Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Матуть
Геннадий Андреевич

Модель и программное обеспечение обнаружения угроз в интегрированной корпоративной информационной сети

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Вишняков Владимир Анатольевич
д.т.н., профессор

_____

Минск 2018

ВВЕДЕНИЕ

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют: увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации; сосредоточение в базах данных информации различного уровня важности и конфиденциальности; увеличение числа удаленных рабочих мест; широкое использование глобальной сети Internet и различных каналов связи; автоматизация обмена информацией между компьютерами пользователей.

Анализ наиболее распространенных угроз, которым подвержены современные проводные корпоративные сети, показывает, что источники угроз могут изменяться от неавторизованных вторжений злоумышленников до компьютерных вирусов.

Перед разработчиками систем защиты информации стоит важная задача повышения надёжности разрабатываемых систем и охват наибольшего количества известных угроз информационной безопасности. В связи с этим используемые сегодня механизмы защиты охватывают широкий диапазон методик и технологий.

Целью диссертации решение задачи обнаружения угрозы ложного пользователя через аутентификацию. Разработанное решение реализуется, в виде мобильного приложения обеспечения криптографической защиты данных корпоративной сети, с использованием протокола взаимной аутентификации.

В работе определяются и классифицируются угрозы информационной безопасности в контексте компьютерных сетей, обосновывается применение аутентификации для решения задачи обнаружения ложного пользователя, рассматриваются элементы системы аутентификации, факторы аутентификации и требования к построению систем аутентификации. Приводится модель взаимной аутентификации с использованием сертификатов открытого ключа. Реализуется национальный протокол аутентификации в составе мобильного приложения, реализующего протокол IPsec.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современным корпоративным компьютерным сетям присущ широкий спектр угроз информационной безопасности и способов их реализаций. Проектируя систему защиты информации особенно важна возможность своевременного обнаружения таких угроз. Одной из таких угроз является угроза ложного пользователя, обнаружение которой можно решить применением механизмов надёжной аутентификации. Пренебрежение механизмами надёжной аутентификации позволяет потенциальному злоумышленнику реализовать угрозы конфиденциальности, целостности, доступности и подлинности по отношению к данным, передаваемым по сети. Тематика исследования является актуальной, в связи с тем, что в Республике Беларусь проблема аутентификации недостаточно хорошо разработана и покрыта соответствующими стандартами.

Связь работы с научными программами и темами. Работа выполнялась по заданию «Разработка устройства активной защиты аналоговой и цифровой речевой информации по НЧ каналам» (шифр «БАС»), в рамках программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 гг, утверждённой постановлением Совета Министров Союзного государства 20.04.2012 г. №6. Заказчик – ОАЦ при Президенте РБ.

Цели и задачи исследования. *Целью* диссертационной работы решение задачи обнаружения ложного пользователя через аутентификацию. Для достижения поставленной цели необходимо решить следующие *задачи*:

– провести обзор угроз информационной безопасности;

− провести анализ проблемы аутентификации;

− предложить протокол надёжной аутентификации;

− практически реализовать предложенный протокол аутентификации в составе мобильного приложения;

Объект исследования – угрозы информационной безопасности, системы, методы и протоколы сетевой аутентификации. Предмет исследования − создание приложения, использующего надёжный механизм аутентификации для решения задачи обнаружения угрозы ложного пользователя.

Основные положения исследования, выносимые на защиту:

1. Обнаружение угрозы ложного пользователя через применение аутентификации.

2. Модель и протокол надёжной аутентификации BSTS.

3. Практическая реализация протокола BSTS в составе мобильного приложения.

Опубликованность результатов. По результатам выполненных исследований опубликована 1 научная работа: статья.

Структура и объем диссертации. Структурными частями диссертации являются: общая характеристика работы, введение, 3 главы, заключение, библиографический список, состоящий из 22 наименований, Работа изложена на 54 страницах и включает в себя 15 рисунков и 1 таблицу.

В первой главе проведен обзор угроз информационной безопасности корпоративной сети и анализ проблемы аутентификации в компьютерных сетях. Во второй главе рассмотрен протокол взаимной аутентификации BSTS. В третьей главе продемонстрирована реализация протокола BSTS в составе мобильного IPsec-клиента – StrongswanCont.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Понятие и классификация угроз информационной безопасности корпоративной сети. Угроза ложного пользователя

В общем смысле, под *угрозой* понимают потенциально возможное событие, которое может привести к нанесению ущерба чьим-либо интересам. Корпоративные сети относятся к распределенным автоматизированным системам (далее – АС), осуществляющим обработку информации. Таким образом, под *угрозой безопасности корпоративной сети* будем понимать возможность воздействия на эту сеть, которое прямо или косвенно может нанести ущерб ее безопасности.

