COPENHAGUE – Atelier sur les DNSSEC - 3ème partie
Mercredi 15 mars 2017 – 13h45 à 15h00 CET
ICANN58 | Copenhague, Danemark

JULIE HEDLUND : Merci, encore une fois, pour votre participation à la troisième partie de l'atelier DNSSEC. Je m'appelle Julie et je suis membre du personnel de l'ICANN.

Je vais donc organiser la dernière partie de cet atelier. Et ce que j'aimerais vous dire, c'est que je suis très heureuse de vous présenter notre intervenant suivant, Vittorio Bertola, qui est de Open-Xchange, et qui va nous parler de la confiance pour les services d'e-mail.

VITTORIO BERTOLA : Merci beaucoup pour cette opportunité de vous présenter ce qu'on va faire. En fait, je participe à mon premier atelier DNSSEC. Il y a 10 ans, je participais régulièrement aux réunions de l'ICANN. Mais ça fait un moment que je ne suis pas venu, donc je ne savais pas trop à quoi m'attendre. Et donc j'espère qu'on pourra parler un petit peu des problèmes techniques et rentrer un petit peu dans les problèmes plus détaillés à l'avenir. Mais étant donné que c'est la première fois, je vais simplement faire une présentation initiale.

Alors, comme vous le savez, nous sommes une société de logiciels d'e-mail et de DNS, à la base. Donc le transfert des e-mails n'est pas sécurisé aujourd'hui, comme vous le savez. Il y a des personnes qui travaillent dans ce secteur et qui ne le savent même pas. Mais si vous utilisez Apple, en général, les utilisateurs pensent que c'est très sécurisé. C'est vrai qu'il y a protection et authentification, mais en fait, le chiffrement, l'authentification des e-mails, n'est pas suffisant de nos jours. Et donc l'industrie, de manière générale, est responsable de cela. Parce que cette pratique veut dire que les messages, en fait, s'intersectent à différents niveaux. Et pourtant, c'est le choix de tout le monde pour partager des documents et des informations.

Les utilisateurs, souvent, disent que la sécurité leur apporte peu. Mais ce qui se passe au cours des 10 dernières années, c'est que le public commence à mieux s'inquiéter de ces problèmes de sécurité. Donc voilà un exemple. Vous imaginez un petit peu que tout un pays parle de la question de savoir si un compte avait été sécurisé, que ça fait déjà plusieurs mois qu'on en parle aux États-Unis et que c'est dans les grands titres des nouvelles. C'est donc quelque chose qui est devenu complètement public. Il y a eu plusieurs choses qui ont été dites là-dessus.

Il y a aussi des situations qui sont moins connues, mais qui sont inquiétantes. Vous avez, là, deux articles des journaux britanniques — ce sont de grands journaux très renommés —

donc qui expliquent la situation de deux personnes qui, en fait, ont vu leur e-mail intercepté et donc ont eu des problèmes pour vendre leur maison. Donc il y a eu interruption de leur compte e-mail ou plutôt introduction dans leur compte e-mail qui a été piraté, et donc ils ont perdu du fait des transferts des données de leur banque des sommes importantes d'argent.

Donc vous voyez que ce problème peut avoir un impact géopolitique et un impact pour la sécurité des gens.

Alors que peut-on faire ? Ce qu'on voit, c'est donc un risque pour tout l'écosystème des e-mails, parce que si vous souhaitez sécuriser les e-mails, soit vous avez un système fermé dans lequel on s'attend à ce que chacun ait un compte comme Google et Facebook par exemple, ou alors, on peut sécuriser la transmission des e-mails uniquement par le biais de la coopération. Donc les mails passent d'un FSI à un autre. Et donc il y a au moins deux opérateurs impliqués. Donc on ne peut pas avoir de sécurité sans avoir de coopération. Alors autre option, si l'e-mail n'est pas sécurisé, la plupart des gens, en fait, passe au chat, aux messageries instantanées. C'est quelque chose qui se passe aujourd'hui. Donc ce ne sont pas des fournisseurs tels que les e-mails et donc on se retrouve avec d'autres fournisseurs.

Il y a des efforts qui sont en cours un peu partout. Je crois que vous le savez peut-être, pour ceux qui sont présents, mais il y a

des gouvernements, des entités gouvernementales tout du moins, qui commencent à prendre ceci au sérieux et qui commencent à faire des recommandations.

On a déjà parlé de l'Allemagne, ce matin. Donc de plus en plus, ils demandent à leurs fournisseurs d'adopter le DNSSEC. Il y a également des efforts qui sont faits par les fournisseurs de services Internet aussi. Donc voilà pour l'Allemagne. C'est une réponse aux demandes du gouvernement. Et tous les grands fournisseurs d'e-mail aux États-Unis utilisent également le DNSSEC et le DANE pour authentifier le serveur de destination. Donc c'est également un point de marketing pour eux. Les utilisateurs sont mis au courant que la communication en Allemagne est faite par des fournisseurs qui sont plus sécurisés que les autres.

Donc dans le cadre de ce projet, l'Open-Xchange, donc nous sommes présents dans le monde entier. Nous nous sommes dit qu'il fallait absolument améliorer le système des e-mails et donc répartir ces idées ou les faire passer à d'autres.

Donc voilà ce qu'on appelle le TES. Donc c'est un nom qu'on a inventé. Mais ce que cela veut dire, c'est que pour nous il devrait y avoir des normes générales qui sécurisent les e-mails. Alors surtout les ISP Telcos doivent essayer de déployer la technologie

qui existe, mais malheureusement il y a très peu de personnes qui les utilisent.

On m'a demandé également, en fait, c'est une initiative Open-Xchange, donc il y a également Dovecot qui m'a demandé de les mentionner. 70 % des services e-mail qui sont donc hébergés par eux et par le DNS bien sûr. Donc ce sont les leaders en matière de responsabilité qui ont lancé ce type de projet.

