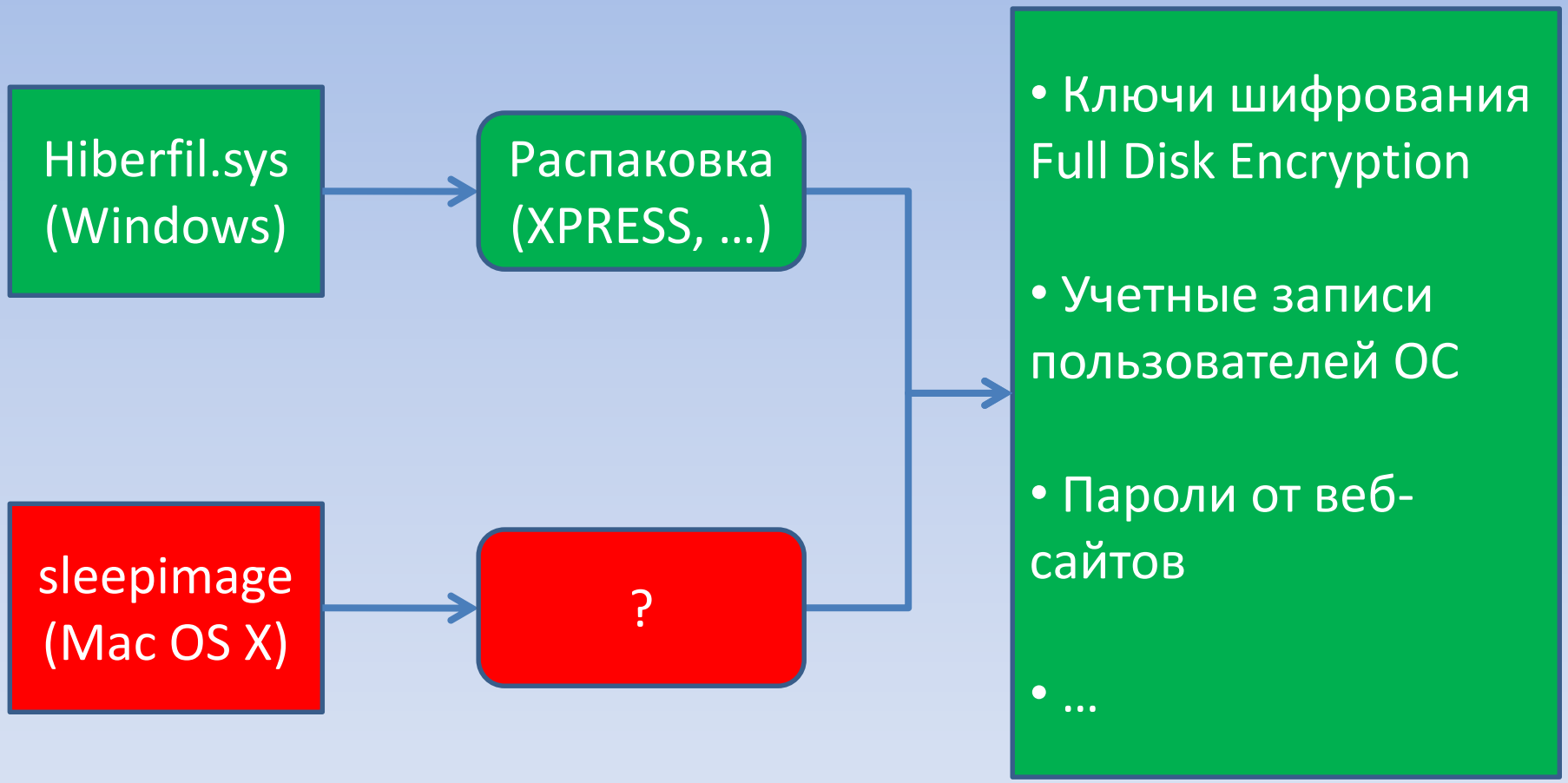
Инженерно-технические аспекты криминалистического анализа MacOS

