现实世界，最安全的系统都是零信任系统

《列宁与卫兵的故事》不知读者们是否还有印象，这是一个现实世界的只认“证”不认“人”的故事，在各种最安全的系统中天天都在严格执行中。再比如坐飞机旅行，就是一个零信任的系统，每个人都必须实名购票，必须持有可信证件(身份证或护照)，通过实名认证才能过安检，并持通过实名认证后签发的登机牌登机。同时，登机通道和下机通道也必须是专用通道(廊桥和摆渡车)。这些都是零信任，个人身份的零信任和传输通道的零信任。

坐飞机旅行的过程对应到数字世界就是基于密码的零信任安全解决方案，每个用户必须有数字证书来证明其可信身份，这个数字证书必须是系统信任的 CA 机构签发，用户要访问某个网络资源，则需要出具其数字身份证书完成数字签名验证，只有通过了可信身份认证，才能访问所需的数据。而数据送达也必须采用 https 加密专用通道传输，同时还可以用用户的公钥加密，只有用户用私钥才能解密收到的数据。

现实世界的银行系统也是一个零信任的系统，银行职员必须持有特定的身份证明文件才能进入特定的工作区，使用特定的身份卡才能登录特定权限的系统。而网银用户必须有一个 USB Key 来证明其可信身份，登录网银系统必须用 USB Key 中的数字证书签名登录行为数据，银行系统端验证签名后才能登录网银系统，同时通信道道都必须采用 https 加密。用户在网银的转账指令也必须用用户的数字证书签名并加密发送到银行支付系统。

笔者就不多举例了，大家一定在现实世界体验和发现了许多这样的系统。可以说，零信任在网络世界的应用实际上是一个现实世界的复制应用，从这一点也可以看出零信任在网络世界的应用前景。

在现实世界，每个人都有不同的证件，不同的场合需要出具不同的证件。常用的身份证可以用于大多数应用场景，而护照则用于出国旅行。小区门禁卡或办公楼工卡则用于进入小区和办公楼，大型会议的出入证则仅一次性用于此次参加会议。在数字世界也一样，用户也可以有多种不同认证级别的数字身份，用户可以根据不同的应用场景使用不同的身份证书用于身份认证。有仅验证邮箱或者手机号码的身份证书，有验证个人身份的身份证书，验证单位身份的身份证书，以及同时验证单位身份和单位员工身份的身份证书，用户可以有多个身份，而业务系统可以根据访问数据的性质不同而要求用户提供什么认证级别的身份证书。

而网络世界的第一流量就是 Web 网站，其身份则是通过 SSL 证书来标识的，没有部署 SSL 证书的网站，所有浏览器都会显示为“不安全”，这不仅仅是因为明文传输，而且还是因为网站身份没有通过认证。网站身份有 4 种不同级别的身份认证，仅验证域名所有权的 DV SSL 证书为最低一级的网站身份认证，因为并没有验证网站主的真实身份，所以 DV SSL 证书中的使用者信息只显示网站域名。如果网站主是个人，则验证网站主个人身份后签发的 SSL 证书称之为“IV SSL 证书”，这个证书名称不常见是因为个人网站一般只申请便宜的 DV SSL 证书。如果网站主是单位，则验证网站主单位身份后签发的 SSL 证书称之为“OV SSL 证书”，证书中的使用信息会显示单位名称。还有一个单位用户的扩展认证，就是更加严格地按照国际标准验证网站主的单位身份后签发的 SSL 证书称之为“EV SSL 证书”，浏览器地址栏展示为绿色地址栏，让网站访问者非常醒目地了解网站主的可信身份。有了这 4 个不同级别的网站身份认证，可以让网站访问者可以非常容易识别网站的真实身份，从而正确做出网站访问的安全决策。

现实世界最安全的系统都是零信任系统，零信任理念应用到网络世界是现实世界的人类智慧在网络世界的绝妙应用，这是经过了实际考验的，是解决网络安全问题的最高效的理念，再加上密码技术的零信任安全实现，一定会成为解决网络安全的利器，能有效保障互联网和万物互联的安全健康发展。

王高华

2022 年 2 月 14 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。