МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технологический университет»
МИРЭА
Институт кибернетики
Кафедра информационной безопасности

Дипломная работа

по теме:

Оценка влияния программного продукта «Мобильный банк» на уровень защищенности абонентского терминала.

Дипломник: Трунов М.А.
Группа: ККСО-01-11
Научный руководитель: Лебедев С.Л.

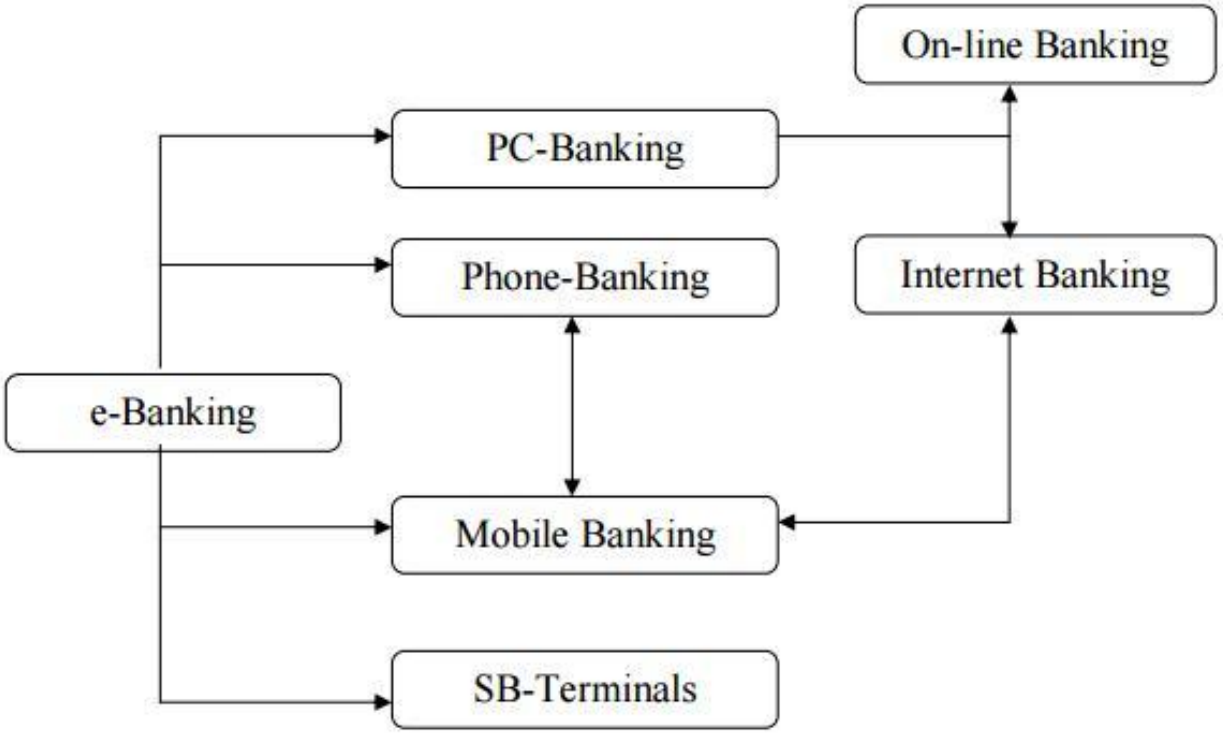
Москва, 2017

Количество атак на мобильные устройства за третий квартал 2016 года

Статистика «Лаборатории Касперского за третий квартал 2016 года»

- 1 520 931 вредоносных установочных пакетов;
- 30 167 установочных пакетов мобильных банковских троянцев;
- 37 150 установочных пакетов мобильных троянцев-вымогателей.

Классификация банковского обслуживания



Мобильный банкинг

Классический

Мобильные приложения

Уязвимости мобильных приложений

Пример: **M2: Insecure Data Storage – Небезопасное хранение данных**
Содержит в себе 4 основные особенности:
-Hardcored and forgotten
-Некорректные права файлов
-Хранение данных приложения на SD-карте
-Логирование

Угрозы мобильным приложениям

- Root доступ
- Вирусы, вшитые в устройство на уровне системного ПО
- Троянские программы
- Банковские трояны
- Трояны, под видом обычного приложения
- RiskTool
- Мнение о том, что мобильные антивирусы защищают от всех угроз