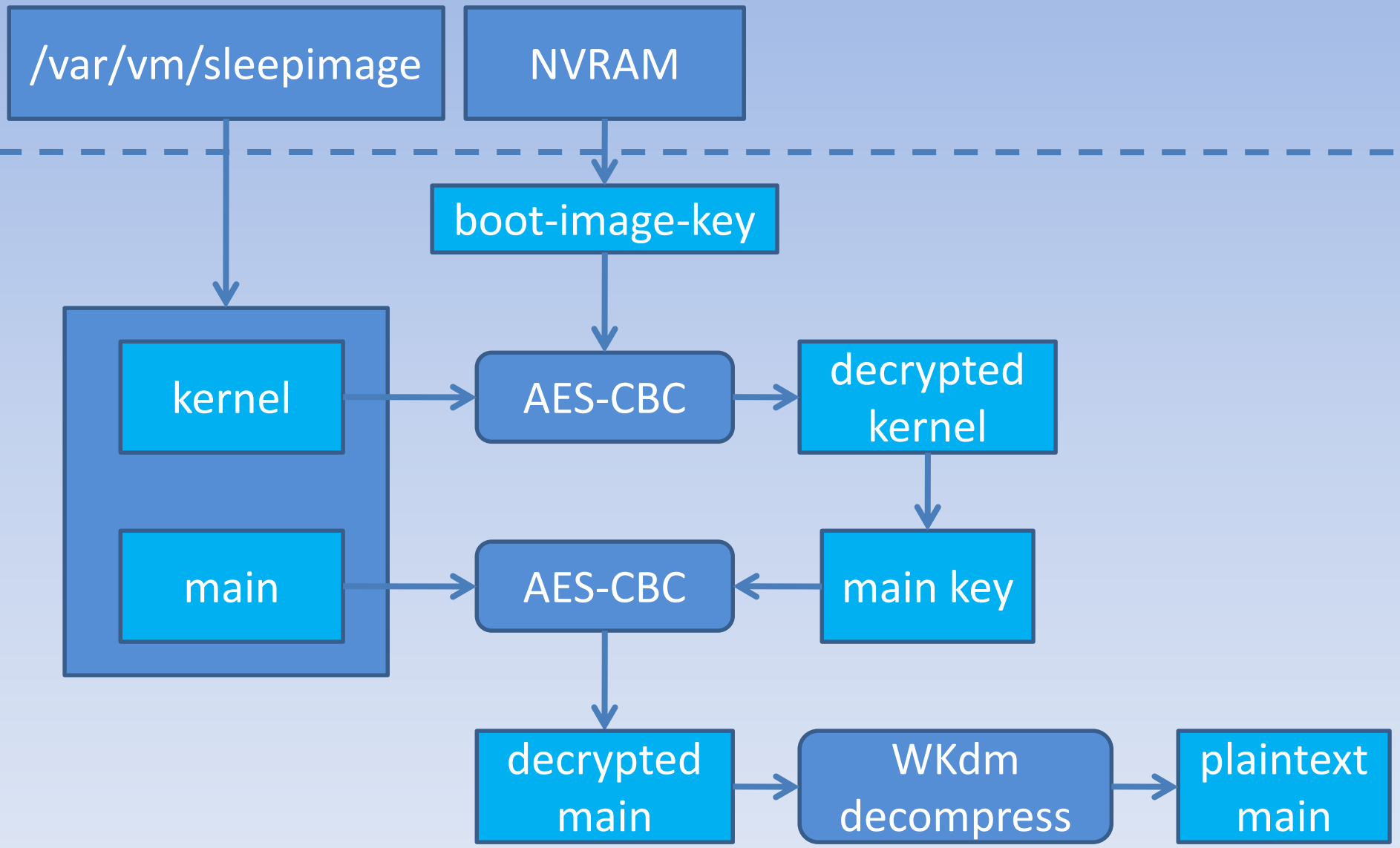
Чиликов А.А.,
МГТУ им.Баумана, Passware Inc.

24 марта 2016 г.

