

续写《SSL 的三大误区》

笔者在 2005 年 1 月 31 日的《计算机世界》报发表了文章《SSL 的三大误区》，这是十几年前的文章了，现在读来仍然感觉不错，虽然文字中有点推销 GeoTrust 证书的嫌疑，因为当时刚刚开始代理销售 GeoTrust SSL 证书。这篇文章可能是我国权威报刊上第一篇关于 SSL 证书的文章，将近十七年的光阴飞梭而过，今天笔者在 CEO 博客重写这个话题，希望能给读者带来一丝新意。

十七年前只有少数网银网站部署了 SSL 证书，而现在几乎所有网银网站都部署了 SSL 证书，所有主流的电商网站都实现了全站 https 加密，部分政府网站也在登录页面部署了 SSL 证书。也就是说，进步还是有的，只是作为我国 SSL 证书的力推者和引领者之一的笔者仍然感觉步伐还可以再快点。

今天是笔者在创立沃通 CA 后再次创业的新公司官网上线之日，笔者有感而发，提笔续写新的《SSL 的三大误区》，希望对广大读者能有所启发。

误区一：以为 SSL 证书仅用于网站，其实更多地方都需要 SSL 证书。

网站需要 SSL 证书，这毋庸置疑，通过各大主流浏览器的努力，没有部署 SSL 证书的网站，浏览器地址栏都会显示“不安全”，因为用户在网站上输入的机密信息如果不通过 https 加密传输，则在传输过程中是明文，就很容易被非法窃取和被非法利用。这非常值得一网通办网站高度重视，因为用户在一网通办系统上输入的信息都是机密信息！

但是，光在网站部署 SSL 证书是不够的，由于现在移动 App 几乎已成主流的获取信息的方式，浏览器反而退居第二位了。而目前大量的移动 App 同服务器通信时并没有采用 https 方式实现加密通信，这个问题又不会像浏览器一样有明显的“不安全”提示，使得这个安全问题虽然非常严重，但由于没有有效监督机制，使得移动 App 开发者有意或无意忽略了必须为 App 与之通信的服务器部署 SSL 证书的问题，导致通过 App 泄密事件频发。

还有，邮件服务器不仅 Web 页面需要部署 SSL 证书，同时 SMTP 和 IMAP/POP3 服务器也必须部署 SSL 证书，保障邮箱密码安全和邮件内容传输安全。更加紧迫的是各种物联网设备(包括车联网、工业互联网)，目前都是采用 http 明文采集数据和明文同云端通信，非常容易遭遇恶意攻击，这就是为何最近的几次大规模的 DDOS 攻击都是来自物联网设备的根本原因。

只要有从客户端到云端传输数据的所有应用都需要在服务器端部署 SSL 证书实现 https 加密传输，这是唯一一个能保证数据传输安全的可靠技术和必用技术，而不仅仅是浏览器一种

客户端。

误区二：以为只要安装了 SSL 证书就万事大吉，其实正确部署证书可能比已安装证书更重要。

网站安装 SSL 证书是必须的，但是正确部署更重要。打个比方吧，没有部署 SSL 证书等于只对外打开了一道门(80 端口)，而部署 SSL 证书必须再打开一道门(443 端口)，如果不能正确部署 SSL 证书，等于又增加一道风险。而通常的出现的证书部署问题有：没有关闭不安全的 SSL 2.0/3.0 和 TLS 1.0/1.1 协议、没有停用不安全的加密套件、不支持安全重协商等等。最重要的是，既然部署了 SSL 证书，则应该关闭不加密的大门(80 端口)，只使用加密通道(443 端口)，并在部署了 SSL 证书后使用第三方 SSL 部署安全检测网站：<https://www.ssllabs.com/ssltest/> 检测部署是否还有问题，必须确保检测结果评分为 A 以上。

