COPENHAGUE – Taller sobre las DNSSEC -- Parte 3
Miércoles, 15 de marzo de 2017 – 13:45 a 15:00 CET
ICANN58 | Copenhague, Dinamarca

JULIE HEDLUND: Gracias nuevamente por estar en la parte III del Taller de DNSSEC. Soy Julie Hedlund, soy del personal de ICANN y voy a comenzar moderando la última parte de este taller. Debo decir que para mí es un orgullo presentar al siguiente moderador, Vittorio Bertola, de Open-Xchange, que nos va a contar un poquito sobre los Servicios de Email de Confianza.

VITTORIO BERTOLA: Gracias por la oportunidad de explicar lo que estamos haciendo. Es mi primer taller de DNSSEC. Hace un tiempo que estoy con ICANN, pero hubo un tiempo en que estuve ausente. Quisiera contarles lo que estamos haciendo, también contarles los problemas técnicos. Quizás algunos temas más específicos. Pero es una descripción general de lo que hacemos. La próxima diapositiva, por favor.

Con e-mail tenemos una compañía de *software* y una de las cosas que notamos es que el transporte de correo electrónico hoy en día no es demasiado seguro. La gente que está en este

sector ya sabe esto. El usuario final suele pensar que el mail es seguro, que está encriptado y protegido, autenticado, etc. pero no es del todo así.

De hecho, hoy en día la autenticación del correo electrónico es insuficiente, y la industria tiene una responsabilidad aquí porque se puede generar problemas como interceptación, etc. el correo electrónico es el medio de comunicación para la mayoría de los documentos importantes y datos. Usualmente, cuando recibimos *feedback* las empresas de telecomunicación dicen que no es su preocupación, pero en los últimos años el público ha tomado una verdadera percepción del tema y de los problemas relacionados.

La siguiente diapositiva.

Este es un ejemplo. Podemos en la presentación comparar si el mail es seguro o no, pero este es un buen ejemplo. En los Estados Unidos este es un tema que hace tiempo que está en los titulares. Hubo varios casos. La próxima diapositiva, por favor.

E incluso ha habido situaciones menos conocidas pero más preocupantes.

Artículos de los periódicos británicos, no sé si conocen estos casos, de *scammers*, cuentan dos situaciones de estafas a familias que vendían sus casas porque sus *mails* fueron

interceptados. O sea, podían leer los correos entre la familias y sus agentes de bienes raíces. Como resultado, les dieron las coordenadas de la transferencia bancaria equivocada o fraudulenta y perdieron mucho dinero.

O sea que no es sólo una cuestión de geopolítica y espionaje, es la seguridad cotidiana de la gente. Entonces, ¿qué es lo que nosotros intentamos hacer?

Bueno, acá lo que percibimos es un riesgo para todo el ecosistema, porque si queremos tener correo seguro tenemos que tener un sistema donde esperamos que todos tengan una cuenta como Google o Facebook, si no sólo se puede asegurar la transmisión por cooperación. El correo va desde un ISP del remitente hasta el ISP del receptor. Son distintas partes involucradas. Entonces no habrá seguridad sin cooperación.

Otra opción es que si un *e-mail* no es seguro la mayoría de las personas pasarán a chats o a mensajería instantánea, entonces el problema es que no hay normas abiertas como sucede con el correo electrónico, entonces terminaremos teniendo una mezcla de códigos propietarios.

En todos los lugares, en todas partes están haciendo esfuerzos. Los gobiernos, algunos gobiernos han comenzado a tomar con seriedad este tema y empiezan a elaborar recomendaciones. El gobierno alemán, como mencionó otro delegado hoy por la

mañana, exige adoptar DNNSEC y otros gobiernos en los Estados Unidos también. Y también algo más importante es que los mismos proveedores están tomando medidas.

Este es el proveedor alemán bajo la presión del gobierno. Los principales proveedores de correo electrónico en Alemania ahora hacen autenticación DNSSEC y DANE. Incluso lo convierten en una ventaja de marketing, lo publicitan para que los usuarios sepan que la comunicación entre dos direcciones de correo alemanas, aun cuando sean de proveedores distintos, son seguras.

En este proyecto, en Open-Xchange, pensábamos que estábamos en un buen lugar para diseminar la palabra en el mundo, para el bien del correo electrónico en general y para beneficio de otros países.

Entonces iniciamos esto que se llama el TES, el proyecto TES, que es un nombre nada más, que apunta a tener algún tipo de estándar general para el correo electrónico seguro. En especial las telecomunicaciones, los ISP, los alojadores, o sea los que tienen millones de direcciones de e-mail tendrían que implementar tecnologías que ya existen pero lamentablemente no las usan o muy pocos las usan.

El Comité del Proyecto, bueno aquí están los miembros, Open-Xchange, que es la compañía matriz, también Dovecot, que tiene el 72% del *software* [inaudible]. Dovecot es el principal.

Comenzamos como una compañía interna pero intentamos ampliar el alcance, por eso en parte estoy aquí hoy. Hemos trabajado con proveedores, [inaudible], que son dos proveedores de *software* y servicios de correo.

