конференция РусКрипто

И ещё раз о корректности встраивания

Хенкин Петр

ЗАО «Перспективный мониторинг»

Зачем это нужно… common knowledge

- **Высокий риск потери устройства**
  - Каждую минуту в США крадут **113** телефонов
  - Каждый день в Лондоне крадут **314** телефонов
  - **120 000** телефонов забывают в такси Чикаго
- **Угроза НСД к устройству и данным**
  - Родственники/дети
  - Инсайд
  - Вендоры (spyware)
- **Январь 2013 украден телефон израильской чиновницы с секретными данными**

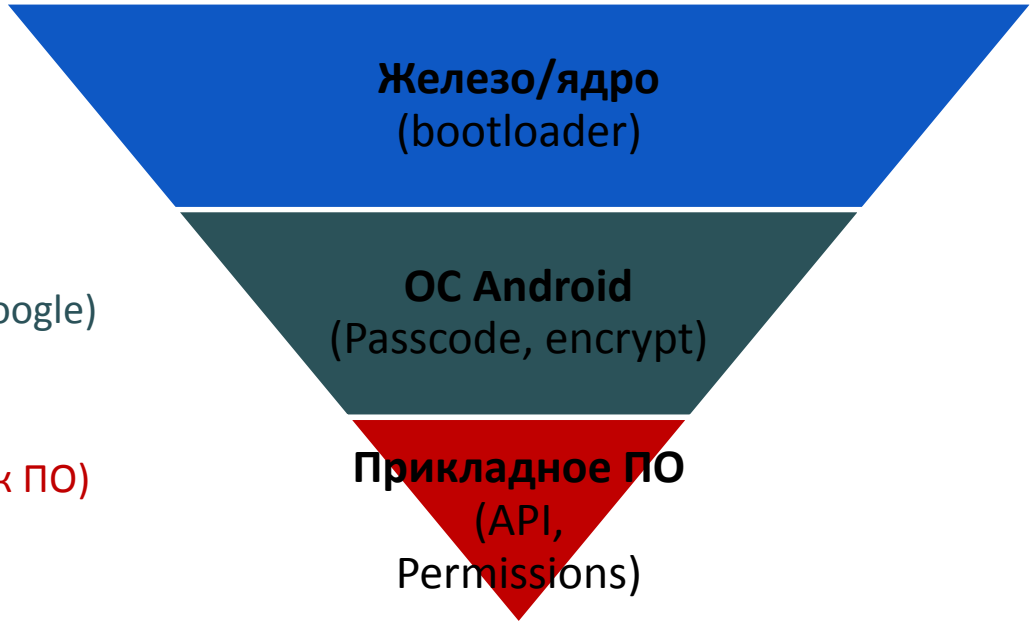
NATIONAL Mobile Phone Crime Unit

http://www. norton.com

http://www.bbc.co.uk/news/uk-england-london-21018569

С(К?)ЗИ в мобильных устройствах

- Hardware Security Features (железо, вендор)
- Secure Bootloader (S-ON, вендор)
- System Software Security (обновления, вендор)
- Passcode Protection (система, Google + вендор)
- Mobile Device Management (вендор)
- Remote Wipe (Google)
- Runtime Process Security (система, Google)
  - Sandbox,
  - APIs
- Application Code Signing (разработчик ПО)
- SSL, TLS, VPN (Google + вендор)
- Settings (Google)
  - Permissions / Restrictions
  - Configurations
- File Data Protection (разработчик ПО)



