



La signature des messages : une réponse contre le spam ?

Une nouvelle approche, le MTA de l'expéditeur endosse le message et le signe.
Une réputation se mérite.



Plan

- La signature réponse à l'usurpation
- Les limites de PGP, S/MIME
- Signature par le MTA (Message Transfer Agent)
 - DKIM (DomainKey Internet Mail)
 - SSP (Sender Signing Policy)
- Questions sur le déploiement de DKIM et SSP



Constat

- Les spammeurs agissent masqués
 - Adresses usurpées
 - Adresses sans rapport avec leur nom ou leur raison sociale : p234tty@ayuitjsph.com
- Les gens respectables n'envoient pas de spam
 - Je les connais : mes amis
 - Ils appartiennent à un organisme sérieux
- Notion fondamentale de réputation



Idée

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



Signature d'un message

- Condensé du message
- Chiffre le condensé à l'aide de la clé **privée** de l'**expéditeur** → signature
- Envoi de la signature avec le message



Vérification de la signature

- Réception du message et de la signature associée
- Récupère la clé publique de l'expéditeur
- Déchiffre la signature avec la clé **publique** de l'**expéditeur**
- Calcul du condensé du message
- Comparaison des deux



Ce que garantit la signature

- Intégrité du message
 - Nul n'a pu le modifier
- Celui qui a signé possédait bien la clé privée associée à la clé publique
 - Sinon déchiffrement impossible
- Mais pas nécessairement l'identité du signataire ni que celui-ci est le détenteur légitime de la clé
 - Il faut aussi une certification de la clé publique



Les enjeux

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



Les différentes techniques

- Sécurisation de bout en bout
 - PGP
 - S/MIME
- Sécurisation du canal
 - SMTPS, LMAP (Lightweight MTA Authentication Protocols)
- Signature par le MTA
 - MASS (Message Authentication Signature Standards)
 - DomainKeys (Yahoo) : implémenté
 - Identified Internet Mail (Cisco)
 - DKIM (DomainKeys Identified Mail) : en devenir



PGP, S/MIME

- De bout en bout
 - Signé par l'expéditeur
 - Vérifié par le destinataire
- Objectif premier confidentialité (chiffrement)
- Signature ajoutée dans le corps du message
 - Séparateur ----- BEGIN PGP SIGNATURE ---
 - Attachement MIME pkcs#7 (S/MIME)
- Signé : corps du message, pas les en-têtes
 - Subject : Cheap Viagra
 - From : Vérification au niveau du MUA



PGP, S/MIME

- Technologies éprouvées
 - Résiste bien au transit dans les différents MTA
 - Ignore les en-têtes
 - Certains sites refusent les messages signés
 - Impossibilité d'ajouter un texte (listes, avertissement)
 - Relativement bien géré par les MUA
 - Certains MUA n'apprécient pas les messages signés
- Mais peu utilisées
 - Complexité
 - Produits mal adaptés
 - Difficultés organisationnelles : IGC



SMTPS

- Sécurise le canal de transmission entre 2 MTA
 - SSL/TLS
 - Chiffrement
 - Authentification mutuelle (certificats)
- Epruvé
- Apporte peu dans la lutte contre le spam
 - Seul le MTA adjacent est authentifié
- Contrôle des émetteurs sur le réseau interne
 - Authentification des expéditeurs
 - Relais ouvert pour des nomades authentifiés



LMAP

- Lightweight MTA Authentication Protocol
- SPF
 - MARID SenderID (SPF + CallerID) : fini
 - Survivant
- Vérification que le MTA distant a bien le droit d'émettre pour cet expéditeur
 - Au niveau de l'enveloppe
 - DNS



Faciliter le déploiement de la signature

- Signature et vérification par le MTA et non plus le MUA
 - Plus facile d'agir sur les MTA que les MUA
 - Difficile (impensable ?) de changer les applications sur les postes utilisateurs
- Se passer d'IGC
 - Récupération de la clé publique : DNS



DKIM

- Ajout d'un en-tête spécifique
 - DomainKey-Signature
 - DKIM-Signature
- Syntaxe
 - Différents champs, séparateur : ;
 - Champ : paramètre=valeur
- Rien d'autre => impact minimal
 - MTA
 - MUA



DKIM Algorithmes

- Paramètre : a
- Chiffrement
 - rsa
- Hachage
 - sha1
- Exemple : a=rsa-sha1
- Prévoir de nouveaux algorithmes



DKIM : ce qui est signé

- En-tête
 - Séquence ordonnée de champs
 - Paramètre : h
 - DKIM-Signature – la signature (b=)
- Corps du message
 - Limite possible : paramètre l
 - Permet des ajouts en fin de messages
 - Très controversé



