扩展验证(EV) SSL / TLS简介

直接在浏览器中显示HTTPS和经过验证的企业品牌标识，向访问者表明您的网站是安全的，并且实际上是由您的公司运营的

WHITE PAPER

目录

简介

SSL/TLS[1], https背后的加密协议，对于网站来说不再是一件好事。网站访问者期待看到网站地址栏上的一个挂锁，主流浏览器已经宣布计划将所有HTTP网站标记为不安全。所有迹象都表明SSL是任何运营网站的必备工具。

密码并不一定意味着安全

虽然SSL使用的增加通常是一件好事——更多的加密等于更高的安全性，对吗?-网络钓鱼和其他恶意网站已经开始利用这种"挂锁=安全"的心态，通过安装低保证SSL证书来显示合法和安全。

实际上，这些低级证书只能确保所有者实际操作了这个域名(因此才有了域名验证[DV] SSL证书)，这使得这些类型的证书相当容易获得——恶意者只需要注册一个域名并展示管理控制。例如，运营钓鱼网站"paypall.com"的人只需要证明他们拥有该域名。没有对网站背后的实体进行验证，因此证书中没有包含任何身份信息供网站访问者查看。

大多数颁发SSL证书的公共证书颁发机构(CAs)都有适当的检查来捕获这种类型的不良行为，并防止钓鱼者为此目的获取SSL，但是免费SSL服务的兴起，往往没有资源进行这些类型的检查，使钓鱼者很容易溜走。

所有这些都是在说，网站安全不仅仅是加密。越来越重要的是你的品牌身份——证明你的网站是合法的而不是钓鱼网站。

在这篇白皮书中，我们讨论了将您的企业身份放在网站前端和中心位置的重要性，以及如何使用扩展验证(EV) SSL实现这一点。

SSL的类型

SSL有三个保证级别。虽然这三个级别都对服务器和客户端之间的通信进行加密，但它们在证书中包含多少身份信息以及如何在浏览器中显示方面有所不同。

域名验证(DV) –域名的管理控制是唯一需要验证的东西。证书中没有验证或包含网站背后的公司信息。

组织验证 (OV) –组织的身份会被审查并包含在证书中，但不会显示额外的浏览器UI。

扩展验证(EV) –对组织进行严格的身份验证，浏览器会在URL中显示组织名称。

[1]虽然SSL协议已经被弃用，应该使用TLS协议，但大多数人都熟悉SSL这个术语，所以我们在这里只是为了简单起见使用它。使用我们免费的SSL配置检查器来查看你是否使用了正确的协议。在我们相关的博客中了解更多关于SSL和TLS之间的区别。

身份的重要性

即使网站使用SSL加密，单凭这一点并不意味着它是安全的。如上所述，它可能是一个使用廉价、低可信度证书来看起来安全和可信的钓鱼网站。

然而，当你将加密和身份结合起来时，欺骗网站就变得更加困难了。除了上面提到的DV之外，还有两种证书类型将身份与域绑定，即扩展验证(EV)证书和组织验证(OV)证书。为取得EV和OV证书，签发证书的核证机关会检查申请人使用某一特定域名的权利，并对机构进行审查，以证明域名持有人的身份。

典型的EV SSL审核过程

1. The Certificate Authority reviews the application for EV SSL.
2. The Certificate Authority confirms the organization's legal name, registration number, registered address, physical business address and any assumed business names.
3. The Certificate Authority verifies the applicant's right to use the domain name.
4. The Certificate Authority substantiates that the applying organization has approved the issuance of an EV SSL Certificate
5. Once everything checks out, the Certificate Authority issues the EV SSL Certificate.

EV SSL证书

除了启用HTTPS和加密数据传输，EV证书还允许网站背后的组织向网站访问者展示其经过验证的身份。EV证书为网站所有者通过EV指南(由CA/浏览器论坛批准的一套审查原则和政策)中定义的全面、全球标准化的身份验证过程提供了更有力的保证。

EV证书身份验证过程要求申请人证明域名的专有权，确认其合法、运营和物理存在，并证明实体已授权颁发证书。

EV SSL浏览器显示

OV SSL 证书

虽然OV证书也需要一些身份证明(虽然不如EV证书那么多)，但它们不像EV证书那样受欢迎，因为身份信息不会直接显示在地址栏中，而且它们会得到与DV证书相同的浏览器处理(例如标准挂锁和HTTPS)。为了查看身份信息，网站访问者需要查看证书的详细信息，这个过程因浏览器而异。

结论:谁应该使用EV SSL?

EV SSL证书将您经过验证的品牌身份放在网站的中心位置，应该在所有需要身份保证、可见信任和强加密的应用程序中使用。

经常遭受钓鱼攻击的知名网站，如大品牌、银行或金融机构，应该对所有面向公众的网站使用EV SSL证书，但任何收集和交易数据、登录或在线支付的网站也可以从这种更高级别的SSL中受益。数字商务依赖于信任，通过让网站加密和网站背后的人都很容易看到，EV证书帮助访问者决定是否信任它。