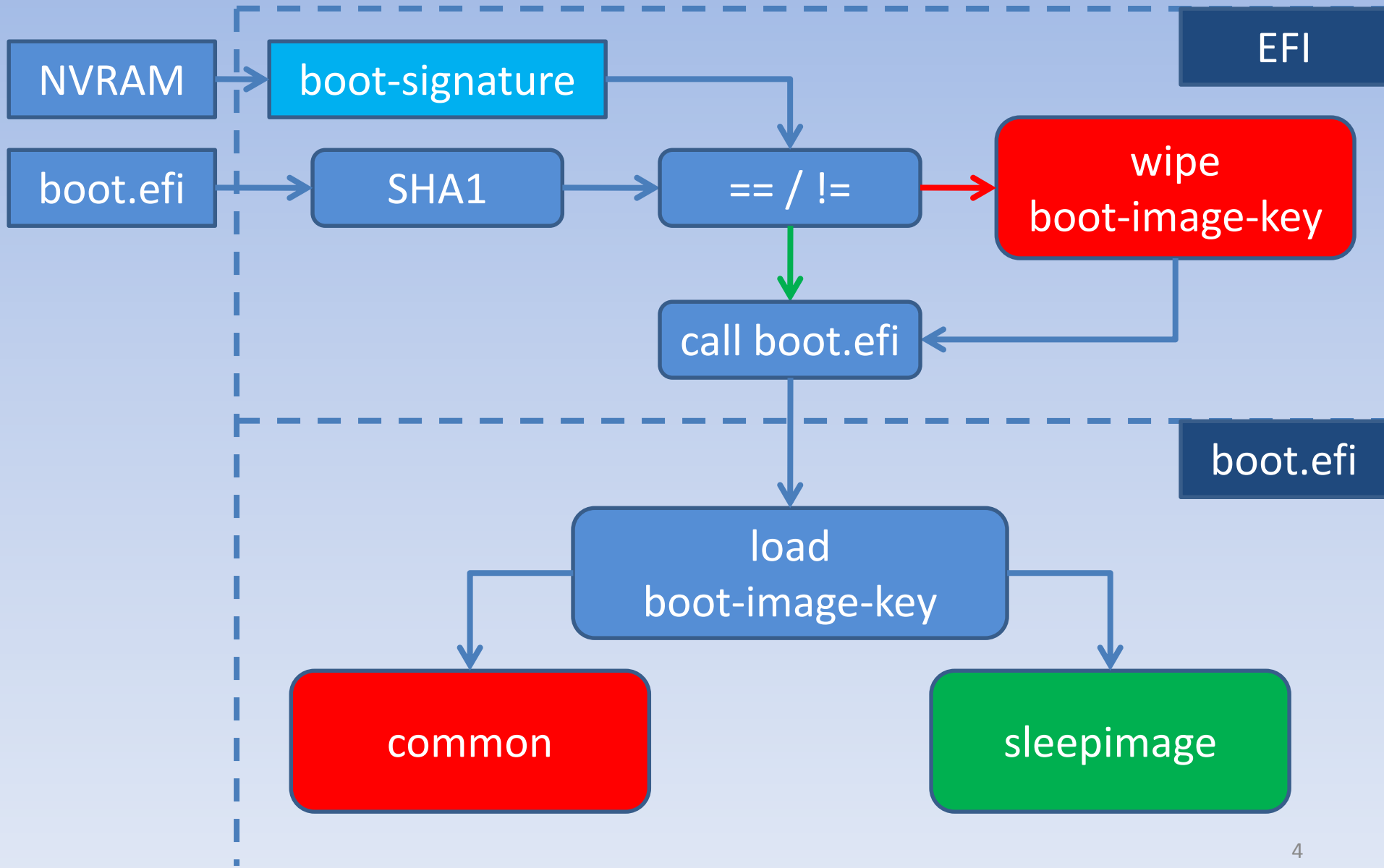
Актуальность



Описание схемы защиты (без FV2)



