Let's Encrypt @LetsEncrypt.

"Let's Encrypt" es un proyecto de la "Electronic Frontier Foundation" en colaboración con la "Linux Foundation" para promover uso del protocolo HTTPS.

> For english speakers: this is a merely translation into castilian language of an article year ago published by "Electronic Frontier Foundation" (also known as EFF acronym) where it announces the starting project "Let's Encrypt".

Let's Encrypt: Vamos a encriptar.

Esta es una mera traducción al idioma castellano de un artículo publicado a hace un año atrás por la "Electronic Frontier Foundation" (también conocida por su acrónimo EFF) donde anuncian el comienzo del proyecto "Let's Encrypt" (vamos a encryptar -la web-). Los enlaces web originales del artículo están en idioma inglés sin embargo algunos otros que agregué por mi cuenta están en castellano para rápidamente ayudar a entender algunos conceptos, si es que deseaís ampliar tus horizontes. Sin más, aquí va:

Hoy la EFF se complace en anunciar "Let's Encrypt", una nueva iniciativa de Autoridad de Certificación (CA por sus siglas en inglés) que hemos comenzado junto a Mozilla, Cisco, Akamai, IdenTrust e investigadores de la Universidad de Michigan cuyo objetivo es limpiar las barricadas restantes para la transición de la web del protocolo HTTP al protocolo HTTPS.

A pesar de que el protocolo HTTP ha tenido un éxito enorme, es inseguro de manera inherente. Cada vez que usted utilice una página web HTTP, siempre estará vulnerable a los problemas, incluyendo robo de cuentas y usurpación de identidad, vigilancia y seguimiento de gobiernos, compañías o ambos en conspiración; inyección de guiones maliciosos dentro de páginas; y censura cuyo objetivo son palabras específicas o sitios web específicos. El protocolo HTTPS, aunque todavía no es perfecto, es una gran mejora en todos los frentes, y necesitamos mudar a futuro cada sitio web al protocolo HTTPS por defecto. Con un lazamiento programado para el verano (boreal) del 2015 la Autoridad de Certificación "Let's Encrypt" automáticamente expedirá y administrará certificados sin costo para cualquier sitio web que los necesite. Configurar un servidor web de HTTP al HTTPS con esta Autoridad de Certificación será tan fácil como emitir un comando, o hacer click en un botón.

El más grande obstáculo para el despliegue del HTTPS ha sido la complejidad, la burocracia y el costo que los certificados que HTTPS requiere. Estamos familiarizados con los mensajes de advertencias y error producidos por certificados mal configurados. Esas advertencia son una pista de que HTTPS (y otros usos del TLS/SSL -seguridad de la capa de transporte/capa de conexión segura-) depende de una complejidad horrororosa y una burocracia estructuralmente disfuncional para la autenticación.

Instalación rápida y segura.

La necesidad de obtener, instalar y administrar certificados de esa burocracia es la mayor razón para que los sitios web sigan usando HTTP en vez de HTTPS. En nuestras pruebas, típicamente le toma a un programador web de 1 a 3 horas habilitar la encriptación por primera vez. El proyecto "Let's encrypt"apunta a resolverlo reduciendo el tiempo a 20 ó 30 segundos. Usted puede ayudar a probar e indagar más sobre cómo funciona el agente de software "Let's Encrypt" en su vista previa para desarrollador u observe un video de éste en acción:

"Let’s Encrypt" empleará un número nuevo de tecnologías para una verificación automatizada de manejo seguro de dominios y emisión de certificados. Usaremos un protocolo que estamos desarrollando llamado ACME entre servidores web y la Autoridad de Certificación, la cual incluye apoyo para nuevas y fuertes normas de validación de dominios. También emplearemos conjuntos de datos de certificados distribuidos a lo largo y ancho del internet, tales como el propio Observatorio Descentralizado SSL de la EFFF, el de la Universidad de Michigan, y el Registro Transparente de Certificados de Google, para tomar decisiones de mayor seguridad con respecto si un certificado es de emisión segura.

La Autoridad de Certificación "Let's Encrypt" será operada por una nueva organización sin fines de lucro llamada Grupo de Investigación de Seguridad en Internet (Internet Security Research Group -ISRG-). "Electronic Frontier Foundation" ayudó a juntar esta iniciativa con Mozilla y la Universidad de Michigan, y se ha unido en el lanzamiento con socios tales como Cisco, Akamai e IdenTrust.

El equipo central que trabaja en la Autoridad de Certificación "Let's Encrypt" y agente de software incluye a James Kasten, Seth Schoen, y Peter Eckersley por parte de la EFF; Josh Aas, Richard Barnes, Kevin Dick y Eric Rescorla por parte de Mozilla; Alex Halderman y James Kasten por parte de la Universidad de Michigan.

Por último (y fué publicado el 19 de octubre de 2015) les invito a ver el fruto del trabajo realizado durante largos años de colaboración unificada, la primera página "¡Hola mundo!" con certificados intermedios de referencia cruzada, de nuevo traduzco para ustedes (si usted sabe traducir mejor

POR FAVOR registrese y comente esta entrada):

"Let's Encrypt" es segura.

Estamos muy complacidos en anunciar que hemos recibido las firmas cruzadas proporcionadas por IdenTrust, lo cual significa que nuestros certificados son ahora seguros en la mayoría de navegadores web. Esto es un hito significativo debido a que los visitantes de sitios web con certificados "Let's Encrypt" pueden disfrutar de una experiencia de navegación segura sin que requiera ninguna configuración especial.

Ambos certificados intermedios "Let's Encrypt", llamados "Autoridad X1 Let's Encrypt" y "Autoridad X2 Let's Encrypt", recibieron firmas cruzadas. Los servidores web necesitarán ser configurados con el certificado de firmas cruzadas apropiado como aprte de la cadena de confianza. El cliente "Let's Encrypt" manejará esto automáticamente.

Usted puede ver un ejemplo de un servidor utilizando un certificado "Let's Encrypt" bajo una nueva firma cruzada intermedia aquí.

Información personal vital y de negocios está circulando por internet con más frecuencia que nunca, y es tiempo de encriptar todo esto. Es por eso que hemos creado "Let's Encrypt", y estamos animados en ser el *gran* paso que nos acerce a brindar conexiones seguras a cada rincón de la web.

> We are trusted! https://t.co/8hSWk3Y6Hi
>
> — Let's Encrypt (@letsencrypt) October 20, 2015

Actualizado el lunes 18 de abril de 2016.

https://twitter.com/hpe_voltage/status/720676790453317632

Cada día son más y más personas que reportan del éxito de "Let's Encrypt" y aseguran sus sitios web con este protocolo seguro de comunicación para mantener la privacidad y seguridad de los internautas.

Estamos seguros que algún día aseguraremos esta vuestra página web para ustedes ¡pero @CaracasHosting ***POR AHORA no me deja siquiera instalar mi propio certificado autogenerado!***