Основы безопасной разработки программного обеспечения. Лекция 1

ТЮРИН КАЙ АНДРЕЕВИЧ

УК РФ

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

…и другие классификации законности

Про что безопасность вообще?

Безопасность – это про противостояние злоумышленнику во время достижения некоторой цели

Цель vs. Злоумышленник

(adversary/attacker/…)

Безопасность это про

1. Политики (Policy) – что система должна делать?
2. Модель угроз (Threat Model) – какими возможностями обладает злоумышленник?
3. Механизмы – программное или аппаратное обеспечение, которое определяется политикой

Политики

Конфиденциальность

Целостность

Доступность

В чём сложность с политиками?

Например, имеется политика доступа.

Доказать, что доступ есть у определённых лиц – достаточно просто.

Но как доказать, что доступа больше ни у кого нет?

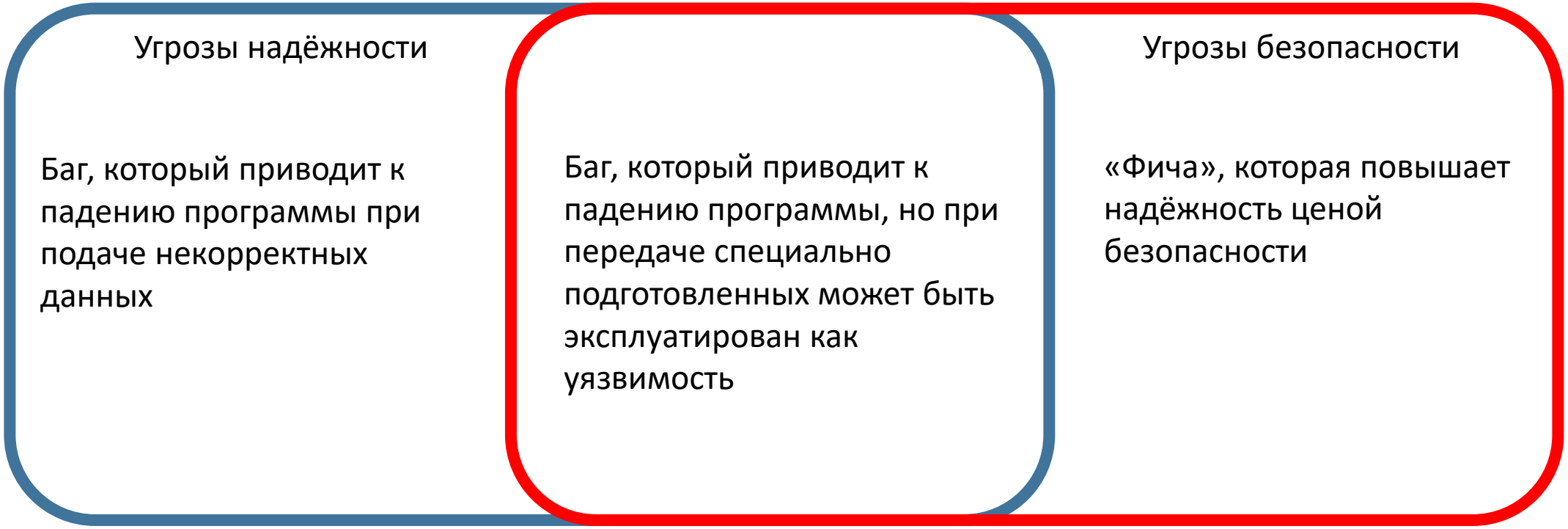
Как достичь абсолютной безопасности?