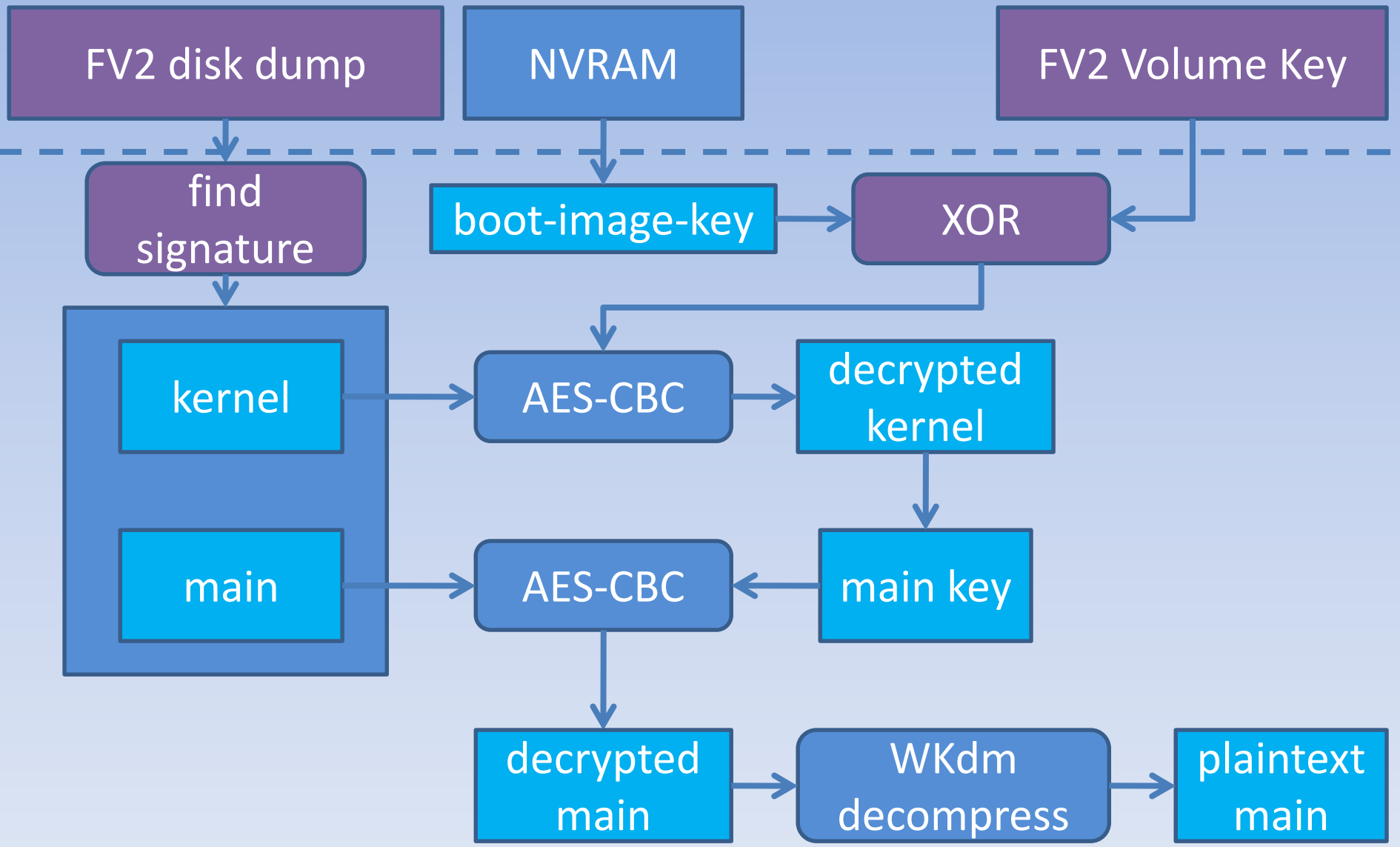
Контроль целостности загрузчика



Получение доступа к NVRAM

- Извлечение чипа (chip-off)
- **Внутрисхемное программирование (SPI-интерфейс)**