Queremos un generar un impulso detrás del proyecto. Hay otros esfuerzos como los que hace [ISOC], pero nosotros estamos en una buena posición porque varios de nuestros clientes son las grandes empresas de telecomunicaciones en Europa, entonces lo que queremos es diseminar la palabra en conjunto con cualquier otro que quiera educar a los operadores para adoptar la tecnología.

La próxima.

Esto es lo que hacemos. Comenzamos con una serie de normas técnicas que contribuyen a la seguridad del correo, como vimos en DNSSEC y DANE y comenzamos con un modelo donde invitamos a los operadores nacionales a una reunión. Tenemos reuniones cerradas con una lista de correo. Ya tuvimos ocho o nueve. Entonces invitamos tanto a la gente técnica como de marketing, la que vende los servicios, y les explicamos cuáles son las amenazas, cuáles son las normas abiertas, y suelen

sorprenderse, incluso la gente técnica no se da cuenta de lo que está pasando, entonces quieren saber más porque quieren resolver los problemas.

Tenemos una lista de correo. Incluso tenemos un grupo de Facebook cerrado porque lamentablemente a la gente le gusta Facebook, y estamos tratando de diseminar la palabra más allá de los operadores. Cada vez hay más ISPs, así que lo que hicimos fue armar un sitio web para explicar qué es en DNSSEC y DANE, cuáles son los tecnologías, e invitamos a la gente a que lo adopten.

Entonces estas son las tecnologías que recomendamos. No las vamos a ver todas. La típica reunión de test que lleva dos o tres horas seguramente algunos de los presentes saben cómo usar DNSSEC y DANE para el correo seguro. Seguramente algunos de ustedes lo inventaron, pero no todo el público lo sabe. Entonces por eso voy a explicar por qué DANE es tan importante para asegurar la transmisión de correos.

Esto es lo que sucede cuando enviamos un correo por Internet. Las dos MTAs, entre los servidores de correo, el que lo origina y el receptor, tienen que iniciar un diálogo. El MTA receptor dice que acepta el encriptado porque lamentablemente el encriptado en la transmisión SMTP es totalmente oportunista. Entonces no es obligatorio. El otro problema es que no se sabe

realmente si el receptor lo va a soportar, así que tiene que solicitar. El MTA receptor busca si hay encriptado.

¿Qué pasa después? Es un área sujeta a varios ataques de intermediación. Si alguien intercepta la comunicación, recibe el STARTTLS y si no hay soporte de encriptado, ¿qué pasa? El MTA receptor asume que la comunicación está bien. La comunicación es interceptada antes incluso de llegar al destino, al MTA receptor. Entonces no se sabe. Otra manera de interceptar el correo es a través del ataque del DNS. Cuando la comunicación busca el registro MX, el MTA de envío recibe un registro MX, el incorrecto que fue manipulado por el atacante y la comunicación parece estar bien pero en realidad es un ataque. Incluso se puede dar un certificado válido, autenticado. EL MTA de envío no sabe que está enviando un correo al destino incorrecto, y aun cuando esté encriptado se lo desencripta del otro lado. DNSSEC y DANE son las tecnologías que previenen estos dos tipos de ataques.

No creo que sea necesario para mí explicar qué hace DANE. Pero lo que quiero básicamente rescatar de aquí es que DANE es muy bueno para el encriptado de correos, porque da un ancla de confianza que no depende de una autoridad de certificación. Esa es la dificultad, de que todas las autoridades de certificación sean seguros. Incluso aunque una sola sea violada, ahí podrían conseguirse certificados válidos para todos.

Pero aun lo más importante, lo más importante que hace DANE es proporcionar una manera para que los receptores reciban correos realmente encriptados, o de lo contrario no reciban nada. El problema es en la comunicación de texto claro si se publica un registro TLSA, esto significa que hay que encriptar. Porque no hay manera de bajar a la comunicación de *clear text* o de texto claro. En esto también hay un problema práctico de despliegue.

Esto es lo que pasa. El registro MX si se valida el certificado del MTA de envío, si se puede mostrar un certificado se puede garantizar que es realmente quien dice ser por la cadena de confianza que establece DNSSEC.

Si hay un ataque, el certificado no va a coincidir entonces el *e-mail* no se va a enviar.

Hay varias cuestiones operacionales. Lo interesante de este proyecto es que realmente podemos conocer a los operadores, que muchos de ellos no tienen *feedback* operacional porque muchos no lo han probado, no han implementado DNSSEC, y mucho menos DANE, entonces están básicamente aprendiendo qué hay, qué existe. Algunos sí.

El *feedback* que recibimos es que sigue esta percepción general de que DNSSEC es difícil, es complejo, todas estas cuestiones de

configuración. Y eso ya no es así, incluso yo hice una prueba a mi propio dominio personal de correo y funcionó muy bien.

Lo verdaderamente difícil es el registro DS, algunas empresas de telecomunicaciones dijeron, “Bueno, vamos a empezar a implementar en nuestros dominios”, y dos o tres meses después dijeron, “No, no los podemos manejar los registros DS porque el registrador no lo soporta” o, “porque no sabemos qué hacer” o, “porque es un departamento distinto el que hace DNS”. Entonces hay que ir con la gente de red o con la gente de DNS y convencerlos de su utilidad.

