佐罗软件 PluginOK 中间件安全解决方案

一、 概述

众所周知，IE 浏览器的 ActiveX 控件及 Chrome 浏览器的 NPAPI 插件作为浏览器功能扩展的技术方案为丰富网页交互功能做出了巨大贡献，但其一直因为安全性和稳定性原因备受非议，即使程序采用了数字签名和安全等级控制也无法完全解除用户的担忧。同时这些插件往往是直接在浏览器进程中运行的，而一些开发商发行的插件质量参差不齐，可能导致浏览器运行缓慢、留下安全漏洞甚至运行时直接导致浏览器崩溃。浏览器开发公司谷歌等索性在 2015 年直接取消了 Chrome 新版本对 NPAPI 插件的支持，随后 Firefox 浏览器也取消了 NPAPI 插件的支持，从而导致商业领域原来大量采用了 ActiveX 控件和 NPAPI 插件的信息化系统在新版 Chrome、Firefox 等浏览器中再也无法兼容运行，更急迫的是，微软已经官方宣布 2022 年 6 月正式淘汰 IE，这些系统再无浏览器可用的窘迫局面即将出现。针对这个迫切的需求，成都佐罗软件有限公司依靠长期的技术积累和持续不断的艰苦攻关，成功研发出 PluginOK 中间件来作为替代 ActiveX 和 NPAPI 的技术解决方案，对 Windows XP 及以上版本操作系统、各品牌及主流浏览器兼容性很好。为了保障中间件及之上运行的小程序安全性、稳定性、易部署及易维护，特别设计实现了一整套自主可控的安全解决方案。

PluginOK 中间件承诺本身无任何木马或病毒代码，无任何非授权的网络请求，发布的程序可以自行在线提交到各杀毒软件公司进行验证，每个正式版我们也会提交到 360 做白名单，也可以在线提交到 http://virscan.org/ 验证。

二、 方案

PluginOK 中间件的安全解决方案主要体现在以下几个方面：

1、程序发布时的文件数字签名及哈希校验机制(借鉴 ActiveX 及 NPAPI 的机制)；

2、额外引入小程序调用方的用户授权机制，针对每个调用方分配一个唯一的用户 ID，同时针对每个小程序的连接会话生成一个有时间期限的安全校验的 Token，PluginOK 及小程序开发商都可以对 Token 中内容进行校验，校验通过才提供正常的服务；

3、中间件主服务的前端请求重启、配置、卸载、移机(网络版)及小程序的安装、升级请求中都需要做 Token 的安全校验，Token 可由打包工具生成，只有校验合法才可执行正确的请求；

4、一旦发现某个小程序功能危害电脑安全或功能描述不符而被用户投诉确认的，PluginOK 中间件在升级版中可对此小程序进行封杀；

5、一旦小程序开发商发现自己的小程序被非授权调用，可联系我们协助屏蔽其在升级版中非授权的使用;