Метод CVSS количественной оценки уязвимостей

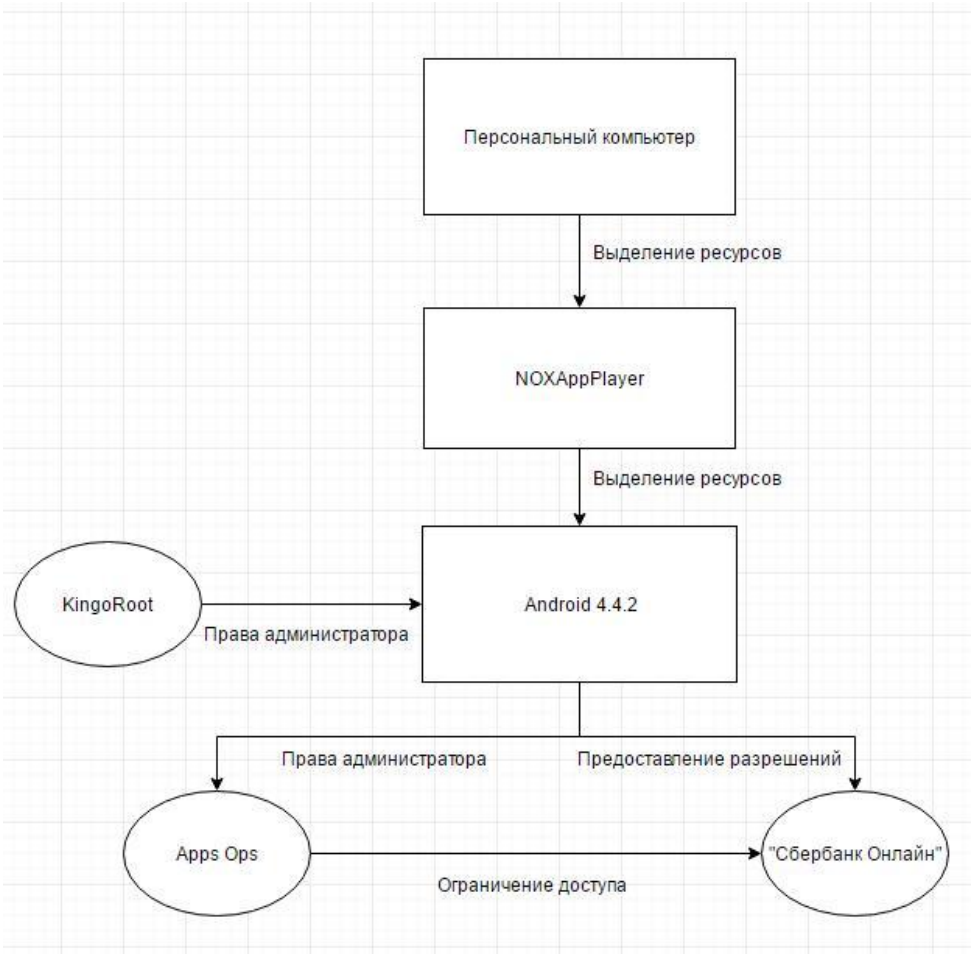
$$R = \sum_{j=1}^{n} P_r^j \cdot I^j$$ - Значение риска согласно стандарту ISO/IEC 27005

P_r^j – вероятность реализации -й угрозы;

I^j – значение ущерба от реализации j – й угрозы;

n – число угроз.

Экспериментальный стенд



Потенциальные угрозы на основе анализа приложения

Уязвимость	Потенциальная угроза	Рекомендации по защите
Отсутствие защиты идентификатора при первом входе в приложение	Кража данных доступа	Использование голосового набора. Запрет на использование нестандартных средств ввода (клавиатур)
Перехват SMS сообщений с уникальными паролями для доступа в систему/подтверждения платежей	Утрата денежных средств/потеря доступа к учетной записи	Запрет установки приложения на устройство, в котором установлена SIM-карта, связанная с банковским счетом
Отсутствие ограничений на переводы	Утрата денежных средств	Введение в мобильное приложение ограничений на разовый/суточный перевод
Запрос слишком высоких прав доступа к приложению без острой необходимости	Утрата денежных средств, нарушение конфиденциальности информации	Отключение необязательных разрешений встроенными или сторонними решениями.

Некоторые рекомендации разработчикам ПО и пользователям

- Учитывать root-доступ при разработке приложений
- Не хранить конфиденциальные данные на устройстве
- Учитывать возможность пользователя копировать/вставлять данные, делать сним
- ки экрана, резервировать данные, использовать сторонние клавиатуры
- Не использовать отправку конфиденциальных данных через SMS/MMS
- Использовать локальные инструменты по обнаружению изменений в коде
- Запретить приложению писать информацию на SD-карту

- После покупки устройства переустанавливать ОС не средствами восстановления, а с официального сайта разработчика
- Отключать «лишние» права установленным приложениям
- Не использовать банковские приложения на одном устройстве с SIM-картой, на которую привязан счет.
- Не использовать ПО, заменяющее стандартную клавиатуру пользователя

Выводы

В ходе данной дипломной работы были решены следующие задачи:

1. Рассмотрены угрозы и уязвимости мобильных устройств и мобильных приложений, их классификация и общий принцип работы.
2. Введена система количественной оценки риска и приведен пример ее использования.
3. Разработан экспериментальный стэнд, представляющий из себя эмуляцию Android системы, рассмотрены запрашиваемые разрешения при установке мобильного приложения «Сбербанк Онлайн», на этом основании сделаны выводы и разработаны рекомендации для разработчиков и пользователей по защите мобильных приложений.