O sea, el *feedback* del mundo real es que no es un problema de la tecnología sino más bien un problema de organización. Incluso en mi caso personal, yo ejecuto mi propio servidor autorizado, y tengo mi propio servidor de correo con soporte de DNS y registros DENSSEC no lo pude hacer porque hay un bug en la plataforma y el soporte no sabe qué es DNSSEC. O sea, hay que trabajar para ampliar el trabajo y resolver los problemas prácticos que enfrenta la gente cuando quiere implementar.

Esto ya me parece que lo vimos. Nuevamente, no es una cuestión de software sino de operaciones.

Por último, lo último que quería mostrarles son algunas estadísticas muy interesantes. Debo decir que está todavía en fase beta, o sea que tomen los datos con pinzas. Son pruebas de

nombres de dominios de soporte de correo en lo que hace a seguridad, parte con encriptado STARTTLS, TLS. Antes de comenzar la conexión TLS y también si tienen soporte de DNSSEC DANE y SPF.

Seguimos trabajando en la integración de estos datos. Lo podremos públicamente en el sitio web. Estamos -- para prepararme para esta reunión que era aclarar que esto es de tráfico web. Tomamos los 1000 nombres de dominio más grandes para verificar si tenían soporte de seguridad de correo y si soportaban las tecnologías DNSSEC DANE, y esto es lo que surgió de estas pruebas.

Hay una gran parte que o bien no tienen los registros MX o si existen no están bien configurados, un 20%. Una parte importante pero todavía estoy analizando estos datos porque parece ser más un problema de compatibilidad.

Más allá de esto la buena noticia es que el 72,5% soporta TLS. Si queremos chequear qué versión de TLS está soportada, lo que es importante porque las versiones más antiguas son inseguras, la gente debería soportar la última versión de los protocolos de encriptado de seguridad. Aquellos que tienen correo que funciona, bueno, menos del 60% tienen soporte de TLS 1.2, que es la última versión. Y el 6.5 todavía tiene TLS 1.0. Y como decía antes, el 20% no tiene ningún tipo de soporte de encriptado.

Bueno, por último, DNSSEC y DANE. Tenemos más de 1000 dominios. ¿Cuántos tienen DNSSEC y DANE? Bueno, apareció esto. sólo 15 dominios soportan DNSSEC, así que es un 2% o menos. La mayoría son .gob y son solo tres los que tienen DNSSEC y también DANE.

De hecho aquí los podríamos haber listado por nombre, que lo hicimos. Uno es Comcast y los otros dos son web.de y gmx.net, que son dos proveedores alemanes que son parte del proyecto alemán que mencioné antes. Entonces, por ejemplo, los otros nombres de dominio que están en esta lista que soportan DANE están en el sitio.

Hay buenas y malas noticias. La mala noticia es que la adopción es despreciable. La buena noticia es que hay operadores muy grandes como Comcast y Web.de que ya lo están haciendo, así que con esto podemos ir a los otros y decir, “Miren, si esta gente lo está haciendo, es posible hacerlo”.

La siguiente diapositiva. Bueno, los datos de contacto, por supuesto estoy abierto a preguntas, pero el motivo por el cual estoy aquí es que estamos intentando ampliar este proyecto que empezó como una actividad interna de una compañía pero ahora queremos involucrar en especial a los operadores. Y desde un punto de vista organizamos reuniones.

La semana pasada estuvimos en Polonia, muchos de los proveedores nacionales, no todas las empresas de telecomunicaciones, porque en algunos países es difícil conseguir la gente pero quizá con foros como este, el de ICANN, esperamos ampliar el alcance y llegar aquí a los operadores que están presentes.

También sería interesante conseguir contactos con los registros de ccTLDs, en especial en los países europeos, conseguir cooperación con los registros. Por un lado porque podrían ayudarnos a mejorar las reuniones y también, si les interesa, participar y promover DNSSEC entre las empresas de telecomunicaciones nacionales, porque creo que es importante tener una acción cooperativa en la comunidad. Las normas existen, está bueno hablar de los detalles técnicos pero este es un momento en que la comunidad tiene que ponerse en serio y desplegar la tecnología en todas partes, porque el riesgo es muy grande y existe la necesidad de tomar medidas lo antes posible. Gracias.

JULIE HEDLUND: Gracias, Vittorio. Ahora podemos responder preguntas. ¿Alguien tiene alguna pregunta para Vittorio?

PATRICK: Hola Vittorio. Soy Patrick de una de estas empresas que hizo mucho para DANE en Alemania. Quisiera agregar algo. Usted dijo que muchas personas piensan que tienen problemas con DNSSEC. El problema, usted tiene razón, es que la mayoría de las empresas con las que yo hable vienen usando DNS desde hace muchos años y DNS siempre fue un paso pequeño. Por supuesto todos saben que es muy importante. Entonces cuando pasan a DSSEC tienen miedo de quebrar algo en su infraestructura existente, y es algo que no quieren.

