РУТОКЕН

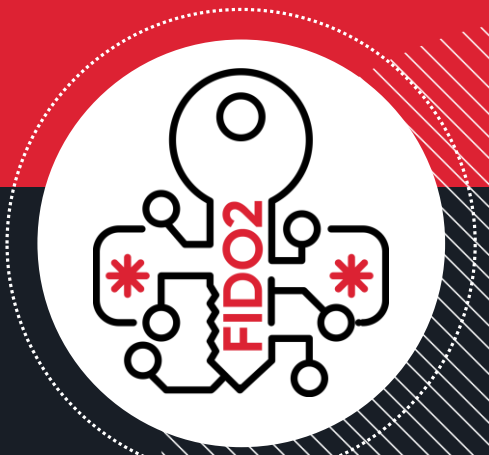
конференция РусКрипто

Обзор атак на протоколы технологии FIDO2

Эдуард Сабиров,
инженер-программист

Марина Скоробогатова,
аналитик

Евгений Мироненко,
руководитель отдела исследований

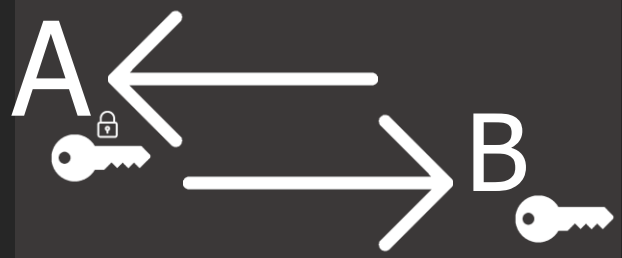


Что такое FIDO2?

FIDO2 – технология строгой беспарольной двухфакторной аутентификации

Аутентификатор | Клиент | Проверяющая сторона (RP)

Объективные причины: безопасность

Строгая аутентификация	Подтверждение действия пользователем	Несвязываемость аккаунтов пользователя	Неотказуемость
• Challenge-Response • Асимметричная криптография 	PIN-код, биометрия, нажатие кнопки 	Для каждого ресурса своя учетная запись (и ключевая пара) 	Пользователь видит что и зачем подписывает 

Объективные причины: безопасность

- Строгая аутентификация
- Подтверждение действия пользователем
- Несвязываемость аккаунтов пользователя
- Неотказуемость
- Учетные данные не подсмотреть
- Учетные данные не раскрыть
- Утечка из Аутентификатора не влияет на других пользователей
- Утечка из RP не влияет на другие RP
- Минимальное использование ПДн
- Аттестация характеристик Аутентификатора
- Возможность оценить уровень безопасности Аутентификатора
- Согласованность с механизмами безопасности ОС

Объективные причины: безопасность

- Строгая аутентификация
- Подтверждение действия пользователем
- Несвязываемость аккаунтов пользователя
- Неотказуемость
- Учетные данные не подсмотреть
- Учетные данные не раскрыть
- Утечка из Аутентификатора не влияет на других пользователей
- Утечка из RP не влияет на другие RP
- Минимальное использование ПДн
- Аттестация характеристик Аутентификатора
- Возможность оценить уровень безопасности Аутентификатора
- Согласованность с механизмами безопасности ОС
- Защита от DOS
- Защита от Replay-атак
- Защита от атак с использованием параллельных сессий
- Защита от проксирования входа пользователя

Обеспечение целей безопасности

Предположения безопасности

- Нет неизвестных слабостей Аутентификатора
- Механизмы безопасности на платформе пользователя
- Клиент: доверенное ПО
- Защищенный канал до веб-сервера (TLS)
- RP: доверенное ПО
- Время играет против безопасности

