eToken

Лазарев А.А. 5821

ПОЧЕМУ ИМЕННО USB-КЛЮЧИ?

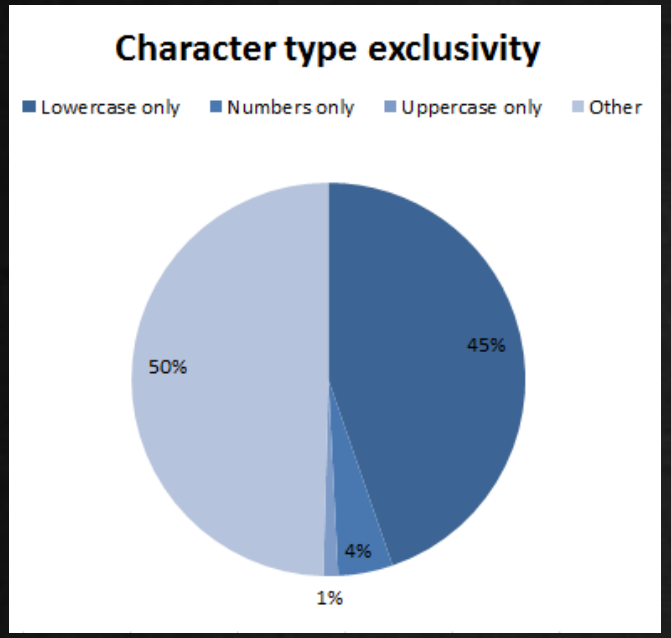
НЕМНОГО СТАТИСТИКИ ПО ПАРОЛЯМ ОТ SONY PICTURES ~~(ДА Я ЛЮБЛЮ ЦИФЕРКИ)~~

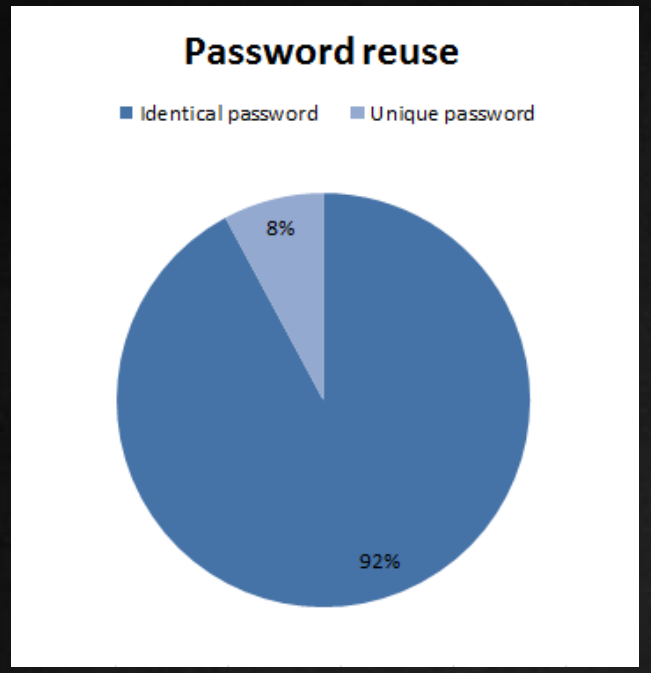
1% – ТОЛЬКО БУКВЫ ВЕРХНЕГО РЕГИСТРА

4% – ТОЛЬКО ЦИФРЫ

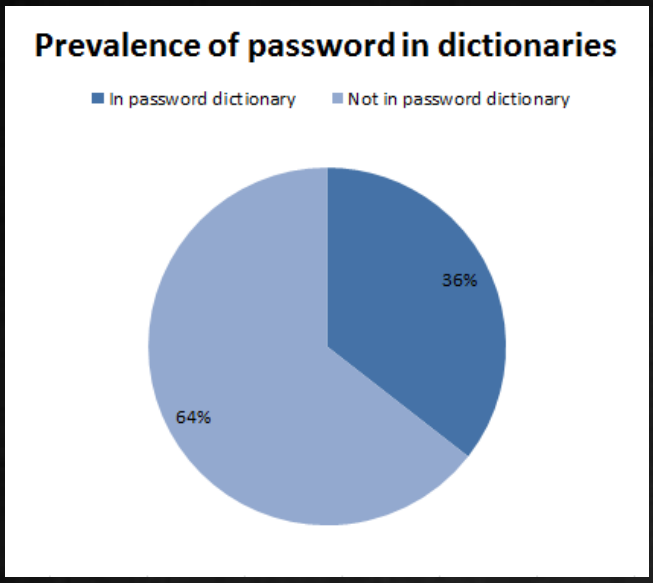
45% – ТОЛЬКО БУКВЫ НИЖНЕГО РЕГИСТРА

50% – ДРУГИЕ ВАРИАНТЫ





ЛИШЬ 8% ПОЛЬЗОВАТЕЛЕЙ ИСПОЛЬЗУЮТ УНИКАЛЬНЫЕ ПАРОЛИ...



А ЗДЕСЬ ВИДНО, ЧТО БОЛЬШЕ ТРЕТИ ПАРОЛЕЙ СОДЕРЖИТСЯ В СЛОВАРЕ

– СЛОВАРЬ ОБЩЕДОСТУПНЫЙ НА 1.7 МЛН

```
Hashmode: 0 - MD5

Speed.#1.........:  2096.5 MH/s (191.26ms) @ Accel:64 Loops:1024 Thr:1024 Vec:1

Hashmode: 100 - SHA1

Speed.#1.........:  1154.0 MH/s (348.10ms) @ Accel:64 Loops:1024 Thr:1024 Vec:1

Hashmode: 1400 - SHA2-256

Speed.#1.........:   428.0 MH/s (469.66ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1

Hashmode: 1700 - SHA2-512

Speed.#1.........:   166.8 MH/s (301.05ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
```

ЛЮБОЙ ЖЕЛАЮЩИЙ МОЖЕТ ПРОДЕЛАТЬ ТАКОЕ САМОСТОЯТЕЛЬНО НА СВОЁМ КОМПЬЮТЕРЕ.

