique puisse tout résoudre
- L'anti-spam c'est aussi et surtout
  - Régulation
    - Lois et leur application
    - Codes de bonne conduite
    - Contrats entre FAI, avec les utilisateurs
  - Comportements des différents acteurs
  - Economie
    - Le spam rapporte



Conclusion

- La signature des messages peut être une aide pour lutter contre le spam
- Sûrement pas une panacée
- A suivre