Donc il y a eu une première société qui a lancé l'initiative, mais maintenant, nous avons évolué ; nous sommes au niveau des vendeurs. Pour donc fournir ces logiciels d'e-mail, donc on souhaiterait qu'il y ait davantage de choses qui soient faites à ce niveau. Nous souhaitons croître. Par exemple l'ISOC a essayé de faire avancer ces technologies. Nous sommes en position tout à fée positive puisqu'il y a plusieurs opérateurs de télécommunications en Europe et en dehors de l'Europe qui travaille avec nous. Donc on espère vraiment que le monde pourra vraiment continuer d'adhérer à ces nouvelles technologies.

Donc voilà. Nous avons commencé avec certaines directives techniques qui avaient pour but de vous aider à sécuriser vos e-mails. C'est ce qu'on voit ici. Ensuite, on a commencé avec un modèle qui, en fait, invite les opérateurs d'un pays ou d'un autre

avenir à une réunion, de manière à pouvoir communiquer avec eux. Nous en avons maintenant huit ou neuf qui sont avec nous.

Nous avons donc invité les gens du marketing comme les gens de la technique de ces sociétés. Et nous leur avons expliqué quelles sont les tendances, quels sont les systèmes de normes ouvertes. Et en fait, même les gens de la technique ne comprennent pas tous les risques et qui sont impliqués. Et donc ils commencent à poser des questions, et d'essayer de réfléchir à des solutions à ces problèmes.

Donc bien sûr, nous avons une liste de diffusion. Nous avons un groupe Facebook, parce que bien sûr les gens ont Facebook. Et on essaie également de répandre les informations au-delà de la communauté des opérateurs. Donc nous parlons aux gros FSI, aux Telcos. Nous avons un site Web qui nous permet d'expliquer le DNSSEC, ceux à quoi ça correspond, la technologie, et nous essayons d'encourager les gens à l'adopter.

Donc voilà l'ensemble des technologies que nous recommandons. Nous n'allons pas parler de tout bien sûr, parce que sinon il faudrait trois heures, quatre heures. Donc je vais simplement mentionner, et je pense que tous vous connaissaient ce que nous pouvons utiliser, donc DNSSEC et DANE pour sécuriser la technologie. Pour certains d'entre vous, vous les avez même inventés. Mais je pense que ce n'est pas le

cas de tous. Donc je voulais simplement vous montrer exactement pourquoi DANE est aussi important que ça pour sécuriser la transmission.

Donc ça, c'est un récapitulatif de ce qui se passe lorsqu'on envoie un e-mail sur l'Internet. Donc vous voyez les deux MTA, donc les deux serveurs d'e-mail, celui qui a envoyé et celui qui a reçu, sont en dialogue. Donc ce qui se passe c'est que celui qui reçoit va dire, va en fait chiffrer. Parce que vous savez que le chiffrement SMTP est opportuniste, totalement opportuniste. Et il y a également le problème de savoir si oui ou non il va y avoir compatibilité. Donc en général, le MTA qui reçoit demande le chiffrement et c'est comme ça qu'il y a chiffrement. Alors ce qui se passe, c'est que, en fait, il y a beaucoup de possibilités d'attaque. S'il y a interception de la communication, vous allez recevoir l'indication « STARTTLS » et ensuite cela va être indiqué au MTA. Il n'y a pas de chiffrement. Ce qui se passe, c'est que le MTA qui a envoyé va ensuite faire suivre la communication et donc la communication sera interceptée avant de recevoir le MTA. Donc il ne sait absolument pas qu'il y a eu interception.

Autre également moyen pour intercepter les e-mails, on utilise le *cache poisoning* classique. L'empoisonnement de cache classique. Donc il y a l'enregistrement MX. Donc même chose. Vous recevez le mauvais enregistrement MX qui a été empoisonné par l'attaquant. Donc il semblerait que les bons,

mais en fait c'est celui qui attaque. Donc il y a des problèmes d'authentification, etc. Donc en fait, le MTA qui envoie ne sait pas qui l'envoie son e-mail au mauvais endroit, et de toute façon, il y a un problème de chiffrement.

On ne peut pas empêcher ces deux types d'attaques de se passer, donc que faire ?

Pas la peine d'expliquer ce que fait DANE. Mais les deux points que j'aimerais mentionner, c'est que tout d'abord DANE marche très bien pour le chiffrement des e-mails parce qu'à cause de l'encre de confiance. Et ça c'est important parce que nous avons vu des difficultés pour sécuriser l'authentification. Et même s'il n'y a qu'une autorité de certification qui est bonne, cela veut dire qu'on peut avoir des certificats pour tout. Et ce qui est encore plus important, ce que fait DANE et qui est particulièrement important, c'est donc de fournir la communication comme quoi on veut vraiment recevoir des e-mails chiffrés.

Donc le vrai problème de la norme actuellement pour la communication, si les opérateurs publient un enregistrement TLSA, eh bien, c'est qu'il faut absolument chiffrer. Parce qu'il n'y a pas d'autres possibilités sinon. S'il y a un problème, si quelqu'un arrive au milieu, il n'y a pas de solution. Mais bon, il y a problème de déploiement et donc on va en parler. Voilà. Voilà

ce qui se passe en fait. Donc envoi de rapport TLSA et trafic chiffré. Et donc si celui qui reçoit le MTA peut voir l'enregistrement, en fait, on peut voir si c'est vraiment lui. Alors si on a une attaque, on n'envoie pas le mail.

Donc il y a plusieurs problèmes opérationnels. Et l'autre partie de ce projet, c'est qu'on rencontre donc les opérateurs et pour la plupart ils n'ont pas encore de feed-back à nous donner. Parce que pour la plupart d'entre eux, ils n'ont pas nécessairement le DNSSEC ou le DANE, donc ils ne savent pas exactement où ils en sont. Pour certains, ils l'ont.

Mais les renseignements que nous obtenons, c'est que d'une manière générale, ils ont l'impression que le DNSSEC c'est complexe avec tout ce qui est cryptographique dans la configuration, etc. Donc c'est un peu complexe. Mais ce n'est pas vrai. Ce n'est plus vrai. J'ai fait le test dans mon propre nom de domaine. Et ça a très bien marché. La partie vraiment difficile, c'est l'enregistrement DANS.