Сценарии использования

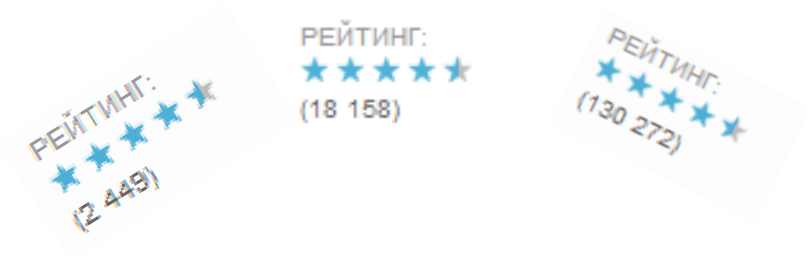
- **Защита устройства**
  - passcode
  - ✖ Инсайд
  - ✖ Вредоносное ПО на устройстве
  - ✖ Съемные носители
- **Штатное шифрование**
  - Шифрование памяти/SD-карты
  - ✖ Редко поддерживается прошивкой
  - ✖ Вредоносное ПО на устройстве
  - ✖ Инсайд
- **Дополнительное ПО для шифрования**
  - Шифрование файлов/контактов
  - Защищенная переписка
  - ✖ ….

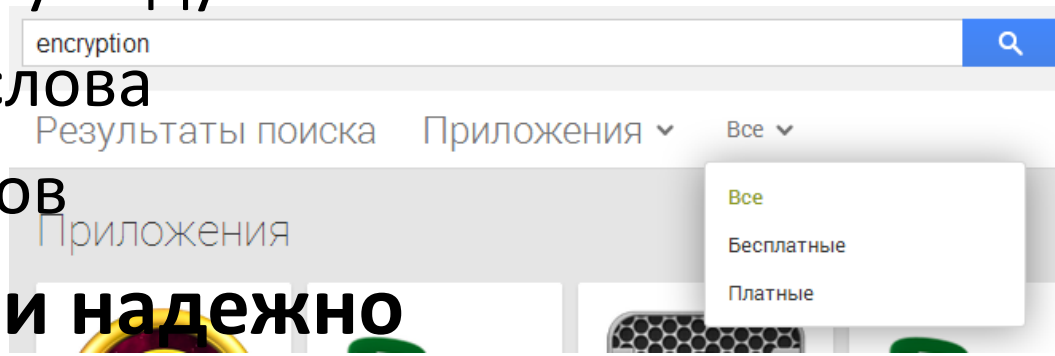
Прикладное ПО нас спасет!

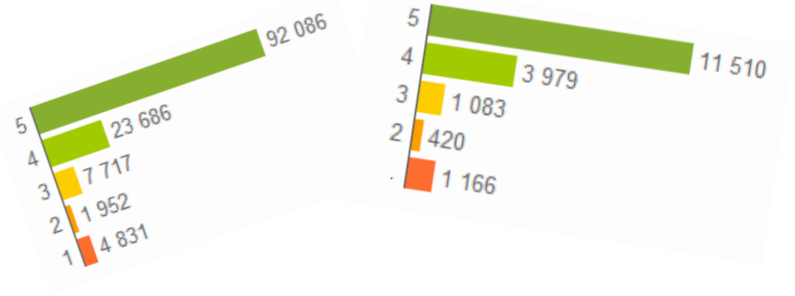
- **Огромное количество приложений**
  - “encryption” более 300 приложений
  - “protect data” аналогично
- **Многообещающе и надежно**
  - «industry standard AES encryption»
  - «Keep confidential information safe using 256bit AES algorithm»
  - «Представьте, что ваш телефон потерян или украден, при этом Вы можете быть спокойны»

Проблема выбора

- **Огромное количество приложений**
  - Выбор по внешнему виду
  - SEO на ключевые слова
  - Отсутствие фильтров
- **Многообещающе и надежно**
  - Отзывы, звезды, тесты
  - Реальная безопасность?







Предположим что…

- **Злоумышленник может**
  - Получить доступ к устройству (украден? забыт? вирус?)
  - Получить доступ к OS телефона
- **Злоумышленник хочет**
  - доступ к конфиденциальным данным – чтение:
    - Заметки
    - Файлы
    - Учетные данные

Выбор приложений

- Google play only
- Free-app
- Не менее 100 тыс. скачиваний
- Поиск по ключевым словам:
  - Encrypt
  - Protect files
  - Protect images

Два класса:

1. шифрование текста и учетных данных
2. Шифрование и сокрытие файлов (user-friendly)

Методы исследований

- Функциональность приложения (user-mode)
- Тестовые данные
- Анализ External Storage (SD)
- Анализ Internal Storage (data/data/…):
  - SQLite Databases
  - Shared Preferences (XML)

- **без реверсинга** APK файла приложения
- 12 проблемных приложений из 20
- Общее число установок более **12 млн**.