VITTORIO BERTOLA: Estoy de acuerdo. Esos son los comentarios que recibimos. Debe haber un impulso para vencer esta resistencia, porque siempre es más fácil no hacer nada y hacer cuenta que el problema no existe. Si pasara algo realmente malo, habría grandes titulares en algún país y entonces todo el mundo va a apurarse para implementarlo o quizá si hay presión del gobierno. Pero sí, es difícil convencer a que la gente para que actúe.

PATRICK: En Alemania la gente lo adoptó. Por ejemplo, .DE ya lo tiene desde hace muchos años. Es un poco como hacer un *backup* y restaurar. Es como DNSSEC. La gente piensa que es un costo adicional y que quizá no va a obtener nada a cambio.

VITTORIO BERTOLA: Yo vengo de Italia. Tuvimos una reunión así en Italia. El primer problema que tuvimos es que todavía no tenemos el TLD firmado, y estamos en 2017. Así que hablábamos con los operadores, nos mirábamos a la cara, y decíamos, "Aunque quisiéramos, no podríamos hacerlo".

PATRICK: Sí, lo entiendo.

JULIE HEDLUND: Gracias. ¿Hay más preguntas?

[DAN]: ¿Alguien más? ¿Hay tanta gente ahí atrás y nadie tiene preguntas? Yo tengo una pregunta. De los proveedores de correo electrónico con los que están hablando, ¿cuántos apoyan esta iniciativa? ¿Y qué se puede hacer al respecto? Son dos preguntas en realidad.

VITTORIO BERTOLA: La parte de las reuniones fue así. Elegimos una cuenta, empezamos con las grandes, trabajamos en Francia, Reino Unido, Italia, fuimos a Polonia y tratamos de contactar a todas las empresas, incluso las grandes empresas de

telecomunicaciones que tienen millones de clientes y las principales empresas de hosting en algunos países la gente usa la cuenta de e-mail a través de la empresa de hosting, y no recurre a los ISPs, así que depende del país.

Lo que necesitamos es poner a todos, sentar a todos en la misma mesa. Hay algunos capítulos locales de ISOC. Yo trabajo en ISOC Italia desde hace unos 20 años y esa podría ser otra buena alternativa. Tenemos que compartir las ideas y encontrar la forma de comenzar un debate significativo.

En general, lo que también es interesante es que la gente tiende a ser un poco más nacionalista, entonces si decimos, “Miren, los alemanes ya hicieron esto y nadie más lo está haciendo y en su país no están haciendo nada, van a decir Bueno, empecemos algo nosotros también”. Esa es una buena carta que podemos jugar con los gobiernos.

Quizás esta sea una forma. Pero es una cuestión de crear, generar conciencia, porque a veces la gente escucha acerca de DNSSEC pero no sabe cuáles son los peligros que trata de encontrar DNSSEC. No saben de qué manera DNSSEC puede ayudarlos a resolver problemas de seguridad. Hay que comunicar esto, y si alguien quiere ayudar, por favor, que contacte conmigo.

WES HARDAKER: Wes Hardaker, de USC. Un problema con el que nos encontramos es asegurarnos de que la gente que está implementando un certificado para actualizar los registros de DANE. ¿No tienen la forma de implementarlo? Es decir, en general hay un SMTP, y el que administra el SMTP no administra el DNS, entonces quizás actualizan el certificado y no actualizan DNS. ¿Hay algo que verifique eso en la implementación?

VITTORIO BERTOLA: No, no tenemos nada porque todavía estamos en el punto en el que no estamos verificando estos registros. Pero creo que podría hacerse si hubiera un conjunto de herramientas compartidas por todos. Y estoy de acuerdo también. Yo traté, por ejemplo, de seguir el tutorial y el sitio web de implementación de DANE y los clientes todavía tienen problemas con DANE porque continúa cambiando la clave. Hay una serie de cosas que se podrían simplificar. Creo que podríamos pensar juntos acerca de estas cosas también.

WES HARDAKER: Hay un sitio web en donde uno puede dejar un sitio web y no notifican si hay algún problema. Yo no confiaría siempre en un servicio sin ese tipo de relaciones, pero el servicio notifica cuando el certificado no coincide con los registros DNS.

JULIE HEDLUND: ¿Alguien más?

ORADOR NO IDENTIFICADO: Se puede conservar la misma clave pública y regenerar el certificado. Nosotros tuvimos el mismo problema. Nosotros queremos seguir usando la misma clave.

VITTORIO BERTOLA: Creo que hay que preparar un archivo específico, de lo contrario lleva tiempo, no es inmediato.

JULIE HEDLUND: ¿Alguna otra pregunta?

Entonces vamos a dar las gracias a Vittorio por haber estado aquí con nosotros.

Vamos a continuar ahora con Carsten Strotmann sobre SMILLA, encriptación automática S/MIME. Y va a ser una demostración pero creo que va a ser una presentación, ¿no, Carsten? Se esconde, puede venir acá al frente, si quiere.

CARSTEN STROTMANN: No, acá estoy bien. Al lado de mí está Patrick. Patrick va a cubrir la primera parte de la presentación y yo voy a hacer la segunda parte.

JULIE HEDLUND: Perdón. No sabía que estaba acá, Patrick. Entonces comienza Patrick y después Carsten.