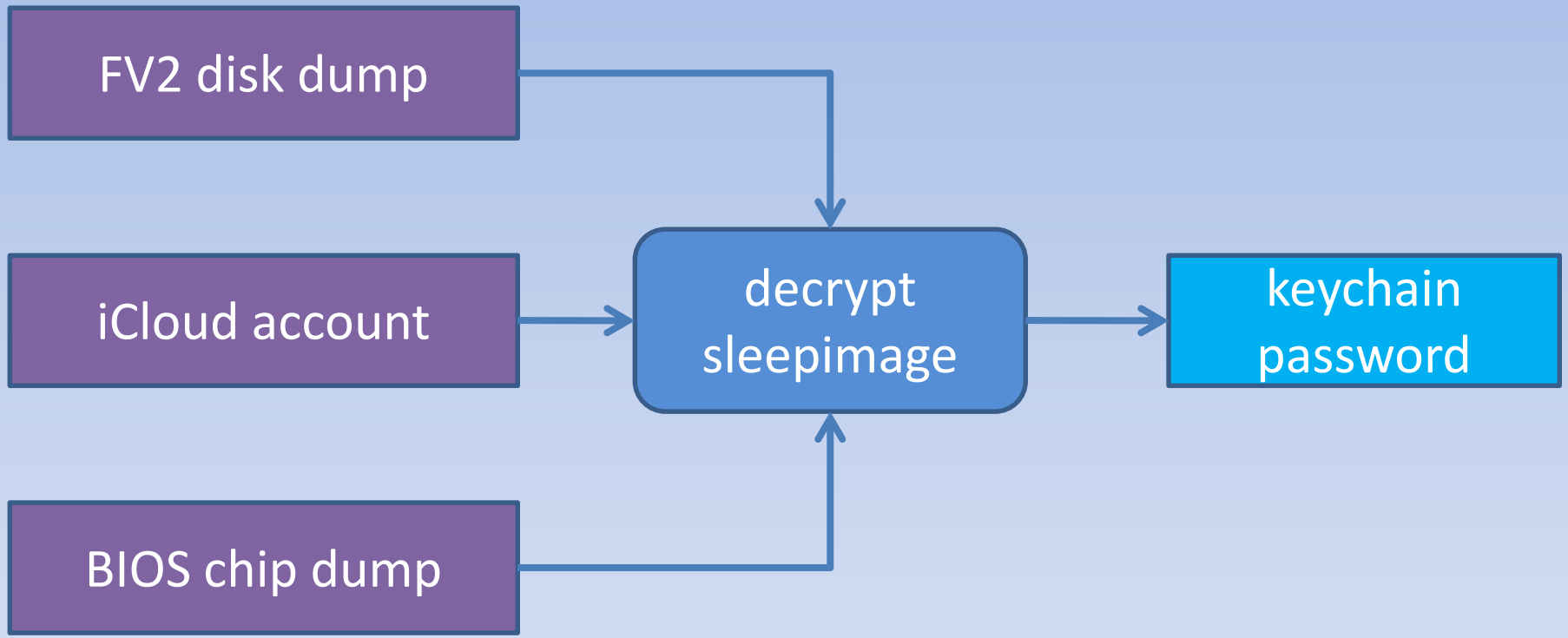
Описание схемы защиты (FV2)



Получение FileVault2 Volume Key

- Пароль пользователя
- Пароль восстановления (Recovery password)
- **Учетная запись в iCloud (по умолчанию, начиная с Mac OS X Yosemite)**
- Анализ памяти (Live-memory analysis)

Сценарий использования (FV2)



Расшифровка kernel

зашифрованная kernel-часть:

```
000274E9BC: 5A 18 C2 3D E6 E3 86 D0 | FF 0A 9C A0 86 C0 A7 4B
000274E9CC: 2F 66 44 13 22 B7 32 63 | 12 94 F1 C6 77 F9 85 FF
000274E9DC: 4B 58 2A 28 60 9C 73 26 | F0 0D 61 D6 59 F7 A2 2B
000274E9EC: 5A E4 A1 6D 1D 38 0F 86 | F3 7F EF E2 D7 88 43 88
000274E9FC: E3 A6 D8 F0 45 E3 D2 B7 | 4E 32 C7 27 C6 9E A5 7F
000274EA0C: DD 15 52 91 87 FD DF 9A | 92 BD 25 B6 6B 2B 04 94
000274EA1C: D9 E2 E4 33 C7 66 D4 6A | A4 D6 13 98 D7 81 AF 39
```

