基于进程模拟和中间语言的密码算法识别

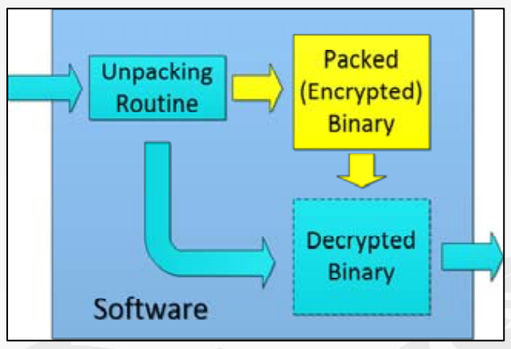
上海交通大学 密码与计算机安全实验室
Lab of Cryptology and Computer Security
http://loccs.sjtu.edu.cn

联系人： 谷大武 教授 Email: dwgu@sjtu.edu.cn

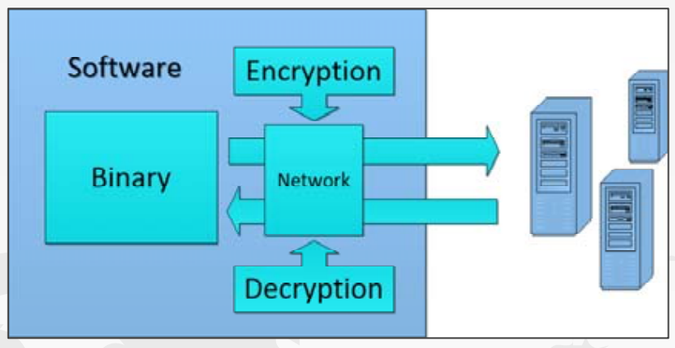
摘要

应用软件通常加密关键代码和数据来避免逆向分析，因此检测软件中的加密函数并提取密钥是程序安全分析中的关键步骤。在大量二进制数据中进行自动化密码算法检测是一个复杂的过程，其主要挑战在于需同时保持高效性和精确性。我们提出了一种增强的检测方案，该方案首先使用新的进程级模拟技术来进行程序的高效模拟执行，进而使用基于中间语言的程序划分和翻译方法来简化分析流程，最后使用基于模板的算法匹配和动态数据验证来检测算法并提取参数。我们将该方法应用于使用常用密码库或自行编写的示例程序，有关结果表明这些密码库和示例程序中的加密算法能够被高效检测。该分析系统也为分析人员提供了方便易用的接口，用于检测除密码算法外的通用算法。

简介



商业软件通常加壳保护，入口点脱壳函数包含解密算法



程序与远程服务器通信时通常将数据加密以防止信息泄露

获取程序中包含的密码算法是程序分析的关键步骤

研究目标：
(1) 二进制程序的模拟执行环境
(2) 自动化识别程序中的密码算法

LochsEmu进程模拟器

LochsEmu程序分析引擎

相关成果

- Caballero et al. (2009)：特征指令
- Gröbert et al. (2011)：数据IO关系；算法特征
- Zhang et al. (2011)：运行时数据
- Zhao et al. (2011)：数据IO关系

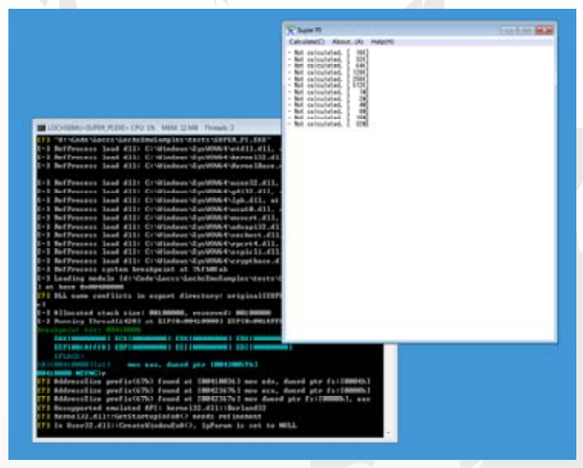
待解决问题

- 性能开销过大，不适合大规模分析
- 难以应对软件保护
- 难于扩展分析环境
- 无法防范可能的恶意行为

LochsEmu进程模拟器

技术优势

- 较传统模拟器有10^1~10^2性能提升
- 采用DBT/JIT技术达到接近真机性能
- 防止恶意行为干扰
- 对分析进程无修改、无挂载调试器
- 模拟与分析同步进行，减少或消除磁盘IO