Шифрование текста, учетных данных

- Keeper
  - Установок 1 000 000–5 000 000
- Secret Safe lite
  - Установок 100 000 - 500 000
- Password Safe lite
  - Установок 100 000 - 500 000
- Safe Notes
  - Установок 500 000 - 1 000 000

Много приложений со скачиваниями
1 000 - 10 000

Keeper

- Установок 1 000 000 – 5 000 000

Хранение данных, зашифрованных с помощью 256-разрядного алгоритма AES

Генерация ключей шифрования по стандарту PBKDF2

- В БД - md5 хэш от пароля
- Хэш пароля без соли
- Поле не проверяется при запуске ПО

b59c67bf196a4758191e42f76670ceba

00000000000000000000000000000000

*хэш удален в текущей версии

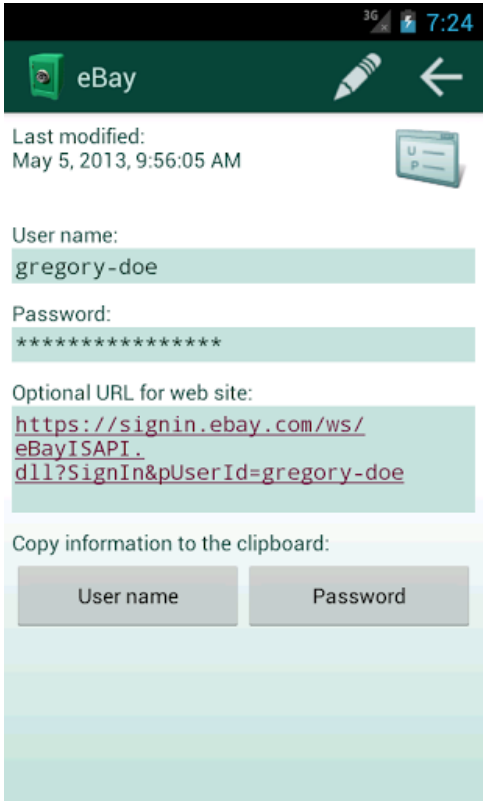
Secret Safe lite

- Установок 100 000 - 500 000

шифрование данных с 256-bit ключом основано на комбинировании SHA-256, AES и Twofish алгоритмах, известных как наиболее безопасных и сложных алгоритмов смешивания и шифрования данных, доступных сегодня в криптографии

пароль шифрования не связан с главным паролем, для предотвращения попыток взлома пароля