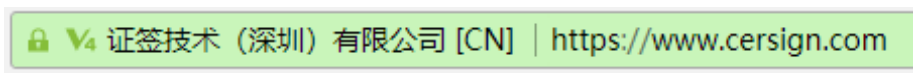
同时，不能仅在网站登录身份认证系统部署 SSL 证书，必须实现全站 https 加密，因为用户登录后的页面含有许多用户机密信息，同保护用户登录密码一样重要，并且全站 https 加密能有效防止 SSL 中间人攻击。

而对于移动 App 的 https 支持，不能仅仅是启用 https 加密，App 还应判断与之通信的服务器的域名是否同 SSL 证书绑定的域名一致、证书是否被吊销、是否是 App 信任的 SSL 证书等重要信息，而安卓 App 默认的模式是不做这些判断的，需要 App 开发者自己编程增加这些安全判断，这也是目前笔者发现的比较常见的 App 安全问题，值得 App 开发者高度重视，特别是网银 App！笔者将单独写一篇博文指导用户如何解决这个安全问题。

误区三：网站身份认证同传输加密一样重要。

这是一个曾多次在国际标准组织--CA/浏览器论坛上争议过的话题，浏览器厂商并没有认识到网站身份的重要性，硬是把部署了 EV SSL 证书的网站显示为绿色地址栏的功能给阉割了，使得部署了只验证域名所有权的 DV SSL 证书网站同部署了严格验证了网站身份的 EV SSL 证书网站一样地址栏只显示安全锁标识，这些浏览器厂商认为只要加密了就是安全的，并没有认识到网站身份认证的重要性。

笔者在主持研发密信浏览器时不仅坚守了显示 EV SSL 证书为绿色地址栏，而且创新的把部署了 OV SSL 证书的网站也显示出网站所有者的身份信息，为部署了 OV SSL 证书的网站体现其身份已验证的价值。



网站身份可信，同加密一样重要，一个假冒银行网站也部署了 SSL 证书，浏览器也会显示安全锁标识，这比没有部署 SSL 证书的假冒网站更隐蔽，危害更大！所以，笔者一方面呼吁浏览器厂商能正确认识到网站身份的重要性，另一方面也希望广大用户能在确认网站身份时点击安全锁看看证书中的 O 字段是谁。笔者非常喜欢 IE 浏览器对 EV SSL 证书的绿色地址栏展示效果。



但是，浏览器现在不在地址栏显示 EV SSL 证书的单位信息已经导致了张冠李戴的 SSL 证书部署情况，许多政府网站部署的 SSL 证书 O 字段(网站拥有单位)显示的系统集成商的单位名称！这显然是违反了有关标准的，也不符合 SSL 证书的使用用途。



如果使用 IE 浏览器访问广东省人民政府网站，会显示此网站的主办单位为数字广东网络建设有限公司，显然这是错误的，该公司只是政府网站的系统建设单位，并不是此网站的拥有方。由此可见，浏览器正确显示 SSL 证书中单位名称信息是何等之重要。



总之，SSL 证书在所有信息系统的全面部署是必然的，特别是《密码法》、《数据安全法》和《个人信息保护法》的出台，使得 SSL 证书全方位广泛正确部署成为必须，希望本文能对读者的 SSL 证书部署能有所帮助。

王高华

2021 年 12 月 9 日于深圳



SSL 证书的三大误区

王高华

网站欺诈 (Phishing) 目前日益猖獗, 而很多安全厂商对此却束手无策, 在目前条件下, 这类攻击不是靠技术能解决的, 需要靠人们擦亮眼睛。此外, 网站作为受害方之一, 也可以采取一定的措施自我保护。SSL 认证曾经被认为是好方法, 但目前存在认识误区。那么, 还有什么好方法呢?

