HTTPS 加密就是最大的安全收益

笔者在中秋国庆假期看了经济学者薛兆丰在上个月的“腾讯全球数字生态大会”的演讲《关于数字安全的经济规律和行动策略》的 PPT，讲得非常好，本文就在其观点基础上讲一讲 HTTPS 加密的投入和收益的经济学思考。

先讲第一个观点-“**安全就是收益**”。对于网站和 Web 业务系统，最重要的安全就是 HTTPS 加密，因为如果没有实现 HTTPS 加密，则从浏览器到 Web 服务器之间的所有信息交互都是明文传输，用户的账户登录用户名和口令以及各种重要数据就非常容易在传输过程中被非法窃取，包括管理员的账户，这等于整个系统就沦陷了，所有用户数据都可以被人拿走！而造成这个局面的不是黑客，而是你自己！你可能会花大价钱购买了一堆防火墙、杀毒、IDS、IPS、WAF 等等网络安全设备，防住了你的系统无法被攻击，但是重要的客户数据和业务数据出了你的城堡是明文，攻击者根本不用攻击你的城堡，只需等在数据走过的路边就可毫不费力地获得所有数据，而你毫无知觉，因为数据如期到达了用户手中，如期为用户提供了服务。这个数据打劫非常容易，让你毫不察觉，可能还会为系统没有被攻和正常为用户提供服务而沾沾自喜。大家普遍忘了保护信息系统的目的是什么，是保护业务数据的全生命周期安全，而不仅仅是保护服务器系统的安全，现在是“人不走数据走”的时代，所以不能只是死守数据在城堡内的安全，还要重点保护数据在路上和在云上的安全。

为了保护数据在路上的安全，唯一可靠技术是 HTTPS 加密，把明文的 HTTP 加一个“S”(安全)就是 HTTPS 加密传输，你的数据出了城堡到用户手中的通道是加密的，是无法被非法侦听获取和无法被非法篡改的。而要实现这个 HTTPS 加密，你必须向 CA 机构购买 SSL 证书部署

在 Web 服务器上实现数据传输 HTTPS 加密，这是必须的投入，这个投入的收益就是保证了你的数据在路上的安全，保证了你的数据不会在流通传输环节出问题。这个 HTTPS 加密安全的投入就是收益，保护了你的数据的在途安全。

再讲第二个观点-“**成本越低，责任越大**”。实现 HTTPS 加密有多种方式，都是有实施成本的，符合“实施成本越低，你的责任越大”的经济规律。目前有三个选项，笔者一一分析这三个选项的成本和责任。

(1) 第一个选项：选购和部署 SSL 证书

这也是传统的选项，向 CA 选购和申请一张 SSL 证书，部署到 Web 服务器上，每年申请和部署一次，并且必须记得提前续期和重新部署，因为一旦证书过期就不能正常实现 HTTPS 加密了。这个选项，对于管理一个网站还行，但是如果要管理几十个、几百个，甚至成千上万个网站，把运维工程师累死也管不过来，因为申请和部署一张证书最快也要半天时间，如果申请的是 OV 证书，则可能费时费力好几天。这就是目前各省市大量的政务网站没有部署 SSL 证书的根本原因。

而为了 HTTPS 加密密钥的安全，谷歌正在推动缩短 SSL 证书有效期为 90 天，意味着每年需要折腾 5 次为服务器申请和安装 SSL 证书，这将给运维人员增加 5 倍的工作量，意味着这个手动申请和部署 SSL 证书的选项将来会是不可选的选项。

(2) 第二个选项：使用免费 SSL 证书

这个选项费用最低，市场上已有多家公司提供完全免费的 90 天有效期的 SSL 证书。有两种方式，一是同第一个选项一样，每 90 天内人工申请和部署一次证书，一年要操作 5 次。证书费用省了，但是人力成本上升了 5 倍！请单位管理者自己评估在人力成本居高的今天这个选项是否合适。另一个更加流行的方式就是 ACME 自动化证书管理，就是在 Web 服务器安装一个 ACME 客户端软件，如目前非常流行的 Let’s Encrypt 自动化方案，由 ACME 客户端软件自动化每 90 天内自动申请和部署 SSL 证书，这是“一劳”(安装一个软件)就可以做到“永逸”(长期免费实现 HTTPS 加密)的方案，这似乎是最佳解决方案，似乎是违反了“成本越低，责任越大”经济规律的超好解决方案。