+

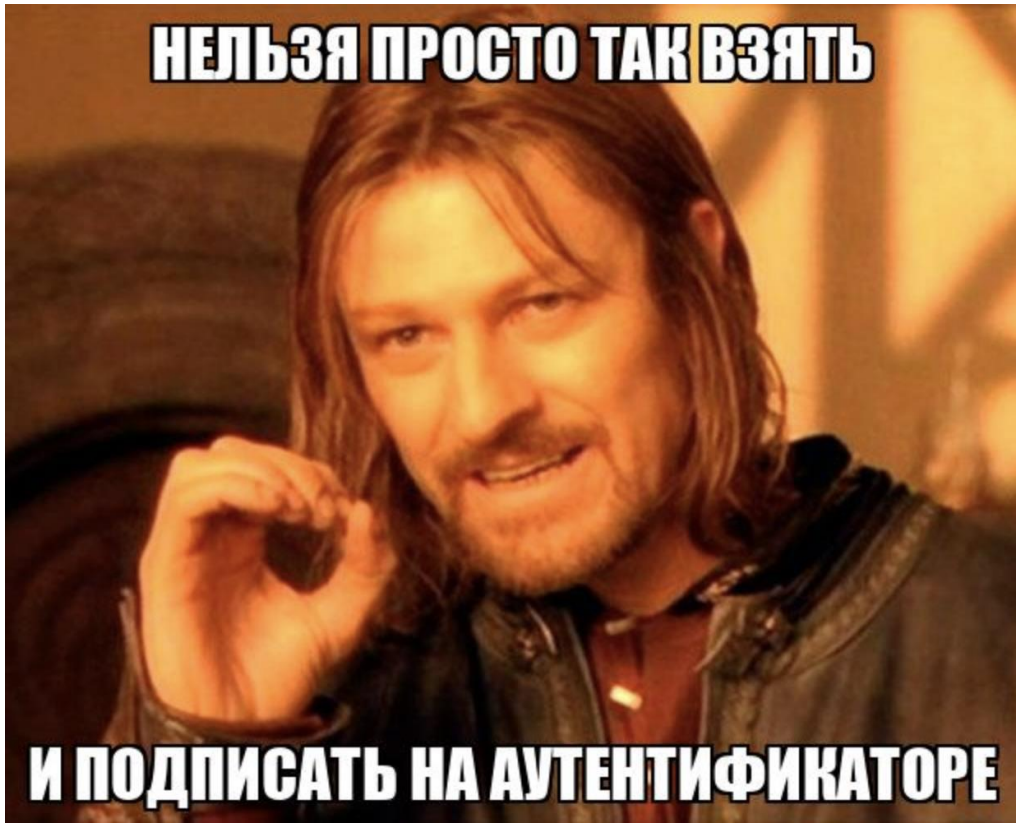
Механизмы безопасности FIDO2

Механизмы безопасности FIDO2

PIN/UV Auth Protocol	Подтверждение действия	Обнаружение чужого входа	Нераскрытие учетных данных
• Анонимный ECDH • PIN не в открытом виде • Связь выполнения UV с подписью	• Нажатие на кнопку • Диалоговые окна на Клиенте	Счетчик подписей	Аутентификатор не раскрывает учетные данные, относящиеся к другой RP

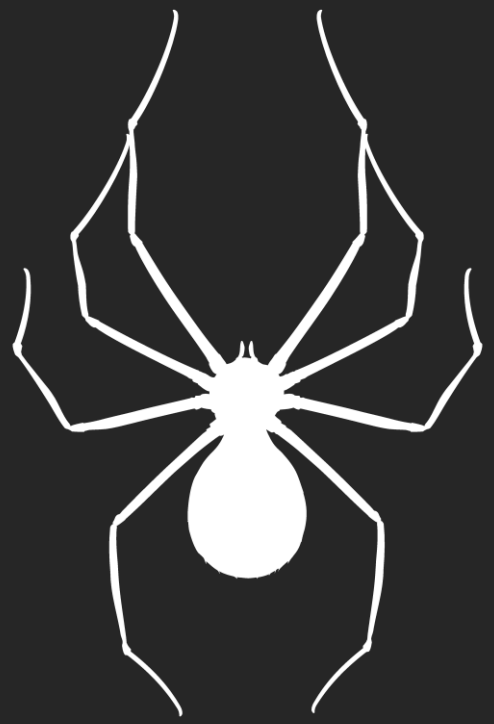
Атаки: причины и последствия

Нарушитель в канале Аутенти-тор-Клиент



- PIN/UV Auth Protocol:
  анонимный Диффи-Хеллман
  используя MITM получаем хэш ПИН
- Ждем authenticatorGetAssertion
- Заменяем на свой
  authenticatorGetAssertion
- ??? (Пользователь нажимает на кнопку)
- Profit!