PATRICK BEN KOETTER: Quiero aprovechar la oportunidad para hacer un chiste cuando hablamos acerca de DANE en Dinamarca, que estamos acá.

Ya escuchamos hablar acerca de DANE, correo electrónico, la protección y qué podemos hacer al respecto. Carsten y yo querríamos agregar algo nuevo a este tema, queremos hablar acerca de un programa que escribimos con el texto anterior, hace falta un código especial, nosotros tuvimos una propuesta que se llama SMIMEA y es encriptación S/MIME. Primero vamos a hablar de qué se trata y para qué necesitaríamos esto.

El otro día hablé con un técnico de un servicio de radiodifusión alemán grande y me hizo algunas preguntas del *e-mail*, acerca de cómo desarrollar los sistemas, y yo le dije, “Usted trabaja con periodistas y los periodistas trabajan con información, y debería haber alguna forma de proteger la comunicación porque la comunicación en el periodismo probablemente solamente funcione bien si uno tiene canales de confianza y privacidad”. Entonces, sí, él estuvo de acuerdo, pero hoy en día tenemos algunos problemas.

Uno de los problemas – la próxima diapositiva, por favor. La siguiente, por favor.

Uno de los problemas que solemos tener con la encriptación hoy en día es que es complicado. Tenemos dos modelos que compiten entre sí y ninguno de ellos es fácil de utilizar. Uno de los modelos exige que hagamos cierta magia en la línea de comando, tenemos que usar una clave, la gente tiene que descargarla y luego que tiene que haber una especie de proceso de verificación. No es especialmente útil para la comunidad instantánea, si bien necesitamos privacidad instantánea. Lo mismo se aplica al otro estándar S/MIME. Es complicado usarlo y, por supuesto, tenemos a las autoridades que nos hacen comprar certificados y eso lo simplifica un poco más.

La próxima diapositiva.

Tenemos la siguiente pregunta, ¿son realmente de confianza? Tenemos algunas autoridades de certificación de las que se hizo un uso indebido en los últimos años, entonces que alguien nos represente en la comunicación S/MIME no es lo que buscamos, porque alguien puede robar un certificado de una autoridad de certificación.

Entonces, ¿qué podemos hacer para sortear estos problemas que mencioné? Una de las cosas que se puede hacer probablemente sea controlar mejor qué certificado es un

certificado de confianza. Y lo otro que se puede hacer es acelerar el proceso de encriptado. Esa es la idea de S/MIME.

Pasemos a la siguiente diapositiva, por favor.

La idea básica es utilizar DANE que, por supuesto, se apoya en un dominio habilitado para DNSSEC y poner algunos criterios, alguna información que ayude a otros a identificar algunas cosas. En primer lugar, un registro especial que nos dice que la persona con la que estamos tratando de contactar tiene soporte para encriptado. Y además, el hecho de que haya un registro nos indica que esa persona quiere encriptado y hay una clave especial de encriptado que también nos indica qué clase de encriptado usa esa persona. Entonces no usamos PDP cuando la otra persona utiliza otro tipo de encriptado.

Esa es una de las cosas que hacemos. Por otra parte, agregamos un canal de confianza como DNSSEC y de esta forma tenemos un mayor control por parte de aquellas personas que están a cargo de DNS que también son los que tienen los dominios. Entonces lo alejamos un poco de la autoridad de certificación que podría ser manipulada y la ponemos en una plataforma con todos los problemas que tenemos que enfrentar, los temas de seguridad, etc. para que sea lo más seguro posible.

Básicamente, lo que obtenemos es lo siguiente. Tenemos un cliente de *mail* que puede mirar hacia adelante, ver cuál es la

persona que está tratando de escribirnos y ver si reside en un dominio con DNSSEC. Hay un registro especial y ese registro envía cierta información que el cliente de correo electrónico puede utilizar para encriptar la comunicación con esa persona de forma instantánea, oportunista, en el momento en que encuentra la información. Entonces estamos un paso por delante de todo el proceso, no necesitamos pedirle a alguien si entiende, si tiene encriptado, etc.

La próxima, por favor.

Ahora le toca continuar a Carsten. Gracias.

CARSTEN STROTMANN: Entonces el registro SMIMEA es una parte del registro TLSA que ya utilizamos para asegurar nuestro *e-mail* y esto nos da seguridad punto a punto con certificados SMIMEA, entonces el archivo SMIMEA puede utilizarse de distintas formas. Puede utilizarse para almacenar el *hash* o el certificado en un dominio con DNSSEC.

En nuestro caso acá utilizamos todo el certificado x509 que queda almacenado en un nombre de dominio que tiene el *e-mail* con *hash*, es decir, antes de que sea firmado.

Podemos utilizar acá certificados que podemos comprar a través de autoridades de certificación pero también podemos

utilizar certificados auto-firmados. El uso de certificados auto-firmados ofrece incluso algunos beneficios adicionales porque nosotros mismos podemos controlar durante cuánto tiempo son válidos esos certificados y cuándo los queremos descargar.

La próxima, por favor.