НЕБОЛЬШОЕ ПОЯСНЕНИЕ:
MH\S = 1 000 000 HASH IN SECOND

ДА СУЩЕСТВУЕТ МНОЖЕСТВО УСЛОВНОСТЕЙ, НО ЭТО ЛИШЬ ПРИМЕР, ПРИЗВАННЫЙ ПОКАЗАТЬ НЕКИЕ НЕДОСТАТКИ ИСПОЛЬЗОВАНИЯ ПАРОЛЯ КАК СРЕДСТВО АУТЕНТИФИКАЦИИ.

```
Hashmode: 1500 - descrypt, DES (Unix), Traditional DES

Speed.#1.........:   178.2 MH/s (281.43ms) @ Accel:128 Loops:1024 Thr:64 Vec:1

Hashmode: 500 - md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5) (Iterations: 1000)

Speed.#1.........:   333.9 kH/s (291.21ms) @ Accel:16 Loops:1000 Thr:1024 Vec:1

Hashmode: 3200 - bcrypt $2*$, Blowfish (Unix) (Iterations: 32)

Speed.#1.........:     4179 H/s (134.15ms) @ Accel:16 Loops:16 Thr:12 Vec:1

Hashmode: 1800 - sha512crypt $6$, SHA512 (Unix) (Iterations: 5000)

Speed.#1.........:     6554 H/s (372.78ms) @ Accel:2 Loops:1024 Thr:1024 Vec:1
```

~~ЧЕСТНО ГОВОРЯ~~

~~ЛЮБЫЕ НЕДОСТАТКИ ПАРОЛЯ ПЕРЕКРЫВАЕТ СЛОЖНОСТЬ ОБЪЯСНЕНИЯ ТОГО, КАК РАБОТАТЬ С ТОКЕНОМ ПОЛЬЗОВАТЕЛЯМ~~

ДЛЯ ПРИМЕРА СКОРОСТЬ ПЕРЕБОРА ХЭШЕЙ ПАРОЛЕЙ

ЧТО ТАКОЕ ETOKEN?

