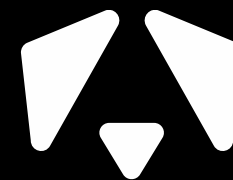


Cryptography **RE** vs Security Programmers



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Насколько полезен реверс-инжиниринг при исследовании защищенности программно-аппаратных решений?

Main questions and answers



Способы исследования защищенности ПАК:

- построение стенда, реализующего типовые сценарии ПАК
- исследование системы управления ПАК (в большинстве случаев WEB)
- исследование функциональных сервисов
- исследование взаимодействия компонентов ПАК при помощи RE

Для каких задач применяется реверс-инжиниринг при поиске уязвимостей:

- анализ причин аномального поведения служб при эксплуатации
- изучение принципов функционирования ПАК и его отдельных механизмов
- отладка и реализация инструментов эксплуатации (PoC)

Others research



CVE-2016-1287 NCC Group Approach

- POC – N/A for community
- **Descriptor** `struct malloc_tree_chunk @ 0x7ffffb8092530 {`
`prev_foot = 0x4141414141414141`
`head = 0x4140 (PINUSE)`
`events/blogs`
`fd = 0x7ffffbfa372a0`
`overflow-ove`
`bk = 0x7ffffb628b010`
`left = 0x7ffffbfa372a0`
`right = 0x38`
`parent = 0x96c2b00`
`bindx = 0x7ffffbfa372a0`
`struct mp_head`
`alloc_pc`
`free_pc`
`(gdb) |`
- **Protocol**

| Fragment | Address | Value | Comment |
|-----------------|------------|------------|---------|
| frag Z seq no 0 | 0x00000000 | 0x00000000 | |
| frag Z seq no 1 | 0x00000000 | 0x00000000 | |
| frag Z seq no 2 | 0x00000000 | 0x00000000 | |
| frag Z seq no 3 | 0x00000000 | 0x00000000 | |
| frag Z seq no 4 | 0x00000000 | 0x00000000 | |

