

Криминалистический анализ RAM: обнаружение, расшифрование и интерпретация зашифрованных криптографических объектов и данных

Чиликов А.А., к.ф.-м.н., доцент кафедры «Информационная безопасность»,
МГТУ им.Баумана, Passware Inc.

Хоруженко Г.И., аспирант кафедры «Криптология и дискретная математика»,
НИЯУ МИФИ , Passware Inc.

19 марта 2015 г.

Актуальность

Получение доступа к защищенным данным с помощью анализа RAM

Критичные данные в открытом виде

Критичные данные зашифрованы

- Full Disk Encryption
- Учетные записи пользователей ОС
- Пароли от веб-сайтов
- ...



ПО, использующее механизмы защиты данных в памяти

Программное средство	Механизм защиты	Зашифрованные данные
WinRAR 5.20 for Windows	CryptProtectMemory (OC Windows)	Пароль от архива
KeePass 1.28 (Classic)	CryptProtectMemory (OC Windows)	Ключ шифрования БД
KeePass 2.28 (Professional)*	CryptProtectMemory (OC Windows)	Мастер-пароль
1Password 5.1 for Mac**	Собственная реализация	Мастер-пароль

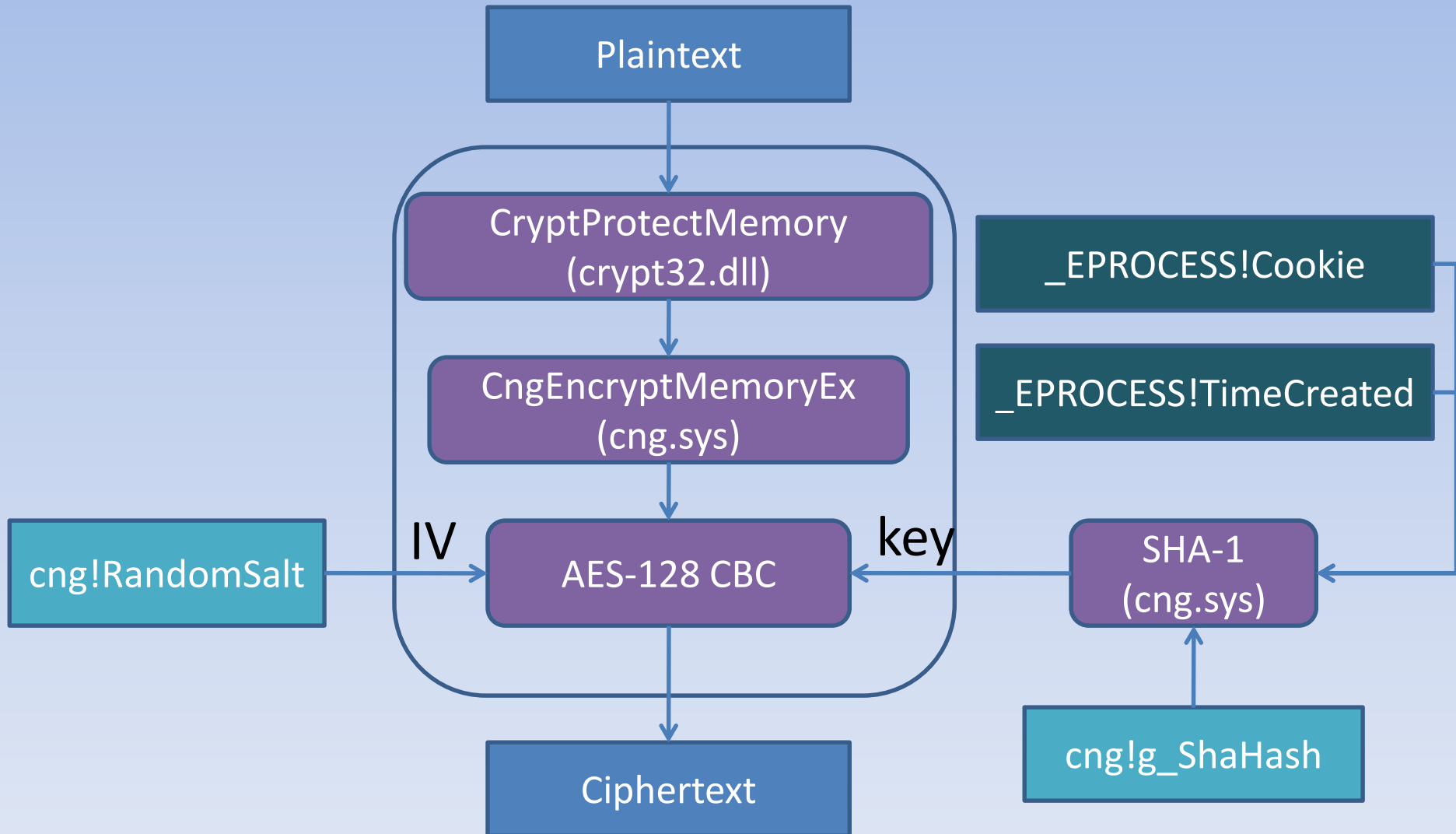
* KeePass Professional хранит ключ шифрования БД в открытом виде

