guardant DAY

КОМПАНИЯ АКТИВ

Автоматическая защита и Guardant Sign — тонкости взаимодействия

Михаил Бакаляров,
Руководитель департамента разработки Guardant

Шифрование секций исполняемого файла

Требования:

- Криптографически стойкий генератор случайных чисел (CSPRNG)
- Симметричный ключ и алгоритм шифрования AES
- Алгоритм генерации таблиц вопросов/дополнений
- Алгоритм восстановления ключа шифрования AES с помощью таблиц вопросов/дополнений и электронного ключа Guardant Sign

Алгоритм генерации таблиц вопросов/ дополнений

Таблица вопросов

	Случайный блок
312	39 9D 73 21 ...
313	2E 52F0 AB ...
314	90 83 E1 11 ...
315	[...]
316	[...]
...	[...]

AES ключ шифрования файла

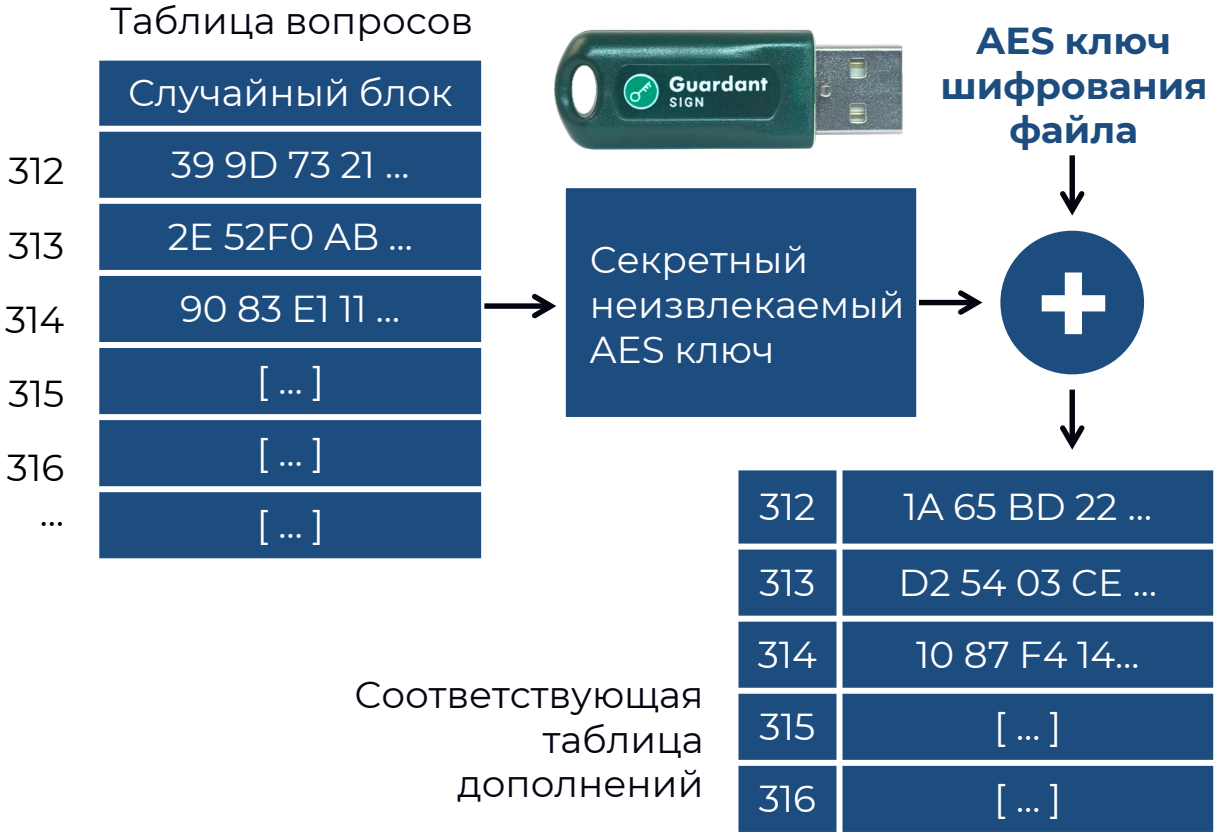
Секретный неизвлекаемый ключ

312	1A 65 BD 22 ...
313	D2 54 03 CE ...
314	10 87 F4 14...
315	[...]
316	[...]