Exec on x64 x32

NOFF ONE 2018

November 15 - 16

<https://www.youtube.com/watch?v=4QV0CTfeRzw>

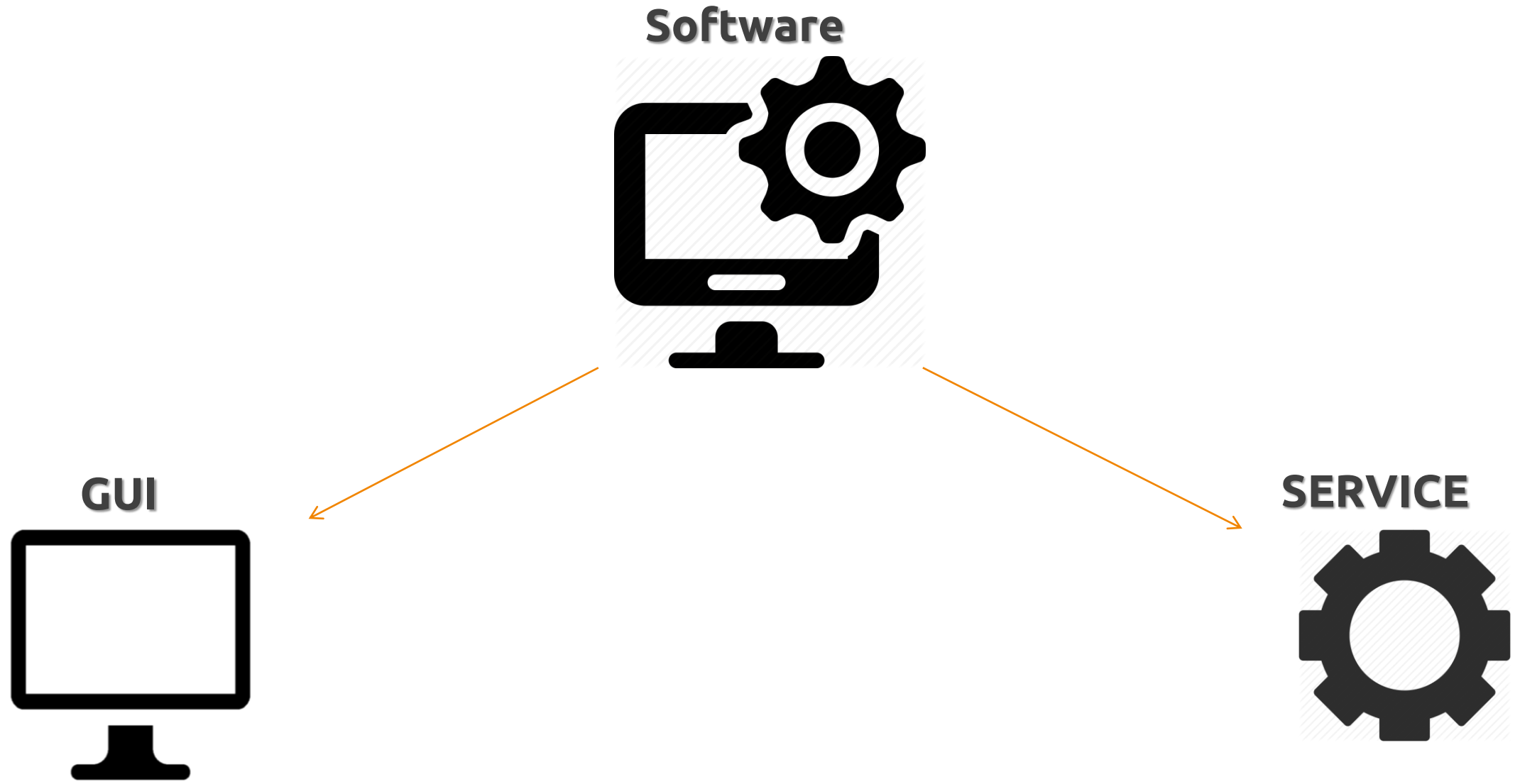
Package managers & Software installers



The image displays three overlapping software management interfaces:

- Windows Store (left):** Shows the 'Менеджер программ' (Program Manager) window with a sidebar for categories and a main area for the 'Store'. It features a search bar, navigation tabs (Home, Top charts, Categories, Collections), and a list of collections like 'Getting started', 'Better together', 'Red Stripe Deals', and 'Music lovers'. A notification at the bottom indicates '70841 пакетов' (70,841 packages).
- Chocolatey (middle):** A terminal window showing the command 'chocolatey' and its output: 'This PC', 'internal_server', 'chocolatey', and 'chocolatey.licensed'. It includes a search bar and filters for 'All Versions', 'Include Prerelease', and 'Match Word Exactly'. A 'Popularity' dropdown is also visible.
- Steam (right):** The Steam Store interface for a user named 'craiggrannell'. It shows a search for 'os=mac&specials=1' and a list of games with their release dates, discounts, and prices. The 'Narrow by OS' filter is set to 'Mac OS X'. Games listed include 'TRI: Of Friendship and Madness', 'The Marvellous Miss Take', 'Lost Lands: The Golden Curse', 'Splatter - Zombie Apocalypse', 'hocus', 'VOI', 'AppGameKit: Easy Game Development', and 'AppGameKit - Premium Bundle'.

“Under the hood”



User mode



"C:\Program Files\CUSTOM_PATH"

OK

System



- \Program Files\ *
- \Windows\system32\ *
- \Program Files (x86)\ *

<https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations>

User mode



RE

Command: Copy A to B

.

System



PIPE



- \Program Files\ *
- \Windows\system32\ *
- \Program Files (x86)\ *

<https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations>

RE Counter : 1

User mode



+

Evil "version.dll" in User folder

Command: Copy A to B

System



SERVICE



PIPE

RE

```
BOOL  
GetNamedPipeClientProcessId(  
HANDLE Pipe,  
PULONG ClientProcessId  
);
```



Decryption/Encryption method
error!