** 1Password for Windows хранит ключ шифрования в открытом виде

Защита участка памяти на уровне прикладных программ в ОС Windows

- Рассматривается случай **Windows 8.1 x64**
- Пара функций **CryptProtectMemory/**
CryptUnprotectMemory (crypt32.dll),
управление передается
CngEncryptMemoryEx (cng.sys).
- Различные варианты защиты:
 - Отсутствие привязки (CROSS_PROCESS)
 - Привязка к пользователю (SAME_LOGON)
 - **Привязка к процессу (SAME_PROCESS)**

Схема работы функции CryptProtectMemory



Структуры `cng!g_ShaHash` и `cng!RandomSalt`

```
3: kd> db cng!g_ShaHash
```

```
fffff801`fb97dd60 19 03 40 fa 14 6b 91 e2-83 76 77 e3 a6 6e 36 3b
fffff801`fb97dd70 44 de d6 8f 29 2a c4 3c-00 00 00 00 00 00 00 00
fffff801`fb97dd80 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
fffff801`fb97dd90 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
fffff801`fb97dda0 01 23 45 67 89 ab cd ef-fe dc ba 98 76 54 32 10
fffff801`fb97ddb0 f0 e1 d2 c3 00 00 00 00-00 00 00 00 00 00 00 00
fffff801`fb97ddc0 18 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
fffff801`fb97ddd0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

■ buffer
■ SHA-1 registers
■ buffer size

Поиск в памяти структуры `cng!g_ShaHash` осуществляется по начальному заполнению регистров SHA-1 и длине буфера

`cng!RandomSalt` – массив размера 0x10 байт

Для каждой версии ОС Windows смещение `cng!RandomSalt` относительно `cng!g_ShaHash` разное, но для всех версий обе структуры расположены на одной странице образа памяти

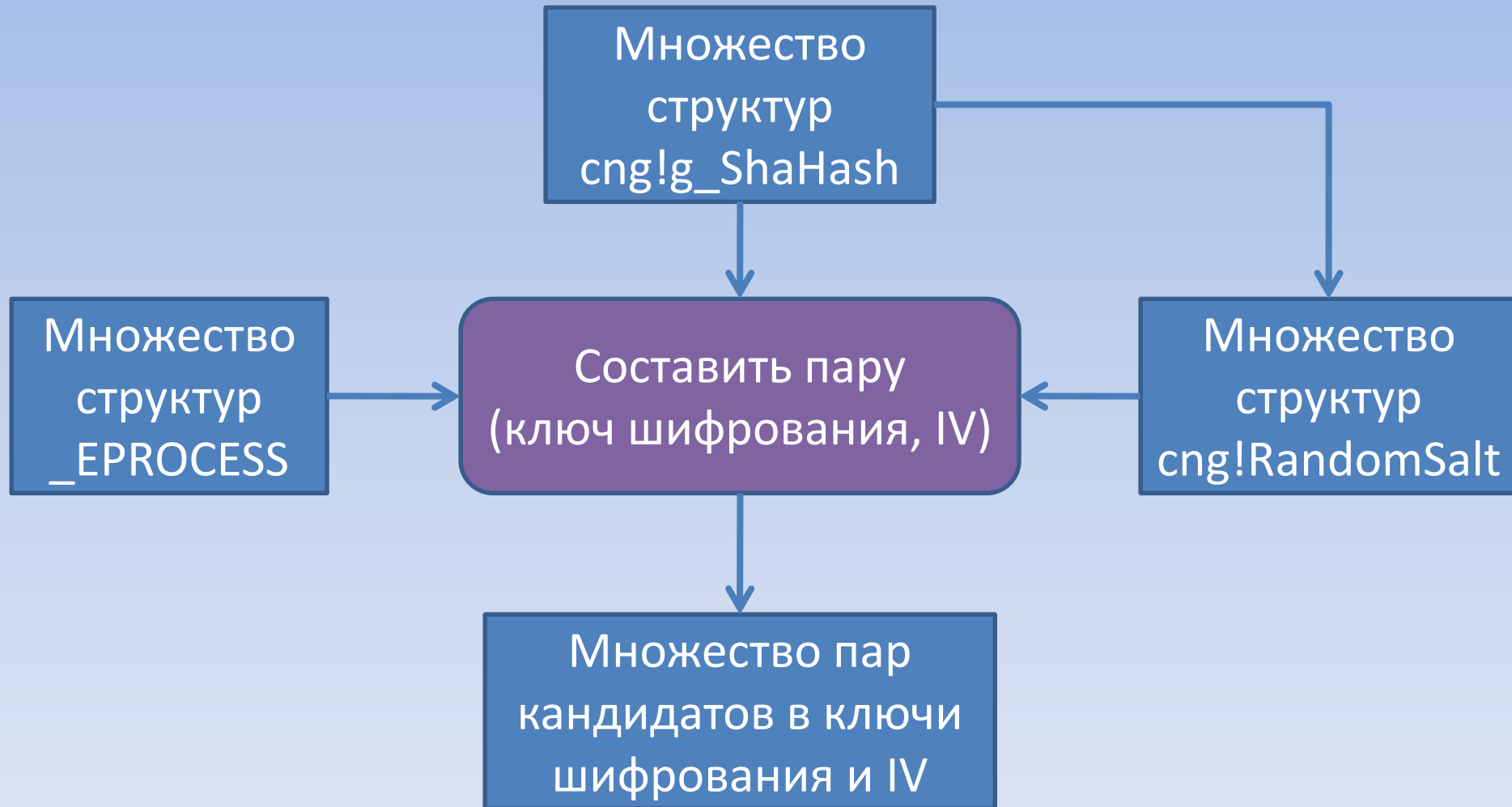
Структура **_EPROCESS**

- Задача поиска и восстановления структур **_EPROCESS** решена (например, ПО Volatility)
- Подход заключается в поиске сигнатуры структуры **_POOL_HEADER** и в исключении неверных вариантов на основе анализа значений полей предполагаемой структуры **_EPROCESS**

Вычисление ключа шифрования функции CryptProtectMemory