Donc l'autre commentaire qu'on nous fait, c'est qu'on rencontre des Telcos qui nous disent, « Bon d'accord, on va déployer le DNSSEC sur nos noms de domaine ». On les pingue deux à trois mois plus tard, et ils ne disent, « Non on n'y est pas arrivé. On n'a pas réussi à changer les enregistrements DANS ». Ou alors, « On ne sait pas vraiment quoi faire, c'est un autre département qui

s'occupe du DNS ». On discute avec les gens du DNS et on essaie de les convaincre que c'est vraiment utile. Donc en fait, le commentaire qu'on nous fait c'est que ce n'est pas seulement un problème de technologie, mais c'est un problème d'organisation.

Dans mon cas personnel, j'ai mon propre e-mail. J'ai mon propre serveur faisant autorité. Et mon bureau d'enregistrement soutient le DNSSEC. Il ne me laisserait pas le faire. Mais le soutien ne serait pas ce que c'est que le DNSSEC, etc. Donc en fait, il y a vraiment un moyen d'expliquer au monde que c'est possible et que cela peut résoudre les problèmes auxquels sont confrontés les gens.

Donc encore une fois, on en a déjà parlé. Ce n'est pas un problème de logiciel, en fait, c'est surtout un problème opérationnel.

Donc dernière chose que je voulais vous montrer, c'est déjà les statistiques. De bonnes statistiques. Donc le vol de données, des informations. Donc bien sûr qu'il faut prendre ceci avec précaution. Mais les noms de domaine en matière de sécurité, de recommandation, à savoir s'ils soutiennent le chiffrement, s'ils acceptent l'authentification, avant de commencer la collection. Et le [DOS] SPF également.

Donc nous travaillons encore à l'intégration de ceci pour que cela fasse partie du site Web, mais nous avons essayé en fait de tester 1000 noms de domaine. Donc un millier d'entre eux qui sont les plus utilisés. Donc nous avons pingué les noms de domaine et nous avons essayé de voir s'ils pouvaient être compatibles avec les e-mails. Et on a commencé avec DNSSEC, avec DANE, etc., toutes ces technologies. Donc voilà quels ont été les résultats.

Alors, tout d'abord, pour beaucoup d'entre eux, nous n'avons pas d'enregistrement MX. Donc il n'existe pas. Ils n'ont pas été configurés. Donc je crois que nous avons environ 20 %. Et la partie la plus importante qui n'est pas validée dans le DNSSEC, même si le DNSSEC était activé, c'était en fait un problème de compatibilité pour l'utilisateur final.

Mais en dehors de ça, vous voyez que la bonne nouvelle c'est que 72, 5 % de ces domaines sont compatibles avec le mail chiffré. Mais de l'autre côté, il y en a quand même beaucoup qui ne le sont pas. Plus de 12 %. Donc c'est important. Et si vous regardez là, vous voyez– vous devez savoir en fait quelle est la version compatible ; c'est important parce que vous savez que les versions plus anciennes ne pouvaient pas être sécurisées. Et nous n'avons pas vraiment vérifié c'était 2 ou 3, mais je crois qu'il faut en être à la dernière version des protocoles de chiffrement. Sinon, ça ne fonctionnera pas. Et parmi ceux qui

ont des mails, moins de 60 % ont la dernière version. Et donc 6,5 sont encore au TLS 1. Et donc, comme je disais moi, plus de 20 % n'ont pas du tout de chiffrement.

Ensuite, DNSSEC et DANE. Donc nous avions mille domaines. Et c'est sans doute plus important si on regarde le trafic par e-mail, et voilà ce que nous avons trouvé. Nous avons trouvé 15 domaines qui étaient compatibles avec le DNSSEC. Donc 2 % à peine. Et pour la plupart, c'est les .gov, les domaines .gov ; et uniquement trois d'entre eux avaient le DANE.

Donc je pourrais les mettre ici. Je pourrais même vous donner les noms. Vous avez Comcast, web.de et gmx.net, qui sont donc allemands. Par exemple, il y a des noms de domaine sur cette liste qui ne sont pas compatibles avec le DANE, etc., Mais la mauvaise nouvelle, c'est que l'adoption est encore négligée.

La bonne nouvelle, c'est qu'il y a de grands opérateurs tels que Comcast et web.de qui le font déjà. Donc vous pouvez aller voir les autres et leur dire, « Écoutez, regardez, ils le font donc c'est possible ».

Alors je crois que j'ai mis mes coordonnées sur la dernière diapositive. Donc je suis prêt à répondre à vos questions. Mais la raison pour laquelle je suis ici, c'est vraiment pour que nous essayions de commenter une activité interne au sein de la société. Mais nous souhaitons impliquer surtout les opérateurs.

Et de mon point de vue, nous organisons des réunions. Nous en avons eu en Pologne. Tout le monde n'était pas là parce que donc ce n'est pas forcément évident de rentrer en contact avec les gens. Donc le fait de se rendre dans ce genre de forum peut être intéressant pour élargir l'ampleur de notre travail, pour parler aux opérateurs, aux grands opérateurs au moins.

Nous avons plusieurs registres ccTLD qui ont été en contact avec nous. Et je crois que ça serait utile, surtout dans le continent, d'avoir une coopération entre les registres ccTLD. Je pense que cela pourrait nous aider à améliorer nos réunions et puis pour également participer à l'expérience DNSSEC et à les pousser dans leur pays, pour les inciter d'accepter dans le pays. Je crois que l'effort doit être coopératif. Il doit impliquer toute la communauté. Donc il est intéressant de parler des détails très techniques. C'est bien. Mais je crois que maintenant, on n'en est à un point où la communauté doit vraiment prendre les choses au sérieux et déployer. Parce que le risque est trop important. Et il faut absolument faire quelque chose dès que possible. Merci.

JULIE HEDLUND : Merci, Vittorio. Donc j'aimerais maintenant passer la parole au public pour les questions. Avez-vous des questions pour Vittorio ?

PATRICK : Vittorio, nous sommes une des sociétés qui a fait beaucoup pour DANE en Allemagne. J'aimerais ajouter quelque chose.

Vous avez dit que beaucoup de personnes pensent qu'ils ont des problèmes avec le DNSSEC pour la mise en place. En fait, ce n'est pas vraiment le problème. Vous avez raison. Le problème c'est que la plupart des sociétés auxquelles j'ai parlé, c'est qu'ils utilisent le DNS depuis beaucoup d'années. Et bien sûr que tout le monde sait que c'est très important. Maintenant le DNSSEC, ils savent très bien que cela peut en fait casser quelque chose, briser quelque chose dans leur structure. Et donc ils ont peur de ça.