Принято считать, что вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечивается и поддерживается требуемый уровень, следующих важных свойств информации и систем ее обработки:

– *конфиденциальности*, невозможности несанкционированного получения какой-либо информации;

– *целостности*, невозможности несанкционированной или случайной ее модификации;

– *доступности*, возможности за разумное время получить требуемую информацию.

В связи с этим выделяют три вида *непосредственных* угроз – *конфиденциальности*, *целостности* и *доступности*.

Передача информации через корпоративные компьютерные сети (далее – КС) связана со следующими проблемами защиты информации:

– перехватом информации (угроза *конфиденциальности*);

– модификацией информации (угрозы *целостности* и *подлинности*);

– подмена авторства информации (угроза *подлинности*).

– нарушение работоспособности системы (угроза *доступности*).

К более общему классу угроз подлинности можно отнести конкретную *угрозу ложного пользователя* – реализация которой, приводит к получению злоумышленником несанкционированного доступа к системе, под видом санкционированного пользователя.

На реализацию *угрозы ложного пользователя* направлены следующие виды сетевых атак: *подслушивание* (sniffing), *«человек посередине»* (man-in-

the-middle), *перехват сеанса* (session hijacking), *парольные атаки и атаки на криптографические ключи*.

Важным моментом является возможность *обнаружения попытки реализации угрозы ложного пользователя*, для дальнейшей блокировки атакующего. Эту задачу можно решить через использование надёжных механизмов аутентификации.

Аутентификация в системе защиты информации корпоративной сети

Аутентификация – это процедура проверки подлинности *субъекта*, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой *идентификатор*, на самом деле является именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.). Аутентификация, в первую очередь, решает проблемы передачи данных через компьютерные сети связанные с угрозой подлинности (пользователей и данных).

Система аутентификации состоит из следующих элементов: *субъекта аутентификации*, *контрольной характеристики*, *хозяина системы* (аутентификации), *механизма аутентификации* и *механизма управления доступом*.

Характеристика, выделяющая субъект аутентификации, может существовать в трёх формах, называемых факторами аутентификации: *что знает субъект*, *чем владеет субъект*, *что присуще субъекту*. Хорошей практикой является применение многофакторной аутентификации.

В зависимости от степени доверительных отношений, структуры, особенностей сети и удаленности объекта аутентификация может быть односторонней или взаимной. Также различают простую и строгую (криптографическую) аутентификации. К простым системам относятся парольные системы аутентификации. У пользователя есть идентификатор и пароль, то есть секретная информация, известная только пользователю (и, возможно, системе), которая используется для прохождения аутентификации. В зависимости от реализации системы, пароль может быть одноразовым или многоразовым. Системы строгой аутентификации подразумевают использование криптосистем с открытым ключом.

Аутентификация с использованием паролей считается ненадежной, так как пароли часто можно подобрать, а пользователи склонны использовать простые и одинаковые пароли в разных системах. Кроме того, разработчики

приложений могут допустить ряд концептуальных ошибок, упрощающих взлом учетных записей.

Аутентификация с использованием сертификатов открытого ключа гораздо более надёжна, по сравнению с парольным аналогом. Безопасность достигается использованием в процессе аутентификации механизма электронной цифровой подписи, наличие которой доказывает факт применения личного ключа. Сложность и недостаток такого подхода заключается в необходимости наличия действующей инфраструктуры открытых ключей.

К реализации, для решения задачи обнаружения ложного пользователя, был выбран способ аутентификации на основе *сертификатов открытого ключа*. Такой способ свободен от недостатков парольной аутентификации; надёжен, благодаря использованию криптографических методов; подходит для чисто программной реализации.

Непосредственной реализацией способа аутентификации с использованием СОК, выбран национальный протокол аутентификации *BSTS*, определённый в СТБ 34.101.66-2014. Выбранный протокол аутентификации реализован в *составе протокола IPsec*.