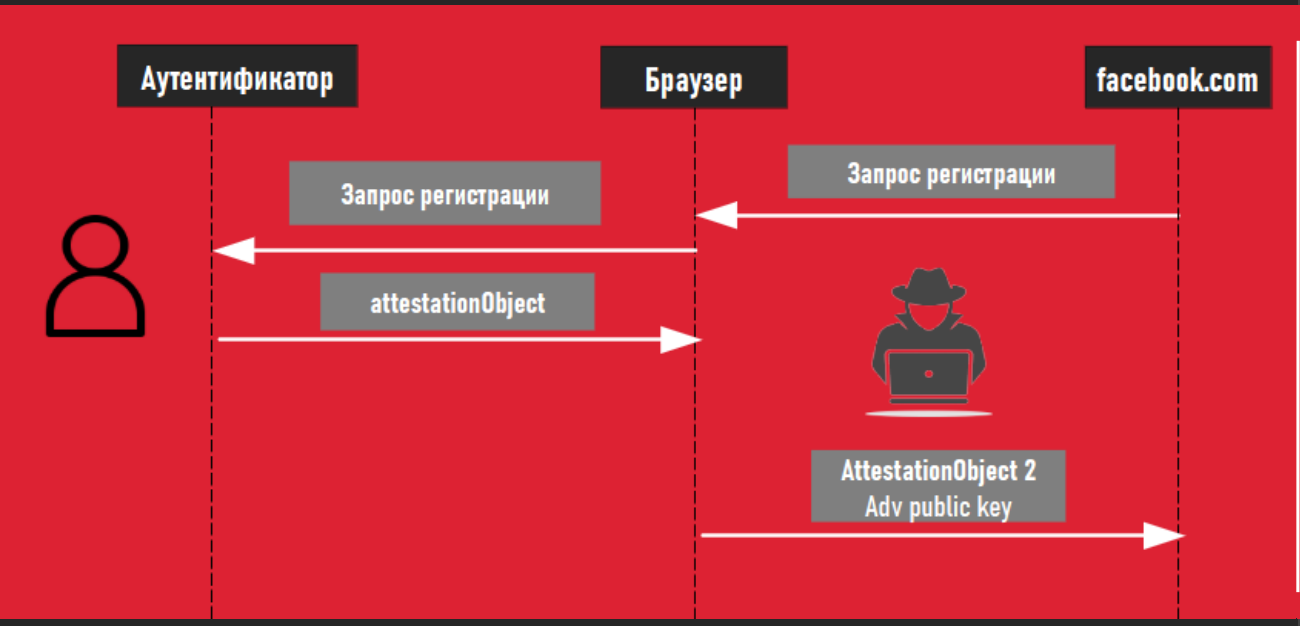
Браузерные расширения



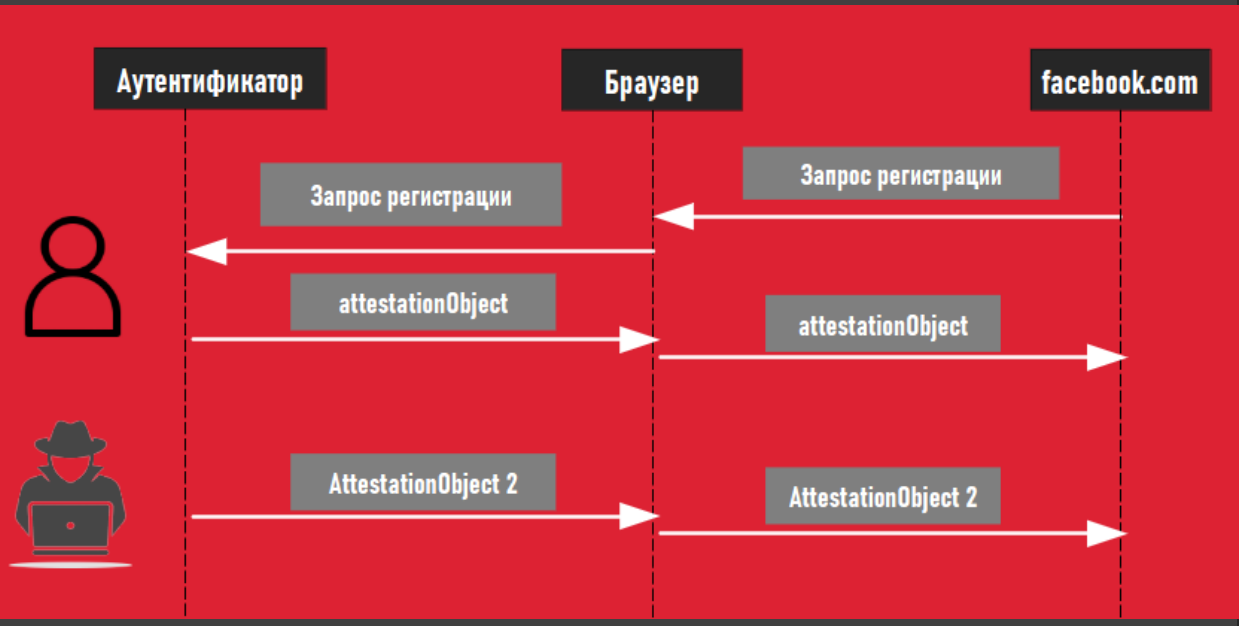
- Информирование о разрешениях при установке
- Предупреждение, если расширение будет иметь доступ на чтение/модификацию веб-страницы
- Известные истории про кражу паролей и финансовой информации

