密码技术高效保障物联网设备系统免遭远程升级攻击

2026 年 1 月 7 日

目前，针对各种物联网设备系统的恶意攻击的不断出现，如加油站设备、供水设备、供电设备等等，由此造成的后果也是非常可怕的。当然，各大安全厂商也纷纷推出了其物联网安全防护系统和解决方案，是否有效，笔者没有做调查，但是笔者相信这些重要的系统不可能没有购买和部署安全防护系统，但是仍然不断出现各种攻击事件和勒索事件。这不得不让人怀疑传统的安全防护是否真的有效。本文给出了一个新的解决思路，采用基于密码技术的零信任安全解决方案，能简单高效保障物联网设备系统免遭远程攻击，包括各种勒索软件攻击。这个解决思路同样适用于日益火爆的智能网联汽车的安全保障。

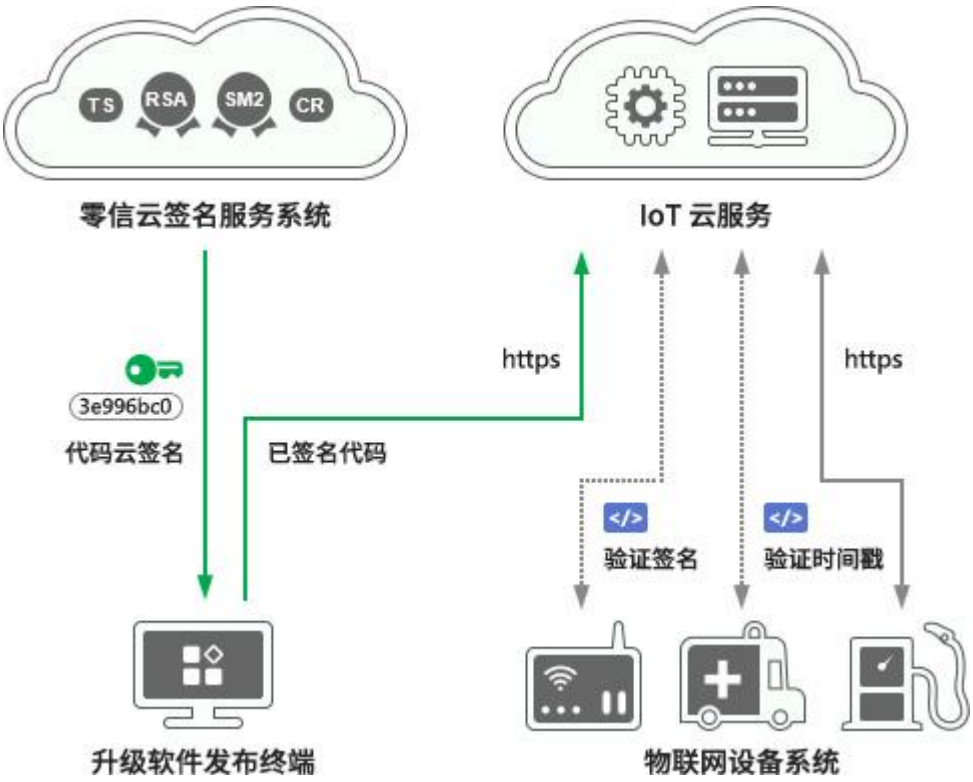
笔者分析了多个攻击案例，大多数都是通过空中 OTA 远程升级设备软件导致的恶意攻击。由于各种物联网设备系统都已经联网，特别是 5G 的普及应用，设备联网已经成为必须的默认配置。这不仅为了实现设备与云端系统的数据交换和远程控制，而且为了非常方便远程维护和升级设备系统软件，以适用用户对设备功能的不断完善需求。但是，远程升级普遍存在两个极大的安全隐患非常容易让攻击者得手，其一就是使用 HTTP 明文传输协议同云端系统通信，使得各种通信数据非常容易被非法窃取而导致攻击者能非常容易找到攻击机会；其二就是 OTA 远程软件升级时设备系统并没有验证软件的合法来源。

为了有效防范远程升级攻击，依据零信任原则三：不信任无数字签名的软件代码，只信任有可信数字签名的软件代码。所有 OTA 空中升级软件必须有可信数字签名，设备系统必须验证升级软件有可信的数字签名才能安装，“永不信任”没有数字签名的升级包，“始终验证”收到的升级软件包是否有数字签名和是否有可信的数字签名！就这么简单，无需复杂的昂贵的安全防护系统，就能有效防止恶意软件的远程升级攻击，从而保障物联网设备系统的安全！

实现验证代码的数字签名，这只是有效措施之一。还需要依据零信任原则一：不信任 HTTP 明文连接，只信任 HTTPS 加密连接。设备系统同云端系统连接如果采用 HTTP 连接，则攻击者会窃取各种通信数据，一旦知道通信流量是给设备下发升级软件的，则可以通过篡改流量中的数据包，把升级软件替换为用于攻击的恶意软件，设备系统一旦不验证软件是否有可信数字签名，则按照隐式信任的原则就会自动安装这个恶意攻击软件，从而导致设备系统瘫痪或者遭遇软件勒索。

也就是说，为了防范设备系统的远程升级攻击，必须实现 HTTPS 加密连接服务端，而不

是 HTTP 明文连接服务端，从而杜绝设备与云端系统通信的数据泄密和篡改攻击，切断其下发恶意代码的通道。同时，设备端还需要始终验证每次下发的升级包的数字签名，是否有系统信任的数字签名和时间戳签名，时间戳签名也用于验证升级软件的可信时间来辅助判断升级行为是否可疑。



远端物联网设备系统必须验证 HTTPS 加密连接中的 SSL 证书是否可信，是否与连接的域名匹配和 SSL 证书是否被吊销等重要信息，确保 HTTPS 能正确连接到正确的云端服务器。并且，验证升级包的数字签名也需要验证证书签发者是否是系统信任的证书签发根证书，用于数字签名的代码签名证书是否已经被吊销，数字签名者是否是设备系统指定的软件开发商，时间戳签名是否可信，签名时间是否需要定期升级计划的升级时间，只有完成这些必要的验证才能保证通过 HTTPS 加密通道接收到的升级包的代码签名的有效，才能依据验证结果来决定是否安装升级软件包。

对于重要的物联网系统，除了以上的设备系统验证服务器身份和升级代码身份外，服务端也应该验证设备系统的可信身份，否则可能会遭遇假冒的设备系统连接，从而实现对服务端的攻击，找到攻击物联网设备的通信机制。依据零信任原则六：不信任无可信数字身份的设备，只信任有可信数字身份的设备，每个设备都必须有可信身份证书，用于同服务端连接时证明其可信身份，服务端才会同其实现安全连接和加密通信，可以用设备的身份证书公钥加密设备控制数据，设备收到控制指令后用其私钥解密并验证指令的数字签名后才执行控制命令，只有这

样才能保障远程设备的通信和运行安全。这个密码应用安全机制同样适用于车联网的通信安全。

总之，要保障物联网设备系统不会遭遇恶意攻击，必须依据零信任原则，加强密码应用，不仅要加密设备同服务端的连接，而且要验证下发的软件代码是否有可信数字签名，同时服务端也要验证设备的可信身份，实现设备可信、代码可信和通信链路加密可信，只有这样才能真正保护物联网设备系统不会遭遇恶意攻击，切实保障物联网设备的安全可靠运行。

王高华

2026 年 1 月 7 日于深圳