Соответствующая таблица дополнений

- Секретный ключ всегда находится внутри электронного ключа
- Таблицы можно создать повторно без изменения секретного ключа
- AES ключ шифрования файла возникает в памяти процесса непосредственно только в момент расшифровки исполняемого файла
- AES ключ шифрования файла уникален для каждого файла

Алгоритм восстановления ключа шифрования AES



- Случайный выбор вопроса
- Переключение между несколькими таблицами
- Редкие вопросы в зависимости от календарной даты
- Разные вопросы в зависимости от версии операционной системы

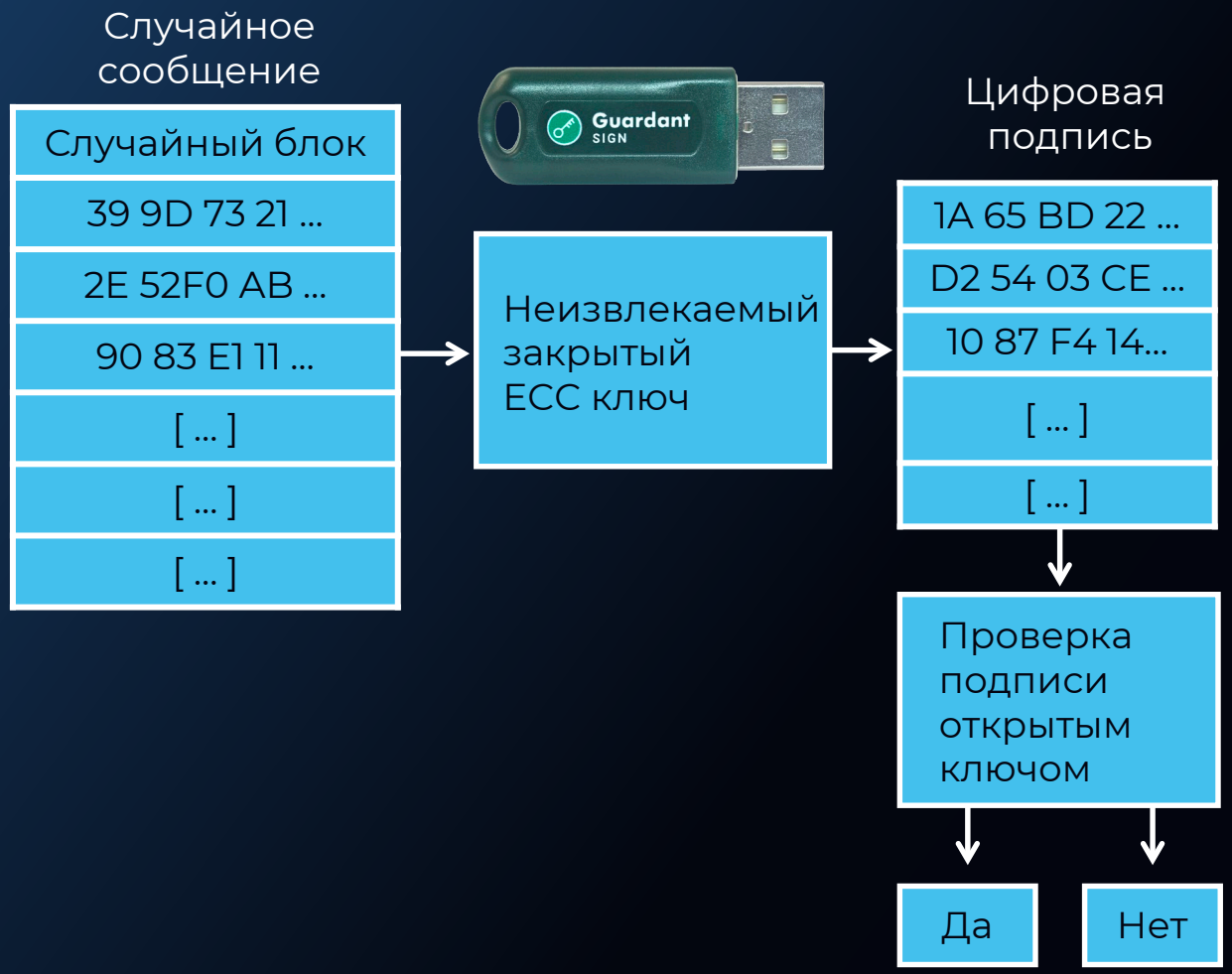
Потенциальные атаки на алгоритм восстановления ключа

- Атака на генератор случайных чисел
- Логирование всех данных передающихся в электронный ключ и возвращаемых из электронного ключа (табличный эмулятор)
- Физический дамп памяти электронного ключа

Guardant Sign

- Шифрование трафика протокола обмена между приложением и электронным ключом
- Цифровая подпись на эллиптических кривых
- Симметричный алгоритм шифрования AES

Алгоритм цифровой подписи для защиты



- Закрытый ключ надёжно хранится внутри электронного ключа
- Открытый ключ интегрируется в исходный код приложения
- Позволяет убедиться что приложение работает с оригинальным электронным ключом

Шифрование секций исполняемого файла

Плюсы:

- Файл нельзя расшифровать без электронного ключа
- Невозможно создать универсальный эмулятор ключа Guardant Sign без изменения кода приложения или физического дампа ключа

Минусы:

