用户需要什么样的零信任？

零信任安全理念中有一个重要的技术措施是“最小权限授权”，“持续验证，动态授权”。看到某大厂介绍其零信任安全解决方案中的快递威胁感知检出率从基于特征库的 60%提升到 96%，这实际上是一个很可笑的指标，机密文档如果仍然有 4%的概率泄漏出去，100 个闯关者有 4 个能过去拿到机密文件，这还是安全的系统吗？这样的零信任有用吗？

这就是我今天要讲的话题：用户到底需要什么样的零信任？用户到底应该如何从小处做起迈进零信任？如何正确评估一个零信任安全解决方案？笔者在这里提出一些评估思路供参考。

1. **如果一个零信任身份认证解决方案仍然是基于用户名和口令的方案，特别是如果用户输入用户名和口令的页面居然没有 https，则绝对是一个不能用的方案，无论这个厂商的名气有多大都不能用。**

不仅仅是登录认证系统需要 https 加密，所有业务系统、所有数据采集系统无论是在内网还是外网，都必须部署 SSL 证书实现 https 加密 Web 流量，确保机密信息在传输过程中不会被非法窃取和非法篡改，明文 http 流量的 https 加密是零信任安全的第一要求。

这里可能还有一个隐藏的安全隐患，那就是有些认证系统不再是基于 Web 页面的直接输入用户名和口令，而是基于手机 App 的认证，支持指纹和刷脸认证，看似不用记住繁琐的口令，非常方便，但是如果这个 App 同认证服务器通信没有采用 SSL 证书实现 https 加密传输，则仍然是不安全的。即使是采用了 https 加密通信，但是这个 App 没有检查 https 的各种正确使用，仍然可能是有安全问题的，读者可以参考我的另一篇博文《手机 App https 加密宝典》。

2. **如果一个零信任方案的威胁检出率不是 100%，则仍然是值得怀疑是否可用的，除非业务系统能容忍 4%的漏检率。那么，如何才能做到 100%检出率？一定会有安全专家说：96%已经非常高了，很了不起了，不可能做到 100%的！的确，96%真的是不错了，但是对于零容忍的系统还是有问题的，那么如何实现 100%？则需要我们从“福尔摩斯式”的传统安全防护思路跳出来找答案！**

试想一下乘飞机旅行，航空公司能接受 100 名乘客中有 4 名是恐怖分子？“福尔摩斯式”的传统安全防护思路的问题就在于不知道用户是谁，只能靠猜(判断其特征和行为)，这是不靠谱的，所谓的“安全大脑”也不一定能猜得准！那怎么办？只有乘飞机旅行的实名认证方式才能确保飞行安全。

基于密码技术的零信任解决方案就是给每个个体一个可信数字身份，用户必须出具其可信身份才能通过验证而获得相应的数据访问权限，并以加密方式获得所需的数据，同时通过时间戳签名来记录数据访问时间。这才是 100%可靠的解决方案，我们称之为“**内生信任**”机制，用户首先就是可信任的身份，出具的证件就是可信证件，通过数字签名算法就能验证身份的真实可信，那该用户就能顺利通过安检登机，这比“福尔摩斯式”的持续甄别验证更快更准。这就是密码技术的魅力！

3. **如果一个零信任解决方案只是一个身份认证系统，则是远远不够的。身份认证不是目的，目的是保护后面的各种数据！所以，零信任安全解决方案一定是一个系统工程，必须把网络中的五大关键元素：身份、设备、网络、应用和数据统一纳入零信任安全架构，给出完整的解决方案。**

零信技术的零信任安全解决方案是基于密码技术的解决方案，能完美地把 PKI 数字证书应用到五大关键元素的安全防护中，使得网络中的每个个体(人和设备)都有可信数字身份，不信任没有可信数字身份的个体，个体要于其他元素通信必须出具其可信身份证书才能通过认证获得所需的数据。而网络中第一大流量 http 流量必须全 https 加密，第二大流量电子邮件流量也必须全程端到端 S/MIME 加密，而最关键的 DNS 流量也必须采用 SSL 证书实现 DoH 或 DoT 加密，不信任网络中没有加密的流量。

还有各种应用软件都必须有数字签名，不信任没有数字签名的软件代码，不信任没有可信数字签名的 OTA 空中升级软件，切实有效保障应用软件的安全。而数据的安全则是通过证书加密来实现，用有权获得此数据电文的用户的公钥加密此数据，只有此用户才能解密阅读，这

是唯一可行的数据安全解决方案。

当然，数据加密离不开密钥管理系统，不仅要实现用户可以随时随地使用任何设备都可以获取密钥来解密其数据，而且也必须实现用户可以随时随地使用任何设备获得数据电文接收方的公钥来实现全自动加密机密数据。当然，也离不开时间戳服务，确保数据的生成时间可信和数据的使用时间可信、不可否认和不可篡改。

总之，零信任绝对不是一个身份认证产品就能搞定的事情，也不是一天部署一套系统就能搞定的事情，是一个旅程，不是目的地。必须从一个很简单的 https 加密开始，逐步改造现有系统和业务流程，逐步实现个体身份可信、流量加密、应用可信和数据加密等各种基于零信任原则的全元素安全可信。

王高华

2021 年 12 月 23 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。