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

УДК 004.93'1:004.738

Семеняк
Никита Сергеевич

СИСТЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГРИД-СЕТИ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Автореферат
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
доцент кафедры защиты
информации, кандидат технических
наук
Белоусова Елена Сергеевна

_____

Минск 2023

ВВЕДЕНИЕ

В наше время грид-сети, также известные как сети распределенных ресурсов, играют все более значимую роль в современной науке и технологиях. Они позволяют объединять вычислительные мощности и хранилища данных, распределенные по всему миру, и предоставляют доступ к этим ресурсам широкому кругу пользователей. Однако, совместное использование ресурсов в таком масштабе неизбежно создает ряд проблем безопасности, связанных с конфиденциальностью данных, защитой от несанкционированного доступа, а также с управлением ресурсами и службами, которые могут быть использованы в злонамеренных целях. Поэтому безопасность в грид-сетях является критически важной темой, которая требует постоянного внимания и развития со стороны специалистов в области информационной безопасности.

Целью работы является разработка системы аутентификации пользователей для защиты данных от несанкционированного доступа при работе в грид-сетях.

В Национальной грид-сети Республики Беларусь в качестве ядра для управления всей грид-сети используется ПО ПУ Unicore. Обеспечение безопасности в грид-сетях с использованием Unicore является критически важным и включает такие меры безопасности как: шифрование данных, аутентификацию и авторизацию пользователей, управление доступом к ресурсам, мониторинг и аудит безопасности. Это позволяет обеспечить защиту данных и ресурсов в грид-сетях и снизить риски возможных нарушений безопасности.

Полноценная работа и взаимодействие с Национальной грид-сетью на данный момент реализована только на двух платформах: Linux и Windows. Так как наблюдается тенденция к переходу от настольных компьютеров к мобильным устройствам, возникла необходимость переноса ПО и сервисов для работы с Национальной грид-сетью на платформу Android. Однако для мобильных устройств на данный момент не существует ПО и сервисов, отвечающих требованиям пользователей и поддержки необходимых стандартов безопасности.

Данная диссертация посвящена программному решению задачи безопасного подключения и визуального взаимодействия с узлами кластеров Национальной грид-сети используя сервисы Unicore и VNC-протокол на устройствах под управлением ОС Android.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» используя материальную базу Межгосударственной программы инновационного сотрудничества государств-участников Содружества Независимых Государств (Проект «ГРИД-СНГ») (2014-2020 гг.).

Цель и задачи исследования

Целью диссертационной работы является разработка системы аутентификации пользователей для защиты данных от несанкционированного доступа при работе в грид-сетях.

Объектом исследования является аутентификация пользователей в грид-сетях.

Предметом исследования выступают криптографические алгоритмы для аутентификации пользователей при передаче данных в грид-сетях.

Для достижения поставленной цели в диссертации решены следующие задачи:

1 Изучение архитектуры грид-сети и принципы обеспечения безопасности.

2 Оценка уязвимостей и возможных кибератак в грид-сетях.

3 Обзор криптографических алгоритмов для аутентификации пользователей при передаче данных в грид-сетях.

4 Разработка системы аутентификации пользователей грид-сети на основе криптографических алгоритмов.

Личный вклад соискателя ученой степени

Все основные результаты и выводы получены соискателем самостоятельно. Система аутентификации пользователей грид-сети на основе криптографических алгоритмов разработана самостоятельно. Определение целей и задач исследований, интерпретация и обобщение полученных

результатов проводилась совместно с научным руководителем кандидатом технических наук, доцентом кафедры защиты информации Е.С. Белоусовой.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на: XVII Международной научно-практической конференции «Управление информационными ресурсами» 12 марта 2021 г. в Академии управления при Президенте Республики Беларусь; I Международной научно-технической конференции «Актуальные вопросы и передовые технологии сварки в науке и промышленности» 24 ноября 2022 г. в Белорусско-Российском университете.

Опубликование результатов диссертации

По теме диссертационной работы опубликовано 2 печатные работы. Из них 2 статьи и тезисы в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, библиографического списка, восьми приложений.

Общий объем диссертационной работы составляет 78 страниц, из них 68 страниц текста, 17 рисунков на 13 страницах, 2 таблицы на 2 страницах, список использованных библиографических источников (22 наименования на 2 страницах), список публикаций автора по теме диссертации (2 наименования на 2 страницах), 2 приложения на 6 страницах, графический материал на 4 страницах.

Проверка на уникальность

Проведена экспертиза диссертации *Семеняка Никиты Сергеевича* «*Система аутентификации пользователей грид-сети на основе криптографических алгоритмов*» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 10.05.2023 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 84,17 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрена значимая роль грид-сетей в современной науке и технологиях. Однако, совместное использование ресурсов в грид-сетях вызывает проблемы безопасности, связанные с конфиденциальностью данных и управлением ресурсами. Целью диссертации является разработка системы аутентификации пользователей для защиты данных от несанкционированного доступа в грид-сетях. В работе рассматривается безопасность в грид-сетях с использованием ПО Unicore, используемого в Национальной грид-сети Республики Беларусь. Описывается необходимость переноса ПО и сервисов на платформу Android, так как она становится все более популярной. Диссертация посвящена программному решению задачи безопасного подключения и взаимодействия с узлами грид-сети на устройствах под управлением ОС Android, используя сервисы Unicore и VNC-протокол.