- Ключ - однократный md5 хэш от пароля
- Хэш пароля без соли
- AES в режиме ECB



*хэш исправлен в текущей версии

Password Safe lite

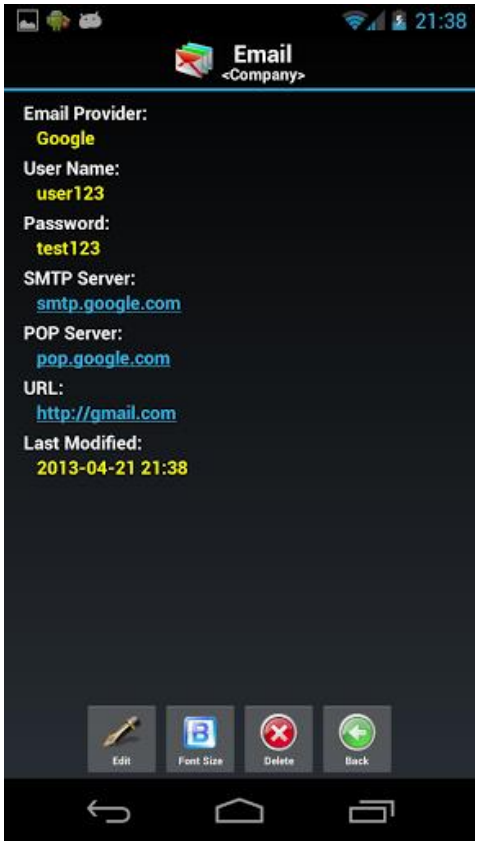
- Установок 100 000 - 500 000

Encrypt password data using 256bit AES algorithm

- Шифрование записей БД на фиксированном ключе
- Хэш в XML файле

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
    <boolean value="true" name="masterkey_encrypted"/>
    <string name="master password">A5A46C34ECE9BD47DECCC76BCE8C8A7F</string>
    <long value="1369052260887" name="timeout_track"/>
    <string name="hint"/>
  </map>
```

- Зачем ломать если можно заменить?

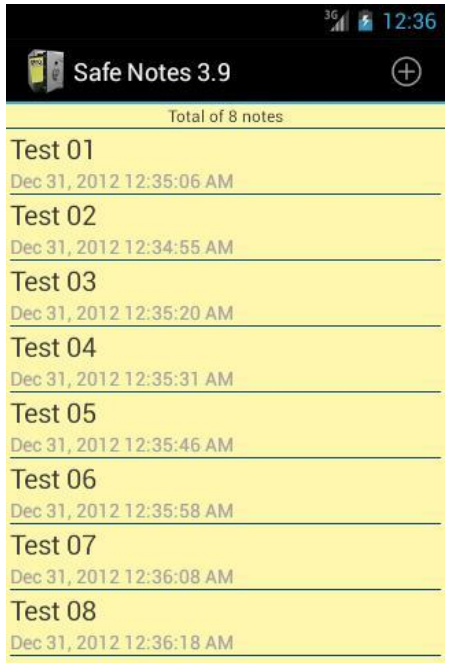


Safe Notes

- Установок 500 000 – 1 000 000

All data encrypted (128 bit encryption)

- Шифрование записей БД на фиксированном ключе
- БД на SD
- Ключ шифруется паролем в БД
- Соли нет
- Заменяем поле с паролем в БД




```
00001B70  00 00 00 00 00 00 81 07   01 07 00 4D 81 4D 0D 0D          M M
00001B80  37 38 43 32 34 38 42 43   30 46 39 39 34 35 44 39  78C248BC0F9945D9
00001B90  35 30 41 39 43 41 36 32   46 32 46 37 46 33 36 46  50A9CA62F2F7F36F
00001BA0  36 35 36 30 46 46 36 35   36 35 45 32 30 36 34 33  6560FF6565E20643
00001BB0  35 33 35 45 46 42 43 45   33 45 44 44 37 39 36 38  535EFBCE3EDD7968
00001BC0  31 46 37 30 39 38 31 31   41 42 42 34 32 32 31 35  1F709811ABB42215