VITTORIO BERTOLA : Je suis d'accord. Effectivement, ce sont les commentaires que nous recevons. Je crois qu'il faut absolument inciter les gens et répondre à leur résistance. On ne peut pas ignorer le problème, certes. Mais si quelque chose de vraiment mauvais se passe, je ne sais pas, s'il y a un problème de connectivité, tout le monde va se dépêcher.

PATRICK : En Allemagne, le gouvernement a accepté ; tout ce qui est [inaudible] a accepté ceci depuis déjà un certain nombre d'années. Donc c'est un peu comme le DNSSEC. Les gens

pensent que ça coûte trop cher et que ça ne vaut pas le coup pour l'instant.

VITTORIO BERTOLA : L'Allemagne est première. Mais moi je viens d'Italie. Nous avions une réunion comme celle-ci en Italie. Et le problème, c'était qu'on n'a pas les TLD jusqu'en 2017. Donc les gens se regardent droit dans les yeux et se disent, « Bon, voilà. Qu'est-ce qu'on fait ».

PATRICK : Oui. Oui je comprends tout à fait.

JULIE HEDLUND : Merci. D'autres questions ?

INTERVENANT NON IDENTIFIÉ : Les gens à l'arrière, vous n'avez pas de question ? Moi j'ai une question. Les fournisseurs e-mail, les prestataires de services e-mail, qu'est-ce qui vous ont dit ? En fait, c'est deux questions.

VITTORIO BERTOLA : En général, lorsqu'on rencontre les gens, on fait la chose suivante. On commence déjà par les plus grands. On a fait la

même chose au Royaume-Uni, en Pologne, en France, etc. Donc on essaie de contacter toutes les sociétés. Et si ce sont de grands Telcos qui ont des millions d'utilisateurs, vous savez dans certains pays les gens prennent des services e-mail gratuits, donc ça dépend. Mais ce qu'on fait, c'est qu'on essaie de rassembler tout le monde autour de la table pour pouvoir en discuter.

Moi j'aime bien aussi parler aux gens qui travaillent au niveau local. C'est un autre groupe au niveau de l'ISOC. Donc je pense qu'il nous faut en fait que commencer la discussion.

En général, ce qui est intéressant, c'est que les gens ont tendance à être un petit peu nationalistes pour ainsi dire. Donc si on leur dit les Allemands le font déjà, ils vont dire bon d'accord on va faire quelque chose dans notre pays. Donc c'est un petit peu l'idée. Ça commence par le gouvernement en fait.

Donc ça, ça peut être un des moyens. Mais donc déjà, sensibiliser les gens ; il est possible qu'ils aient entendu parler du DNSSEC, mais ils n'ont pas nécessairement entendu parler des dangers et de la raison pour laquelle le DNSSEC a été créé. Donc, n'hésitez pas si vous souhaitez me contacter.

WES HARDAKER : Wes, USC. Premièrement, merci. J'aime beaucoup cette technologie. Il y a eu un problème que nous avons eu fréquemment. C'est de nous assurer que les personnes se rappellent de mettre à jour des enregistrements DANE. Est-ce que vous avez quelque chose dans le système qui permette de vérifier ? Parce que par exemple il y a des personnes qui gèrent le DNS SMTP. Donc il est possible qu'ils mettent à jour leurs certificats, mais qu'il y ait un problème au niveau du DNS. Est-ce que vous avez quelque chose à dire là-dessus ?

VITTORIO BERTOLA : Non. Nous en sommes toujours au point où il n'y a pas de vérification des enregistrements TLSA. Donc on pourrait effectivement le mettre en place. Et je crois qu'il serait utile s'il y avait un ensemble d'outils qui pourraient être partagés par tout le monde là-dessus. Je suis d'accord. J'ai essayé par exemple de suivre les tutoriels sur le site ISOC. Très bien. Et j'ai eu un problème avec mon propre serveur au niveau des certificats. Il y a toujours de réels problèmes pour travailler avec le DANE. Donc il y a un certain nombre de choses qui pourraient être améliorées à mon avis. Et je pense qu'on pourrait effectivement partager nos idées là-dessus.

WES HARDAKER : Vittorio, je dois dire qu'il y a un site de suite de tests. Alors, moi je n'aimerais pas avoir une partie tierce sur laquelle je dois me reposer. Mais je pense qu'il faut faire attention lorsque le certificat ne correspond pas à l'enregistrement DANE.

INTERVENANT NON IDENTIFIÉ : Un commentaire. Vous pouvez conserver votre clé privée et générer un certificat. Donc, par exemple, l'outil fonctionne bien. On va, en fait, continuer à utiliser la même clé.

VITTORIO BERTOLA : Je crois qu'il faut utiliser un fichier CSL, me semble-t-il. Mais ça prend un petit peu de temps. Ce n'est pas immédiat.

JULIE HEDLUND : Des questions supplémentaires ? Non. Si c'est le cas, je vais remercier Vittorio d'être avec nous et on va l'applaudir. Alors nous allons maintenant passer à une présentation de Carsten Strotmann sur SMILLA, le chiffrement S/MIME automatique. Donc on va lui demander de faire la présentation. Allez-y, Monsieur.

Non. Vous pouvez venir au centre, si vous voulez.

CARSTEN STROTMANN : Non. Ce n'est pas la peine. Patrick est à mes côtés. Il sera chargé de faire défiler les diapositives et je prendrai la parole.

JULIE HEDLUND : Ah très bien. Donc Patrick Ben Koetter est là et Carsten Strotmann.

PATRICK BEN KOETTER : Oui. J'ai eu l'occasion de faire une petite blague sur DANE et le Danemark puisqu'on est là.

Donc on entend parler de DANE et le mail, et de DANE sur la protection de STARTTLS et de ce qu'on peut faire dans ce domaine. Carsten et moi avons ajouté quelque chose d'autre à cette possibilité. On a nous-mêmes développé un programme. Lorsqu'on a besoin d'avoir consensus donc, on a ajouté un code pour une proposition qui s'appelle SMIMEA. C'est une possibilité d'avoir un chiffrage opportuniste automatisé pour les systèmes d'e-mails.

