Identidad y Reputación en línea

ESQUEMAS DE CONFIANZA

"Querido amigo: Soy la señora Mariam Abacha[1], viuda del finado General Sani Abacha, ex-jefe de gobierno de Nigeria. (…) Para salvar a mi familia de una total bancarrota, estoy buscando transferir el total de US$24,000,000 a través de una institución bancaria confiable. (…) Como pago por su ayuda, le ofrezco el 30% de lo que podamos rescatar de la fortuna de mi querido esposo."

El tema conducente del presente ejemplar de SG, Pagos en línea, cruza necesariamente por el tema de los esquemas de establecimiento de reputación en línea. Cada vez menos gente asume confiable cualquier dato que encuentra en Internet sencillamente por estar ahí. Un logro del que puede enorgullecerse la comunidad de expertos que apuntan a la necesidad de concientización en nuestro quehacer en red es que la generalidad de los usuarios, por lo menos, ya desconfía cuando le piden datos para tener acceso a su dinero. Sin embargo, ¿qué es lo que nos lleva a confiar en determinados proveedores?

El problema de establecer la reputación de un tercero puede presentarse como un muy interesante ejercicio académico, con anclas en muy diversas áreas del conocimiento, desde las ciencias sociales hasta las matemáticas.

En un plano mucho más aplicado, todo el problema de la reputación puede resumirse en las preguntas, ¿Puedo confiar en que la contraparte es quien dice ser? y ¿Puedo confiar en que dice la verdad? Enfocándonos a las aplicaciones actuales, podemos principalmente traducir estas preguntas en:

Confianza en la identidad

Seguramente habrán recibido alguna vez un correo similar a aquel cuyas primeras líneas reproduje. Afortunadamente, es poca la gente que cae en estos esquemas[2]. Lo primero que debe venir a nuestra mente es, ¿estoy realmente intercambiando correo con la Sra. Abacha?

Hemos aprendido a desconfiar de la identidad de los extraños. Y cuando un extraño nos propone una transacción económica, nuestra primera reacción es desconfiar. Cuando efectuamos transacciones a través del navegador, nos hemos acostumbrado a buscar indicaciones de que estemos hablando con un servidor seguro. ¿Qué es esto? ¿Cómo lo valida el navegador?

Más allá de aplicar el sentido común, hay dos esquemas principales que nos permiten confiar la identidad de una entidad –individuo o empresa– con la que podamos tener un intercambio que incluya información confidencial (que requiera mantenerse a resguardo de terceros, como el número de nuestra tarjeta de crédito) o no-repudiable (que nos interese tener un comprobante de haber realizado determinada transacción¸ sea pública o privada, con la persona o entidad en cuestión; lo que se ha dado por llamar firma electrónica): El esquema centralizado, basado en autoridades certificadoras (CAs), firmas corporativas y el esquema descentralizado que está basado en llaveros de confianza y firmas personales. Ambos están basados en la criptografía de llave pública, con implementaciones derivadas de la criptografía de llave pública. No profundizaré en cómo estos pueden utilizarse para el intercambio de información, sino sobre la metainformación: Cómo apuntan a la confiabilidad sobre la identidad de un actor.

Por un lado, tenemos a la infraestructura de llave pública (PKI). Este es el esquema que siguen los navegadores Web, punto de contacto que casi todos tendremos con los pagos en línea. Además de los navegadores y el ocasional cliente de correo, muchos otros servicios pueden emplear certificados de esta naturaleza para realizar autenticación o cifrado[3] — Pero estos dos son los más visibles a los usuarios en general.

Bajo un esquema PKI, nuestro navegador confiará ciegamente en la identidad de un conjunto de CAs centrales, definidas por el proveedor del software[4]. Mientras un certificado esté firmado por una autoridad conocida, el navegador mostrará la conexión como segura.

Tenemos por otro lado a los esquemas basados en el esquema de llaveros de confianza. Éste esquema fue dado a conocer en los 1990 con el sistema de criptografía PGP, de Phil Zimmermann. Un llavero de confianza podría definirse como un sistema colaborativo, par a par: Cada participante del llavero firma la llave de los otros participantes a los que conoce personal-

Gunnar Wolf es administrador de sistemas para el Instituto de Investigaciones Económicas de la UNAM y desarrollador del proyecto Debian GNU/Linux.
www.gwolf.org

mente, certificando confianza en que su identidad es verdadera[5]. Cuando un usuario quiere comunicarse con otro, puede ver cuál es el camino de confianza yendo entre individuos, con base en la distancia y grado de conexión (y, por tanto, de certificación) que tiene determinada identidad, decidir el nivel de confianza que depositará en ésta.

Entonces, un servidor seguro no es sólo el que implementa una conexión cifrada, sino que aquél en cuya identidad puedo confiar. Emplear cifrado sólo tiene sentido cuando podemos confiar en la identidad de nuestra contraparte. De muy poco serviría que garantizáramos que toda nuestra comunicación llega cifrada hasta nuestra contraparte si dicho sistema no es el sistema destino. Si no verificamos la identidad de nuestra contraparte, un atacante podría interponer un servidor entre nosotros y nuestro destino, descifrando y cifrando nuevamente la comunicación, modificando o guardando los datos que juzgara necesario.