DKIM : forme canonique

- Résister aux modifications effectuées par certains MTA : ajout, suppression d'espaces
- En-tête
 - simple : aucun changement
 - relaxed : minuscule, 1 seul espace
- Corps
 - c=simple : ignore lignes vides à la fin
 - c=relaxed : blancs en fin de lignes, 1 seul espace
 - Controversé
- Exemple c=relaxed/simple



DKIM : signature

- Paramètre b
- Base64



DKIM : clé publique

- `d=example.com` : domaine pour récupérer la clé
- `s=dec2005` : sélecteur
- `q=dns` : méthode
- `i=user@eng.example.com` : pour qui le MTA signe
- Requête DNS (RR TXT) :
`nov2005._domainkey.example.com`



DNS : clé publique

- k=rsa; h=sha1; p=...
 - p vide => clé révoquée
- Options
 - t=y : DKIM en test, commencer par là
 - s= : usage de la clé *, email
 - g= : * (défaut) ou partie locale de i=



DNS vs IGC

- Plus simple
- Non sécurisé
 - Nombreuses attaques possibles
 - DNSSec
- Aucune certification de l'émetteur de la clé
 - Pas de chaîne de confiance
- Objectifs limités
 - Décourager les usurpations d'identité
 - Pas une preuve absolue de l'engagement de l'expéditeur



SSP

- Sender Signing Policy
 - Le plus intéressant et prometteur
 - Objet de multiples discussions sur les implications
- Politique définie au niveau du domaine
 - Expéditeur (à droite de @)
 - Si non définie on remonte d'un niveau



SSP DNS

- Publication DNS (TXT) :
_policy._domainkey.<domain>
<user>._policy._domainkey.<domain>
- 0=
 - ~ : certains mais pas tous
 - - : tous, signature par un tiers permise
 - ! : tous, pas de signature par un tiers
 - . : n'envoie pas de message
 - ^ : répéter au niveau utilisateur



SSP avantages

- Gain immédiat et égoïste
 - Un domaine qui signe tout, pourra refuser tout message non signé provenant de son propre domaine : usurpation certaine
 - N'implique pas les autres
- Domaines de confiance
 - Listes blanches fiables pour les domaines qui signent et que je connais
 - Déploiement dans notre environnement réaliste. Pas besoin d'attendre que tout le monde signe.



DKIM répétition (replay)

- DKIM vulnérable au spam signé
 - Envoi d'un message à partir d'un FAI sérieux qui signe
 - Récupère le message et envoi massif tel quel
- Pas de lien entre les RFC 2821 et RFC 2822 pour le destinataire
 - RCPT TO (enveloppe), To, Cc, Bcc (en-tête)
 - Imposer des contraintes : tentant mais dangereux



Situation

- DomainKey implémenté
- DKIM draft
 - Consensus difficile à trouver
 - Dérives : trop en demander
- SSP draft
 - Protocole : des points en suspend
 - Utilisation pratique : tout reste à faire



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
 - Appose son tampon
 - Virus qui envoie le message



Conditions au déploiement

- Opérateurs, FAI
 - Signent après vérification préalable de l'expéditeur
- Un long chemin à parcourir
 - Actuellement peu d'opérateurs interdisent 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
 - Analogie avec la politique de certification et la déclaration des pratiques de certification



Réputation

- Qualité des contrôles par le signataire
 - Plus ou moins laxistes
- Nature du signataire
 - FAI avec des clients \neq entreprise avec des employés
- Déterminer la réputation
 - Elle se gagne par son comportement
 - Liste locale
 - Serveur : agences de notations (S&P AAA \rightarrow D)
- Domaine totalement ouvert



MTA vérificateur

- Rejeter des messages
 - Signé ou non, signature valide ou non
 - Politique de l'émetteur
 - Sa propre politique
- Authentication-Results: mail.exemple.fr
from=alice@yahoo.fr; domainkey=pass
 - La « bonne solution »



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

- Beaucoup de questions ouvertes
 - Liste de distribution qui signe ?
 - Simple redistribution : expéditeur ?
 - Modérée : liste ?
 - Forward
 - Bounces
 - Tout ce que l'on n'a pas prévu
 - Avancer avec une grande prudence



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
 - marchand.com : des échanges et de la pub
 - FAI : des expéditeurs connus et d'autres inconnus
- Authentification permet des listes blanches fiables
 - Domaine
 - Individu



Engagements du signataire

- Identifier, authentifier l'expéditeur
 - Gestion des identités
- Approbation implicite du contenu
 - Respect de la politique interne
 - Chartes
- Prestataire extérieur
 - Contrat



Conclusion

- La signature des messages peut être une aide pour lutter contre le spam
 - Sûrement pas une panacée
 - Attention à l'illusion de la technique
 - Complémentaire avec d'autres techniques
 - Droit, contrat
- A suivre : norme ou sélection darwinienne ?
- Impose une réflexion
 - Architecture
 - Politique