- ETOKEN — ПЕРСОНАЛЬНОЕ УСТРОЙСТВО ДЛЯ АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ ДАННЫХ, АППАРАТНО ПОДДЕРЖИВАЮЩЕЕ РАБОТУ С ЦИФРОВЫМИ СЕРТИФИКАТАМИ И ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСЬЮ (ЭЦП).
- НА ТЕКУЩИЙ МОМЕНТ РАЗРАБОТЧИК ETOKEN — «ALADDIN KNOWLEDGE SYSTEMS», БЫЛА СНАЧАЛА ВЫКУПЛЕНА КОМПАНИЕЙ «SAFENET», А ДАЛЕЕ В ЕЁ СОСТАВЕ ОБЪЕДИНИЛАСЬ С КОМПАНИЕЙ, «THALES GROUPS». В СВЯЗИ С ЧЕМ В ОПИСАНИИ МОЖЕТ ФИГУРИРОВАТЬ ИМЕННО «THALES», КАК ТЕКУЩИЙ ДИСТРИБЬЮТОР ПРОДУКЦИИ ETOKEN.

КАК ЭТО РАБОТАЕТ

ДЛЯ РАБОТЫ ИСПОЛЬЗУЕТСЯ ОДНОСТОРОННЯЯ ФУНКЦИЯ (НАЗОВЁМ ЕЁ F). СИСТЕМА ОДНОРАЗОВЫХ ПАРОЛЕЙ НАЧИНАЕТ РАБОТАТЬ ОТ НАЧАЛЬНОГО ЧИСЛА S, ЗАТЕМ ГЕНЕРИРУЕТ ПАРОЛИ.

$$F(S), F(F(S)), F(F(F(S))), \ldots$$

СТОЛЬКО РАЗ, СКОЛЬКО НЕОБХОДИМО. ЕСЛИ ИЩЕТСЯ БЕСКОНЕЧНАЯ СЕРИЯ ПАРОЛЕЙ, НОВОЕ НАЧАЛЬНОЕ ЧИСЛО МОЖЕТ БЫТЬ ВЫБРАНО ПОСЛЕ ТОГО, КАК РЯД ДЛЯ S ОКАЗЫВАЕТСЯ ИСЧЕРПАННЫМ. КАЖДЫЙ ПАРОЛЬ РАСПРЕДЕЛЯЕТСЯ В ОБРАТНОМ ПОРЯДКЕ, НАЧИНАЯ С $F(F(\ldots F(S))\ldots)$, ЗАКАНЧИВАЯ $F(S)$.

ЕСЛИ ЗЛОУМЫШЛЕННИКУ УДАЁТСЯ ПОЛУЧИТЬ ОДНОРАЗОВЫЙ ПАРОЛЬ, ОН МОЖЕТ ПОЛУЧИТЬ ДОСТУП ТОЛЬКО НА ОДИН ПЕРИОД ВРЕМЕНИ ИЛИ ОДНО СОЕДИНЕНИЕ, НО ЭТО СТАНОВИТСЯ БЕСПОЛЕЗНЫМ, КОГДА ЭТОТ ПЕРИОД ЗАКОНЧИТСЯ. ЧТОБЫ ПОЛУЧИТЬ СЛЕДУЮЩИЙ ПАРОЛЬ В ЦЕПОЧКЕ ИЗ ПРЕДЫДУЩИХ, НЕОБХОДИМО НАЙТИ СПОСОБ ВЫЧИСЛЕНИЯ ОБРАТНОЙ ФУНКЦИИ.

ЭТО ВСЁ ETOKEN

USB-КЛЮЧ С ГЕНЕРАЦИЕЙ ПАРОЛЯ

СМАРТ КАРТА

USB-КЛЮЧ

ТОКЕН ОТР

VPN

CHECK POINT VPN, SECUREMOTE И VPN SECURECLIENT ПОДДЕРЖИВАЮТ АУТЕНТИФИКАЦИЮ, ОСНОВАННУЮ НА ИСПОЛЬЗОВАНИИ СЕРТИФИКАТОВ ОТКРЫТОГО КЛЮЧА И ЗАКРЫТЫХ КЛЮЧЕЙ В ПАМЯТИ СМАРТ-КАРТ И ИХ АНАЛОГОВ.