Браузерные расширения vs FIDO2

Регистрация вместо пользователя

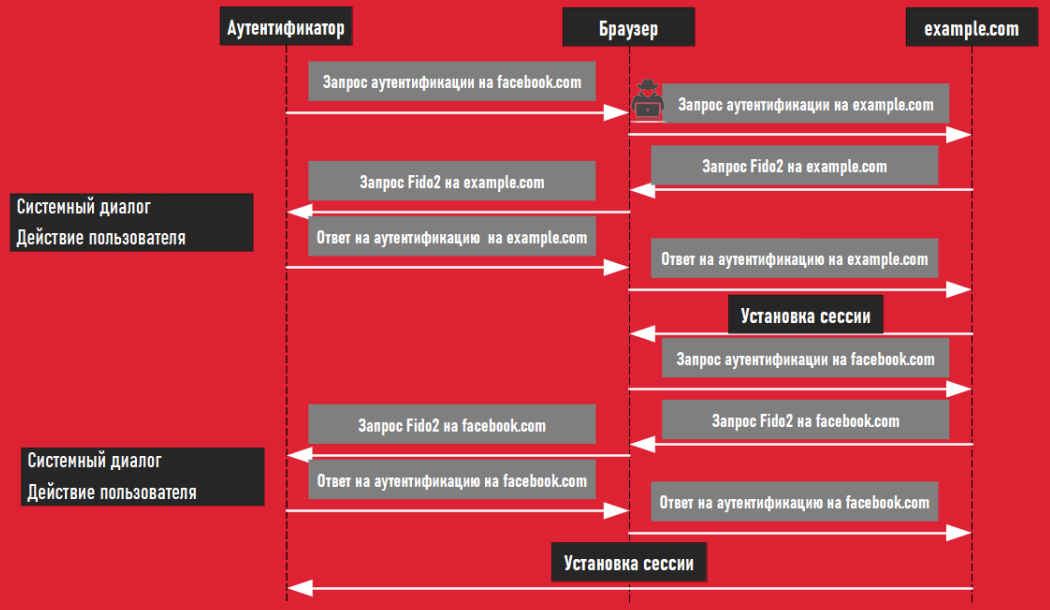


Регистрация вместе с пользователем

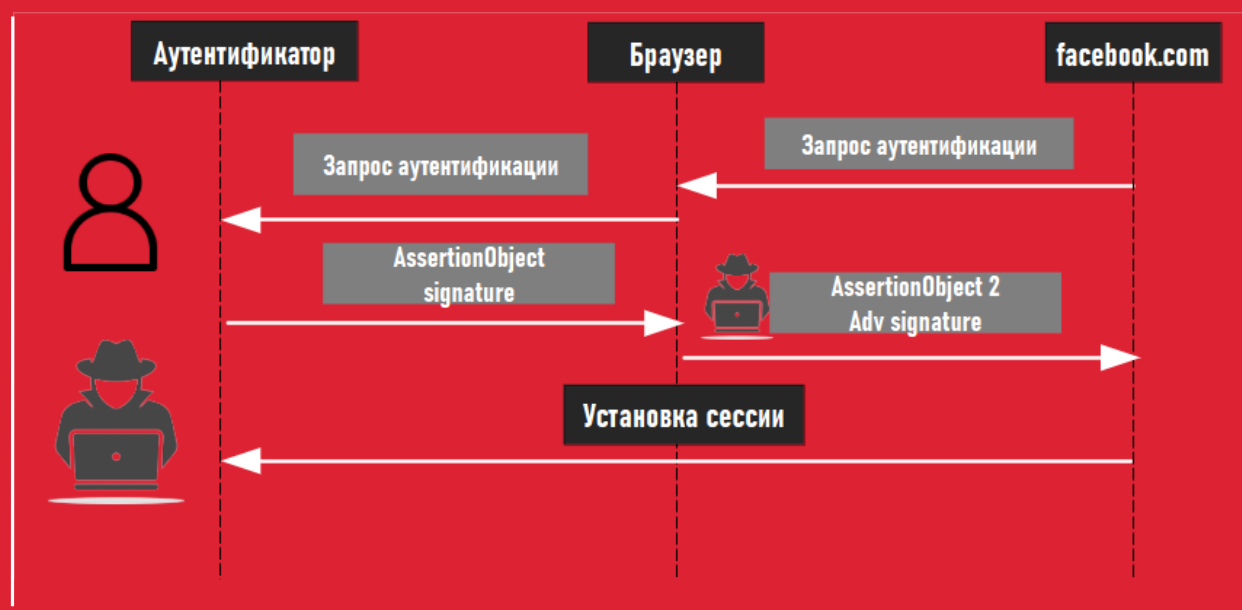


Браузерные расширения vs FIDO2

Параллельный вход на другой ресурс



Вход на ресурс вместо пользователя



Клонирование аутентификатора

12000$

- Специальное оборудование
- 10 часов на атаку
- Экспертные знания

Клонирование Google Titan

5$

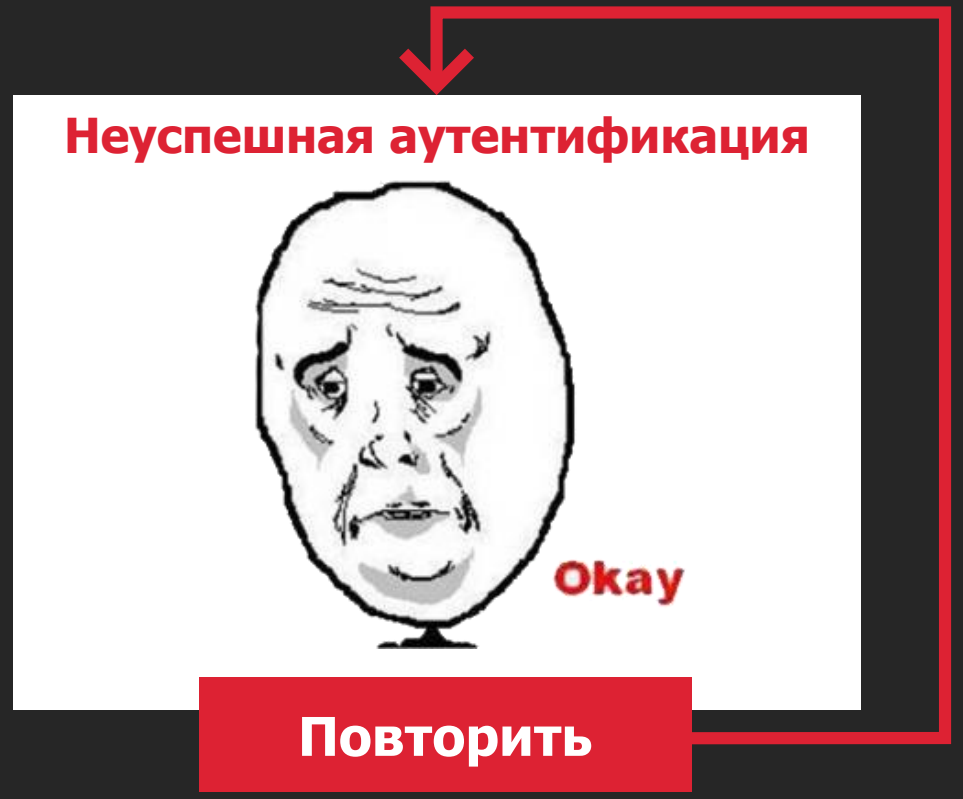
Power glitching attack

Клонирование Nordic nRF*

Клонирование аутентификатора vs FIDO2

1 Неинформативная ошибка от RP,
отсутствие блокировки аккаунта