RE Counter : 2

User mode



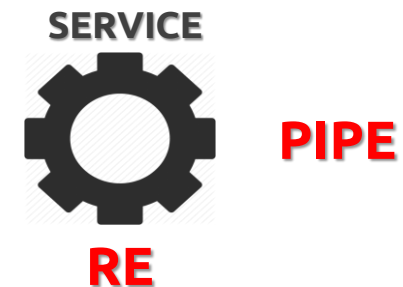
IV ? Key?

RE

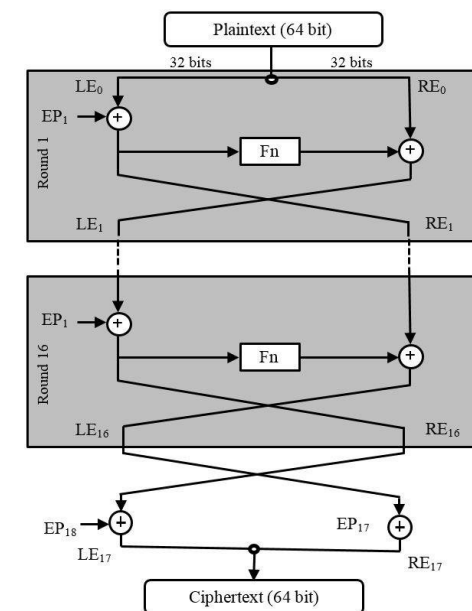
IV – is a hardcode value

KEY – in “public” folder with read permissions

System



Blowfish



RE Counter : 4

User mode



IV – is a hardcode value

KEY – in “public” folder with read permissions

+

Evil “**version.dll**” in User folder

Command: Copy A to **B**

System



PIPE

Error! Incorrect folder

RE

substr (**destination_path**,
“**C:\Program Files\Company Prod**”)

RE Counter : 5

User mode



- ..\..\..\..\..\
- %2e%2e%2f
- %c0%af

RE

Command list:

- Copy A to B
- Register
- Start Process

System



PIPE

substr (destination_path,
"C:\Program Files\Company
Prod\")

