GnuPG y el grupo de firmas (Keysigning Party)

Author : muammar

1.1 Qué es exactamente un Grupo de Firmas?

Un Grupo de Firmas es la forma de reunir a personas que utilizan sistemas criptográficos tipo PGP con el propósito de permitir a dichas personas el firmado mútuo. Los Grupos de Firmas sirven para extender la confianza por la red. También los grupos de Firmas son una gran escusa para discutir temas políticos o sociales bajo una fuertes medidas de seguridad criptográfica, libertades individuales, soberanías e incluso implementar tecnologías criptográficas o posibles trabajos de software criptográfico gratuito.

1.2 Qué es una Llave firmada?

El Firmado de llaves es el acto de firmar digitalmente una llave pública y un id asociado con dicha llave. La Firma nos sirve para verificar que el id y la llave pública pertenecen realmente a la entidad que aparece en la firma que representa esa llave.

Cada uno puede firmar su propia llave pública y los id asociados a ella, o otras entidades y asociarlas a la llave pública.

En esencia, las firmas validan las llaves públicas. Es una forma de validar una llave pública y una identidad gracias a una tercera parte. Esta es la forma en la cuál las firmas crean un sistema de confianza.

1.3 Qué es un sistema de confianza?

Un sistema de confianza es el término utilizado para describir la relación de confianza entre un grupo de firmas. La firma es un enlace, o una ramificación, en el sistema de firmas de confianza. Estos enlaces son llamados Vias de confianza (Trust Paths). Las Vías de Confianza pueden ser bidireccionales o de una única dirección. El ideal de un sistema de confianza es que cada uno esté conectado de forma bidireccional con los demás. De hecho, cada uno confia en que cada llave pertence a su propietario legítimo. El sistema de confianza es la suma de la confianza de todos las vías de confianza, o enlaces, entre todas las firmas participantes. Aquí tienes un ejemplo visual de un sistema de confianza.

1.4 Puedes darme un ejemplo aplicativo de llaves firmadas?

Como ejemplo podemos explicar que Alicia y Benito crean sus propias llaves con GPG y firmadas en un Grupo de Firmas. En el Grupo, Alicia y Benito verifican otras llaves y luego las firman. GPG, por defecto, firma de forma automáticamente la llave pública asociada a la llave privada cuando se crea. Entonces Alicia y Benito tienen como mínimo dos firmas validando sus llaves. La llave de Alicia ha sido firma por ella misma y por la firma de Benito, mientras que la llave pública de Benito está firmada por él mismo y por Alicia.

En un futuro, Alicia y Benito conocen a Carmen. Carmen crea un par de llaves y les dice a Alicia y a Benito que les enviará su llave pública. Pero a Alicia no le gusta Carmen y no quiere que Benito intercambie comunicaciones cifrada con ella. Ambas, Alicia y Carmen, crean nuevas llaves que dicen ser de Carmen y ambas se la envia a Benito. Ambas llaves tienen una firma, la firma asociada a la llave privada. Benito no sabe cuál es realmente la llave de Carmen, pero ésta se entera de que Benito tiene dos llaves suyas y sospecha de Alicia. Carmen, ahora enfadada, quiere obtener información que utilizar contra Alicia y para obtener dicha información Carmen debe comprometer las comunicaciones entre Alicia y Benito. Para hacerlo, Carmen decide falser un correo hacia Benito diciendo que ella es Alicia y que ha creado una nueva

Llave Pública. En el correo, Carmen incluye la "nueva" llave de Alicia (que en realidad es la falsa que ha generado Carmen). Sin embargo Benito está seguro de que es un truco, porque Benito tiene dos llaves de Alicia, una de las cuales ha sido firmada por multiples personas (él mismo y Alicia) verificando que proviene de Alicia, mientras que la otra llave (la falsa de Carmen) sólo tiene su propia firma.
Este ejemplo tan sencillo puede complicarse muchisimo más. Puedes leer más documentación sobre PGP o un buen libro de PKI para ejemplos más detallados. El ejemplo explica claramente las bases del firmado y su importancia. Carmen no podrá introducir su falsa llave de Alicia por que existe un sistema de confianza entre Benito y Alicia.
Sin embargo, las firmas y los sistemas de confianza no garantizan la credibilidad de las llaves. Por ejemplo, cuando Benito y Alicia conocieron por primera vez a Carmen, esta traía a un amigo consigo: David. David tenia creadas unas llaves falsas para Alicia y Benito, firmadas por él mismo y por las llaves falsas resultando que cada firma poseía tres firmas y se las había enviado a Carmen. Carmen posee una serie de falsas firmas. Como las firmas pueden ayudar a Carmen a resistir un ataque? Bien, hay que decir que todas las firmas que la gente intercambia existen en un servidor de llaves público. Si Carmen hubiese buscado en el servidor de llaves las llaves de Alicia y Benito, encontraría dos pares de llaves para Alicia y para Benito. Si Alicia y Benito recopilaron veinte firmas en el Grupo de Firmas es obvio que Carmen podría confiar en las llaves con mayor cantidad de firmas que no en las llaves con sólo tres firmas. Carmen debería sopechar algo más sobre la existencia de esas llaves públicas, podría sospechar de las fechas de generación y del sistema de confianza de dichas llaves. Las veinte llaves del Grupo de Firmas han sido firmadas veinte o más veces en diferentes periodos de tiempos, muchas de ellas firmadas por Alicia, Benito y por otras personas. Ese no sería el caso si David hubiese generado veinte falsas llaves con un falsa confianza.

1.5 Por qué debo firmar mi llave en grupo

Existen tres razones principales para tener tantas firmas como se pueda.
La primera y la más importante, debes tener la mayor cantidad de firmas para expandir tus vías de confianza. Cuanto más profundo y extrechamente interconectado sea el sistema de confianza, más difícil será comprometerlo. Esto tiene un significado especial para Free Software Community (Comunidad de Software Libre), sean desarrolladores o usuarios. Los miembros de esta comunidad delegan sobre la tecnología criptográfica PGP la protección e integridad de sus paquetes de software, avisos de seguridad y anuncios. La fuerza y robustez del sistema de confianza es directamente proporcional a la fuerza de protección que PGP provee a la comunidad.
La segunda razón es que los grupos de Firmas ayudan a otras personas a integrarse dentro de la cultura de las seguridad y les anima a adquirir conocimientos sobre PGP y otras tecnologias de criptografía. Para conseguir toda la fuerza de la criptografía la gente debe usarla y usarla correctamente.
Finalmente, los grupos de Firmas ayudan a construir comunidades. Ayudan a juntar nuevos conocimientos y discusiones importantes sobre libertades civiles, cripto-derechos y regulación de internet. La discusión es importante por que no sólo es el primer paso, pero es el paso antes de la acción. Ahora que estoy escribiendo este artículo no existen sistemas de seguridad demasiado complejos en el mundo. Si trabajas para construir un sistema de seguridad en tu localidad, es muy probable que esos primeros participantes sean los líderes asentando las bases de internet en su comunidad. Ellos son los individuos que podrán escoger construir el sistema criptográfico seguro y sus protocolos dentro de la infraestructura local, si pueden

escoger. La integración de sistemas y protocolos pueden transformar sistemas como el Carnivore del FBI en inservibles.

Este texto fué sacado de http://www.gnupg.org
Para leer el artículo completo haz click aquí =======>