

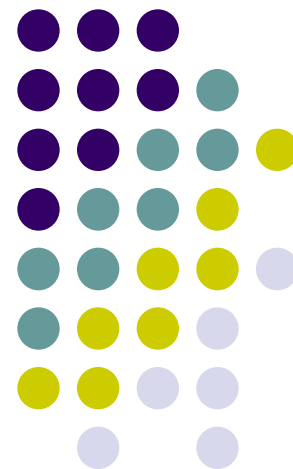
Применение самокорректирующихся кодов в области защиты информации

Автор:

Кадан М.А.

Научный руководитель:

доцент Ливак Е.Н.



Цель



Разработка методов и механизмов, предназначенных для обнаружения похищенных мобильных телефонов.

Задачи

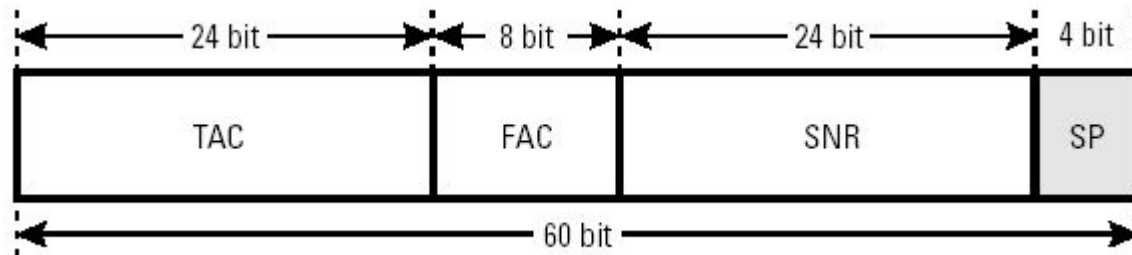


- Определить общие подходы к решению проблемы обнаружения похищенных мобильных телефонов.
- Изучить основные алгоритмы теории кодирования и технологии внедрения вирусов в исполняемые файлы.
- Изучить основы программирования прошивок мобильных телефонов.
- Разработать модель ПО, позволяющего осуществлять идентификацию похищенных мобильных телефонов.

IMEI



IMEI (International Mobile Equipment Identity) – число, состоящее из 15 десятичных цифр, служащее для идентификации мобильного телефона в пределах сотовой сети.



«Черный список» IMEI



Это список IMEI похищенных аппаратов, поддерживаемый оператором связи.

- Существует возможность модификации IMEI при помощи специальных аппаратных средств.

Главная функция утилиты



В ответ на идентификационный запрос оператора отправляется не собственный IMEI мобильного телефона, а его хранимый эталон, подлинность которого достоверно известна.



Ключевые особенности

- Утилита должна быть абсолютно прозрачна для пользователя телефона, чтобы злоумышленник даже не подозревал о ее присутствии.
- Подмена IMEI должна осуществляться в момент его передачи оператору связи в ответ на запрос идентификации.
- Утилита должна храниться в ПЗУ телефона вместе с кодом BIOS.

Использование утилиты



- Сначала требуется «заразить» BIOS телефона утилитой, что осуществляется на сервисной станции во время продажи или технического обслуживания аппарата.
- В ответ на идентификационный запрос оператора BIOS телефона будет отправлять не прошитый внутри аппарата (и, возможно, измененный) идентификатор IMEI, а его достоверную копию, записанную при инфицировании BIOS.

Использование методов EPO-вирусов



- EPO (Entry Point Obscuring) – вирусы без точки входа.
- Они записывают свой вызов в середину файла и получают управление не непосредственно при запуске, а при вызове процедуры, содержащей код передачи управления на тело вируса.

...

```
call [VirusEP]
```

...

Алгоритм работы утилиты



- Найти блок инструкций вызова, начиная с адреса сброса.
- Проверить, является ли найденный блок вызовом обработчика запроса идентификации.
- Если является, то заменить его на переход к собственной программе-обработчику, иначе продолжить поиск.



Пример работы алгоритма

- Структура образа памяти мобильного телефона напоминает структуру PE EXE.
- Рассмотрим работу алгоритма на примере:

```
01285D50    53          push ebx
01285D51    56          push esi
01285D52    57          push edi
01285D53    8965E8      mov  [ebp-18], esp
01285D56    FF1568D02801 call [0128D068]
```

Поиск



- Искомый блок был найден по адресу 01285D56:

```
01285D56      FF1568D02801      call [0128D068]
```

- FF1568D02801 представляет собой:

```
15FF          ->      косвенный CALL  
0128D068     ->      указатель на точку входа
```



Проверка

- В секции импорта по адресу 0000D068:

```
0000D068    0000E824
```

- В ней же по адресу 0000E824 хранится символьное имя функции:

```
0000E824    4C 01 GetIMEI 00
```

Замена



- Эталон IMEI и процедура его возврата дописываются в конец образа.
- Вызов стандартного обработчика заменяется на вызов этой процедуры.

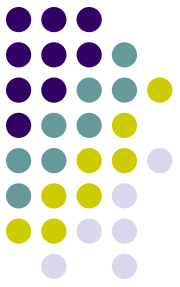


Конкретные данные

Для платформы x86 и линковщика VC:

- Блок вызова:
`call = 15FF`
- Формат символьного имени:
`4C 01 FunctionName 00`

Заключение



- Изучены основные алгоритмы теории кодирования.
- Изучены методы внедрения файловых вирусов.
- Изучены основы программирования мобильных телефонов.
- Разработана модель ПО, позволяющего добиться решения проблемы поиска похищенных мобильных телефонов.

Перспективы



В перспективе разработанное ПО можно использовать для поиска и других похищенных сетевых мобильных устройств (например, смартфонов и новейших наладонников).