encrypted main key

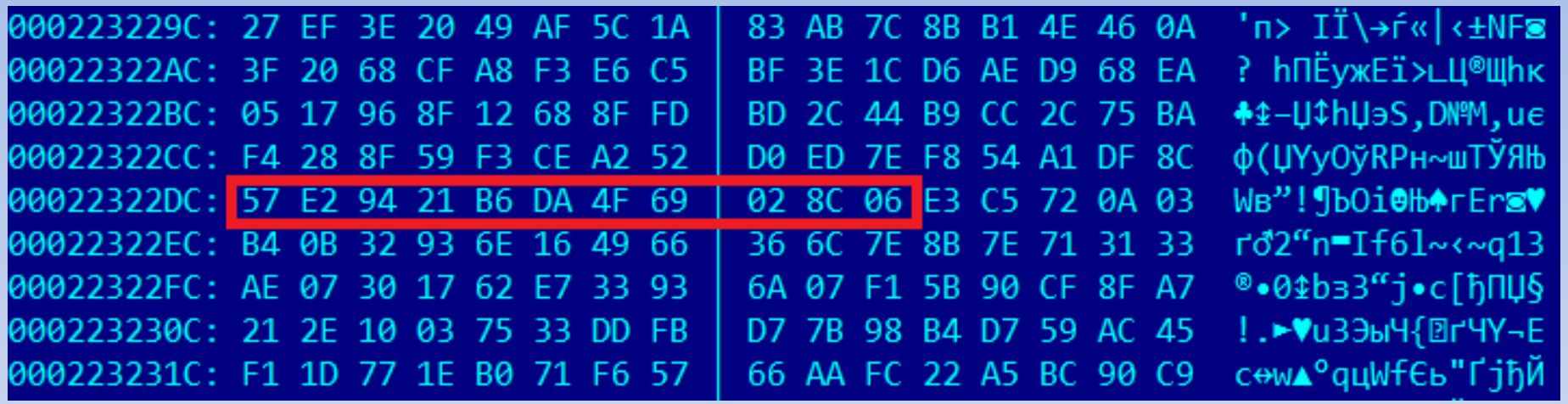
расшифрованная kernel-часть:

```
000274E9BC: 00 00 02 00 00 C0 3F B9 | 5C 18 00 00 00 F0 89 16
000274E9CC: 01 00 00 00 00 00 00 80 | 5C 28 76 02 30 40 01 00
000274E9DC: D0 CF 74 02 E6 E9 B9 17 | C0 36 0C 2A C0 5A 16 2A
000274E9EC: 5E 2D CC 41 F1 DA 30 50 | C2 10 B9 59 AD 53 D0 2B
000274E9FC: 4B B9 C8 3C E0 97 34 0E | D3 48 18 FC 5B D0 E7 16
000274EA0C: B7 03 B4 68 57 94 80 66 | 84 DC 98 9A DF 0C 7F 8C
000274EA1C: 06 D2 10 AD 51 46 90 CB | D5 9A 08 51 0A 96 77 DD
```