Модель взаимной аутентификации с использованием СОК

Ниже, приведена математическая модель взаимной аутентификации с использованием сертификатов. Введём следующие обозначения:

– X – клиент (субъект аутентификации);

– SA – сервер аутентификации;

– CA – доверенный удостоверяющий центр;

– C_X – сертификат клиента;

– K_X – личный ключ, клиента;

– C_{SA} – сертификат сервера аутентификации;

– K_{SA} – личный ключ сервера аутентификации;

– M – сообщение протокола аутентификации;

– SIGN(M, K) – ЭЦП от сообщения M, вычисленная на ключе K;

– V_C – признак действительности сертификата C;

– A – признак успешности аутентификации.

Модель аутентификации имеет следующий вид:

$X \rightarrow SA$;

$SA(M_{SA}) \rightarrow X$;

$X(M_X, SIGN(M_{SA}, K_X), C_X) \rightarrow SA$;

$SA(C_X) \rightarrow CA$;

$CA(V_{Cx}) \rightarrow SA$;

$SA(A, SIGN(M_x, K_{SA}), C_{SA}) \rightarrow X$;

$X(C_{SA}) \rightarrow CA$

$CA\ (V_{Csa}) \rightarrow X$;

$X(A) \rightarrow SA$.

Таким образом, стороны проводят взаимную аутентификацию. Факт владения личным ключом подтверждается посредством проверки ЭЦП, вычисленной на личном ключе стороны, открытым ключом, содержащимся в сертификате этой стороны. Действительность сертификата подтверждается доверенной третьей стороной, в данном случае, удостоверяющим центром.

Общая характеристика протокола BSTS

Протокол выработки общего ключа и взаимной аутентификации определён в документе СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

Протокол BSTS позволяет сторонам сформировать общий ключ, используя долговременные личные ключи и обмениваясь соответствующими открытыми ключами. Этот протокол дополнительно обеспечивает анонимность – злоумышленник, который не вступает во взаимодействие со сторонами, а только перехватывает их сообщения, не получает информации о том, какие стороны участвуют в протоколе. Протокол предусматривает проверку того, что та или другая сторона сформировала корректный ключ, совпадающий с ключом противоположной стороны. Такая проверка называется явным подтверждением ключа. Явное подтверждение ключа является обязательной частью BSTS.

Успешное подтверждение ключа в протоколе BSTS означает, что сторона с определенным идентификатором владеет долговременным личным ключом, который соответствует отосланному ею открытому ключу. Данный протокол также *может использоваться для аутентификации*, если дополнительно проверяется соответствие между идентификатором и долговременным открытым ключом стороны. Такое соответствие

фиксируется в сертификатах, передаваемых сторонами в процессе выполнения шагов протокола.

Стойкость механизма аутентификации основана на стойкости механизма подтверждения ключа и на надежности связывания идентификаторов сторон с их открытыми ключами в сертификатах. Если связывание задается с помощью ЭЦП доверенной стороны, то надежность связывания определяется стойкостью алгоритмов ЭЦП.

Программная реализация протокола BSTS в составе мобильного IPsec-клиента

В качестве основы для реализации алгоритма аутентификации BSTS, в соответствии с СТБ 34.101.66-2014, выбран *Strongswan* (рисунок 1). Программное обеспечение Strongswan является полной, кроссплатформенной реализацией протоколов IPsec с отрытым исходным кодом, распространяющееся под лицензией GNU GPLv2.

Одним из главных достоинств программной архитектуры Strongswan является её расширяемость. Исходный код Strongswan включает в себя API для создания динамически подключаемых расширений (плагинов). Это позволяет расширять функционал Strongswan путём добавления нового исходного кода, без изменения старого.