00001BD0  42 31 31 46 43 44 33 39   45 36 31 42 38 36 42 46  B11FCD39E61B86BF
00001BE0  32 42 36 31 45 30 39 41   37 34 41 36 41 41 41 44  2B61E09A74A6AAAD
00001BF0  31 30 37 45 45 36 38 37   35 38 35 39 38 42 39 44  107EE68758598B9D
```

Типовые проблемы

- Использование фиксированных ключей
- Слабые алгоритмы хэширования
- Применение хэшей а не KDF функций
- формирование ключа непосредственно из пароля
- Слабые режимы шифрования

Шифрование/сокрытие файлов

- File hide expert
  - Установок 1 000 000 – 5 000 000
- Hide it pro
  - Установок 5 000 000–10 000 000
- Smart lock free
  - Установок 1 000 000 – 5 000 000
- Vault-hide
  - Установок 10 000 000–50 000 000

Популярны для хранения личных данных

Меньше миллиона не рассматриваем ☺

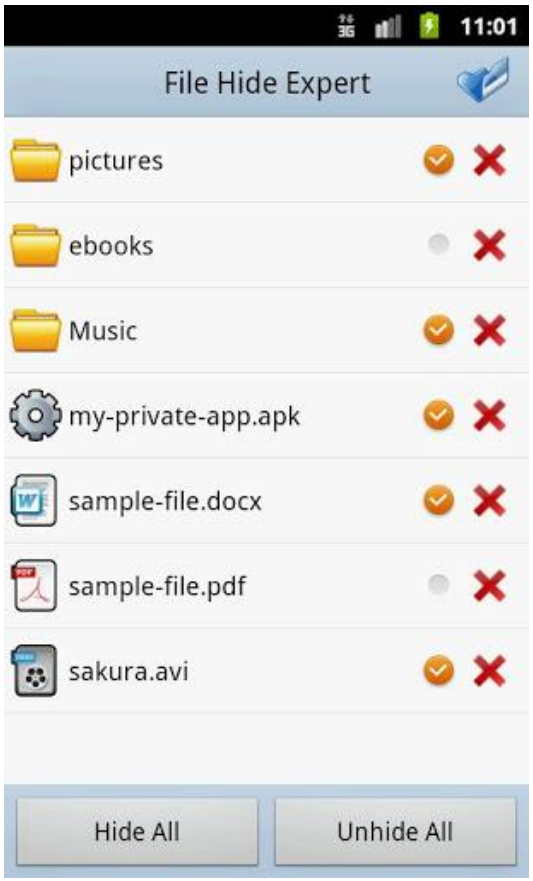
File hide expert

- Установок 1 000 000 – 5 000 000

Password protection to protect the app itself to prevent others from using this app

- Скрытая папка .hermit
- Файлы перемещаются в свою файловую БД на SD (переименованы)
- Пароль в plaintext

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
    <string name="file_list_fontsize">16</string>
    <string name="password_true_value">1111</string>
    <string name="file_sort">0</string>
    <boolean name="check_password_key" value="true"/>
    <string name="browser_list_fontsize">17</string>
  </map>
```