```
# первоначальное заполнение массива структуры cng!g_ShaHash  
buffer = g_ShaHash.buffer  
  
# 4-байтовое значение поля Cookie структуры _EPROCESS  
buffer += process[ COOKIE ]  
  
# 8-байтовое значение метки времени создания  
# процесса из структуры _EPROCESS  
buffer += process[ TIME_CREATED ]  
  
# 0x10 - размер ключа шифрования AES-128  
key = SHA1( buffer ).digest()[ 0 : 0x10 ]  
  
# массив cng!RandomSalt  
iv = RandomSalt
```


Построение множества кандидатов в ключи шифрования и векторы инициализации



Зашифрованные CryptProtectMemory данные в ПО KeePass, WinRAR

	KeePass 1.28 (Classic)	KeePass 2.28 (Professional)	WinRAR 5.20
Идентификация зашифрованных данных	Сигнатура (на основе данных из файла БД – тип шифрования, число раундов)	Перед буфером с зашифрованными данными расположен QWORD или DWORD с размером буфера	Сигнатура, фиксированная длина (0x100)
Зашифрованные данные	Ключ шифрования БД	Пароль, хеш (SHA-256) от пароля	Пароль
Проверка расшифрованных данных	Проверка по файлу БД	Валидные данные в терминах UTF-8, соответствие одному из хешей SHA-256	Проверка по файлу архива

Пример – WinRAR 5 (1)

The image shows a Windows 8.1 desktop environment. The background is the Windows 8.1 Start screen. In the foreground, the Windows Control Panel 'System' window is open, displaying system information. A red box highlights 'Windows 8.1 Enterprise N' under 'Windows edition' and '64-bit Operating System, x64-based processor' under 'System type'. To the right, the WinRAR 5.20 (64-bit) 'About' dialog box is open, showing the WinRAR logo, version information, and a '40 days trial copy' notice. A red box highlights 'WinRAR 5.20 (64-bit)' in the dialog box. The taskbar at the bottom shows the Start button, Internet Explorer, and several application icons. The system tray in the bottom right corner shows the date and time as 09.03.2015, 5:15.

System

Control Panel > All Control Panel Items > System

Control Panel Home

View basic information about your computer

Windows edition

Windows 8.1 Enterprise N

© 2013 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz 2.29 GHz

Installed memory (RAM): 2,00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: TestPC

Full computer name: TestPC

Computer description:

Workgroup: WORKGROUP

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00261-80244-06317-AA520

See also

Action Center

Windows Update

Desktop - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

About WinRAR

WINRAR

WinRAR 5.20 (64-bit)

Copyright © 1993-2014 by Alexander Roshal

Published by win.rar GmbH

40 days trial copy

OK

License

Acknowledgments

Home page

Total 2 901 bytes in 6 files

5:15 09.03.2015

Пример – WinRAR 5 (2)

The image shows a Windows 8.1 desktop environment. On the left, the Windows Control Panel 'System' window is open, displaying system information. On the right, the WinRAR 5 'Archive name and parameters' dialog is open, with a sub-dialog 'Enter password' in the foreground. The password 'winrar-5-password' is entered in the 'Enter password' field, which is highlighted with a red rectangle. The 'Show password' and 'Encrypt file names' checkboxes are checked. The WinRAR status bar at the bottom indicates 'Selected 19 bytes in 1 file' and 'Total 2 901 bytes in 6 files'. The taskbar at the bottom shows the Start button, Internet Explorer, and several application icons. The system tray on the right shows the date and time as 5:19 on 09.03.2015.

System Information (Control Panel):

- Windows edition: Windows 8.1 Enterprise N
- © 2013 Microsoft Corporation. All rights reserved.
- System:
 - Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz 2.29 GHz
 - Installed memory (RAM): 2,00 GB
 - System type: 64-bit Operating System, x64-based processor
 - Pen and Touch: No Pen or Touch Input is available for this Display
- Computer name, domain, and workgroup settings:
 - Computer name: TestPC
 - Full computer name: TestPC
 - Computer description:
 - Workgroup: WORKGROUP
- Windows activation:
 - Windows is activated [Read the Microsoft Software License Terms](#)
 - Product ID: 00261-80244-06317-AA520

WinRAR 5 Dialogs:

- Archive name and parameters:
