RFC 7444 : Security Labels in Internet Email

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 février 2015

Date de publication du RFC : Février 2015

https://www.bortzmeyer.org/7444.html

On a souvent besoin, lorsqu'on transmet un document, d'indiquer le niveau de sensibilité ou de confidentialité du document. Quelque chose du genre **SECRET** ou **CONFIDENTIEL**. Cela peut être fait de manière non structurée, par du texte (par exemple dans l'objet du message) mais cela ne permet pas aux logiciels d'agir automatiquement sur la base de ce texte. D'où l'idée d'un nouveau champ dans l'en-tête du message, `SIO-Label:`, pour indiquer de manière structurée la sécurité souhaitée pour ce message.

Dans beaucoup d'organisations (l'armée étant un exemple typique), la présence d'une telle indication a des conséquences pratiques comme « les documents marqués **CONFIDENTIEL** ou supérieur doivent être enfermés dans un coffre quand on sort du bureau » ou bien « on ne doit envoyer les documents marqués **SECRET** qu'aux gens disposant de telle habilitation ». D'où l'importance de pouvoir indiquer ces niveaux de sécurité. À noter qu'ils sont présentés et discutés dans la norme UIT X.841 <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.841>, "*Security information objects for access control*".

Le protocole XMPP avait déjà une norme pour les niveaux de sécurité, XEP-0258 <http://xmpp.org/extensions/xep-0258.html>. Ce nouveau RFC part des mêmes concepts et les applique au courrier électronique (RFC 5322 [1]).

La section 1.1 de notre RFC rappelle les anciennes méthodes. Typiquement, on met en avant un texte qui indique le niveau de sécurité. Par exemple :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5322.txt

```
To: author <author@example.com>
From: Some One <someone@example.net>
Subject: [SECRET] the subject

SECRET

Text of the message.

SECRET
```

Dans ce message à la syntaxe RFC 5322, le niveau de sécurité (SECRET) a été mis dans le champ `Subject:` (encadré entre crochets pour être clairement séparé de l'objet normal), et répété au début (marquage FLOT "*First Line Of Text*") et à la fin (LLOT "*Last Line Of Text*") du message. De telles conventions sont fréquentes dans une communauté donnée (par exemple dans la même organisation, ou bien dans un groupe de gens travaillant sur le même projet). Elles vont sans doute continuer à être utilisées pendant longtemps, le nouveau système venant juste d'être spécifié. Pour un humain, même distrait, ces marques indiquent clairement le caractère secret du message. Mais, comme indiqué plus haut, ce n'est pas exploitable par un logiciel.

On notera que le RFC 2634 proposait déjà un mécanisme pour ces niveaux de sécurité, lié à l'utilisation de S/MIME. Notre nouveau RFC spécifie une solution alternative (S/MIME n'a pas été un grand succès...), plus légère. La solution du RFC 2634 était très perfectionnée (avec signature pour éviter qu'un tiers malveillant ne modifie les marques). Ici, on fait plus simple et on suppose qu'il existe un autre mécanisme pour assurer l'intégrité.

Donc, la solution nouvelle est de mettre un champ `SIO-Label:` dans le message. On suppose que le MUA proposera à l'utilisateur une liste de choix possibles et, une fois le choix fait, le logiciel le traduira dans le format standard. Les MTA et MDA pourront utiliser ce champ pour prendre des décisions. Par exemple, si un MTA a été configuré pour faire suivre automatiquement le courrier de `jean@example.com` à `marie@internautique.fr`, il pourra refuser de faire suivre un message marqué SECRET, ne sachant pas si la destinataire a l'habilitation nécessaire. Autre utilisation, le MUA du destinataire pourra afficher clairement le niveau de sécurité. On peut imaginer bien d'autres usages, comme le tri automatique des messages dans des dossiers différents selon le niveau de sécurité.

Les intermédiaires comme les MTA sont autorisés à modifier le champ `SIO-Label:` (ou l'ajouter s'il n'est pas présent) et, dans ce cas, il doivent indiquer les anciennes valeurs dans le champ `SIO-Label-History:` qui, comme son nom l'indique, garde trace des changements effectués.