Entonces SMILLA. ¿Qué es SMILLA? SMILLA es un MILTER, un MILTER es una API estándar para servicios de correo electrónico de Código Abierto Postfix, Sendmail y algunos más. SMILLA apunta no al usuario privado en su casa sino a organizaciones que tienen su propia infraestructura de correo electrónico.

Entonces SMILLA intercepta todo correo electrónico que pasa por el servidor de *mail* y se fija si ese correo electrónico ya está encriptado, y si no está encriptado, entonces busca en el DNS para ver si el receptor, el destinatario de ese correo electrónico, tiene un certificado x509, y si es así, lo descarga y utiliza el certificado que tiene la clave pública, encripta el correo electrónico con la clave pública y se lo envía al destinatario.

La próxima.

Acá vemos dos casos de uso diferente. Puede utilizarse para encriptar el *mail* saliente, cuando se utiliza del lado de quien envía el correo electrónico, el que envía el correo electrónico busca el certificado del destinatario, encripta y luego lo envía a

través de la peligrosa Internet al destinatario, donde es recibido, y el destinatario luego puede desencriptarlo y leerlo o utilizarlo para encriptar el *e-mail* entrante. Si el e-mail llega de una forma no segura y no encriptada, al ser recibido puede ser encriptado y luego almacenarse encriptado en el disco rígido.

Ese es un caso de uso al que se puede recurrir cuando el servidor de mail está en una plataforma que no es de confianza, digamos un servicio en la nube alquilado en algún lado en donde el operador no es el dueño del equipo, entonces como alguien podría robar el servidor o el almacenamiento y utilizarlo, y por lo tanto se pueden encriptar los correos electrónicos para el destinatario.

Acá vemos cómo funciona DANE con SMIMEA. Tenemos el registro de SMIMEA publicado en el DNS. Acá Bob necesita apoyo de parte de su operador de e-mail y de DNS. Bob almacena este registro que contiene su certificado x509 en DNS en el servidor de ejemplo [inaudible] y después Alice, que está a la izquierda, quiere enviarle un e-mail a Bob. Nunca antes intercambiaron certificados ni claves. Es decir, nunca se conectaron y nunca intercambiaron nada.

Alice envía entonces el correo electrónico sin ningún cambio y sin ningún *software* del cliente de correo electrónico al servidor de mail, y Alice ni siquiera necesita saber que está SMILLA en

medio. Lo envía al servidor de mail, el servidor de mail utiliza el SMILLA MILTER; SMILLA se fija si el correo electrónico ya está encriptado, y si no está encriptado por PGP ni por S/MIME, después, en la próxima diapositiva, vemos que busca el registro SMIMEA en DNS.

Entonces busca el resolutor de DNSSEC y este resolutor va a al servidor autorizado para llegar al dominio del destinatario, vuelve la respuesta en la próxima diapositiva. DNSSEC está validado, ahí vuelve al SMILLA MILTER que recibe y extrae el certificado de la respuesta, encripta el correo electrónico para Bob con el certificado, que es lo que vemos en la próxima diapositiva, y luego se lo envía al servidor de e-mail, del servidor utilizado por Bob. Y luego en la próxima diapositiva Bob busca el correo electrónico a través de su programa de correo electrónico preferido y puede desencriptar el correo electrónico utilizando su clave privada, que tiene configurada en su *software* de correo electrónico.

En la próxima diapositiva vemos que esto ya está funcionando. El SMILLA MILTER no es grande, está escrito en Python, es código abierta, y tenemos planes para fusionar eso con el OPENPGPKEY MILTER que básicamente hace lo mismo para PGP. Hay una clave abierta de PGP en DNS donde se puede almacenar la clave publica de PGP en DNS y funciona básicamente de la misma manera. Es completamente transparente para los usuarios. Los

usuarios no necesitan cambiar nada. Una vez que está implementado en la infraestructura de mail automáticamente encripta todos los correos electrónicos para SMIMIEA o PGP. Funciona en correo entrante y saliente. Lo hicimos con código abierto, con una licencia para que se vea el código en nuestra cuenta *github*.

Es abierto. Si a alguien no le gusta y quiere utilizarlo en [inaudible] o en otra de las cosas que se usan hoy, no hay problema porque no hay mucha línea de código y por lo tanto lo podemos adaptar. Cualquier puede adaptarlo solo o nosotros podamos ayudarlos a hacerlo.

Estamos interesados en que los que quieren implementar esto nos lo hagan saber; los que quieren implementarlo, los que quieren usarlo en un entorno de producción o de prueba, por favor, avísennos.

Y este es el mensaje final. A los usuarios de mail les importa la seguridad. Lo hemos visto en los clientes con los que trabajamos, que quieren vender un servicio de correo electrónico seguro y quieren alejarse de otros servicios de mail. Y hay un grupo de usuarios a los que realmente les preocupa la seguridad y que quieren tener mayor seguridad en su correo electrónico pero para simplificarles las cosas podemos utilizar DANE porque permite este encriptado punto a punto

oportunista. Y quizás es una pieza que podemos utilizar para que el correo electrónico y la comunicación por Internet sean más seguros. Eso es todo. ¿Alguien tiene alguna pregunta?

JULIE HEDLUND: Gracias por las presentaciones a ambos. Abrimos el turno de preguntas. Adelante.