Hide it pro

- Установок 5 000 000 – 10 000 000

Built in encryption tool(with military standard 256-bit AES encryption) to secure your most important files

Two lock screen options viz Pin and Password

- маскировка под ПО Audio Manager
- Скрытая папка на SD в SD/ProgramData/Android/Lang/.fr
- Создает мнимую структуру каталогов в SD/ProgramData/Android
- Шифрование есть, завязано на мастер-пароле
- В xml пароль в открытом виде

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
    <int value="1" name="launchCount"/>
    <boolean value="true" name="setupCompleted"/>
    <string name="slideshowDuration">5000</string>
    <string name="slideshowAnimation">fade</string>
    <string name="lockType">pin</string>
    <string name="pin">1111</string>
```

Smart lock free

- Установок 1 000 000 – 5 000 000

Smart Lock provides your privacy in mobile phone from others

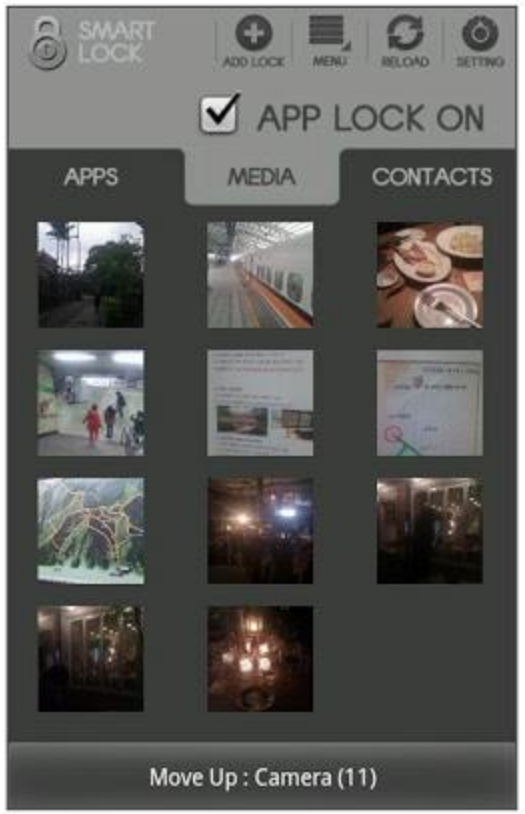
Lock media files in Gallery

- Приложения/контакты/медиа
- Скрытая папка на SD .smart_lock
- Шифрования нет, свой формат

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	33	30	7C	2F	6D	6E	74	2F	73	64	63	61	72	64	2F	56	30|/mnt/sdcard/V
00000010	4B	2F	74	49	4F	59	46	54	57	30	4C	53	38	2E	6A	70	K/tIOYFTW0LS8.jp
00000020	67	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	g
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000003F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000400	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48	яШяа JFIF H
00000410	00	48	00	00	FF	DB	00	43	00	04	03	03	04	03	03	04	H яЫ C

- В xml хэш md5 от пароля

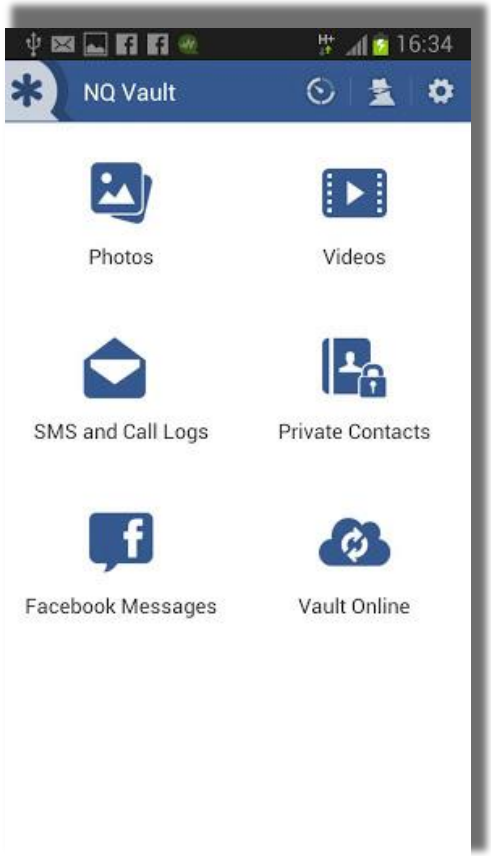
```
<boolean value="true" name="preferences.service.remote.running.use"/>
<string name="preferences.appprotector.passwd">b59c67bf196a4758191e42f76670ceba</string>
<string name="preferences.appprotector.passwd.hint">Initial PINs is 0000.</string>
<boolean value="false" name="preferences.is.language.ko"/>
<long value="1369063626944" name="preferences.install.time"/>
<boolean value="true" name="preferences.screen.portrait"/>
<string name="preferences.appprotector.install.app.list.target">DOWNLOAD</string>
```



Vault-hide

- Установок 10 000 000 – 50 000 000

Photos & Videos will be encrypted and only viewable in Vault when you enter the correct password



- Более 10 млн установок!
- Обещано Encryption
- Папки на SD в SD/SystemAndroid/Data/…
- В своей БД все пути и имена
- От пароля зависят пути
- Файлы зашифрованы: ……

Vault-hide

- Только заголовок
- Циклический байт
- Зависит от пароля

- Стандарты для файлов