Donc je voudrais vous expliquer de quoi il s'agit et pourquoi c'est intéressant de la voir. L'autre jour, je discutais avec un technicien d'un grand service de radiodiffusion allemand. Il m'a envoyé un mail, qui m'a posé des questions au sujet de nos services de messagerie de courrier électronique et du développement du nouveau système. Et je disais, « Vous

travaillez avec des journalistes, les journalistes travaillent avec des sources confidentielles ; or, il faudrait qu'il y ait un moyen pour protéger vos communications, n'est-ce pas, puisque les échanges journalistiques ne fonctionnent bien que si on a des canaux auxquels vous faites confiance en matière de confidentialité ». C'est tout simple. On doit faire face à différents problèmes dans ce domaine aujourd'hui.

On avance ? Non. On avance encore. Très bien.

Donc l'un des problèmes que nous avons par rapport au chiffrage, sur DANE, c'est que c'est compliqué. Il y a deux modèles qui se font la concurrence. Aucun des deux systèmes n'est simple en fait. L'un exige qu'il y ait une ligne de commande magique par laquelle vous une clé que les gens doivent télécharger et puis, par la suite, il faut qu'il y ait un processus de certification de confiance. Et ce n'est pas vraiment utile pour les communications instantanées s'il vous faut avoir une communication fluide.

D'autre part, on a le standard S/MIME pour lequel il est compliqué, bien sûr, de développer les codes. Mais par la suite, il y a des autorités qui vendent des certificats, des attestations. Ce qui simplifie un peu. Mais la vraie question est, sont-ils vraiment dignes de confiance ?

Il y a des autorités qui certifient, qui ont fait l'objet de différents cas d'abus dans ces dernières années. Et le fait d'avoir votre clé ou d'avoir quelqu'un d'autre qui fait semblant d'être vous dans une communication S/MIME ne serait pas idéal. Une personne peut voler une attestation d'une autorité de certification et faire semblant d'être quelqu'un d'autre, usurper votre identité.

Donc comment peut-on détourner ces problèmes ? Eh bien, d'une part, on pourrait augmenter le niveau de contrôle par rapport aux attestations qui sont dignes de confiance. Et d'autre part, on a également la possibilité d'aller au-delà avec le processus de chiffrement. C'est ça l'idée de S/MIME.

L'idée ou le principe est d'utiliser DANE qui se fonde sur l'authentification basée sur le système de noms de domaine afin d'établir des critères et des informations qui aident les autres à identifier certains aspects. D'une part, il y a un enregistrement spécial qui indique que la personne qui est notre destinataire a fait recours à un service de chiffrement. Et puis d'autre part, le fait qu'il y ait un enregistrement veut dire que la personne veut ce type de chiffrement et qu'il y a un type spécial de clé de chiffrement qui est publié qui vous indique le type de chiffrement que cette personne utilise. Donc on n'utilise pas le PGP alors que l'autre personne utilise un autre service. Il faut qu'il y ait une compatibilité entre les deux.

D'autre part, il faut que l'on ajoute un canal digne de confiance, une chaîne de confiance. Et dès qu'on a établi cette voie digne de confiance, on peut mieux contrôler qui exploite DNS. Ce sont les personnes qui travaillent dans ce nom de domaine. Donc on obtient cette attestation de l'autorité de certification qui pourrait faire l'objet d'un cas d'abus, et cela impliquerait des problèmes de sécurité et le système ne serait pas aussi sécurisé que possible.

Or, avec DANE, on aura un client de mail qui peut aller chercher la personne à laquelle vous voulez écrire, la chercher dans un nom de domaine qui est habilité pour le DNSSEC. Si c'est le cas, il va y avoir un enregistrement pour cette personne qui contient les informations nécessaires pour que le client de mail puisse chiffrer les informations pour cette personne de manière opportuniste dès qu'il aura trouvé ces informations. Donc on saute tout le processus en fait. On vérifie comment chiffrer et on s'assure que les informations pourraient être correctement interprétées.

Donc je donne la parole à Carsten maintenant.

CARSTEN STROTMANN : Bien. Donc l'enregistrement SMIMEA est une authentification du système que nous utilisons déjà. Et ça nous permet d'assurer la sécurité de bout en bout avec un certificat S/MIME. Ça peut être

utilisé de différentes manières. On peut avoir le certificat du condensat stocké, alors avoir le certificat complet dans le domaine sécurisé avec DNSSEC.

Ici, on a utilisé pour SMIMEA tout le certificat, certificat complet de x509, qui est stocké dans le DNS. Cette attestation est stockée dans un nom de domaine qui contient la partie de l'adresse e-mail qui est contenue dans le condensat, c'est-à-dire celle qui est juste avant la signature @.

Ici, on peut utiliser des attestations qui sont achetées auprès des autorités de certification, mais on peut également avoir des attestations qui sont autos signées. Ce qui pourrait être bénéfique. Parce qu'on peut, soi-même, contrôler la validité des attestations et la date à laquelle nous allons les rouler.

Diapo suivante.

Donc SMILLA, spécifiquement, qu'est-ce que c'est ? Il s'agit d'un MILTER. C'est-à-dire une API standard pour les serveurs de mail de code ouvert comme Postfix ou Sendmail entre autres. Et SMILLA est ciblé non pas pour les utilisateurs privés chez eux, mais pour les organisations de fournisseurs de services de courrier électronique dans leurs propres infrastructures.

Donc SMILLA intercepte les courriers électroniques qui passent par le serveur, et vérifie si ces mails sont chiffrés. S'ils ne sont

pas chiffrés, SMILLA ira chercher dans le DNS si le signataire de ce courrier électronique a publié un enregistrement SMIMEA qui contienne le certificat ou l'attestation x509. Si c'est le cas, ça va télécharger cet enregistrement avec les informations qui contiennent la clé publique, et avec l'aide de cette clé, ça va donc envoyer le mail au destinataire grâce à cet enregistrement.