WOTH STUFFBERG: ¿Cuál fue el registro del DNS que tuvieron que añadir para obtener el certificado?

CARSTEN STROTMANN: El registro DNS es el registro SMIMEA y el registro SMIMEA es actualmente un borrador de Internet que acaba de pasar la última sesión del grupo de trabajo por lo que sé, así que probablemente veremos pronto una RC. Y ya está soportado por la versión más reciente del *software* Bind y Unbound. Hay otros *software* que no soportan el registro SMIMEA directamente. Siempre está esta posibilidad de entrar al registro SMIMEA en formato de registro desconocido que es el formato estandarizado para poner cualquiera cosa en DNS y que DNS no conoce.

Así que hoy día ya se puede usar y estamos por desarrollar una pequeña herramienta para dar el certificado y la dirección de correo, y se puede poner en DNS porque hoy en día no existe una herramienta así, entones queríamos hacerlo más sencillo. Esperamos que la semana próxima o en dos semanas esté lista.

PAUL WOUTERS: Perdón por no haber contactado antes con ustedes para cooperar sobre este tema. Estoy recopilando todas estas herramientas en un paquete, todas estas cosas de generación, y no sé si ustedes me pueden dar el comando de SMIMEA.

Y para hacer un comentario: yo en lo personal hice la versión OPENPGPKEY libre en mi servidor y cuando fui a chequear mi servidor tenía varios cientos de e-mails encriptados, así que queda trabajo por hacer del lado del cliente, donde lo preferible es que lo desencripte automáticamente en lugar de dejarlo encriptado en el buzón. Porque si hay 200 e-mails encriptados en el buzón no hay nada que podamos hacer, eso es -- no sé si se puede hacer algo con [Enigmail].

CARSTEN STROTMANN: Hay soporte para [Enigmail], se puede poner un filtro que dice que una vez que se abrió un e-mail encriptado lo almacene desencriptado. Es posible pero no es por omisión. Hay que

poner el filtro. Y sí, es un área de trabajo más que podemos hacer.

JULIE HEDLUND: Veo a Rick Lan. Adelante.

RICK LAN: Hola. Buen trabajo. ¿Están considerando esto extremo a extremo, no sólo en el servidor sino en las máquinas cliente? ¿Han pensado en algún tipo de manera molesta de interceptar el trafico como para que el usuario final de Outlook se beneficie de algo como esto? Estoy pensando en los *masses*, o sea, ser verdaderamente extremo a extremo, es decir, no confiar en nadie.

CARSTEN STROMANN: Es una idea tentadora pero por el momento, bueno, hay muchos proveedores de antivirus que intervienen en las sesiones. No es sencillo, no es una tarea fácil.

RICK LAN: Bueno, yo lo usaría definitivamente.

ORADOR NO IDENTIFICADO: Yo pensaba en lo mismo, y es hacer un servidor mail en el *host* local. Me gustaría agregarlo en mi iPhone, pero no sé cómo funcionaría.

PATRICK BEN KOUTER: Otra cosa es que si usan herramientas de autoconfiguración en el cliente de correo se puede hacer una configuración que comience el TLS en un camino de presentación. Entonces, en lugar de empezar encriptado, cuando el correo llega al servidor se encripta. Esa es una manera de hacer la desencriptación.

JULIE HEDLUND: Gracias. ¿Alguna otra pregunta? No veo a nadie, así que agradezco a Carsten y a Patrick por sus interesantes presentaciones y, por favor, un aplauso. La presentación que sigue es de Dan York y es sobre "DNSSC, cómo puedo ser de ayuda".

DAN YORK: Bueno, no sé cómo pero llegamos de algún modo a cumplir con nuestros horarios. Otra vez perdí el *clicker*. Bueno, llegamos al final de la agenda. De hecho con tiempo de sobra. No sé si esto tiene algún antecedente, pero antes de seguir quiero un aplauso para el Comité Organizador, que preparó este día. También

quiero agradecer y aplaudir y a Julie y a Kathy, que hicieron que todo esto funcionara.

El Comité Organizador se reúne todas las semanas. Tuvimos una reunión con Julie y con el resto de la gente en horarios extraños. Yoshiro, por ejemplo, en Japón está trabajando a la media noche, así que admiro su dedicación.

Hay un grupo de gente muy dedicada que ha venido trabajando en esto ya desde hace 10 años. Bueno no sé si 10 años, pero el programa hace 10 años que existe, así que es mucho el trabajo. Quiero agradecer en especial a Julie, porque es quien ha puesto todo en esta matriz, que ha logrado que esto se concrete.

Vamos a hacer una llamada solicitando la participación en breve para la sesión de Johannesburgo, que es un poquito distinto. Es parecido a lo que hicimos en Helsinki, que los juntamos con el Tech Day. Vamos a hacer el Taller de DNSSEC por la mañana, ¿sí? Por la mañana. Vamos a hacer mañana y almuerzo, y por la tarde vamos a hacer el Tech Day, con presentaciones técnicas que no están relacionadas normalmente con DNSSEC, como ataques de DDoS, mediciones, botnets, etc.

