**Практический обзор безопасности платежей в финансовых услугах**

Системы дистанционного банковского обслуживания знакомы каждому. Могут быть разные аспекты таких систем. Это удаленные банковские услуги? Или удаленное ограбление банка? Вото основные типы таких услуг:

- Цифровые банковские услуги
- Управление личными активами
- Разнообразие финансовых продуктов
- Международные платежи по заказам клиентов
- Инфраструктура как услуга
- Доверительное управление
- Брокерские услуги
- Интернет-банкинг
- Блокчейн технологии

**Векторы типичных атак и нарушений сильной программно-аппаратной защиты**

Условия для выгодного злоумышленникам (“экономичного”) взлома

- Стоимость взлома не должна превышать стоимость похищенных денег и активов.
- Сильные элементы системы безопасности должны требовать от хакеров бюджета за взлом гораздо большего, чем сумма, подлежащая краже. Пример - информация о взломе системы платежей SWIFT, появившаяся несколько лет тому назад , была особенно тревожной. Это пример нарушения сильного элемента.

Важно:

- Чтобы украсть деньги, хакеру достаточно суметь успешно использовать только одну уязвимость.
- Команда информационной безопасности должна обеспечить защиту от всех уязвимостей в системе.

## МНОГОСЛОЙНАЯ ЗАЩИТА ОНЛАЙН ПЛАТЕЖЕЙ

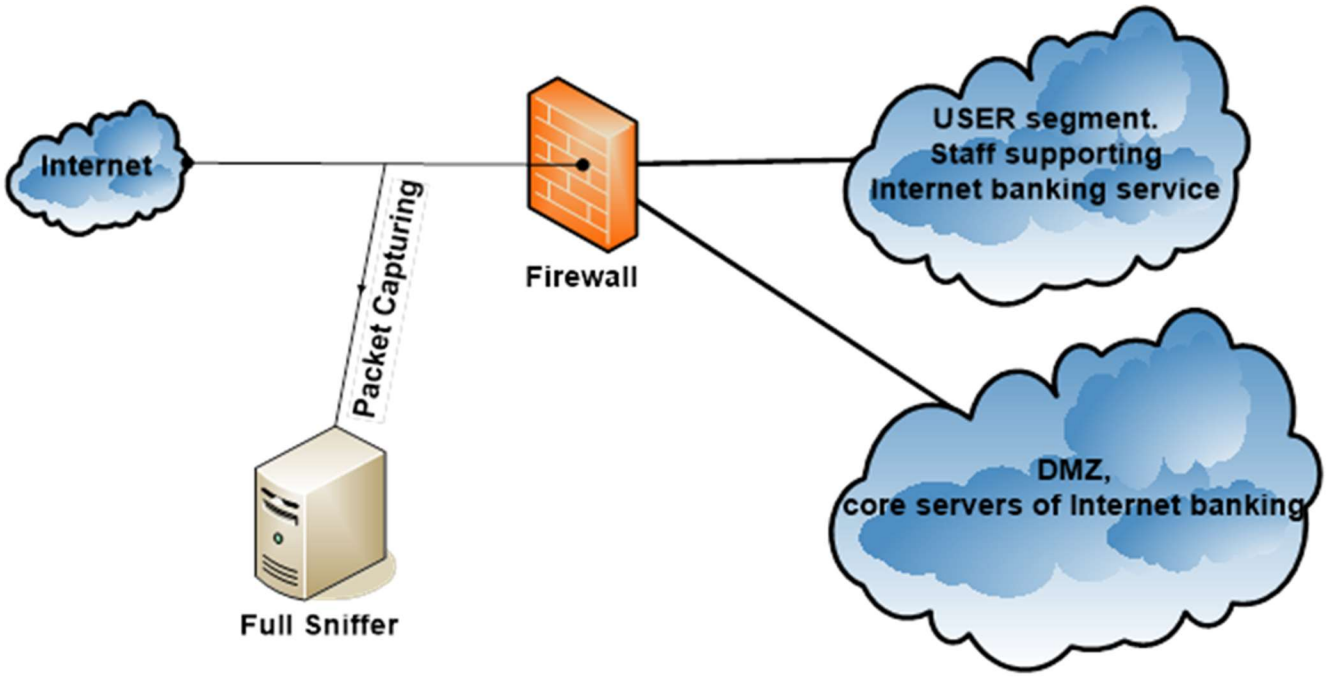
- Первый слой - блокировка несанкционированного подключения к ресурсам доверенной среды на физическом уровне. Инновации – IoT
- Второй уровень - это сетевой уровень. Брандмауэр, защита от сетевых атак.
- Третий уровень - безопасность на уровне приложений.
- Четвертый слой - контроль соблюдения политики информационной безопасности

**Многомерность системы защиты**

- Модель нарушителя
- Модель угрозы

- Разработка программ по принципам безопасной разработки программного обеспечения. Например - используя Checked C