SMILLA peut être utilisé de deux manières. D'une part, pour chiffrer des mails sortants. C'est-à-dire que lorsqu'on l'utilise, ce service, du côté de l'émissaire, serveur de mail émissaire ira chercher le certificat du destinataire. Il va chiffrer le message et puis il enverra au destinataire à travers cet Internet est plein de risques. Et le destinataire pourra utiliser cette même clé publique pour lire le mail. Ça peut également être utilisé pour chiffrer les mails entrants. C'est-à-dire que si un mail est envoyé de manière non sécurisée, non chiffrée, du côté du destinataire, le système peut le chiffrer et le stocker dans le disque dur de l'ordinateur. C'est ce qui est utilisé lorsque les serveurs de mail sont hébergés dans des plates-formes qui ne sont pas sécurisées, dans un serveur dans le nuage qui est loué par exemple, dont l'opérateur n'est pas vraiment le propriétaire des équipements. C'est-à-dire que le serveur peut tout simplement être confisqué et utilisé à mauvais escient, et les mails peuvent donc être chiffrés du côté du destinataire pour empêcher qu'il y ait des fuites d'informations.

Ici, on voit comment fonctionnent DANE et SMIMEA.

Sur la droite, vous voyez ici un enregistrement SMIMEA qui a été publié par Bob dans le DNS. Bob a obtenu de son opérateur de mail des informations, des informations de son opérateur de DNS également. Bob a stocké cet enregistrement qui contient dans son serveur faisant autorité, qui est example.com par exemple. Donc maintenant, Alice, qui est sur la gauche, veut envoyer un mail à Bob. Ces deux personnes n'ont jamais échangé de mail ; elles ne se connaissent pas. Alors, Alice envoie le mail sans changement de logiciel de serveur ou de logiciel client pour le mail. Mais Alice n'a pas besoin de savoir qu'il y a SMILLA appliquer ici. Le serveur de mail pourtant exploite ce filtre SMILLA.

SMILLA, à partir de ce moment-là, va évaluer si le courrier électronique est chiffré. S'il n'est chiffré ni par PGP ni par S/MIME, SMILLA va chercher l'enregistrement SMIMEA dans le résolveur du DNS qui le renvoie au résolveur faisant autorité pour aller chercher cet enregistrement. Le serveur de mail va obtenir les informations et va valider le DNSSEC, rendant cette validation au filtre SMILLA. Ce qui va générer une attestation de réponse. Et le mail va donc être envoyé à Bob avec cette attestation.

Donc voilà. On voit le mail qui est envoyé au serveur de mail qui est utilisé par Bob.

Dans la diapo suivante, Bob reçoit le mail et il ouvre à travers son logiciel préféré pour la messagerie électronique. Et il peut le déchiffrer à l'aide de sa clé privée paramétrée dans son logiciel. Cela fonctionne déjà. Le MILTER de SMILLA a été développé en Python. Ce n'est pas lourd. Ce sont quelques milliers de lignes de code qui sont faciles à comprendre, on espère. C'est un logiciel ouvert, libre, et qui a été fusionné avec l'OPENPGPKEY MILTER de Paul Wouters. Dans le DNS, on a une OPENPGPKEY où l'on peut stocker nos clés publiques du DNS, celles qui fonctionnent de la même manière. Donc ce MILTER fonctionne avec SMIMEA et OPENPGPKEY. Ça va automatiquement chiffrer tous les mails pour SMIMEA et OPENPGPKEY dans le DNS. Ça marche donc dans les deux sens, pour les émissaires et pour les destinataires.

Comme je viens de dire, c'est un logiciel libre, ouvert, pour nos comptes. En ce moment, vous pouvez le trouver. Il est disponible en version python, mais c'est ouvert. Si vous n'avez pas python, vous pouvez le modifier. Puisque ce ne sont pas beaucoup de milliers de lignes, on peut le modifier. Donc vous pouvez l'adapter vous-même. On pourra vous aider dans le processus, si besoin.

Ce qui nous intéresse, c'est surtout d'apprendre des personnes qui pourraient vouloir le déployer dans un environnement de test ou de manière productive. Merci.

Donc voici les leçons à retenir. Les utilisateurs de mail s'intéressent par la sécurité. C'est quelque chose qui est important pour eux de fournir des services de courrier électronique sécurisé. Et les serveurs de mail, en général, essaient de faire une distinction entre eux et les autres à travers la sécurité. On a trouvé de grands groupes d'utilisateurs qui veulent avoir des services de messagerie électronique sécurisée, mais qui craignent ces systèmes de chiffrage. Et DANE peut les aider à le faire plus simple. Donc c'est opportuniste comme méthode de chiffrage de bout en bout, et ça constitue un logiciel complètement légitime que l'on peut utiliser pour sécuriser l'Internet et les communications.

C'est tout. Est-ce que vous avez des questions ?

JULIE HEDLUND : Merci, Carsten et Patrick. Si vous avez des questions, allez-y. Oui. Allez-y.

WOTH STUFFBERG : Quel était l'enregistrement DNS qu'il fallait ajouter afin d'obtenir l'attestation ?

CARSTEN STROTMANN : L'enregistrement était SMIMEA qui, en ce moment, est dans une version préliminaire de l'Internet, a été adoptée par le groupe de travail Internet en automne dernier, que je sache. Donc j'espère qu'il sera disponible sous peu. Il est également supporté par la version la plus récente de la plupart des logiciels ouverts, tant pour les émetteurs que pour les destinataires. Pour ceux qui ne supportent pas SMIMEA directement, il est également possible de saisir cet enregistrement SMIMEA dans un format d'enregistrement non connu. Il s'agit d'un format qui peut être utilisé pour ajouter au DNS quoi que ce soit, même si le DNS n'en est pas au courant.

Donc il est possible d'utiliser ce système dès aujourd'hui. On est également sur le point de rédiger un petit outil que vous pouvez utiliser pour saisir votre attestation et votre adresse de mail, et ça vous permettra d'y ajouter le DNS. Parce qu'aujourd'hui, on n'a pas de tels outils. On voudrait que ce soit plus facile de pouvoir le faire. Donc on espère que ça sera disponible à partir de la semaine prochaine.