Error! Incorrect folder

User mode



IV – is a hardcode value

KEY – in “public” folder with read permissions

+

Evil “**version.dll**” in User folder

Command: Start_process **B**



System



PIPE

Error! Incorrect Process

RE



User mode



version.dll

If run from **system** Evil code 2
If run from **User** Evil code 1

IV – is a hardcode value

KEY – in “public” folder with read permissions

+

Evil “**version.dll**” in User folder

Command: Start_process **GUI**

System



PIPE

SUCCESS

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\WINDOWS\system32>
```

User mode



Reboot machine

System



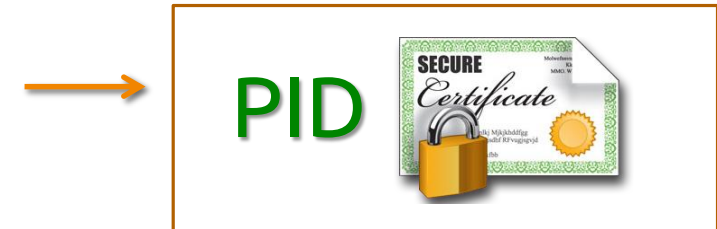
**No Service
No PIPE**



RE

Blowfish → **Some string** →

→ **Int** → **PID** →

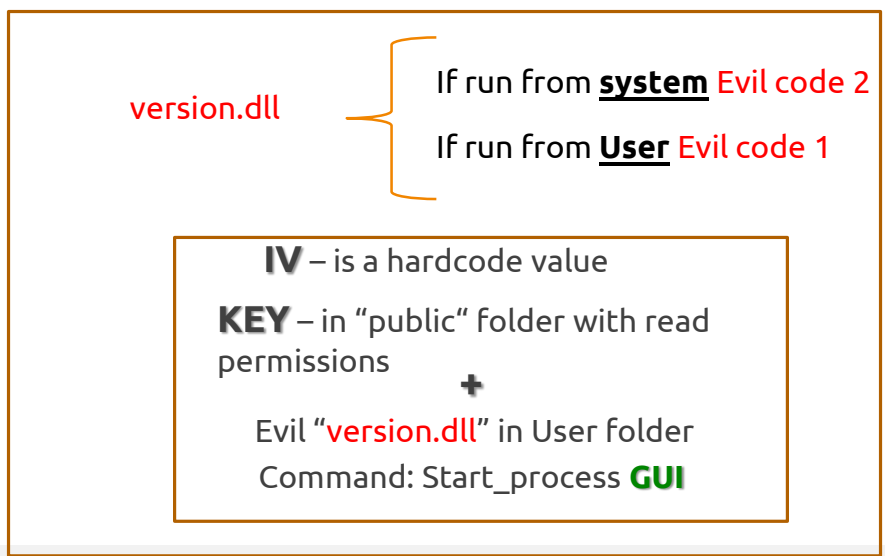
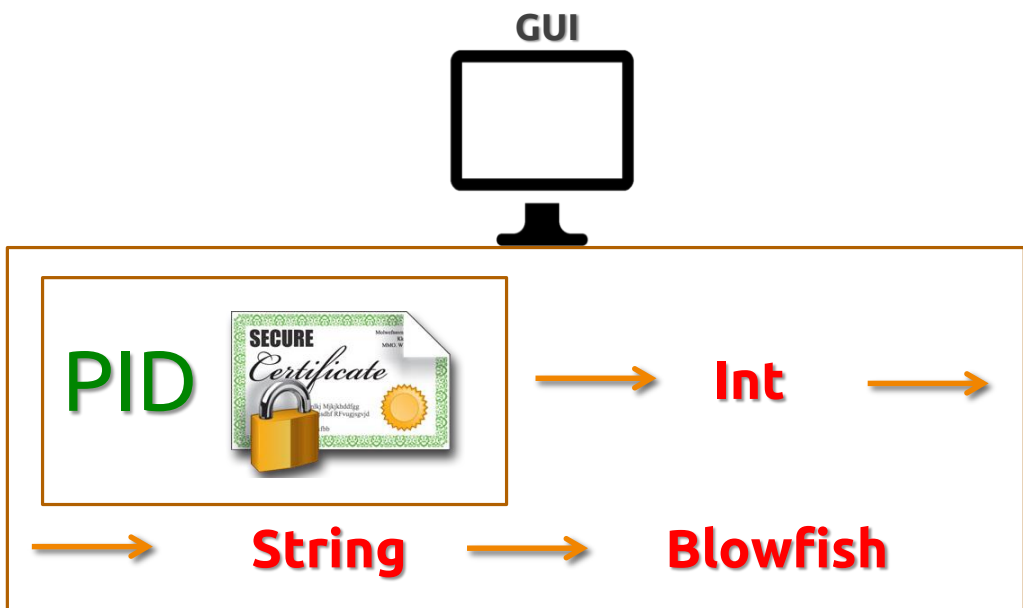


RE Counter : 8

User mode

Reboot machine

System



Service PIPE

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\WINDOWS\system32>
```

Final exploit and results



1. Start Service
2. Pipe for commands
3. Start_process cmd.exe

1. Bypass signature x3
2. Bypass Blowfish x3
3. Root privilege shell



Спасибо за
внимание!

«Ищите да обряцете»

Овчинников Сергей

Эксперт-исследователь

компании «Перспективный мониторинг»

Sergey.Ovchinnikov@amonitoring.ru

Telegram: [@malchikserega](https://www.instagram.com/malchikserega)

Twitter: [@malchikseregas](https://www.instagram.com/malchikseregas)