Jacques Latour, quien no está aquí, de CIRA – sí, ahí está. ¿Por qué no estás con la gorra? Te falta la bufanda. No tienes la camisa a cuadros. Bueno, él no se ha reído, pero yo sí. Si no

miraron todas las cosas que les pusieron en la bolsa habrán encontrado algo muy gracioso.

Jacques también está en el Comité de Programación del Tech Day, así que si alguna vez quieren hacer una presentación técnica ante otro grupo, hay dos sesiones en ICANN, la reunión de ICANN, que son técnicas, esta y otra.

Acá está. Fíjense. ¿Por qué no se ríen? Sé que la organización tiene cierto sentido del humor. Es la misma gente que tenía el castor. Acá hay un reno. Bueno, tenemos que dar crédito al sentido del humor.

Y vamos a terminar con cierta idea acerca de qué pueden hacer cuando se vayan de aquí. Si quieren hacer algo al salir de aquí, tenemos a los operadores de TLD que les sugerimos que participen y que firmen el TLD y que tomen los registros, porque si no está muy bien firmar, o sea marcamos otro casillero como completo, pero no hemos hecho efectivamente nada para que las cosas sean más seguras. Entonces firmen con los registradores.

Y otra cosa que les pedimos a los operadores es que nos ayuden con las estadísticas. Hemos visto muchas presentaciones como lo que dijo Rick Lan con sus estadísticas. Estamos tratando de conseguir más estadísticas. Así que si nos pueden ayudar con eso.

Para los operadores de zona, la gente que tiene dominios, firmen la zona, trabajan con los registradores. Y ayúdennos. De hecho estamos pidiéndole a la gente que firmen los dominios si pueden y que no olviden el traspaso de la clave, que se acerca, el 11 de octubre.

Los operadores de red, les pedimos que por favor activen la validación. No es más que una línea de código. A veces es simplemente tildar un casillero. Les pedimos a la gente que vean el porcentaje de validaciones de APNIC.

Y les pedimos a todos que, por favor, usen DNSSEC, que compartan las lecciones. Como decía, vamos a tener una llamada solicitando participación en Johannesburgo. Si conocen gente que en el foro de políticas quiere presentar algo, siempre nos interesa saber de ideas diferentes. Tendremos otro panel regional, así que si conocen gente de la región, obviamente África, que quiere presentar de lo que hacen en DNSSEC nos encantaría escuchar de ellos.

También buscamos gente que haga cosas, nuevas demostraciones. Con el correo tuvimos un par de cosas aquí. Ya tuvimos presentaciones sobre correo electrónico y gente que presento nuevas herramientas que hacen nuevos sitios. Tuvimos a Rick haciendo *software* y muchas otras cosas que la gente lleva adelante, o sea, siempre nos gusta tener distintas clases de

presentaciones para saber cómo la gente usa DNSSEC y DANE de manera lógica.

Bueno, quiero cerrar agradeciendo – sí, Christian, perdón. Necesitamos un nuevo logo. Hay un nuevo logo muy bonito y brillante. Perdón, Christian. Lo vamos a actualizar en el próximo. Quiero a agradecer a Afilias, a CIRA y a SIDN por el apoyo que nos brindaron. Si lo ven a Christian por ahí estaba sentado aquí, con una camisa blanca, agradézcanle y a Jim Galvin si lo ven. Gracias, Jacques. Él está ahí. Gracias a ellos tuvieron el almuerzo hoy.

Y esto ya lo dijimos, SSAC y el programa Deploy 360. Bueno, eso es todo, estos son algunos sitios de Internet site at org/deploy360, el programa DNSSEC *tools*. Tienen las distintas herramientas que existen y DNSSEC – *deployment* tiene información histórica.

Con esto—lo último, yo sé que ustedes sí que me lo enviaron pero no lo vi. La verdad es que no lo leí.

Bueno, ignoren esta diapositiva. Lo que debo decir es que si les interesan los temas, vamos a tener otra acción que nos mantendrá conectados entre los eventos. Los primeros jueves de cada mes tenemos una llamada en la que todos están bienvenidos a participar.

Hablamos de los nuevos pasos, Rick en California lo vimos caminando porque necesitaba café, era muy temprano. Hablamos de lo que hace la gente, qué cosas hace para implementar los nuevos avances.

Hay una lista de correo, que es DNSSEC-coord, por coordinación. Tenemos estas llamadas, que nos gustaría ver cómo la gente participa porque es bueno saber lo que hace la gente. Vimos muchos ya que se enteran de que hay alguien que dice estoy probando esto, me interesa saber qué hace esta otra persona, entre ellos hablan de distintos programas, etc. es una manera de mantener o de compartir información entre reuniones.

Bueno, con esto hemos terminado. Gracias a todos y nos vemos en Johannesburgo.

JULIE HEDLUND: Gracias, Dan, por moderar, liderar.

DAN YORK: La próxima vez, si alguien quiere ayudar en la moderación, muéstrese porque no quiero ser el único que lo haga siempre. Gracias a todos. También tenemos que agradecer a Irwin por la reunión de anoche, por el apoyo local. Gracias.

[FIN DE LA TRANSCRIPCIÓN]