PAUL WOUTERS : Excusez-moi. Je n'ai pas vraiment beaucoup de cycles pour vous aider. Mais je suis fière d'avoir vu que vous avez pu profiter de mon OPENPGPKEY MILTER. Donc si possible, je suis prêt à

collaborer avec vous pour continuer de fusionner nos travaux. Ce serait génial.

PATRICK : Oui bien sûr.

PAUL WOUTERS : Parfait. Et à titre personnel, je dirais que j'ai essayé d'exploiter ce filtre de PGP ouverte, et j'avais 200 mails chiffrés tout de suite. Et je ne pouvais pas le gérer. Donc définitivement, je dirais qu'il y a du travail à faire du côté du client. Ou ce serait mieux de pouvoir déchiffrer automatiquement les mails entrants dans votre boîte de mail. Parce que si on n'a 200 mails chiffrés dans la boîte de réception, il n'y a rien à faire. Ce n'est pas possible d'ouvrir ces messages. Donc j'espère que quelqu'un pourra le faire, pourra nous aider.

CARSTEN STROTMANN : Oui. L'[Enigmail] soutient déjà cela. Il supporte ce système et vous permet d'avoir des mails chiffrés, stockés dans ce type de serveur. C'est possible. Ce n'est pas fait par défaut. Mais vous pouvez tout simplement ajouter ce filtre. Mais c'est un domaine où on peut vraiment améliorer ce qu'il y a.

JULIE HEDLUND : Rick Lan.

RICK LAN : Félicitations. C'est un très bon travail. Est-ce que vous prévoyez de pouvoir mettre cela en place de bout en bout, non pas dans les serveurs, mais dans les machines client ? Est-ce que vous avez déjà pensé à des manières d'intercepter le trafic entre ordinateurs pour que les utilisateurs moyens puissent également profiter de cela ? Parce que je pense surtout au public général, au grand public, qui ne fait pas confiance à l'environnement général.

PATRIK : C'est une très bonne idée, mais en ce moment, vu qu'on a eu une bonne expérience jusqu'à présent, je pense que ça ne marcherait pas. Ça pourrait échouer sachant qu'il y a beaucoup de virus, beaucoup de fournisseurs d'outils antivirus justement qui ne permettraient pas que ce logiciel accède dans les ordinateurs des personnes. Ce n'est pas facile.

RICK LAN : Oui sans doute. Je vais en profiter parce que je trouve que votre logiciel est très intéressant.

PAUL WOUTERS : Oui. Rick, moi je pensais à ce que vous dites et je pensais qu'on pourrait utiliser un serveur particulier de mail. Mais je ne sais pas si ça fonctionnerait sur mon iPhone, ce qui me semble intéressant comme possibilité.

PATRICK : Oui. Si vous utilisez les outils de configuration [inaudible], vous pourriez paramétrer cela de matière à ce que vos mails suivent une voie de soumission de manière chiffrée, pour que ça soit chiffré à partir du moment où les courriers électroniques arriveront au serveur de mail. Donc c'est déjà une manière de le faire.

JULIE HEDLUND : Merci. Y a-t-il d'autres questions ? Non ? Bien. En l'absence de commentaire, je vous remercie, Carsten et Patrick, de cette présentation qui a été fort utile. Et si vous m'accompagnez, on va les applaudir.

Nous avons maintenant une présentation finale de Dan York qui porte sur le DNSSEC, et spécifiquement comment puis-je aider. Comment collaborer.

DAN YORK : C'est incroyable, mais on n'est pas venu et on a pu rester à l'heure. On n'a pas pris de retard. Il me manque le pointeur pourtant pour les présentations. On va voir si ça marche.

Donc nous voilà à la fin de notre atelier et on est même avant l'heure. Je ne sais pas si on avait déjà eu cette chance. Mais avant de faire cela, je vais vous demander d'applaudir la communauté des programmateurs, des développeurs, qui nous ont aidés à organiser cet atelier. Et je voudrais également remercier et demander un applaudissement pour Julie et Kathy qui ont fait que cela soit possible.

La communauté de la programmation se réunit de manière hebdomadaire tous les jeudis matin. J'ai une réunion hebdomadaire avec Julie et avec le reste du groupe qui ont organisé. Yoshiro arrive à minuit, puisqu'il habite au Japon. Donc ce que demande toujours à ce qu'il est là ? Oui. Il est toujours levé. Mais Donc pour non c'est intéressant de pouvoir se réunir une fois par semaine pour discuter avec toutes ces personnes qui sont tellement dévouées, qui travaillent de manière acharnée dans ce domaine. Ça fait déjà une décennie que ce programme dure, déjà. Ça a déjà duré une décennie. Il date bien de dix ans.

Ça prend beaucoup de travail, mais je voulais reconnaître le travail de Julie spécialement, parce que c'est elle qui prépare

ses programmes et ces documents, et tout ce dont on a besoin pour pouvoir tenir nos réunions.

Nous allons lancer un appel à participants sous peu pour la session de Johannesburg. Cet atelier sera un peu différent. Ce sera comme celui qu'on a tenu à Helsinki, où les personnes pensent toujours qu'on fait partie de la journée du Tech Day. Et le matin, nous allons organiser certaines séances jusqu'à la pause de déjeuner. Et l'après-midi, on va rejoindre les autres présentations techniques qui ne sont pas spécifiques aux DNSSEC. Donc on entend parler des attaques DDoS, des mesures de réseau zombie, de tout type d'initiative technologique et technique en général.

Jacques Latour qui n'est pas là apparemment – ah le voilà, c'est la casquette qui m'a déroutée un peu. Ah il a mis sa casquette parce qu'il n'aime pas la lumière. Et il lui manque l'écharpe en plus. Lorsque vous avez vu l'écharpe de CIRA dans le petit sac, je suis sûr que vous avez rigolé, n'est-ce pas ? Pour moi, c'est une rigolade parce que si vous avez ouvert votre sac et qu'on n'avait pas tout simplement jeté tout ce qu'il y avait, CIRA a fait quelque chose de très beau. C'était magnifique. Mes félicitations donc Jacques.

En tout cas, Jacques fait partie du comité pour l'organisation du Tech Day. Donc si vous avez des présentations techniques à faire

auprès d'autres groupes qui sont là, les deux sessions au sein de l'ICANN qui se réunit ici, qui sont techniques, sont notre journée et le Tech Day.