- Нет защиты от дампа процесса
- Требуется модификация исполняемого кода

Автозащита = конверт + протектор

Преимущества конверта

1. Шифрование секций исполняемого файла
2. Защита импортов

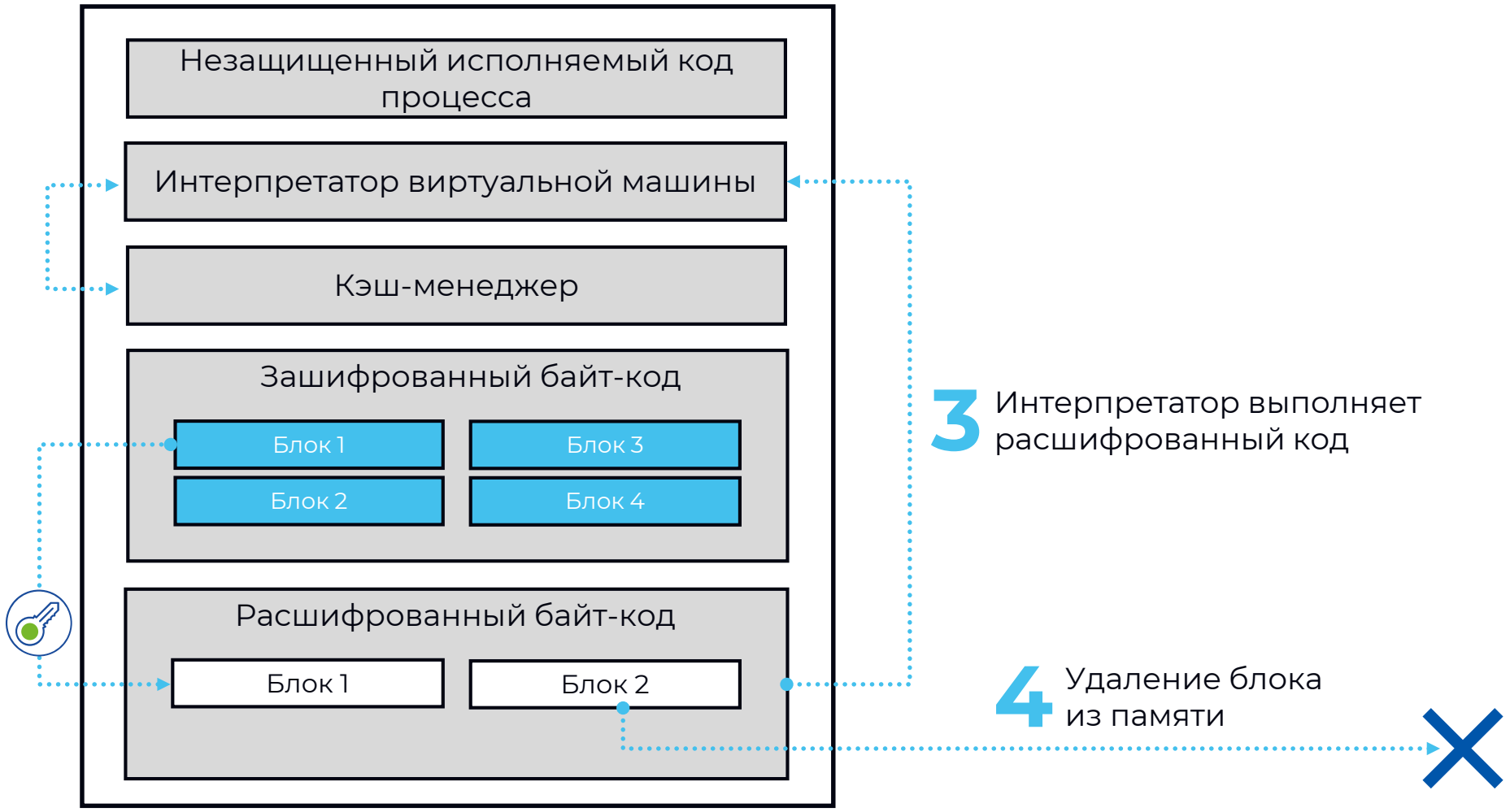
Преимущества протектора

1. Виртуализация кода
2. Мутация кода
3. Защита от дампа

Защита от дампа

1 Интерпретатор указывает кэш-менеджеру, какой блок расшифровать

2 Кэш-менеджер расшифровывает блок



3 Интерпретатор выполняет расшифрованный код

4 Удаление блока из памяти

Автоматическая защита и Guardant Sign

Преимущества:

- Файл нельзя расшифровать без электронного ключа
- Защита от реверс-инжиниринга
- Защита от дампа процесса
- Невозможно создать универсальный эмулятор ключа Guardant Sign без изменения кода приложения или физического дампа ключа

Автоматическая защита и Guardant Sign — сложные технологии для вашей быстрой и надежной защиты!

guardant

Вопросы

guardant DAY

КОМПАНИЯ АКТИВ

Михаил Бакаляров,

Руководитель департамента разработки Guardant

+7 903 198-23-39

bma@guardant.ru

www.guardant.ru