 - Enter password: winrar-5-password
 - Show password
 - Encrypt file names
 - Buttons: OK, Cancel, Help

WinRAR Status Bar: Selected 19 bytes in 1 file | Total 2 901 bytes in 6 files

Пример – WinRAR 5 (3)

004E7A28E4:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A28F4:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2904:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2914:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2924:	AE E3 58 C0 5A 5B 46 27	4D F9 0D 3C 10 E2 89 C2
004E7A2934:	D6 5A 30 6B 20 12 3F CE	9C 82 2C 95 8D 1F 71 8A
004E7A2944:	C8 8C B5 9E BA FB 9C 4A	2C 3F 6E A1 20 49 4D 3F
004E7A2954:	F8 5B 6E AB 1D C7 36 F7	06 E1 DE 19 4B 3B 0D AA
004E7A2964:	C7 31 3E F9 19 E3 0C 06	A8 DD 3F 35 59 04 63 F4
004E7A2974:	13 8E 7A F7 63 85 88 81	97 F5 21 9A BC AE CF 7F
004E7A2984:	E7 7A FF 76 47 CD 0F D4	15 CC 1C 6F 0F 28 E6 9B
004E7A2994:	16 9B ED AA 82 13 3A DE	D2 60 20 6A B5 C8 06 D7
004E7A29A4:	75 64 B5 2C 67 F3 AF 0C	87 72 E3 DD 1C F5 37 1A
004E7A29B4:	15 5F 7F CA 52 BC 07 78	46 4E B6 AD 8F 7C DE 2F
004E7A29C4:	DF 37 84 F3 67 A6 A1 35	4A 45 12 FB A8 FB F4 78
004E7A29D4:	DF CD 2D 59 9F AB 62 14	2E 27 5E 40 85 F9 A7 C9
004E7A29E4:	33 28 68 A3 F0 99 C3 C2	16 E2 1B 86 FA CE 51 04
004E7A29F4:	86 05 E3 75 81 8C 3C BC	0E 72 B8 41 7F C3 82 1E
004E7A2A04:	16 59 05 00 4F 16 FB 71	C3 A0 3F 40 5C 72 F5 4A
004E7A2A14:	00 F0 45 16 B4 7D AC 39	E4 0E C3 7F B6 29 1F 0C
004E7A2A24:	01 00 00 01 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2A34:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2A44:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
004E7A2A54:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

■ prefix
■ ciphertext
■ postfix

Пример – WinRAR 5 (4)

```
00000B4680: 77 00 69 00 6E 00 72 00 61 00 72 00 2D 00 35 00 w i n r a r - 5
00000B4690: 2D 00 70 00 61 00 73 00 73 00 77 00 6F 00 72 00 - p a s s w o r
00000B46A0: 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d
00000B46B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B46C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B46D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B46E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B46F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4710: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4720: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4730: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4740: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000B4770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

В общей сложности проведено 10 успешных экспериментов с различными длинами пароля (до 128 символов включительно)

Пример – KeePass 2 (1)

The image shows a Windows 8.1 desktop environment. The System Control Panel window is open, displaying system information. The 'Windows edition' section shows 'Windows 8.1 Enterprise N' and '© 2013 Microsoft Corporation. All rights reserved.'. The 'System' section lists: Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz 2.29 GHz; Installed memory (RAM): 2,00 GB; System type: 64-bit Operating System, x64-based processor; Pen and Touch: No Pen or Touch Input is available for this Display. The 'Computer name, domain, and workgroup settings' section shows: Computer name: TestPC; Full computer name: TestPC; Computer description: WORKGROUP; Workgroup: WORKGROUP. The 'Windows activation' section shows: Windows is activated; Read the Microsoft Software License Terms; Product ID: 00261-80244-06317-AA520.

The KeePass application is running, and its 'About KeePass' dialog box is open. The dialog box title is 'About KeePass'. The main text reads: 'KeePass Password Safe Version 2.28'. Below this, it says: 'Copyright © 2003-2014 Dominik Reichl. KeePass is OSI Certified Open Source Software. The program is distributed under the terms of the GNU General Public License v2 or later.' There are links for 'KeePass Website', 'Acknowledgements', 'Help', 'License', and 'Donate'. A table lists components and their status/version:

Component	Status / Version
KeePass	2.28
XSL Stylesheets for KDBX XML	Installed
KeePassLibC (1.x File Support)	1.28 (0x0176)

The dialog box has an 'OK' button at the bottom right.