Не включайте компьютер*

*даже в розетку (см. Intel AMT)

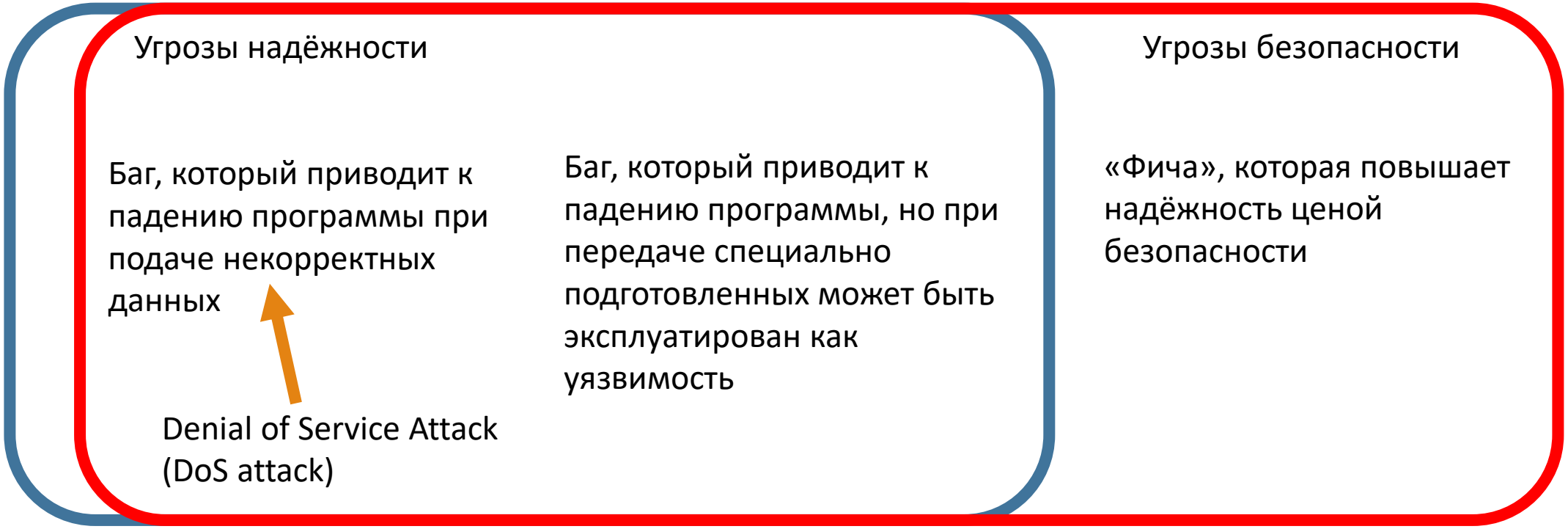
Надёжность vs. Безопасность

Надёжность и безопасность – разные (но пересекающиеся) вещи.



Надёжность vs. Безопасность

Надёжность и безопасность – разные (но пересекающиеся) вещи.