Счетчики подписей		
Пользователь	Атакующий	RP
1337	1337	1337
Вход атакующего		
1337	**1337 –> 1338**	**1337->1338** ✓
Вход пользователя		
1337->1338	1338	1338 ✗
1338->1339	1338	**1338->1339**✓



1448	1337	1337
1448	**1337 –> 1338**	**1337->1338** ✓

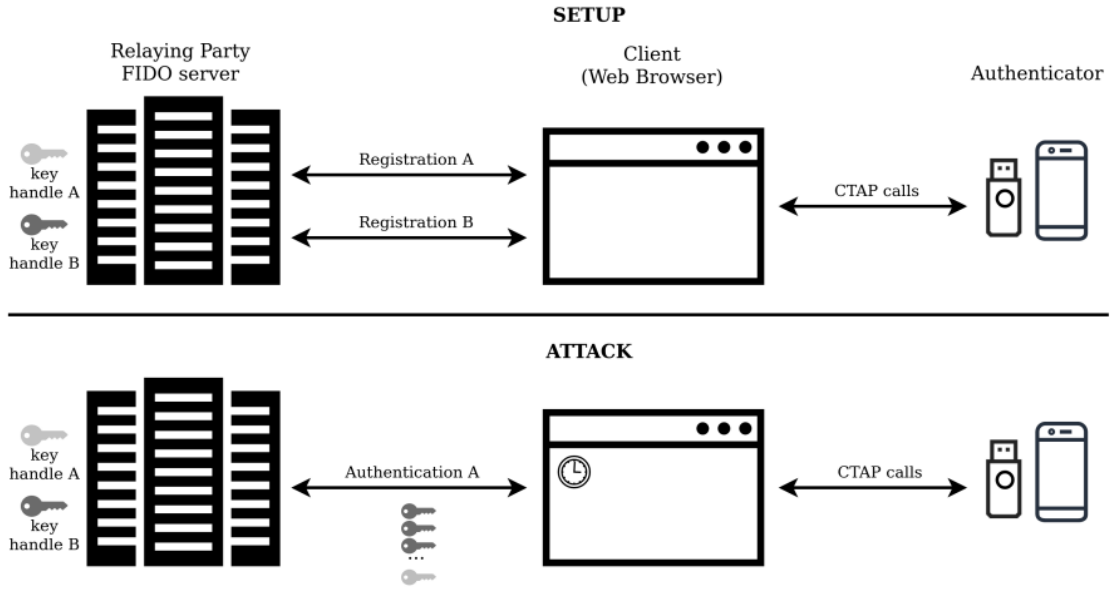
2 «Накрутка» счетчика пользователя
после клонирования аутентификатора

Связывание аккаунтов пользователя

Противник:

- Владеет сервисом A
- Пытается определить, соответствует ли ключ key_handle_B для службы B пользователю, аутентифицирующемуся с помощью дескриптора key_handle_A.

Атака успешна, в случае, если аутентификатору требуется различное время для обработки запроса, содержащего действительные и случайные дескрипторы ключей.



Подведем итоги

Банально:

- Обеспечение безопасности - комплексный подход
- Предположения безопасности - необходимый базис для этого
- Знание о возможных атаках позволяет оценить последствия инцидентов

Конкретно:

- Расширения браузера - зло!
- 2 фактора - не панацея, если встроены некорректно!
- Недостаточно внедрить, важно научить!

Вопросы

Контактная информация

Эдуард Сабиров

sabirov@aktiv-company.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru


30
КОМПАНИЯ
АКТИВ