Пример – KeePass 2 (2)

The image shows a Windows 8 desktop environment. In the background, the 'System' control panel window is open, displaying system information such as 'Windows 8.1 Enterprise N', 'Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz', and '2,00 GB' of RAM. In the foreground, the 'Create Composite Master Key' dialog box is open, showing the configuration for a new KeePass database. The dialog includes a text field for a master password, a key file provider selection, and a checkbox for using the Windows user account. Red boxes highlight the password field, the key file provider, and the Windows user account checkbox.

System Information:

- Windows edition: Windows 8.1 Enterprise N
- Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz 2.29 GHz
- Installed memory (RAM): 2,00 GB
- System type: 64-bit Operating System, x64-based processor
- Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings:

- Computer name: TestPC
- Full computer name: TestPC
- Computer description:
- Workgroup: WORKGROUP

Windows activation:

- Windows is activated [Read the Microsoft Software License Terms](#)
- Product ID: 00261-80244-06317-AA520

See also:

- Action Center
- Windows Update

Create Composite Master Key Dialog:

- File: C:\tmp\sample-3.kdbx
- Specify the composite master key, which will be used to encrypt the database.
- A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.
- Master password:** keepass-professional-password-with-keyfile
- Repeat password: [empty]
- Estimated quality: 153 bits 42 ch.
- Key file / provider:** C:\tmp\wmr.exe
- Windows user account**
- This source uses data of the current Windows user. This data does not change when the Windows account password changes.
- Warning: If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.

Пример – KeePass 2 (3)

002DF37470:	00 00 00 00 00 00 00 00	00 6D 93 32 FE 7F 00 00
002DF37480:	98 01 1A 02 00 00 00 00	00 00 00 00 00 00 00 00
002DF37490:	2A 00 00 00 01 00 00 00	00 00 00 00 00 00 00 00
002DF374A0:	28 7F 93 32 FE 7F 00 00	00 00 00 00 00 00 00 00
002DF374B0:	F8 01 1A 02 00 00 00 00	E0 01 1A 02 00 00 00 00
002DF374C0:	2B 00 00 00 00 00 00 00	2A 00 00 00 01 00 00 00
002DF374D0:	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF374E0:	00 00 00 00 00 00 00 00	B8 11 EF 90 FE 7F 00 00
002DF374F0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF37500:	D0 66 EF 90 FE 7F 00 00	30 00 00 00 00 00 00 00
002DF37510:	15 C0 DF 4E 30 1A C6 77	F8 BA DA 68 BE BC FD E4
002DF37520:	8A C0 93 0C 13 0E E4 89	DC 2C 6F D7 09 DA 10 A5
002DF37530:	A2 B4 B0 BA B9 76 47 68	95 9C 4B ED F3 1E 54 66
002DF37540:	00 00 00 00 00 00 00 00	D0 BB 6D 94 FE 7F 00 00
002DF37550:	04 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF37560:	D0 66 EF 90 FE 7F 00 00	2A 00 00 00 00 00 00 00
002DF37570:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF37580:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF37590:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF375A0:	00 00 00 00 00 00 00 00	D0 BB 6D 94 FE 7F 00 00
002DF375B0:	08 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
002DF375C0:	D0 BB 6D 94 FE 7F 00 00	04 00 00 00 00 00 00 00
002DF375D0:	00 00 00 00 00 00 00 00	D8 0B EF 90 FE 7F 00 00

■ ciphertext size

■ ciphertext

Пример – KeePass 2 (5)