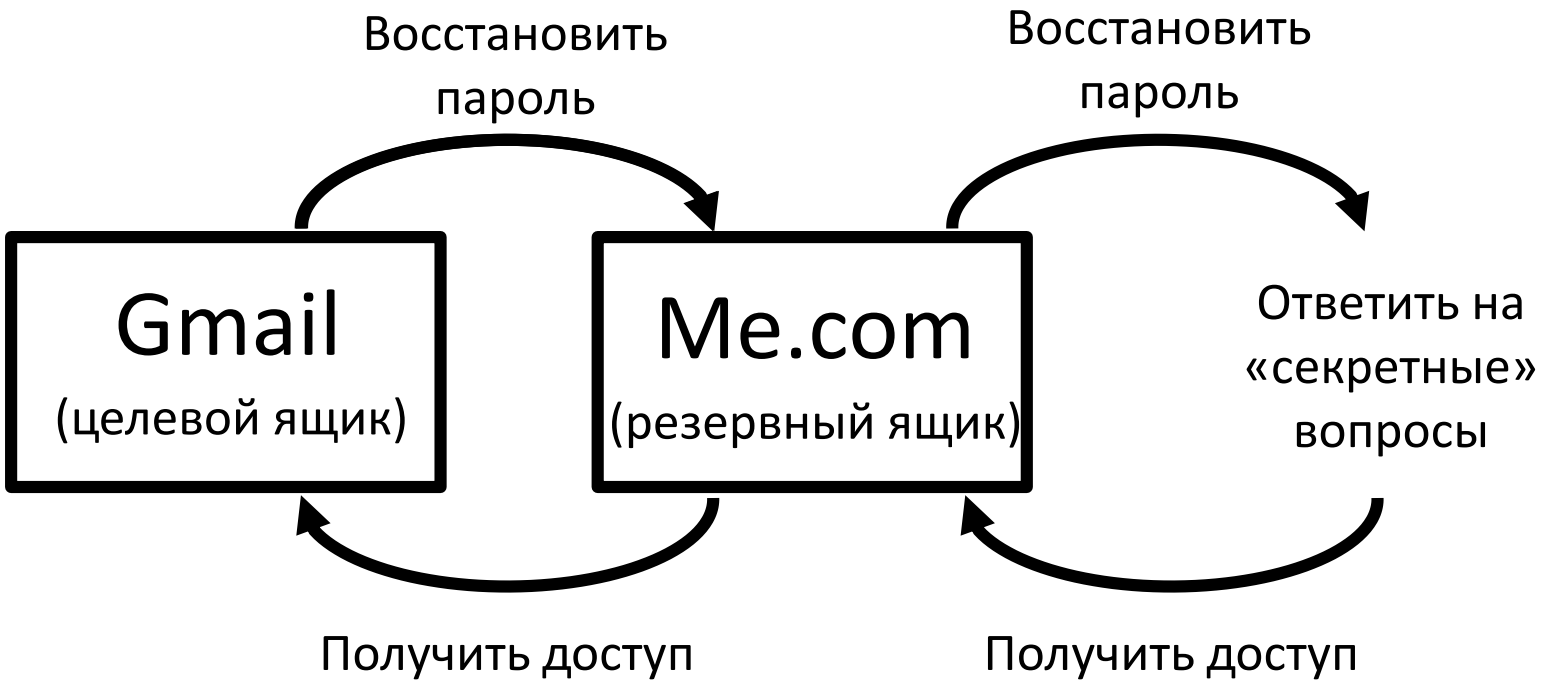
Что может пойти не так с политиками?

Для входа на сайт требуется пароль.

Но его можно восстановить, ответив на секретные вопросы.

Стойкость всей системы сильно снижается, потому что злоумышленнику необходимо знать пароль ИЛИ ответы на «секретные» вопросы.

Более сложный пример



Что не так с моделью угроз?

Модель угроз меняется со временем.

Один из последних примеров – появление уязвимостей Spectre и Meltdown.

Модель угроз – это важно

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Bruce Schneier

Модель угроз SSL/TLS

Протоколы SSL/TLS, используемые для защиты огромного количества передаваемых данных в Интернете, опираются на серьёзную криптографию и…

…неоспоримое доверие к центрам сертификации (Certification authority, CA)