运行实例

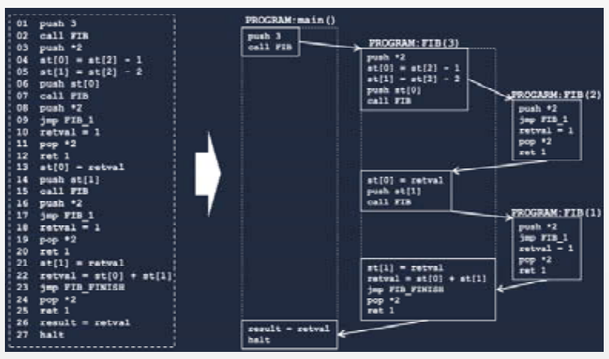
其他典型应用

- 进程调试
- 恶意行为检测和分析
- 程序性能分析
- 内存漏洞检测
- 进程沙盒

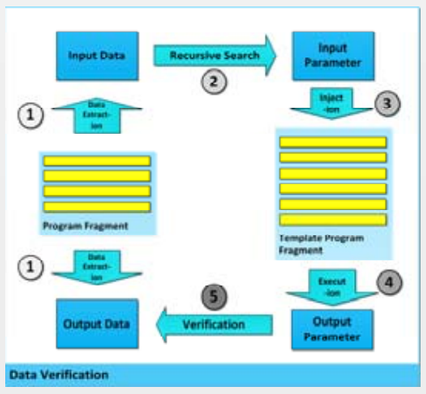
程序分析和算法识别引擎

```
swap proc px:DWORD, py:DWORD
   LOCAL temp:DWORD

   ; temp = *px                  // let px = 0x4000
   mov   eax, px                 t0 = memory[0x4000]
   mov   eax, [eax]              t0 = memory[t0]
   mov   temp, eax               t1 = t0

   ; *px = *py                   // let py = 0x4004
   mov   eax, px                 t0 = memory[0x4000]
   mov   ebx, py                 t2 = memory[0x4004]
   mov   ebx, [ebx]              t2 = memory[t2]
   mov   [eax], ebx              memory[t0] = t2

   ; *py = temp
   mov   eax, py                 t0 = memory[0x4004]
   mov   ebx, temp               t2 = t1
   mov   [eax], ebx              memory[t0] = t2
   ret
swap endp
```

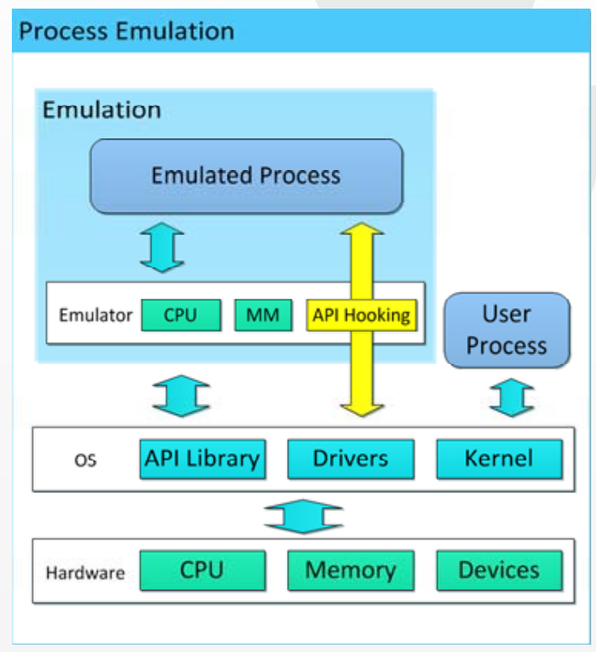
基于中间语言的高性能二进制翻译



程序划分和匹配算法



动态数据验证和数据提取



系统架构

准确性和性能评估

Binary	Algorithm	Template Detected	Description
aes_std.exe	AES 128-bit	aes_subkey_be	Original Rijndael implementation
aes_nettle.exe	AES 128-bit	aes_subkey_le	Nettle crypto library
aes_ssl.exe	AES 128-bit	aes_key	OpenSSL library
aes256_ssl.exe	AES 256-bit	aes_key_256	OpenSSL library
rc4_custom.exe	RC4	rc4_key	Custom implementation
md5_ssl.exe	MD5	md5_core	OpenSSL library
sha1_ssl.exe	SHA1	sha1_core	OpenSSL library
sha2_ssl.exe	SHA2	sha2_core	OpenSSL library

准确性测试，测试程序选取1）OpenSSL库；2）Nettle库；3）自定义实现