Linux下基于签名技术的软件保护

时间：2020-03-06        来 源：中国软件杯

**第九届中国软件杯大赛--高端基础软件（A 本科及以上）**

|  |  |
| --- | --- |
| **赛题名称: Linux下基于签名技术的软件保护**  **组类：A 本科及以上** | |
| 赛题简介：介绍整个赛题的实现目标、实用价值、涉及技术和整体要求 | 实现一个Linux下的二进制签名和验证程序，用于在国产Linux操作系统进行应用的标识和管理，提升应用程序的可追溯性和安全性鉴别能力。    要求：  对于Linux下给定的ELF可执行程序、自行开发签名工具对程序的代码段（Load Segment）首先进行散列，然后对散列值进行签名，签名数据应作为单独的节（Section）附加到原ELF可执行程序的尾部。同时，应开发验证软件并加入操作系统，在运行任何ELF可执行程序前对ELF文件进行验证，若ELF可执行程序没有被签名或者签名验证失败则应停止运行本程序，若签名验证成功则可以正常运行。  签名后的ELF可执行程序可正常运行在带有签名验证的Linux操作系统上，以及不带有签名验证机制的Linux操作系统上；  签名后的ELF可执行程序中的签名数据节应可通过readelf与objdump等程序解析得到正确的值；  运行ELF可执行程序的方式应保持不变，不得通过其他程序运行ELF可执行程序的方式验证签名；  签名验证所需要的公钥、证书以及验证程序可以预先设置在操作系统中；  本题不考察选手对加密算法的实现，因此选手可以选择开源的加密软件库进行加密，但是对应强度应不低于RSA2048；    实现程序主要涉及对ELF可执行格式的理解、Linux操作系统下程序运行的机制的理解，以及对加密算法的运用。 |
| 赛题业务场景：描述赛题相关的真实企业业务背景。从真实场景中，适当简化或者提炼出适合比赛的赛题场景 | 统一操作系统UOS（社区版deepin）作为一款具有全球影响力的Linux操作系统，在中国及全球有着广泛的用户，在世界操作系统排名名列前十，是中国排名最高的操作系统产品。    UOS自带的软件商店也是国产Linux操作系统中最为完善的应用商店，并且形成了完善的应用上架流程，流程要求开发者需对自己开发的应用进行签名，以保证二进制的安全性（非篡改），因此需要一款可以对二进制进行签名和验证的程序。 |
| 基本功能要求 | 参赛作品应在统一操作系统UOS20或社区版deepin上编译生成，并可稳定运行；  对于任意二进制程序、应可以使用签名工具对程序进行签名，在操作系统中预制公钥、证书与验证程序以验证ELF可执行程序的完整性，若验证失败，则ELF可执行程序无法运行；  签名后的ELF可执行程序可正常运行在带有签名验证的Linux操作系统上，以及不带有签名验证机制的Linux操作系统上。 |
| 非功能性要求 | 参赛作品不允许出现侵犯他人知识产权的内容，参赛过程不允许出现违反国家法律规范的相关行为；  签名后的ELF可执行程序可正常运行在带有签名验证的Linux操作系统上，以及不带有签名验证机制的Linux操作系统上；  加密算法限定仅能使用国密算法或者RSA算法；  程序不能依赖其他二进制程序的功能或者文件系统的功能。 |
| 实现条件：开发环境、实验平台、开发语言、数据库、编译器、涉及硬件等实现条件 | １、开发环境为Linux开发环境；  ２、开发语言限定为C语言； |
| 测试数据或平台：提供给参赛者的测试环境和测试数据。 | 无 |
| 开发所需设备及设备指标需求说明 | 统一操作系统UOS(社区版deepin) |
| 文档及其他要求 | 需有设计文档 |
| 评审要点 | 完成设计文档，原理无问题。  完成基于公私玥的签名程序，能对任意ELF程序进行签名，并能通过readelf等程序读取添加的节，且不影响程序的正常运行。  完成基于公私玥的验证程序，能透明地对任意ELF程序在运行前进行签名验证，签名验证通过的可以正常运行，未通过的不允许运行，对比未实施签名验证前的程序启动时间延迟不超过10%。  完成基于证书的签名程序，能对任意ELF程序进行签名，并能通过readelf等程序读取添加的节，且不影响程序运行。  完成基于证书的验证程序，能透明地对任意ELF程序在运行前进行签名验证，签名验证通过的可以正常运行，未通过的不允许运行，对比未实施签名验证前的程序启动时间延迟不超过10%。  不修改内核源码，开发外置内核模块挂钩Linux内核的进程启动流程作为验证程序。 |
| 初赛作品提交要求 | 程序设计文档；  源代码和编译步骤；  部署方法与测试方法；  测试演示视频。 |

**出题企业：统信软件技术有限公司**

答疑老师：王老师   邮箱 [wangzhixuan@uniontech.com](mailto:zhixuan.wang@archermind.com)    电话 13057698853