禪

مشارکت همگانی برای ایمنسازی

رمزنگاری رایگان برای صدور گواهیهای SSL/TLS

Let's Encrypt

پروژه رمزنگاری رایگان از اوایل اکتبر سال 2014 میلادی کار خود را آغاز کرد . بنابر برنامهریزیهای انجام شده کار عملیاتی روی این پروژه نزدیک به یازده ماه بهطول انجامید . Let's Encrypt یک مرجع صدور گواهی دیجیتال است، که مجوزهای آن در اواخر سال جاری میلادی بهطور رایگان گواهیهایی را برای پروتکل امنیتی لایه انتقال بر پایه لایه سوکت امن Secure Sockets Layer/Transport Layer Security ارائه میکند .

Let's Encrypt پروژهای است که با هدف ارائه رایگان و سادهتر کردن روش پیادهسازی گواهیهای دیجیتال (SSL/TLS) برای ایمنسازی سایتها HTTPS در حال اجرا است. با Let's Encrypt هر وب مستری علاقمند به پیادهسازی HTTPS برای سرویسهای خودش خواهد بود. بهدلیل اینکه این گواهی رایگان است یک حرکت بزرگ برای تشویق مردم به رمزنگاری ارتباطات خودشان و وبسایتها بهشمار میرود . Let's Encrypt تلاش مشترک مدافعان حقوق دیجیتال، EFF (سرنام Electronic Frontier Foundation)، بنیاد موزیلا، سیسکو سیستم، توزیع کننده اینترنت Akamai Technologies، صادر کننده گواهی IdenTrust و محققان دانشگاه میشیگان است.

بهطور کلی، روند اجرای پیادهسازی یک گواهی SSL، شامل بدست آوردن و نصب گواهی است که این فرآیند برای بسیاری از توسعهدهندگان کار پیچیدهای محسوب میشود . در اغلب موارد، مسائل مربوط به هزینههای تحمیل شده به مدیران وب آنها را در مقابل پیادهسازی ارتباطات رمزنگاری شده تسلیم میکند . با اینحال، Let's Encrypt بر مبنای دو هدف راهبردی طراحی شده است؛ اول آنکه روند پیادهسازی گواهیهای دیجیتال را ساده کرده و دوم آنکه هزینههای مالی را برای اپراتورها بدون آنکه نگران امنیت باشند کاهش دهد. مشارکتکنندگان در این پروژه بهزودی گواهیهای قابل اعتماد مرورگرها را از طریق یک API عمومی و مستند که هر وبمستر یا مالک سایتی بتواند آنرا پیادهسازی کند منتشر خواهند کرد . آزمونهای رسمی به عمل آمده توسط محققان نشان داده است که یک وب مستر اغلب بین یک تا سه ساعت برای نصب یک گواهی زمان نیاز دارد .

Let's Encrypt توسط ISRG (سرنام Internet Security Research Group) حمایت مالی میشود، یک شرکت دولتی تازه تأسیس مستقر در کالیفرنیا که زمینه کاریش در ارتباط با امنیت اینترنت قرار دارد . این پروژه در 27 جولای اولین گواهی خود را صادر کرد و در مرحله راهاندازی قرار گرفت و در اوایل ماه سپتامبر در دسترس عموم مردم قرار خواهد گرفت . با اجرایی شدن این پروژه در آینده نزدیک یک گواهی

امنیتی رایگان در اختیار مردم قرار خواهد گرفت . با اینحال، اگر وبمستر یا مدیر سایتی، نیازمند یک اعتبارسنجی توسعه یافته (EV) مضاعف برای گواهی SSL باشد، باید نزدیک به هزار دلار هزینه کند . مخزن مربوط به این پروژه منبع باز اکنون روی گیتهاب به نشانی letsencrypt قرار دارد .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
16:56 - 21/05/1394
برچسب:
SSL/TLS - امنیت - Let’s Encrypt - گواهی دیجیتال

□□□□□ منبع: https://www.shabakeh-mag.com/security/1148