误区一：对 SSL 数字证书的功能的误解。

许多网站开发者认为只要部署了 SSL 数字证书就万事大吉了，错误地夸大了数字证书的功能。实际上部署了 SSL 数字证书，只能证明如下三点：

1. 从用户的浏览器到正在访问的 Web 服务器之间所传输的数据是通过加密传输的，是不可被篡改、窃取和破译的，保证了用户输入的机密信息(如银行卡信息)在网络传输过程中是安全的。
2. 浏览器右方有锁标志说明了此数字证书是由信任的机构颁发，并且与用户正在使用的浏览器兼容。
3. 说明用户正在访问的 Web 服务器已经申请了 SSL 数字证书，并且正在访问的网站的域名的所有者与 SSL 数字证书申请时填写的域名所有者是一致的。

误区二：以为在屏幕右下角有“显示锁标志”就可以放心地在线填写信用卡等机密信息了。

有锁标志只能说明机密数据在传输过程是安全的，但是网上用户首先应该搞清楚的是您正在与谁交易，正在付钱给谁。一个假冒在线购物的网站也可以申请一个 SSL 数字证书来麻痹用户，用户应该检查正在访问的网站是否就是要访问的购物网站，域名是否正确。点击锁标志，检查此证书是颁发给哪个网站的？此证书的网址是否就是您要访问的网址？再点击“详细信息”的“主题”项，WoSign 的数字证书一般在“O”或“OU”字段会列出此证书的网站的所有者，即会清楚地告诉您此网站是否是您计划与之交易的公司的网站。而一个假冒的网站即使也有 SSL 数字证书，如果检查证书的详细信息就会发现问题。如招商银行信用卡网站的安全链接网址为：<https://creditcard.cmbchina.com>，访问后会发现浏览器下面有锁标志，点击锁标志后会显示此证书是颁发给 creditcard.cmbchina.com，而再点击“详细信息”的“主题”项后会显示：CN = creditcard.cmbchina.com (Web 服务器公用名称), OU = head office (申请机构的部门信息), O = China Merchants Bank (申请机构信息), L = Shenzhen (机构所在城市), S = Guangdong (机构所在州/省), C = CN (机构国家)。

但是，用户一定要明白，SSL 数字证书仅仅是为了保证数据传输的安全，它并不等于身份验证。要搞清楚的是用户正在访问的网站是否就是用户希望与之发生交易的公司的网站，这是最重要的。所以，要保证网上安全交易，还需要对网站的身份进行验证，验证此网站是否就是交易方的正宗网站。假如有一个假冒招商银行信用卡网站的安全链接网址为：<https://creditcard.cmb-china.com>，该假冒者在注册域名时也是填写域名注册者为 China Merchants Bank，申请 SSL 数字证书(SSL 证书)时也都是填写与域名 [cmbchina.com](https://creditcard.cmbchina.com) 一样的信

息，该假冒者当然也可以申请到 SSL 数字证书，只要申请证书时的信息与注册域名的信息一样。所以，此假冒网站也会显示锁标志，按以上方法验证证书，都可以是同样的正确信息。但是此网站是假冒网站，而用户只能以网站的网址做判断了。

误区三：选择 SSL 数字证书颁发机构的误区

目前国内各种数字证书颁发机构有近百家，网站应该根据自己的业务需要正确选择数字证书颁发机构。对于面向国际市场和希望有国际合作的网站(希望国外用户也能正确浏览安全页面的网站)，推荐申请支持所有浏览器的 WoSign 服务器数字证书，此类证书无需要求客户端浏览器下载和安装根证书，使用非常方便。

总之，目前国内电子商务和网上购物网站越来越多，而且盗版的银行网站也越来越猖狂，通过互联网的欺骗和盗用行为日益增加，作者认为，对于要求用户输入机密信息的网站，一定要部署 SSL 数字证书(SSL 证书)来确保用户输入的机密信息的安全，保护输入的机密信息不会被泄露，让人们放心地进行网上消费。同时，我们建议所有网站都应该申请认证，让现实世界的真实企业与网络虚拟世界的企业网站实现真正的一一对应关系，让假冒网站没有可乘之机。而对于网上消费者，一定要提高安全防范意识，掌握辨别真伪网站的方法，不给网络犯罪分子有可乘之机。

请关注公司公众号，实时推送公司 CEO 精彩博文。