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	BF	98	BF	A0	40	50	0A	06	09	06	40	41	41	41	40	08
00000010	40	08	40	40	BF	9B	40	03	40	44	43	43	44	43	43	44
00000020	44	43	44	45	44	44	45	46	4A	47	46	46	46	46	4D	49
00000030	4A	48	4A	4F	4D	50	50	4F	4D	4F	4E	51	53	58	54	51
00000040	52	57	52	4E	4F	55	5C	55	57	59	59	5B	5B	5B	50	54
00000050	5D	5F	5D	5A	5F	58	5A	5B	5A	BF	9B	40	03	41	44	45
00000060	45	46	45	46	4C	47	47	4C	5A	51	4F	51	5A	5A	5A	5A
00000070	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A	5A
00000080	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A
00000090	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	FF	C0
000000A0	00	11	08	02	5C	01	9B	03	01	22	00	02	11	01	03	11
000000B0	01	FF	C4	00	1D	00	00	01	04	03	01	01	00	00	00	00
000000C0	00	00	00	00	00	00	05	00	02	06	07	03	04	08	01	09
000000D0	FF	C4	00	5C	10	00	01	03	02	02	04	07	08	0D	07	09

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48
00000010	00	48	00	00	FF	DB	00	43	00	04	03	03	04	03	03	04
00000020	04	03	04	05	04	04	05	06	0A	07	06	06	06	06	0D	09
00000030	0A	08	0A	0F	0D	10	10	0F	0D	0F	0E	11	13	18	14	11
00000040	12	17	12	0E	0F	15	1C	15	17	19	19	1B	1B	1B	10	14
00000050	1D	1F	1D	1A	1F	18	1A	1B	1A	FF	DB	00	43	01	04	05
00000060	05	06	05	06	0C	07	07	0C	1A	11	0F	11	1A	1A	1A	1A
00000070	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A
00000080	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A
00000090	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	1A	FF	C0
000000A0	00	11	08	02	5C	01	9B	03	01	22	00	02	11	01	03	11
000000B0	01	FF	C4	00	1D	00	00	01	04	03	01	01	00	00	00	00
000000C0	00	00	00	00	00	00	05	00	02	06	07	03	04	08	01	09
000000D0	FF	C4	00	5C	10	00	01	03	02	02	04	07	08	0D	07	09

Типовые проблемы

– Хранение паролей в открытом виде

– Protection vs Encryption не просто так!

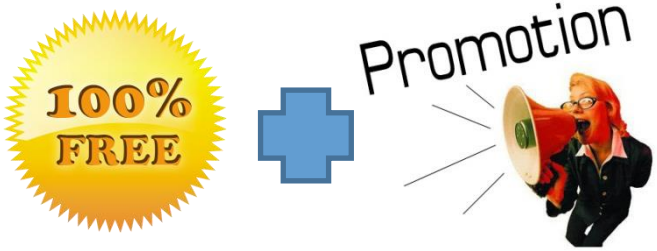
– Псевдокриптография

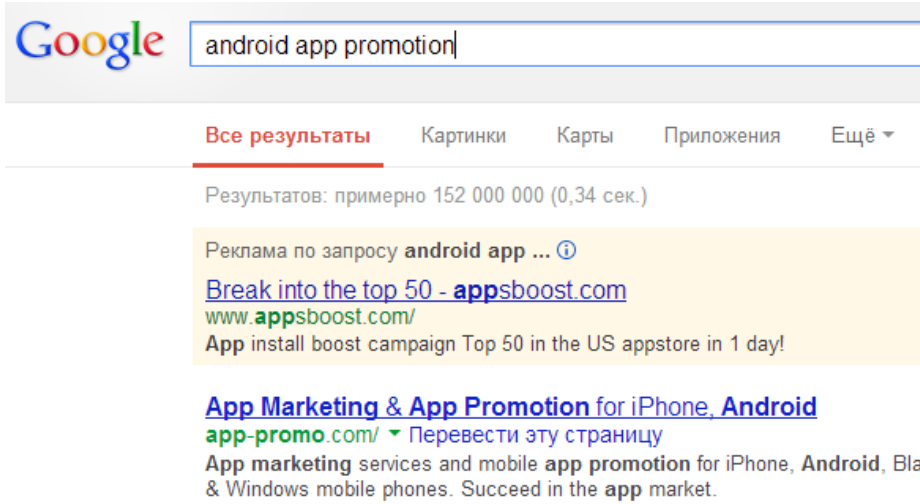
– Только механизмы скрытых папок

– Слабые алгоритмы хэширования

Шифрование? Really?

- **Правильная криптография**
  - Android Cryptography API, WIKI
  - Bouncy Castle, crypto extensions и др.
- **Мнимая безопасность**
  - Опасное заблуждение
  - Специально? APT?





Кому же верить?

- **Google**
  - Статический анализ (?)
  - В основном работа по отзывам и жалобам
  - Контроль источника APK
- **Автор приложения**
  - Безопасная разработка (?)
  - Воровство/взлом приложения
- **Внешний арбитр**
  - Необходимость верификации ПО
  - Современные требования и угрозы

Спасибо за внимание!

Вопросы?

Хенкин Петр
Petr.Khenkin@advancedmonitoring.ru

info@advancedmonitoring.ru
http://advancedmonitoring.ru/
@am_rnd