En un esquema PKI, basta con engañar a una CA respecto a nuestra identidad para tener la puerta abierta a interceptar las solicitudes de usuarios. Y, tristemente, esto ya hace mucho tiempo pasó del terreno del discurso académico al del mundo real: En 2001 fue detectado un certificado firmado por Verisign a nombre de Microsoft, otorgado a un individuo sin relación alguna con dicha compañía[6].

A diferencia de PKI, en que un conjunto de firmas se ve como una serie de árboles con raíces en cada una de las CAs certificadas, una red de firmas basada en las ideas de Zimmermann nos aparece como una red fuertemente interconectada, y nos permite validar varios caminos de confianza entre dos participantes de esta red y evaluar cada a uno de ellos basado en la confianza subjetiva que damos a los actores involucrados[7].

No hay un esquema indiscutiblemente mejor que el otro, solo son utilizados con fines distintos. Ambos tienen su ámbito de aplicación, y si hoy podemos confiar en la confidencialidad, integridad y seguridad de las transacciones en línea, es por estos esquemas. Nuevamente, de muy poco nos serviría cifrar nuestras transacciones en un entorno hostil sin tener confianza en que la contraparte es quien esperamos que sea.

Reputación del individuo

Asumamos, sin embargo, que la Sra. Abacha nos convenció plenamente de ser ella. ¿Debemos por ello confiar en su oferta?

Es aquí donde entra en juego la reputación: Ya que tengo certeza de estar interactuando con la entidad deseada, saber si es una entidad con la que me conviene mantener una transacción es el siguiente albur. Y, en este caso, la reputación es algo que debe establecerse bidireccionalmente. No sólo al comprador le interesa saber que el vendedor le entregará un producto genuino y a tiempo, sino que al proveedor le interesa saber si el comprador tiene cómo pagarlo. No sólo al solicitante de un préstamo le interesa que el banco confíe en su capacidad crediticia, sino que al banco le importa saber si éste no ha faltado a sus obligaciones de pago. Si entro a un sitio de intercambio entre particulares, sea de venta directa o a través de subastas (y seguramente en ambos casos todos habrán pensado en cuál sitio pensé al escribir tan amplia categoría, lo que también entra en el amplio ámbito de la reputación), los individuos participantes tienen una calificación indicando su confiabilidad basada en su comportamiento previo.

O saliéndonos del árido tema de las transacciones económicas, en un foro de discusión puede interesarme filtrar los mensajes para sólo ver los que más vale la pena leer, sin recurrir a un sistema que requiera involucramiento masivo de los editores, la mayor parte de estos sitios basan este filtro dando un valor inicial dependiente de la reputación del autor.

La asignación de reputación es un área completamente dependiente del campo de aplicación, por lo que resulta imposible hablar de implementaciones como en la sección anterior.

Nuevamente, las restricciones de espacio me dejan apenas arañando el campo, apuntando a una gran área a tener en consideración para cualquier desarrollo que emprendamos en que pueda involucrarse el peso o la complejidad de las relaciones entre entidades complejas. Tomar estos elementos en cuenta de forma transversal a los diferentes dominios de aplicación nos llevará a variadas e interesantes consideraciones, que seguramente mejorarán no sólo la confiabilidad de nuestras transacciones, sino incluso la oportunidad y el valor de la información que presentamos a nuestros usuarios. SG

1 El nombre de la Sra. Abacha es el más prevalente en los fraudes de pago anticipado; tristemente, su identidad y reputación son ya demasiado bajos. Mi intención no es dañarlo más, claro está, sino señalar un fenómeno preexistente

2 Sin embargo, una pequeña proporción de una cantidad absurdamente grande de correos enviados sigue resultando en buen negocio... Y es por ello que estos defraudadores siguen saturando nuestros buzones.

3 Encontraremos referencias a estos certificados como X.509; si vamos a implementar directamente operaciones sobre los certificados, conviene hacerlo empleando la biblioteca libre openssl.

4 Por ejemplo, puede consultar la lista de CAs autorizadas por Mozilla en *http://www.mozilla.org/projects/security/certs/included/index.xml*

5 Es muy importante tener en cuenta que lo único que aquí se certifica es la identidad, no la confianza en la entidad en cuestión. La confianza será tratada en la siguiente sección.

6 Bruce Schneier: Fake Microsoft certificates, *http://www.schneier.com/crypto-gram-0104.html#7*

7 Por poner un ejemplo, si yo (llave C1DB921F) obtengo un documento firmado por Marcelo Tosatti (llave E8E1FE55), desarrollador del kernel de Linux, encuentro que (al día en que escribo este texto) estamos a tres "brincos" de distancia: *http://pgp.cs.uu.nl/paths/C1DB921F/to/E8E1FE55.html, http://webware.lysator.liu.se/jc/wotsap/wots/latest/paths/0xC1DB921F-0xE8E1FE55.png*