Супер-безопасная ОС от DARPA

DARPA решили разработать очень безопасную ОС

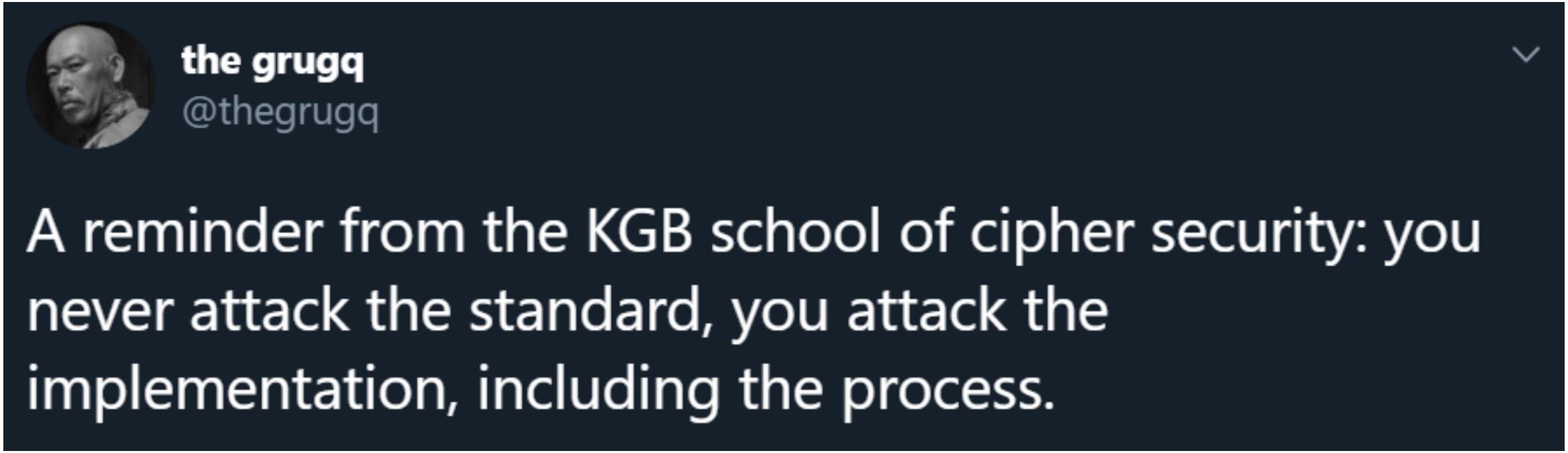
Объявили конкурс на поиск в ней уязвимостей

Кто-то обнаружил, что исходники находятся на незащищённом компьютере и внедрил бэкдор прямо в них