**МОДЕЛЬ КОРПОРАТИВНОЙ СЕТИ. Уровень защиты сети**



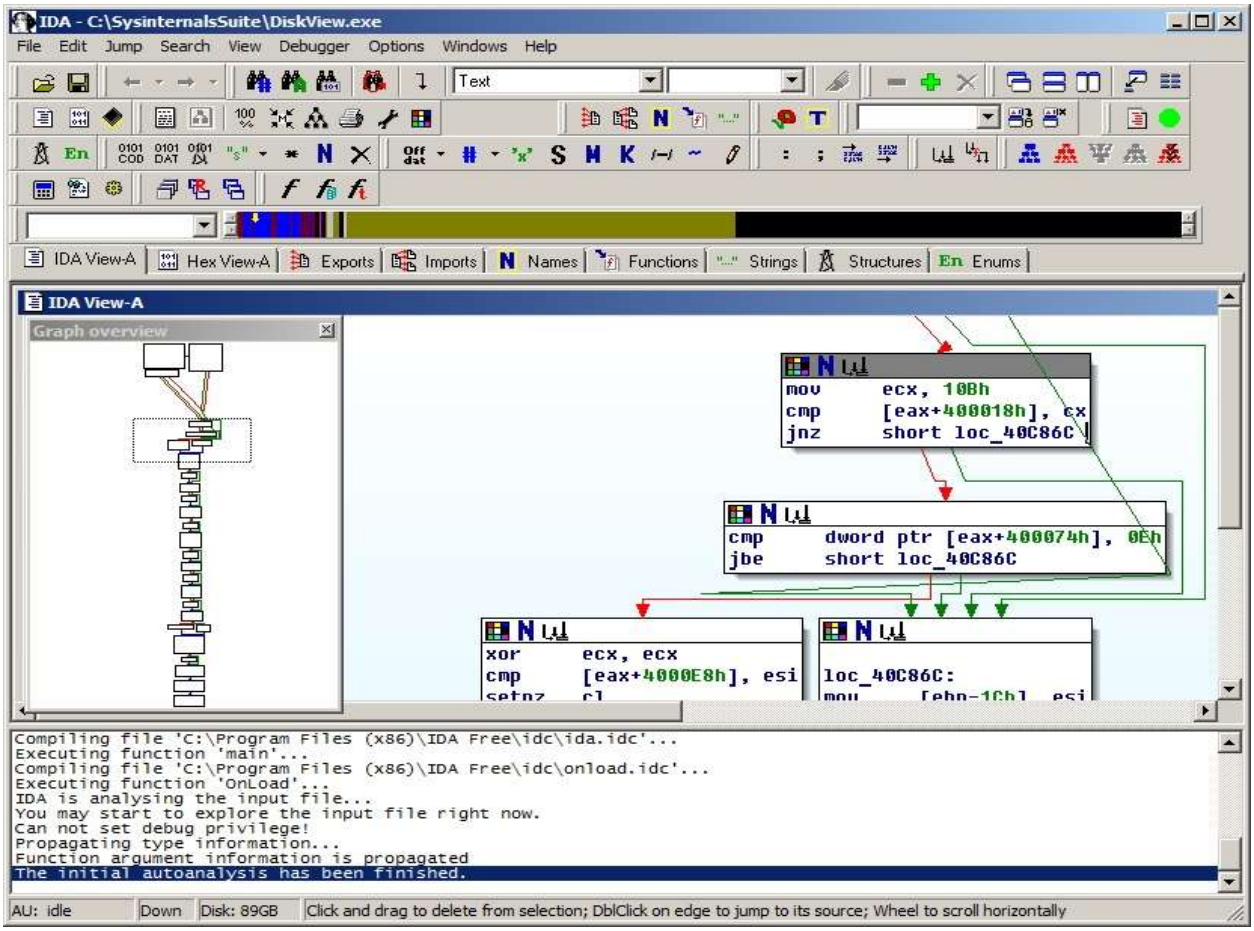

**Уровень безопасности приложения**

При проверке безопасности разработки полезно использовать ролевую модель с привлечением ред тимеров – специалистов информационной безопасности, которые смогут проверить сложность проникновения в сеть или в систему. Для понимания того, что происходит, полезно использовать программы типа Full Sniffer, например WireShark. Также нужно иметь максимальный уровень логгирования происходящего в системе. Это поможет понимать ошибки, учиться на них и не допускать их повторно.

**Недопущение обратного инжиниринга (reverse engineering)**

Безопасная разработка программного обеспечения

- - внедрение кода, запутывание и настраиваемые процедуры запуска
- - батуты функций, бессмысленные распределения, освобождения и фиктивные вызовы
- проверка времени выполнения для отладчиков




Псевдо-кодирование. Полезно иметь псевдо-язык, который использует другие структуры и команды. После разработки псевдоязыка исходный код приложения, которое мы хотим защитить, превращается в псевдокод

Чтобы запустить этот псевдокод, вам нужно создать псевдо-«виртуальную машину», которая преобразует инструкции псевдокода в инструкции псевдо-виртуальной машины в реальном времени и выполняет их.

**Многослойная система защиты**

Используя любимую фразеологию иностранных  безопасников - перевернем стол. Многоуровневая система безопасности создает дополнительные уровни защиты, каждый из которых может остановить  злоумышленника.

Это особенно важно для угрозы нулевого дня, когда сигнатуры уязвимого кода не содержатся в базах данных.

**Расширенные постоянные угрозы.**

Термин – APT, Advanced Persistent Threats.

И нужно понимать основы криптографии. Важность защиты информации обусловлена тем, что

• Телекоммуникационные системы - артерии современных глобальных информационных систем

• Информация в корпоративных системах – существенная ценность и уязвима к злоупотреблениям

• Наука о данных (data science) - раздел информатики, изучающий проблемы анализа, обработки и представления данных в цифровой форме

• Бизнес уже осознал ценность совокупности данных как долгосрочного бизнес-актива и важность информационной безопасности для бизнес-процессов

• Защитой данных, каналов связи и информационной инфраструктуры компаний занимаются квалифицированные специалисты по комплексной защите информации

*криптографические способы защиты сообщений известны людям и успешно применяются много лет

*новые достижения криптографии позволяют решать не только классическую задачу сокрытия информации с помощью шифрования, но и множество других задач, например таких как:

*задача аутентификации пользователей информационных систем

*проблема формирования цифровой подписи к электронным документам

*возможности использования криптовалют

В последнее время много вопросов о возможностях квантового компьютера. Он действительно может подписать электронный документ вашей электронной подисью? Или это фантастика?