0000BA2C70:	75 A6 22 6A 4D 78 2E 03	EF 9B DE 54 EA 56 B3 43
0000BA2C80:	54 A6 69 29 8C AD 97 F4	67 06 D5 E5 47 95 03 F4
0000BA2C90:	3E 21 DD DD 58 76 4C 0B	2F 97 4A 69 92 2C D7 9E
0000BA2CA0:	C6 6E 80 E8 E2 11 9D AF	78 72 96 24 E0 AC AE E7
0000BA2CB0:	70 30 F4 CC 36 9C 02 0A	A1 C9 14 2E 15 C3 5A 4C
0000BA2CC0:	34 A6 69 29 8C AD 97 F4	67 06 D5 E5 47 8F 03 E0
0000BA2CD0:	3F D5 0B 52 B1 6F FD 66	8C DB 28 E5 1E 0E C8 47
0000BA2CE0:	C6 6E 80 E8 E2 11 9D AF	78 72 96 24 E0 AC AE E7
0000BA2CF0:	C0 97 BC 51 58 4D 4C 26	D4 30 14 71 5D 38 6F C2
0000BA2D00:	90 70 B8 7A 56 A0 62 AC	00 A6 1C 2C 0E BB 9F E3
0000BA2D10:	C0 9F BF 06 47 B3 BC CC	21 32 A2 15 24 43 E5 10
0000BA2D20:	54 A6 69 29 8C FC 96 E9	67 1D D5 F0 47 98 03 E4
0000BA2D30:	C6 6E 80 E8 E2 11 9D AF	78 72 96 24 E0 AC AE E7
0000BA2D40:	92 1A 03 C3 56 C4 92 9E	52 CF 9E AC 32 B3 82 8D
0000BA2D50:	F3 06 B0 1A 32 20 06 0D	91 C7 72 7B 42 72 8A 24
0000BA2D60:	26 4B 1D E0 4B BF 50 31	42 80 2F E8 18 67 A3 5F
0000BA2D70:	38 0D 70 99 F4 D0 3E DC	90 A3 7C 2F 76 32 5D 98
0000BA2D80:	DB 89 70 27 71 37 A3 6D	D2 69 43 C0 8B E2 B6 30
0000BA2D90:	A0 E8 8D A4 2A 9B 5E 6A	95 3B BC 00 15 99 88 63
0000BA2DA0:	27 7A 72 CD 00 D1 0F 76	AA 38 FD FB EF 74 8C 92
0000BA2DB0:	8B FF 52 7F 48 5A 04 F2	C9 6A 95 C8 F7 FA A4 CA
0000BA2DC0:	3E 2C 87 26 1F 73 95 A5	A2 8A D9 E8 51 4A 55 C7
0000BA2DD0:	5E D2 F3 40 87 CF 83 D2	7B 98 E3 0E 4C 3B 75 8C
0000BA2DE0:	30 3C 45 75 91 A9 0D 62	2E B6 09 A2 65 11 53 AE
0000BA2DF0:	97 48 AD E8 F7 24 C9 56	82 7A D0 30 F1 6F AA F0
0000BA2E00:	71 20 23 99 4A D9 EA 9E	17 80 1C 25 D8 9A AC 10
0000BA2E10:	BB DA B6 FD 59 CA 74 1C	80 98 2D B5 AD 5A E3 39
0000BA2E20:	9C F5 B3 42 71 6C 63 21	27 1C 07 7C EA 09 34 49
0000BA2E30:	83 8F 17 CC 1A 93 A9 5A	4C 64 FB 1F 50 A5 85 ED

SHA-256('keepass-professional-password-with-keyfile') =
1063ce908562ae6eece8db593151cbe9**264b1de04bbf503142802fe81867a35f**

Пример – KeePass 2 (6)