但是，这个解决方案存在两个巨大的安全责任问题，请一定要牢记“世界上**永远**不会有免费的午餐”这句谚语，证书是免费了，但是你的 Web 服务器必须安装一个外部的软件，时刻守护在你的服务器上，你真的能放心？这个安全隐患和责任你评估过吗？这是第一个安全责任问题。第二个问题是有些 Web 服务器是根本不能动的，别说安装一个外来软件了，就是部署一张证书也都很困难，毕竟部署 SSL 证书也需要动服务器和重启一下服务器。

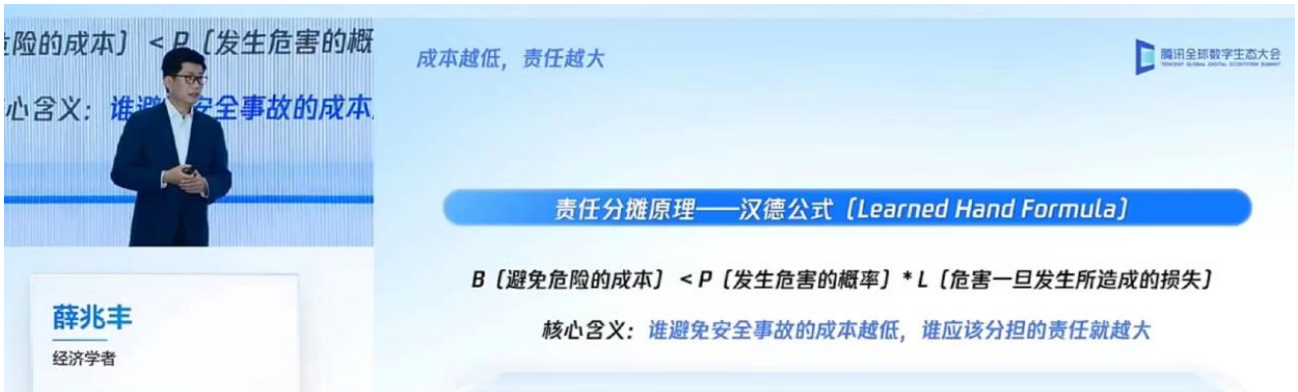
这个需要动正在运行重要的业务系统的 Web 服务器的解决方案是有很大责任风险的，这个风险当然在第一个选项也是存在的。第二个看似完美的成本最低(免费)的解决方案其实仍然是符合“成本越低，责任越大”的规律的，证书免费，但是安全责任由你全部承担。

(3) 第三个选项：部署国密 HTTPS 加密自动化网关

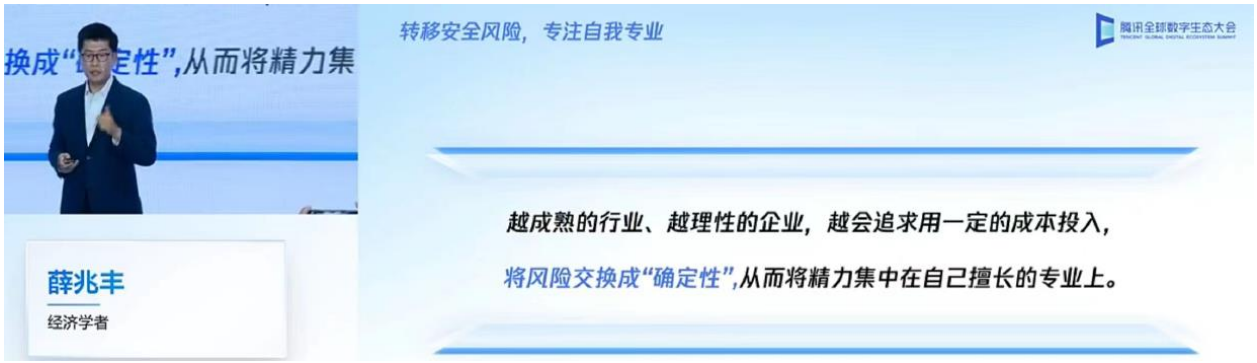
这个选项无需像第一个选项那样每年向 CA 申请和部署 SSL 证书，也无需像第二个选项那样必须在服务器上安装一个软件，原 Web 服务器不用动，零改造，由网关来自动化申请和部署双算法 SSL 证书实现 HTTPS 加密，自适应加密算法，支持国密算法的浏览器如零信浏览器采用国密算法实现 HTTPS 加密，而不支持国密算法的浏览器采用 RSA 算法实现 HTTPS 加密。