Voilà la brochure de CIRA. Vous allez voir. Ils ont un bon sens de l'humour. J'ai beaucoup apprécié. Ils ont les animaux typiques, la feuille d'érable, tout. Ce sont les personnes qui donnaient des petites peluches, des castors, il y a quelques années. Et jamais qu'ils ont un sens de l'humour.

Donc pour conclure, on se demande qu'est-ce qu'on peut faire pour contribuer à la fin de la séance. Donc on demande aux opérateurs de TLD de signer leur TLD pour commencer, d'accepter les enregistrements en plus parce qu'il y a des gens qui signent leur TLD, mais qui n'acceptent pas les enregistrements des bureaux d'enregistrement. C'est-à-dire que si c'est signé, ils vont cocher la case, mais ils ne font plus rien d'autre pour aider à sécuriser le système. Donc on leur demande d'accepter les enregistrements, de travailler avec leurs bureaux d'enregistrement. Et puis, on leur demande également de nous aider avec les statistiques.

On a fait un nombre de présentations. On a discuté de ce que présentait Rick Lan au sujet de ces statistiques. Notre idée est d'avoir davantage d'études et d'analyse de ce type. Donc, aidez-nous à obtenir ces données.

Pour les opérateurs de zone, on leur demande de travailler avec les bureaux d'enregistrement encore une fois pour nous aider. On demande aux personnes de faire signer leur nom de domaine, de signer la zone, de nous aider avec les statistiques également. Et n'oubliez pas s'il vous plaît le roulement de la KSK en octobre.

Aux opérateurs de réseaux, on vous demande d'habiliter la validation. Ça ne vous prend que quelques lignes de cause. Des fois, ce n'est qu'une case. C'est tout simple. Cochez la case, écrivez les lignes. On a vu beaucoup de validations chez APNIC. On avait une grande croissance à ce niveau. Donc on espère que vous suivrez leur exemple.

On demande à tout le monde d'utiliser le DNSSEC, partager les leçons et ce que vous avez appris. Si vous allez assister à la réunion de Johannesburg ou vous connaissez des personnes qui seront présentes à ce forum de politiques, qu'ils veulent présenter leurs travaux, on est toujours intéressé par les différentes idées. On aura un autre panel régional. Donc si vous connaissez des personnes de l'Afrique qui pourraient vouloir présenter ceux qui sont en train de faire en matière de DNSSEC, on voudrait aussi les écouter.

On voudrait savoir qu'est-ce qu'il y a d'autre dans le marché. On a vu des démonstrations pour les mails, par exemple, avec les

différentes parties. On a vu d'autres présentations relatives au courrier électronique dans le passé, par rapport à d'autres outils. On a également vu d'autres démonstrations. On a vu de nouveaux sites qui avaient été créés. Rick nous a présenté un logiciel une fois. On a d'autres types d'initiatives et de projets en cours. Donc on cherche toujours à voir ce qu'il y a d'autres. On se concentre sur la manière dont les personnes utilisent le DNSSEC et DANE à bon escient, de manière utile.

Pardon. J'avais oublié. Il nous faut le nouveau logo de Christian, parce que sur son site Web, il a un très très beau logo qui est tout neuf et qu'on n'a pas mis ici. En tout cas, on remercie à Afilias, CIRA et SIDN, qui ont parrainé cette journée. Si vous voyez Christian dans les couloirs, il était ici. Il portait un T-shirt blanc. Remerciez-le. Remerciez Jim Galvin et Jacques. On peut remercier Jack tout de suite. C'est grâce à eux qu'on a mangé à midi.

Je pense qu'on a déjà dit cela. Le SSAC et le programme Deploy 360. Et j'ai ajouté ici les adresses mail de l'ISOC et de leurs programmes Deploy 360, DNSSEC tools, où vous trouverez les outils disponibles par rapport aux DNSSEC et le site de déploiement du DNSSEC qui a d'autres informations sur l'historique.

Bon. Il va falloir que l'on mette à jour ça. Attendez. On avait oublié. J'ai oublié de corriger ici le Copenhague.

JULIE HEDLUND : On pourra toujours se voir à Copenhague.

DANIEL YORK : Oui. Bien sûr. Donc à l'exception de cette dernière ligne, tout le reste est valable. Donc si vous avez suivi et apprécié les sujets qui ont été présentés aujourd'hui, on a une autre initiative qui nous maintient en contact entre réunions. On a une conférence tous les premiers jeudis du mois qui porte sur la participation du groupe. On a une douzaine de personnes qui participent. Mais ce sont des réunions ouvertes ou tout le monde peut participer.

Et on veut voir ce que le reste du monde est en train de faire. Rick nous montre comment il marche dans la rue le matin pour acheter du café, parce qu'il se connecte dans la rue. Et l'idée est de voir ce que font les autres et quelles sont les mesures qu'ils prennent pour mettre en œuvre de nouvelles initiatives.

Donc vous pouvez rejoindre nos listes de diffusion. Vous avez l'adresse ici. Et on a ces appels mensuels dont je parlais, qui s'appellent DNSSEC-coord ; c'est intéressant pour voir ce que font les autres. On a eu beaucoup de personnes qui nous ont rejoints, qui se sont abonnées. Et grâce à ça, on a vu ce que

faisait K.C. et puis Wes se dit que ce serait intéressant de communiquer avec elle pour profiter de ce qu'elle avait déjà développé. C'est intéressant de voir ce que font les autres au programme. Et ça nous permet d'arriver de réunion en réunion toujours à jour.

Cela dit, nous avons fini. Donc merci et à Johannesburg.

JULIE HEDLUND : Et merci à Dan, bien sûr, de sa direction et d'avoir fait tout ce travail. C'est lui qui a coordonné la réunion aujourd'hui.

DANIEL YORK : Oui. Si la prochaine fois, il y a quelqu'un qui veut m'aider à le faire, faites-le-moi savoir. Parce que moi j'apprécie ça. Merci.

Je voudrais remercier Irwin également pour la réunion des personnes, des déployeurs, de l'autorité danoise [Inaudible]. Merci.

[FIN DE LA TRANSCRIPTION]