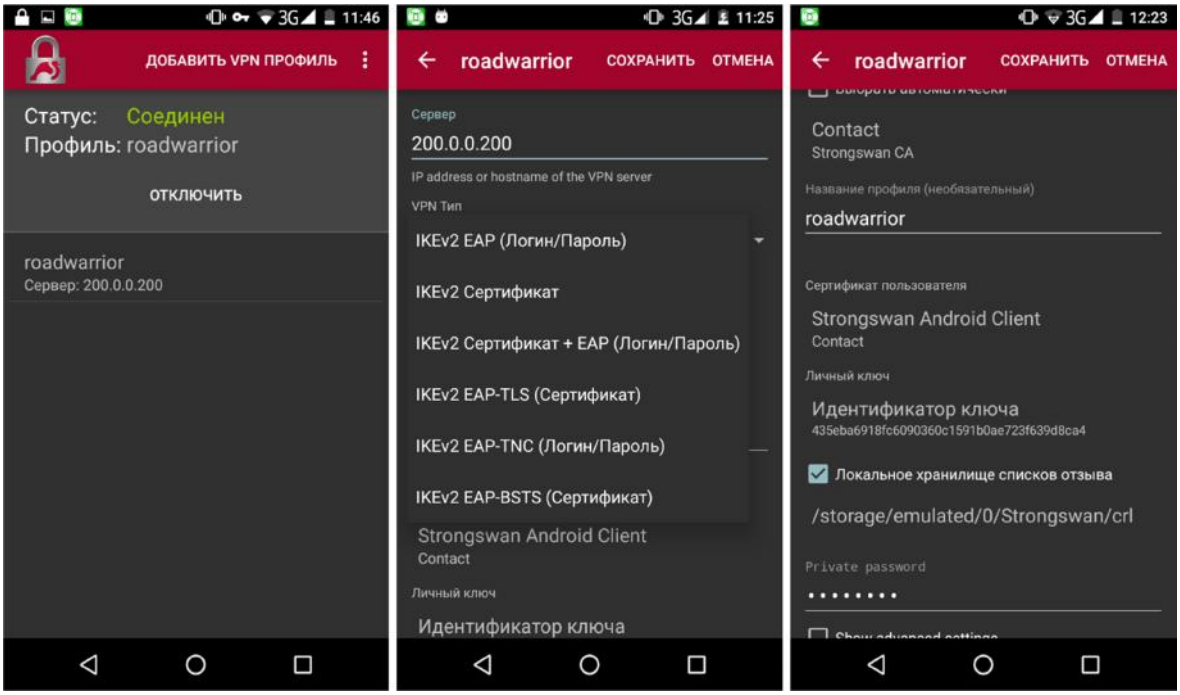

Рисунок 1 – Strongswan

ЗАКЛЮЧЕНИЕ

Цель настоящей работы была поставлена как: обнаружение угрозы ложного пользователя, через применение аутентификации. Для достижения этой цели было выполнено следующее:

1. Даны определение и классификация угроз информационной безопасности корпоративной сети. Определена *угроза ложного пользователя* и существенность влияния её реализации против некоторой сети. Так, реализация этой угрозы позволяет злоумышленнику получить несанкционированный доступ к объектам частой сети. Рассмотрены сетевые атаки, посредством исполнения которых угроза ложного пользователя может быть реализована. Обосновано применение механизмов надёжной аутентификации для защиты от атак, направленных на реализацию угрозы, при этом, тем же способом можно решить задачу *обнаружения угрозы ложного пользователя*. Далее, рассмотрены различные методы и протоколы аутентификации. Способ аутентификации, основывающийся на применении *ассиметричной криптографии* и *сертификатов открытого ключа*, определён, как наиболее подходящий, для решения поставленной задачи.

2. Разработана математическая модель выбранного способа аутентификации. В качестве реализации модели был принят *национальный протокол аутентификации и выработки общего ключа BSTS*, определённый в СТБ 34.101.66-2014. Протокол BSTS является улучшенной версией протокола Диффи-Хеллмана, защищённой от атак вида «человек посередине», посредством применения сертификатов от Протокол BSTS был реализован в рамках сертифицированной библиотеки криптографических преобразований «ContactCrypto32LE», разработанной ЗАО НТЦ «Контакт».

3. Протокол BSTS был встроен в программную реализацию протокола безопасности IPsec – Strongswan, для мобильных устройств под управление ОС Android. Приложение предназначено для обеспечения конфиденциальности, целостности и подлинности данных передаваемых по IP-сетям. Применение BSTS-аутентификации существенно повышает надёжность защиты от угрозы ложного пользователя (а так же обеспечивает обнаружение этой угрозы), по сравнению с решениями аутентификации доступными изначально. Работоспособность BSTS в Strongswan протестирована на тесовых стендах.

Таким образом, поставленные задачи выполнены, а цель – достигнута.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Матуть, Г. А. Средства информационной безопасности голосового тракта / Г. А. Матуть, В.А. Вишняков // Тез. докладов XV Белорусско–российской НТК «Технические средства защиты информации». Минск: БГУИР, 2017. С. 60.