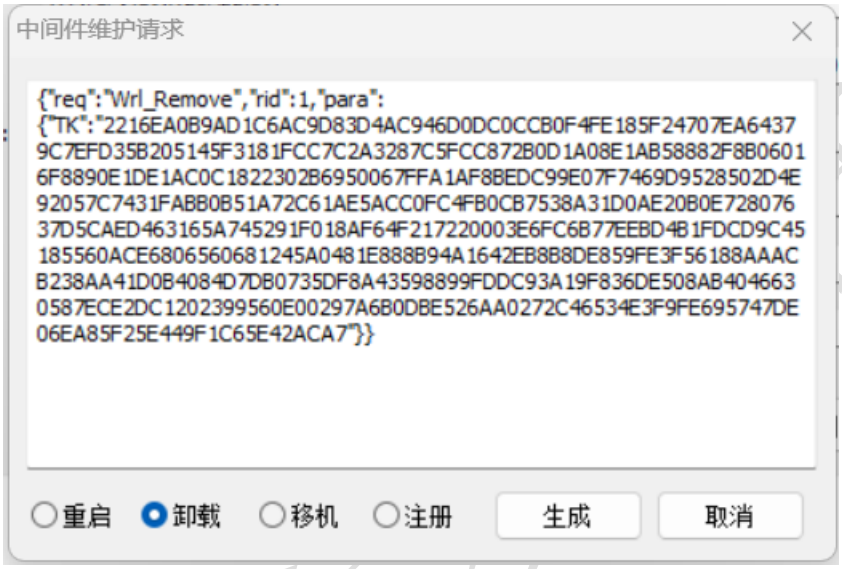
6、一旦发现某个用户的调用权限被滥用，我们会取消此用户后续的升级版本使用权限；

7、如果所有功能都在浏览器中实现，其实也往往存在安全问题，很容易被

模拟网络协议进行攻击等，如果通过 PluginOK 中间件调用一些本地模块小程序来实现增强安全认证，网页端再提供服务其实更安全，有些敏感数据不通过浏览器反而更安全，毕竟所有浏览器的内核源码都来自于海外，并不能完全保证安全。

三、 中间件安全接口

以下为中间件服务重启(Type:0)、卸载(Type:1)、移机(网络版 Type:2)请求生成的校验 Token，打包工具生成时默认 24 小时内有效。



其中 tk 是加密后进行安全校验的传递参数 Token，加密前的内容为 JSON 范例数据包：{"Type":1,"ValidTime":1601917153}，必须包含本次操作类型 Type 和有效期 ValidTime(为 UNIX 时间戳，从 1970 年 1 月 1 号零点零分零秒开始，下同)，为安全起见，有效期不宜设置太长，比如不超过 24 小时，只要保证终端和服务器电脑时差范围之内即可。网络版授权移机，也就是先卸载指定电脑软件并移除授权，Type 为 2。

tk加密方式是RSA公钥非对称2048位加密的，公钥由小程序开发商(主要是本公司)提供，小程序开发商和授权用户需要严格保护公钥的安全，tk生成时需在后台服务中生成后传递到前端调用，尽量避免公钥外泄。RSA加密后生成的字节流，需要转换为十六进制字符串。tk在B/S系统中不能写死，需要在服务器后台动态生成，避免tk生成的源码中时间过期而不可用。

四、 小程序安全校验接口

安全校验主要体现在两个接口上，连接请求小程序服务和小程序卸载。

1、请求小程序服务
请求 DLL 或 EXE 弹窗小程序服务的协议举例：
ws://wrl.zorrosoft.com:83?flag=1&lang=CHS&pid=C38672FA-B5C8-4D9D-89B5-2D71F0760661&sid=321&&cid=zorrosoft&tk=
请求内嵌小程序服务举例：
ws://wrl.zorrosoft.com:83?flag=1&lang=CHS&sid=321&&cid=zorrosoft&tk=

内嵌小程序不需要 pid 参数

其中tk是加密后进行安全校验的传递参数Token，加密前的内容为JSON范例数据包：{"CID":"zorrosoft","SID":"321","ValidTime":1601917153}，必须包含本次连接的会话SID参数、有效期ValidTime(最长30天)和请求的用户CID (本公司提供，zorrosoft是作为范例，正式版中小程序调用方可向PluginOK开发商申请的唯一用户ID)，小程序开发商可以添加更多字段信息到JSON数据包中，PluginOK会把还原后的数据包同时传给小程序中进行校验。

2、小程序卸载

小程序卸载的协议举例：

{"req":"Plugin_Remove","rid":1,"para":{"PID":"A22E18F1-95F8-4FDB-99D2-188E5FB12B23","Type":1,"TK":""}}

其中 PID 为小程序唯一 ID，Type 为小程序类型，TK 为加密后进行安全卸载的传递参数，生成规则和请求连接小程序服务类型，只是加密前的内容差异，JSON 数据包内容如下：

{"PID":" A22E18F1-95F8-4FDB-99D2-188E5FB12B23","ValidTime":1601917153}

注意：以上安全校验机制在线上体验的开发版中不是强制验证的，为了确保安全和避免未经授权的小程序调用，B/S 系统正式发布前时请联系我们以便获得正式授权便于测试这些安全机制，一般来说，使用显示最终客户名称的单机水印授权方式，长期授权是强制启动调用安全机制的，短期授权为了便于开发测试，可以不强制启用安全机制，HTTPS 网站使用域名绑定 SSL 证书使用时，也可以不开启这个安全机制。