main_key

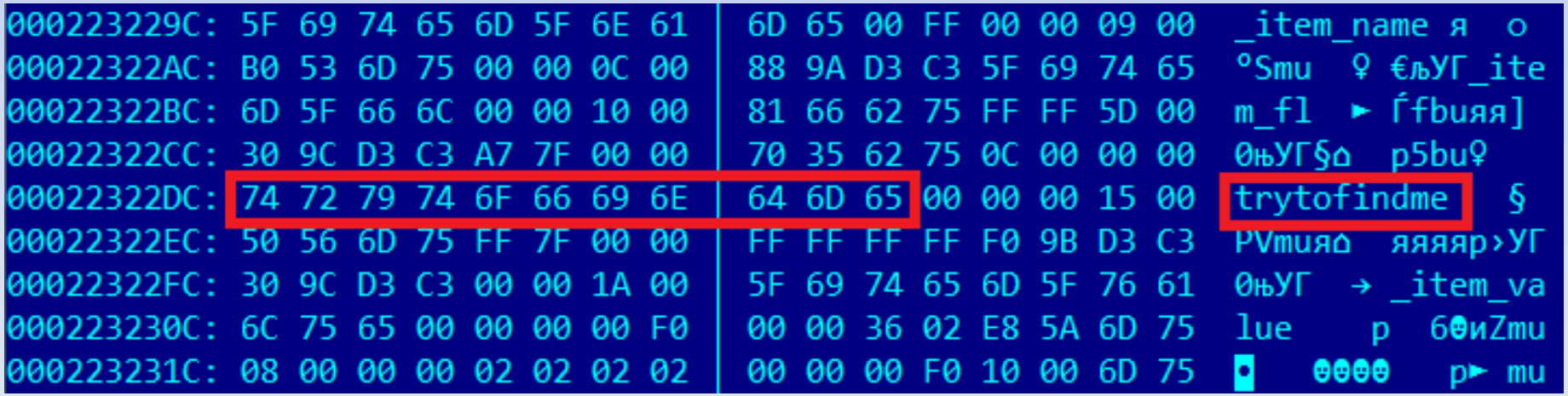
Расшифровка main

зашифрованная main-часть:



```
000223229C: 27 EF 3E 20 49 AF 5C 1A | 83 AB 7C 8B B1 4E 46 0A | 'п> IЇ\→ґ«|‹±NF◙
00022322AC: 3F 20 68 CF A8 F3 E6 C5 | BF 3E 1C D6 AE D9 68 EA | ? hПЁужЕї›ьЦ®Щhк
00022322BC: 05 17 96 8F 12 68 8F FD | BD 2C 44 B9 CC 2C 75 BA | ♣↨–Џ↕hЏэS,D№M,uє
00022322CC: F4 28 8F 59 F3 CE A2 52 | D0 ED 7E F8 54 A1 DF 8C | ф(ЏYyOўRPн~шTЎЯЊ
00022322DC: 57 E2 94 21 B6 DA 4F 69 | 02 8C 06 E3 C5 72 0A 03 | Wв”!¶ЪOi☻Њ♠rEr◙♥
00022322EC: B4 0B 32 93 6E 16 49 66 | 36 6C 7E 8B 7E 71 31 33 | ґð2“n▬If6l~‹~q13
00022322FC: AE 07 30 17 62 E7 33 93 | 6A 07 F1 5B 90 CF 8F A7 | ®•0↨bз3“j•c[ђПЏ§
000223230C: 21 2E 10 03 75 33 DD FB | D7 7B 98 B4 D7 59 AC 45 | !.►♥u3ЭыЧ{▣rЧY¬E
000223231C: F1 1D 77 1E B0 71 F6 57 | 66 AA FC 22 A5 BC 90 C9 | c↔w▲°qцWfЄь"Ґjђй
```

расшифрованная main-часть:



```
000223229C: 5F 69 74 65 6D 5F 6E 61 | 6D 65 00 FF 00 00 09 00 | _item_name я  o
00022322AC: B0 53 6D 75 00 00 0C 00 | 88 9A D3 C3 5F 69 74 65 | °Smu  ♀ €љУГ_ite
00022322BC: 6D 5F 66 6C 00 00 10 00 | 81 66 62 75 FF FF 5D 00 | m_fl  ► Ґfbuяя]
00022322CC: 30 9C D3 C3 A7 7F 00 00 | 70 35 62 75 0C 00 00 00 | 0њУГ§⌂  p5bu♀
00022322DC: 74 72 79 74 6F 66 69 6E | 64 6D 65 00 00 00 15 00 | trytofindme  §
00022322EC: 50 56 6D 75 FF 7F 00 00 | FF FF FF FF F0 9B D3 C3 | PVmuя⌂  ясяяяр›УГ
00022322FC: 30 9C D3 C3 00 00 1A 00 | 5F 69 74 65 6D 5F 76 61 | 0њУГ  → _item_va
000223230C: 6C 75 65 00 00 00 00 F0 | 00 00 36 02 E8 5A 6D 75 | lue    p  6☻иZmu
000223231C: 08 00 00 00 02 02 02 02 | 00 00 00 F0 10 00 6D 75 | ◘   ☻☻☻☻   p► mu
```

Результаты работы

Предложен метод восстановления образа памяти из файла гибернации ОС Mac OS X для следующих случаев:

Наличие защиты FileVault2	Требуемые данные для расшифровки
-	1) образ чипа BIOS 2) файл /var/vm/sleepimage
+	1) образ чипа BIOS 2) образ диска 3) пароль пользователя/пароль восстановления/учетная запись icloud/образ памяти

Спасибо за внимание!