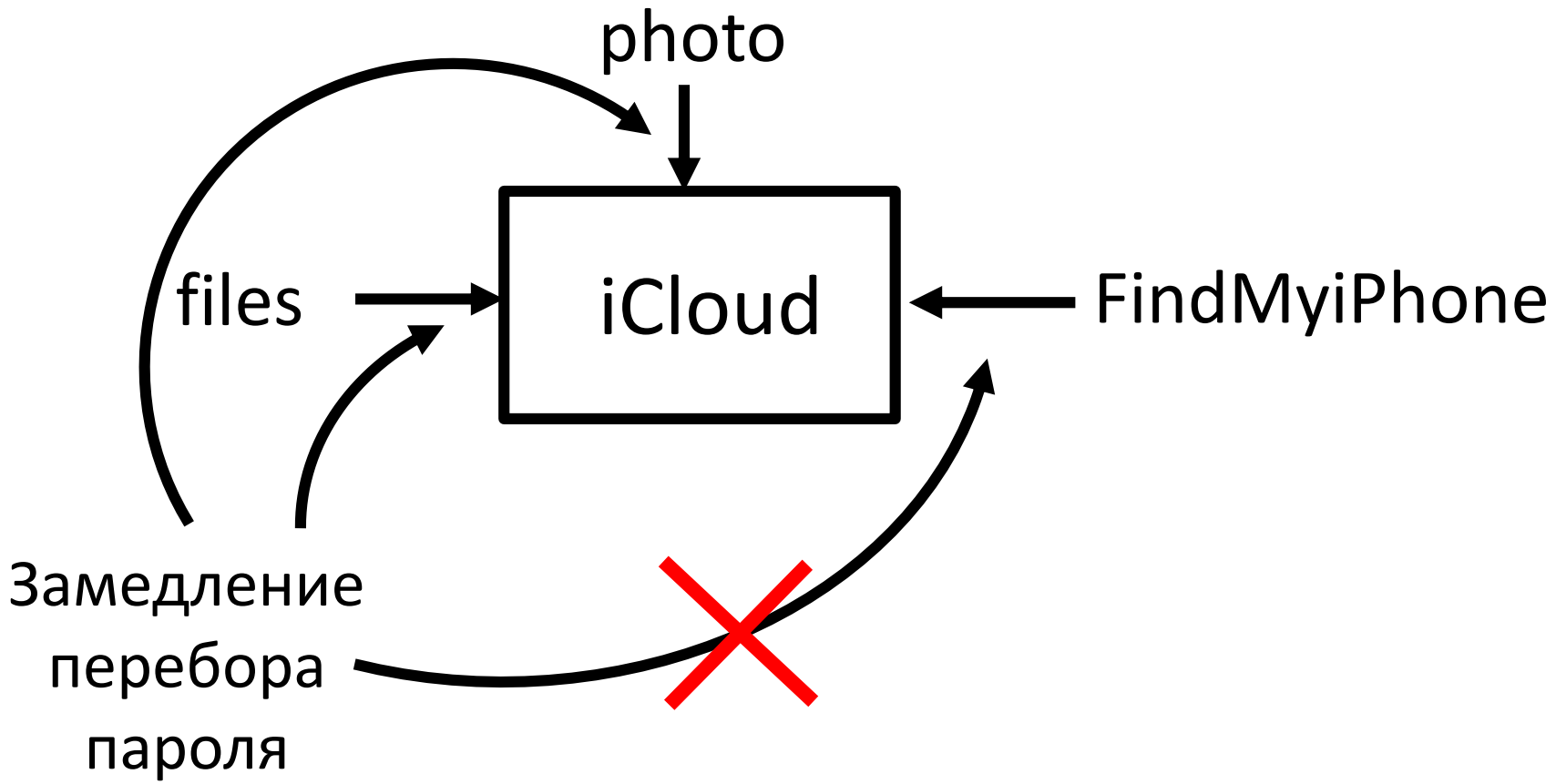
Механизмы

Уязвимости ПО и аппаратного обеспечения

Зачем этот курс, если есть МОЗИ?



Ограничения на перебор кредов



И Visa тоже

Главная / Новости

14:48 / 5 Декабря, 2016

Новый метод позволяет взломать карту Visa за 6 секунд

Теги: Visa, взлом, безопасность

Эксперты описали, как можно обойти защиту платежной системы при помощи метода распределенного перебора.

Исследователи из Ньюкаслского университета продемонстрировали новый метод, позволяющий подобрать номер, дату истечения срока действия и код безопасности карты Visa всего за 6 секунд. В исследовании, опубликованном в журнале IEEE Security & Privacy, эксперты описали , как можно обойти защиту при помощи так называемой атаки распределенного перебора (Distributed Guessing Attack).

Как?

1. Современные системы электронных платежей не фиксируют неудачные попытки платежа на разных сайтах. (можно бесконечно перебирать варианты для каждого из реквизитов карты, используя количество разрешенных сайтом попыток (обычно 10 или 20))

2. различные сайты запрашивают разные реквизиты для подтверждения покупки.

SSL и сложные строки в C

SSL сертификат содержит в себе что-то такое:

. . . 10 a m a z o n . c o m . . .

В памяти браузера это сохраняется как

. . . a m a z o n . c o m \0 . . .

Но что если мы получим сертификат на такой домен?

. . . 20 a m a z o n . c o m \0 x . f o o . c o m . . .

Уязвимости переполнения буфера

План лекций

1	Вводная лекция
2	Бинарная безопасность
3	Бинарная безопасность
4	Сетевая безопасность
5	Сетевая безопасность
6	HTTPS
7	Web security
8	Web security
9	Привилегии
10	Side-channel атаки
11	Аутентификация
12	Тестирование безопасности
13	Шифрование на практике
14	Анонимность в сети

Как получить зачёт?

№	Название	Баллы
1	Лаб. 1 (бин. без.)	13
2	Лаб. 2 (бин. без.)	13
3	Лаб. 3 (сетевая без.)	13
4	Тест 1	11
5	Лаб. 4 (web)	13
6	Лаб. 5 (привелегии)	13
7	Лаб. 6 (аутентификация)	13
8	Тест 2	11