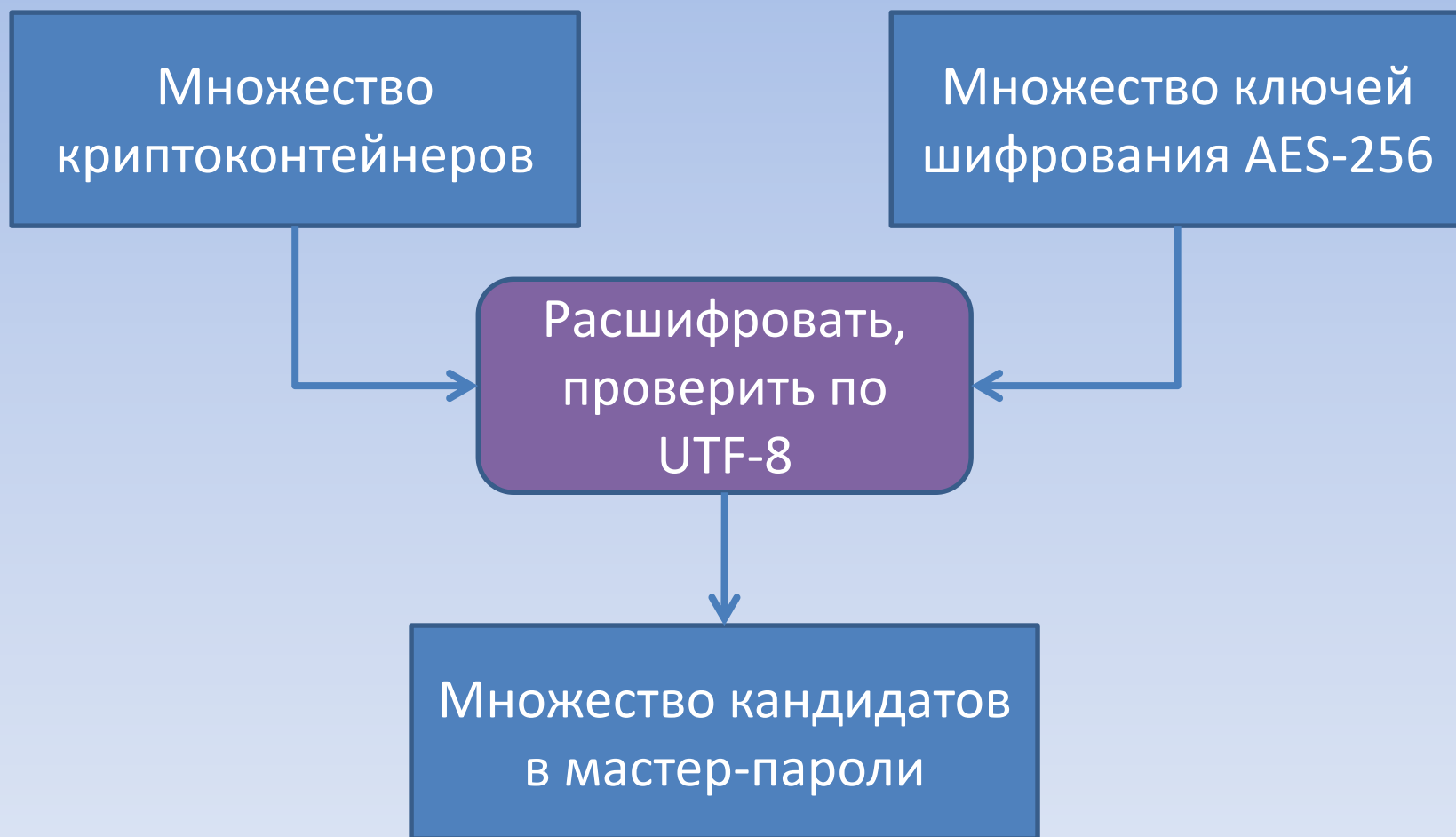
```
(E:\keepass\memory) - Far 3.0.3000 x64 Administrator
Checking password 'keepass-profess'
Checking password 'keepass-professional-'
Checking password 'keepass-professional-p'
Checking password 'ke'
Checking password 'kee'
Checking password 'G~!E†>↓{m^L_←3♀'
Checking password 'k'
Checking password ' @0V◆'
Checking password '!"#%&'()*+,-./'
Checking password 'keepass-professional'
Checking password '4Lp\]o÷8U| |A0á| '
Checking password 'llit-S30bo>uo†iS'
Checking password 'e(d;v◀M~| $←/: -'
Checking password '@w|0j'
Checking password '-0&ktU_4"'
Checking password '†è0jeX5→M[▲↓ò[8>'
Checking password 'keepass-profe'
Checking password 'keepass-profes'
Checking password 'keepass-professional-password-with-ke'
Checking password 'keepass-professional-password-with-key'
Checking password 'keepass-pro'
Checking password 'keepass-prof'
Checking password '%oqM1tVεfll↑τÜÿT→'
Checking password '■aa'-'1.%>H90||'
Checking password 'l+α:°hQ_T!MSM+'
Checking password 'keepass-professional-pas'
Checking password 'keepass-professional-pass'
Checking password '†ÄΔ5}†â->-U|Ax$0'
Checking password 'keepass-professional-password-with-keyf'
Checking password 'keepass-professional-password-with'
Checking password 'keepass-professional-password-with-keyfile'
[+] Password found: keepass-professional-password-with-keyfile

E:\keepass\memory>
1Help 2UserMn 3View 4Edit 5Copy 6RenMov 7MkFold 8Delete 9ConfMn 10Quit 11Plugin 12Screen
```