La section 4 décrit formellement la grammaire des nouveaux en-têtes. `SIO-Label:` comprend une série de paramètres, chacun formé d'une clé et d'une valeur. Le paramètre principal est sans doute `label` qui indique le niveau de sécurité. Quelles valeurs peut-il prendre ? Plutôt que d'essayer de normaliser une liste de valeurs (ce qui ne marchera jamais, chaque organisation ayant déjà sa liste), notre RFC délègue à d'autres normes, indiquées par le paramètre `type`. Ainsi, `type=":ess"; label="MQYGASkCAQM="` indique que le type est ESS ("*Enhanced Security Services for S/MIME*", RFC 2634, déjà cité) et le `label` est alors un encodage en BER d'une étiquette ESS. Un `type :x411` va indiquer un encodage BER d'une étiquette de sécurité X.411. Enfin, un type `:xml` indique que le `label` est l'encodage en Base64 d'un élément XML qui, on le suppose, fera référence à une norme de niveaux de sécurité (si `label` est trop long, il peut être écrit en plusieurs fois, avec un astérisque et un numéro d'ordre derrière `label`). Dans cet exemple, la norme est `http://example.com/sec-label/0` (un exemple imaginaire) :

```
       type=":xml";
       label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
       label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
       label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
       label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
       label*4="YXRpb24+PC9TZWNMYWJlbD4=";
```

Ce qui se traduit, une fois le Base64 décodé, par :

```
<SecLabel xmlns="http://example.com/sec-label/0">
       <PolicyIdentifier URI="urn:oid:1.1"/>
       <Classification>3</Classification>
</SecLabel>
```

Un autre paramètre fréquent est `marking` qui indique le texte à afficher à l'utilisateur (`marking="FOR YOUR EYES ONLY";`). Si vous êtes un vrai paranoïaque, vous avez déjà noté que rien ne garantit que ce texte soit cohérent avec le vrai niveau de sécurité, `label` (cf. section 7). Plus rigolos, `fgcolor` et `bgcolor` permettent de suggérer des couleurs à utiliser pour l'affichage, couleurs indiquées par un code hexadécimal ou un nom (cela me semble une mauvaise idée : l'intérêt des niveaux de sécurité écrits sous une forme structurée est justement que le logiciel qui les affichera aura toute l'information pour choisir une couleur adaptée à son utilisateur). En combinant ces paramètres, un en-tête complet pourrait être :

```
SIO-Label: marking="TOP SECRET";
       fgcolor= #000011; bgcolor=fuschia;
       type=":x411"; label="MQYGASkCAQM="
```

On a vu qu'un logiciel de courrier était autorisé à modifier les niveaux de sécurité. Dans ce cas, pour permettre l'analyse de ce qui s'est passé, il devrait enregistrer le niveau précédent dans l'en-tête `SIO-Label-History:`, normalisé dans la section 5 de notre RFC. Cet en-tête de traçabilité (comme `Received:`) indique si le `SIO-Label:` a été ajouté par le logiciel, supprimé ou modifié. Voici un exemple où le message a été modifié deux fois, par l'ajout d'un niveau, puis par sa suppression :

```
SIO-Label-History: marking="EXAMPLE CONFIDENTIAL";
       type=":ess"; label="MQYGASkCAQM=";
       change=delete;
       changed-by="smtp.example.com";
       changed-at="18 Feb 2013 9:24 PDT";
       changed-comment="Pas confiance dans celui-là, je supprime"
SIO-Label-History: new-marking="EXAMPLE CONFIDENTIAL";
       new-type=":ess"; new-label="MQYGASkCAQM=";
       change=add;
       changed-by="smtp.example.net";
       changed-at="18 Feb 2013 7:24 PDT";
       changed-comment="Pas de niveau indiqué, j'en mets un"
```

Les deux en-têtes `SIO-Label:` et `SIO-Label-History:` sont désormais dans le registre des en-têtes <https://www.iana.org/assignments/message-headers/message-headers.xml>.

La bonne utilisation de ces niveaux de sécurité nécessite quelques précautions (section 7 du RFC). Par défaut, le message, y compris ses en-têtes et donc y compris `SIO-Label:`, n'est pas protégé et un méchant peut donc mettre un faux niveau ou modifier un niveau existant. Ce RFC ne fournit pas à lui seul de services de sécurité et ne dispense donc pas de mettre des protections adaptées, comme PGP pour assurer la confidentialité du message ou TLS pour qu'il soit transporté sans modification.

À noter également un paradoxe des niveaux de sécurité : leur seule présence donne déjà une indication à un éventuel espion. Si OSS 117 est dans un bureau du KGB et n'a que quelques secondes pour choisir les documents à emporter, le fait que les documents les plus intéressants soient marqués en gros « ultra-secret » va l'aider. C'est encore plus vrai si les niveaux de sécurité sont trop parlants, du genre « "*Project Roswell/Area51 Secret*" ».

Je ne connais pas de mise en œuvre de ce RFC. Certains clients de messagerie ont déjà des niveaux de sécurité, utilisant d'autres normes. Voir par exemple TrustedBird `<http://adullact.net/plugins/mediawiki/wiki/milimail/index.php/Security_Labels/fr>`, présenté aux JRES en 2009 `<https://2009.jres.org/planning_files/summary/html/126.htm>`. Si vous êtes intéressés par ces questions, vous pouvez aussi regarder la spécification de XIMF `<http://adullact.net/plugins/mediawiki/wiki/milimail/index.php/XIMF_XML_tags/fr#Element_securityLabel>`.