这个选项的实施成本要比前两个选项高，但是按照“成本越高，责任越小”的经济规律，运维工程师再也不用每年费时费力去申请和部署 SSL 证书，也不用动现有服务器，不会影响现有业务系统正常运行，不需要承担由于安装 SSL 证书导致服务器无法正常运行的风险和责任，也不需要承担由于有大量的服务器需要部署 SSL 证书而不断增加的运维工程师人力成本，因为网关实现了自动化，一个工程师就可以管理成百上千个网站的 HTTPS 加密实施，工程师只需在网关上设置需要启用 HTTPS 的网站域名即可，一台网关就可以连续 5 年为最多 255 个网站提供不间断的 HTTPS 加密服务，大大降低了责任和运维成本。

那么，这三个选项哪个是最佳选项？第三个选项还有一个巨大的责任被规避，那就是密码算法的风险。第一个选项和第二个选项实现的都是 RSA 算法 HTTPS 加密，而俄乌冲突发生后俄罗斯政府和银行网站的 RSA 证书被非法吊销和断供导致这些重要网站无法访问，这是潜在的巨大风险和安全责任。也就是说，第一和第二选项的成本较第三个选项低，但是分担的责任就更大，所以为了进一步降低分担的责任，则应该明智地选择第三个选项。



接着讲完剩下两个观点。第三个观点就不讲了，笔者不想有为会议举办方做广告的嫌疑，直接跳过第三个观点讲第四个观点-“**转移安全风险，专注自我专业**”。“越理性的企业，越会追求用一定的成本投入，将风险交换成确定性”，这句讲得非常好。安全成本的投入就是把可能的安全风险降到最低，并且把风险的不确定性转换为确定性，把有限的人力资源投入到专注自己的业务发展上。



要实现 HTTPS 加密，请单位管理层不要再让运维工程师去人工申请和部署 SSL 证书了，费时费力，这些工作完全可以交给机器去做！这也是一个转移安全风险的明智选择，让宝贵的人力资源专注于自己的业务。这不仅仅可以节省大量的人力成本，而且能大大降到人工操作失误的风险。爱立信的电信设备曾经由于忘了续期已到期的证书而导致移动运营商的业务系统瘫痪，这不仅导致 3200 万手机用户二十多个小时无法使用手机，而且爱立信也因此被移动运营商索赔数百万美元。大量的实践和经验证明：机器比人工可靠，网关自动化证书管理比人工申请证书可靠，绝对不会忘记证书续期。

鉴于目前不确定地缘政治风险，我国要实现 HTTPS 加密，最大的安全保障和最少的责任就是要实现国密 HTTPS 加密，这不仅是国密合规的需要，而且也是降低风险和转移风险的需要，可以规避由于地缘政治事件导致的证书吊销和断供的技术风险和责任。所以，最明智的首选只有第三个选项—部署国密 HTTPS 加密自动化网关，为最多 255 个网站提供 5 年不间断的、无忧的、零改造原服务器的国密 HTTPS 加密自动化服务。

有诗为证：

成本低则责任大，加大投入责任小。

转移风险很重要，安全投入价值大。

数据安全责任重，部署网关最明智。

费力事情机器做，宝贵人力做大事。

王高华

2023 年 10 月 7 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。