零信任安全的四大误区

零信任在网络安全界很火，但是零信任理念不是网络安全大佬提出来的，而是美国市场研究公司 Forrester 的首席分析师约翰·金德维格(John Kindervag)于 2010 年提出来。它既不是一项技术，也不是一款产品，而是一种新的安全理念，其基本原则是“从不信任，始终验证”。这就给各个加入这个领域的厂商提供了无限想象空间，大家都可以根据自己的专业和产品开发出自己的零信任安全产品和解决方案，但整体来看，零信任安全仍处于生态分散化野蛮生长中，不同主体对零信任的基本概念、技术路径等认识差别较大。笔者从事网络信任服务 17 年，从如何解决信任问题出发来谈谈目前存在的零信任安全的三大误区。

误区一：忽视了网站身份的始终验证

说起零信任，大家都知道需要始终验证用户的身份，笔者认为目前市场上的所有零信任方案都忽略了一个最重要的元素的始终验证，那就是网站身份的始终验证，这是一个巨大的技术方向失误。网站是互联网的第一大流量，如果忽视了网站身份的始终验证，那对用户的始终验证就失去了任何意义，因为如果通过始终验证的用户身份是真实可信的，但是这个真实可信的用户访问了一个假冒欺诈网站，那就是非常不安全的访问，让一个真实的身份落入了欺诈网站的手中。

如何实现对网站身份的始终验证，当然必须先验证网站身份，并在每次访问时始终验证身份。实现网站身份认证功能的是 SSL 证书，而执行始终验证任务的是浏览器。所以，现在所有浏览器都对没有通过身份认证的网站显示为“不安全”，只有通过身份认证才能拿到 SSL 证书并部署到网站上才能实现 https 加密传输，浏览器才会不显示为“不安全”，而是显示安全锁标识。因为 SSL 证书具有证明网站身份和加密传输的双重功能。

零信任的首要原则应该是不信任没有通过第三方身份认证的网站，其次才是不信任要访问网站的用户身份并始终验证用户身份。这个顺序不能错，也不能单一强调只验证用户的身份。只有网站通过了第三方(如 CA)的认证、部署了 SSL 证书实现了 https 加密，再每次验证用户身份才是一个完整的信任链，才能真正保证“正确的人”访问了“正确的网站”。

零信任的第一大误区是只关心始终验证用户的身份，而忽视了服务器端网站身份的始终验证。

误区二：忘了为何要实现零信任

零信任之所以在 10 年后才火，是因为目前的网络安全防护机制已经碰到天花板了！已经在“道高一尺魔高一丈”的死循环中出不来了，特别是由于疫情导致的居家办公，使得用户不得不思考如何解决传统的基于防火墙和内外网安全机制已经不能起作用了的安全难题，因为传统的安全机制就是无限信任一次认证和无限信任内网，但是现在没有内网了怎么办？零信任理念就这样得到了大家的认同。

由于很火，大家当然就会一窝蜂的来追这个所谓的“风口”，各种五花八门的解决方案也都纷纷登台亮相！但是，有许多解决方案也许真的是忘了为何要实现零信任。一些看似非常复杂的让人眼花缭乱的零信任身份安全解决方案的确也实现了“永不信任，始终验证”，但是验证之后就把用户数据明文传输给用户了，这样的零信任身份认证方案有用吗？甚至有些基于用户名和口令的零信任认证系统都没有部署 SSL 证书来保障用户名和口令的安全，这样的方案能用？

任何安全方案的最终目的是为了保护数据，是让“正确的人”访问“正确的服务器”，获取“正确的数据”。零信任安全的最终目的也是如此，是为了保护用户数据不会被非法获取和非法使用，而不是仅仅为了身份认证！这是零信任的第一大误区，忘了为何要实现零信任。

误区三：忽视了现有的互联网信任体系

现有的互联网信任体系就是 WebTrust 体系，就是为了解决互联网信任问题而诞生的。简单的讲就是：由 CA 机构签发 SSL 证书来证明网站的可信身份和用于网站传输 https 加密，操作系统厂商或浏览器厂商有一个根证书信任计划，信任某些 CA 签发的 SSL 证书。由 CA 和浏览器厂商联合组成的“CA/浏览器论坛”这个国际组织负责制定 CA 业务技术标准，由加拿大 CPA 负责根据技术标准制定出审计标准，这个标准就是 WebTrust for CA，并认定一些会计师事务所具有从事 WebTrust 审计业务资格。CA 机构每年都需要接受审计机构的 WebTrust 审计，通过审计后就可以拿到 WebTrust 审计报告，并提交浏览器厂商预置和继续信任其根证书，CA 就能继续签发全球信任的 SSL 证书和其他证书。

可以看出，这是一个闭环的信任认证传递机制，此机制保证了 WebTrust 信任体系的正常运转，从而保障了全球互联网的安全快速发展。而 CA 机构在欧洲则被称之为信任服务提供商(TSP)，因为 CA 机构负责采用密码技术(PKI)来为用户签发各种用于解决信任问题的数字身份证书。现在出现了零信任安全理念，不能忽视了现有的运转良好的全球互联网信任体系，必须是在此基础上的补充和拓展。

误区四：忘了或者不知道什么技术才是真正用于解决信任问题的技术

上面我给大家讲了目前互联网是如何解决信任问题的，这可以延伸到万物互联世界。解决信任问题的唯一可靠技术只有密码技术，密码技术的一个最重要和最主要的应用就是 PKI(公钥基础设施)。PKI 就是为了解决信任问题而生，为了解决数据安全而生。PKI 技术彻底解决了 (1) 数据的机密性(**P**rivacy); (2) 数据生产和使用方的身份真实性(**A**uthentication); (3) 数据的完整性(**I**ntegrity); (4) 数据生成行为和使用行为的不可否认性(**N**on-repudiation)等四大令人头痛(**PAIN**)的数据安全问题。这些头痛问题的解决就是解决了信任问题和数据安全问题，PKI 是采用解决信任问题的唯一可靠技术，零信任理念只有同 PKI 紧密结合才能真正彻底解决信任问题和解决信任问题的标的-数据安全问题。

零信技术的零信任安全解决方案就是零信任加密码技术的安全实践。我们的解决方案不是要取代现有的各种网络安全解决方案和丢弃现有的各种网络安全防护设备和系统，而是在现有防护设备和系统上规划和实施零信任安全解决方案，改造现有系统逐步支持零信任安全。

总之，零信任的始终验证不是目的，保护数据资产和确保数据安全才是目的。零信任体系必须是用户端的用户和服务器端的网站都始终验证，并且缺一不可，两端都应该采用数字证书来实现始终验证。基于密码技术的零信任安全不仅适合于互联网安全，而且适合于物联网安全、车联网安全、工业互联网安全。零信任是一个旅程，网络安全实际上一直在往零信任方向不断

发展中!

王高华

2021 年 12 月 24 日于深圳
2022 年 2 月 17 日更新

请关注公司公众号，实时推送公司 CEO 精彩博文。