ПРИ НАЛИЧИИ НА КЛИЕНТСКОМ КОМПЬЮТЕРЕ ДРАЙВЕРА ДЛЯ УСТАНОВЛЕНИЯ VPN-СОЕДИНЕНИЯ МОЖНО ИСПОЛЬЗОВАТЬ ETOKEN, В ПАМЯТИ КОТОРОГО ИМЕЕТСЯ ЗАКРЫТЫЙ КЛЮЧ И СООТВЕТСТВУЮЩИЙ ЕМУ СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА, ДАЮЩИЙ ВЛАДЕЛЬЦУ ПРАВО ПОДКЛЮЧЕНИЯ.

eToken Network Logon

eToken Network Logon — разработанное компанией Aladdin Knowledge Systems приложение, позволяющее сохранять имя пользователя, пароль и имя домена Windows в памяти eToken и затем использовать eToken в процессе аутентификации.

При назначении нового пароля и смене пароля может использоваться встроенный в eToken Network Logon датчик случайных чисел, в результате чего пользователь может даже не знать свой пароль и, следовательно, не иметь возможности входить в систему без eToken.

ETOKEN SAFEDATA И «КРИПТО БД»

ETOKEN SAFEDATA И «КРИПТО БД» — СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ), РАЗРАБОТАННЫЕ РОССИЙСКОЙ КОМПАНИЕЙ «АЛАДДИН Р. Д.». ПОЗВОЛЯЮТ ШИФРОВАТЬ ДАННЫЕ В ОТДЕЛЬНЫХ КОЛОНКАХ ТАБЛИЦ БАЗ ДАННЫХ ORACLE. ПРИ ЭТОМ ПАРЫ КЛЮЧЕЙ ШИФРОВАНИЯ ХРАНЯТСЯ В БАЗЕ ДАННЫХ И В ПАМЯТИ ETOKEN.

В РЕЗУЛЬТАТЕ ДЛЯ ОБРАЩЕНИЯ К ЗАШИФРОВАННЫМ ДАННЫМ ПОЛЬЗОВАТЕЛИ ДОЛЖНЫ ЗАДЕЙСТВОВАТЬ СВОИ ETOKEN, В ПАМЯТИ КОТОРЫХ ХРАНЯТСЯ ЗАКРЫТЫЕ КЛЮЧИ, СООТВЕТСТВУЮЩИЕ ОТКРЫТЫМ КЛЮЧАМ, С ПОМОЩЬЮ КОТОРЫХ ЗАШИФРОВАНЫ КЛЮЧИ ШИФРОВАНИЯ.

ОТЛИЧИЕ SAFEDATA ОТ «КРИПТО БД»:

ETOKEN SAFEDATA:

- ДАННЫЕ: DES, TRIPLE DES, AES И RC4
- КЛЮЧИ ШИФРОВАНИЯ: RSA;

«КРИПТО БД»:

- ДАННЫЕ: ГОСТ 28147-89 И RFC 4357
- КЛЮЧИ ШИФРОВАНИЯL: ГОСТ Р 34.10-2001 И RFC 4490;

ORACLE

~~ЧИТАЙ ИНОСТРАННЫЙ 1С~~

ETOKEN SECURLOGON ДЛЯ ORACLE — РАЗРАБОТАННОЕ КОМПАНИЕЙ «АЛАДДИН Р. Д.» ПРОГРАММНОЕ СРЕДСТВО, В КОТОРОМ ПОДДЕРЖИВАЕМЫЙ В ORACLE 8I DATABASE RELEASE 3 (8.1.7) ENTERPRISE EDITION И ПОЗДНЕЙШИХ ВЕРСИЯХ СУБД ORACLE МЕХАНИЗМ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ СЕРТИФИКАТОВ ОТКРЫТОГО КЛЮЧА И ЗАКРЫТЫХ КЛЮЧЕЙ РЕАЛИЗОВАН С ПРИМЕНЕНИЕМ ETOKEN В КАЧЕСТВЕ КЛЮЧЕВОГО НОСИТЕЛЯ. ПОМИМО ОТДЕЛЬНОГО ПРОДУКТА, ETOKEN SECURLOGON ДЛЯ ORACLE ПРЕДСТАВЛЯЕТ СОБОЙ КОМПОНЕНТ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) ETOKEN SAFEDATA И «КРИПТО БД», УСТАНАВЛИВАЕМЫЙ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ ПОЛЬЗОВАТЕЛЕЙ ЭТИХ СКЗИ.