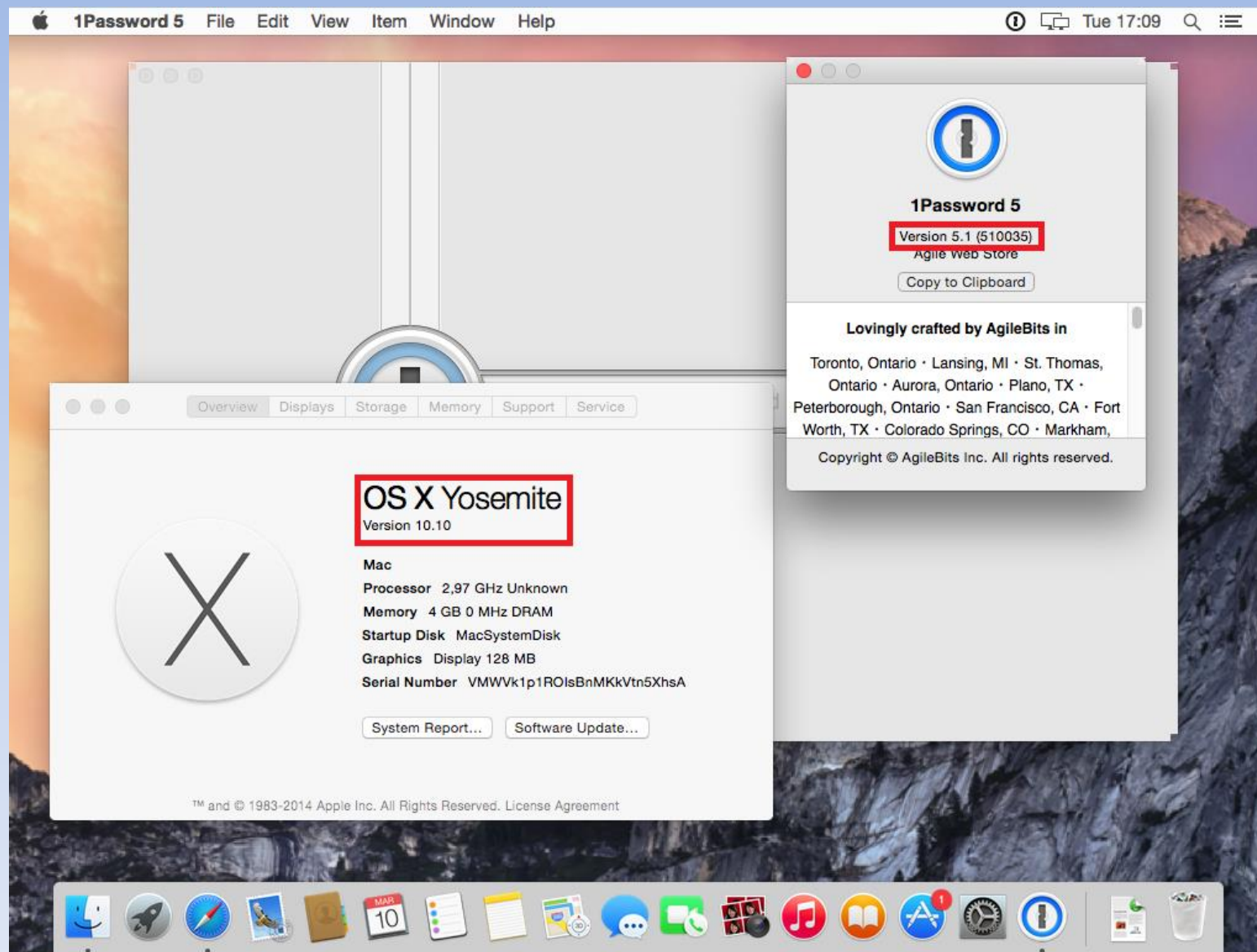
Схема защиты данных в памяти ПО 1Password (Mac OS X)

- Все критичные данные (в том числе, мастер-пароль) хранятся в криптоконтейнерах
- Данные зашифрованы с помощью **AES-256**, ключи шифрования в памяти лежат в открытом виде
- В контейнере данные хранятся в кодировке **UTF-8**

Построение множества кандидатов в мастер-пароли



Пример – 1Password (1)



Пример – 1Password (2)

```
[i] Step 1 - collect possible AES keys
[i] Key count: 7569
[i] Step 1 ran in 311 seconds
[i] Step 2 - collect possible opdata blocks
[i] Full containers count: 35
[i] Step 2 ran in 207 seconds
[i] Step 3 - generate dictionary
[i] AES key = 3a99377ac3548a97c5f046c706ea3c2bd7b1f21ad45f75b3a7dab344f4e47fe7
[i] password = {"title":"Login 2","ainfo":"login2","ps":0}
[i] AES key = 9e8c8fe28f5444f6c1137f4e4e54b53afac078493d549a4c99b3c4409e294f95
[i] password = {"fields":[{"value":"login2","name":"username","type":"T","designation":"username"}]}
[i] AES key = 3a99377ac3548a97c5f046c706ea3c2bd7b1f21ad45f75b3a7dab344f4e47fe7
[i] password = {"title":"Login 1","ainfo":"login","ps":1}
[i] decrypted data = 000000000007b227469746c65223a224c6f67696e2031222c2261696e666f223a226c6f67696e22
...
[i] AES key = 35422038e4edcb5715ada7f97b1be045f3abc390c34f33f3758d4a806c859f3c
[i] password = 1password-mac-password-2
[i] decrypted data = 00000000000000003170617373776f72642d6d616332d70617373776f72642d32
[i] AES key = 08e137ed72f88bff35360e489774614a8975279c22873ac48c0a2fec81e3ae68
[i] password = {"fields":[{"value":"login","name":"username","type":"T","designation":"username"},{"v
[i] Step 3 ran in 2 seconds
Total passwords: 1924
```

В общей сложности проведено 10 успешных экспериментов с различными длинами мастер-пароля (до 128 символов включительно)

Результаты работы

Название ПО	Результат (на основе анализа образа памяти)
1Password 5.1 (Mac)	Восстановление мастер-пароля (независимо от блокировки БД)
KeePass 1 (Classic)	Восстановление ключа шифрования БД
KeePass 2 (Professional)	Восстановление мастер-пароля (в том числе, в случае использования ключевого файла и/или привязки к локальному пользователю)
WinRAR 5.20 (Windows)	Восстановление пароля от архива

Спасибо за внимание!