В общей характеристике работы показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации. Определены основные задачи исследования, которые включают изучение архитектуры грид-сети, оценку уязвимостей и кибератак, обзор криптографических алгоритмов и разработку системы аутентификации на их основе.

В первой главе была рассмотрена организационная структура национальной грид-сети и ее функции. Была подробно изучена архитектура грид-сети, в качестве ядра которой выступает ПО ПУ UNICORE, а также принципы обеспечения информационной безопасности на серверной и клиентской сторонах. Особое внимание было уделено методам аутентификации пользователей в грид-сети. Полноценная работа и взаимодействие с Национальной грид-сетью на данный момент реализована только на двух платформах: Linux и Windows. Поскольку наблюдается тенденция к переходу от настольных компьютеров к мобильным устройствам, возникла необходимость переноса ПО и сервисов для работы с Национальной грид-сетью на платформу Android, готовых решений для которой на данный момент не существует. Для этого необходимо было проанализировать и исследовать существующие криптографические алгоритмы шифрования и хэширования для безопасной аутентификации пользователей и шифрования канала связи, а также изучить основные уязвимости и кебератаки со стороны нарушителя.

Во второй главе были приведены и рассмотрены возможные атаки со стороны нарушителя такие как сниффер, IP-спуфинг, отказ в обслуживании, грубый перебор паролей, «человек посредине», используя возможные уязвимости в грид-сетях при работе в корпоративных, общественных и мобильных сетях. Для защиты от этих кибератак, в особенности от кибератаки «человек посредине», были изучены и подробно рассмотрены два актуальных и эффективных криптографических алгоритма RSA и SHA-256. Применение данных криптографических алгоритмов позволило реализовать многофакторную аутентификацию пользователей на основе сертификатов в национальной грид-сети в разрабатываемом программном решении для ОС Android, которое позволяет решить задачу безопасного подключения и взаимодействия пользователя с аппаратными ресурсами грид-сети в режиме визуализации по протоколу VNC.

В третьей главе представлен результат разработки системы аутентификации пользователей грид-сети на основе криптографических алгоритмов для операционной системы Android. Программное решение производит аутентификацию пользователей по двум сертификатам: первый сертификат X.509, который используется для создания задач и аутентификации в ПО ПУ UNICORE в зашифрованном виде; второй сертификат RSA, который используется для аутентификации VNC-сервером и шифрования соединения. Решение позволяет безопасно работать с ресурсами грид-сети на мобильных устройствах в визуальном режиме и сводит к минимуму возможные кибератаки со стороны нарушителя.

ЗАКЛЮЧЕНИЕ

Таким образом, в ходе диссертации была использована материальная база Межгосударственной программы инновационного сотрудничества государств-участников СНГ (Проект «ГРИД-СНГ») (2014-2020 гг.). Используя данную материальную базу была изучена архитектура грид-сети и принципы обеспечения информационной безопасности в ней. Была произведена оценка уязвимостей и возможных кибератак в грид-сетях. Был произведен обзор криптографических алгоритмов для аутентификации пользователей при передаче данных в грид-сетях.

В конечном итоге, изучив основные аспекты информационной безопасности аппаратно-программной и организационной инфраструктуры национальной грид-сети, была разработана система аутентификации пользователей для защиты данных от несанкционированного доступа при работе в грид-сетях. Данная система аутентификации пользователей решила задачу безопасного подключения и визуального взаимодействия с узлами кластеров национальной грид-сети, используя сервисы Unicore и VNC-протокол на устройствах под управлением ОС Android путем аутентификации пользователей по двум сертификатам: первый сертификат X.509, который используется для создания задач и аутентификации в ПО ПУ UNICORE в зашифрованном виде; второй сертификат RSA, который используется для аутентификации VNC-сервером и шифрования соединения. В разработанном программном решении для ОС Android отсутствует необходимость в установке прав суперпользователя на устройство; реализация основана полностью на открытых исходных кодах; сетевой трафик не проходит через сторонние сервера и не выходит за пределы Республики Беларусь, а также не производит сбор и отправки статистики об использовании; в нем исключена возможность кибератаки «человек посередине»; обеспечивается приемлемая скорость передачи данных; обеспечивается совместимость с устройствами версии Android 5.0 и выше. К недостаткам решения следует отнести высокую сложность в настройке, развертывании и использовании программного комплекса для пользователя; потребность в более 300 мегабайт свободного пространства в памяти устройства. В перспективе планируется объединить весь программный комплекс в единое приложение, а также сделать настройку и развертывание более дружественными для пользователя.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А Семеняк Н. С. Разработка методики аутентификации пользователей в национальной грид-сети под управлением операционной системы Android //Управление информационными ресурсами. Материалы XVII Международной научно-практической конференции. Минск, 12 марта 2021 г. / Минск, Республика Беларусь; [редколлегия: А. С. Лаптенок и др.]. – Минск: Академия управления при Президенте Республики Беларусь. – с. 236-238.

2–А Семеняк Н. С. Технологические возможности научно-образовательного грид-сегмента сборочно-сварочной направленности //Актуальные вопросы и передовые технологии сварки в науке и промышленности. Сборник статей I Международной научно-технической конференции. Могилев, 24-25 ноября 2022 г. / Могилев, Республика Беларусь; [редколлегия: М. Е. Лустенков и др.]. – Могилев: Белорусско-Российский университет. – с. 227-230.