УДК 004.7 DOI: 10.26102/2310-6018/2020.28.1.024

Мониторинг удаленных рабочих станций на основе беспроводной технологии

Ю.И. Синицын
Оренбургский государственный университет, Оренбург, Российская Федерация

Резюме: Одной из задач удаленного беспроводного мониторинга рабочих станций является обеспечение безопасности при совместном использовании данных на основе удаленного мониторинга рабочей станции или портативных устройств на основе Wi-Fi, 4G или Bluetooth. Разработанная модель приложения для мобильных устройств связи (МУС) служит для мониторинга и проверки различных операций на рабочих станциях (ноутбуках), подключенных через компьютерную сеть Wi-Fi. Проведено сравнение протоколов беспроводной информационной безопасности. Приложение работает на основе технологии Wi-Fi, которая защищена беспроводным протоколом безопасности WPA2 [1]. В WPA2 реализован блочный шифр AES для обеспечения более надежного шифрования данных, но он все еще уязвим для нескольких атак из-за передачи незашифрованных кадров управления и контроля и совместного использования группового временного ключа (GTK) между узлами, подключенными к беспроводной сети. Защищенная связь между сервером и МУС создает необходимость в предложении алгоритма безопасности - простого и эффективного для создания надежной платформы под уже существующим протоколом беспроводной информационной безопасности, такого как WPA / WPA2. Приводятся результаты работы системы мониторинга рабочих станций, алгоритма шифрования и дана оценка производительности модуля приложения.

Ключевые слова: платформа, модель, алгоритм, мониторинг компьютерных сетей, WPA / WPA2, шифрование.

Для цитирования: Синицын Ю.И. Мониторинг удаленных рабочих станций на основе беспроводной технологии. *Моделирование, оптимизация и информационные технологии.* 2020;8(1). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/02/Sinizin_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.024

Remote workstation monitoring based on wireless technology

Y.I. Sinitsyn
Orenburg state university, Orenburg, Russian Federation

Abstract: One of the tasks of remote wireless workstation monitoring is to ensure data sharing security by remotely monitoring a workstation or portable devices based on Wi-Fi, 4G or Bluetooth. The developed model of application for mobile communication devices (ICC) serves to monitor and verify various operations on workstations (laptops) connected through a computer network Wi-Fi. Wireless information security protocols are compared. The application is based on Wi-Fi technology, which is protected by wireless security protocol WPA2 [1]. The WPA2 implements the AES block cipher to provide more reliable data encryption, but it is still vulnerable to several attacks due to the transmission of unencrypted control and control frames and the sharing of a group time key (GTK) between nodes connected to the wireless network. Secure communication between the server and the ICC creates the need to offer a security algorithm - simple and efficient to create a robust platform under an already existing wireless information security protocol, such as WPA/WPA2. The results of the workstation monitoring system, encryption algorithm are presented and the performance of the application module is estimated.

Keywords: platform, model, algorithm, computer network monitoring, WPA/WPA2, encryption.

For citation: Sinitsyn Y.I. Remote workstation monitoring based on wireless technology. *Modeling, Optimization and Information Technology*. 2020;8(1). Available from: https://moit.vivt.ru/wp-content/uploads/2020/02/Sinizin_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.024 (In Russ).

Введение

Основной задачей системы мониторинга является предоставление информации для анализа состояния сетевой инфраструктуры и обнаружения возникших неисправностей с оперативным их устранением. Постоянный мониторинг помогает избежать простоев в работе компьютерной сети, поддерживать все сервисы в рабочем состоянии и сохранять необходимый уровень их качества.

В области дистанционного мониторинга существует несколько методов, разработанных для обеспечения удаленного управления устройствами. Большинство архитектур предназначено для управления мобильными устройствами через систему связи. Но они, как правило, не предоставляет функций для одновременного мониторинга и управления различными приложениями, процессами и службами. Одним из популярных аналогичных инструментов является TeamViewer2. TeamViewer - это приложение для удаленного доступа к рабочей станции и совместной работы, которое доступно для Windows, Mac, Linux, Android и т.д. Для TeamViewer требуется согласие подключенного компьютера (аутентификация), прежде чем он сможет совместно использовать рабочие станции [1]. Таким образом, удаленный доступ к рабочей станции для обмена информацией является односторонним. Одновременно два паритета не могут совместно использовать рабочие станции одновременно. Еще одно аналогичное приложение для МУС - PocketDroid3. PocketDroid обеспечивает функциональность для подключения к любому компьютеру, на котором запущено серверное приложение, для управления целевой рабочей станции. Одна машина действует как сервер, а МУС - как клиент. Следовательно, удаленное управление n-машинами не достигается с помощью этого приложения. PocketCloud Remote RDP / VNC 2 - еще одно приложение для удаленного выполнения задач, таких как создание презентаций, совместная работа с другими рабочими станциями, редактирование документов (например, электронных таблиц) по беспроводной сети. Существуют различные типы возможностей установления соединения между целевым рабочими станциями и мобильным клиентом, такие как интерфейс USB, сокеты Java и клиент Android Debug Bridge. Сравнение протоколов WEP, WPA, WPA2 [1] показано в Таблице 1.

Таблица 1 - Сравнение протоколов беспроводной информационной безопасности
Table 1 - Comparison of wireless information security protocols

	WEP	WPA	WPA2
Слабое шифрование	Да	Нет (TKIP и AES надежные протоколы шифрования)	Нет (TKIP и AES надежные протоколы шифрования)
Офлайн атака по словарю	Да	Общий ключ выставлен предварительно	Нет
Атака человек по середине (MITM)	Да	Общий ключ выставлен предварительно	Нет
Спуфинг контроля допуска средств массовой информации (MAC)	Да	Общий ключ выставлен предварительно	Нет
Отказ в обслуживании	Да	Да	Да

Любой тип вычислительной платформы, такой как рабочая станция, сервер, персональный цифровой помощник (PDA), принтер и мобильный телефон, может быть доверенной платформой. Доверенная платформа особенно полезна в качестве подключенной и / или физически мобильной платформы, потому что потребность в более сильном доверии и уверенности в компьютерных платформах возрастает с подключением и физической мобильностью. Смарт-карту или другой карманный компьютер можно запрограммировать для опроса доверенной платформы (локальной или удаленной), получения идентификационной информации и метрик целостности, а также сравнения метрик идентичности и целостности с ожидаемыми значениями [2].

Цель работы состоит в разработке модели приложения для МУС расширенной функциональности и механизмов взаимодействия внешних систем с программными комплексами в рамках единой структуры.

Материалы и методы

Проектируемая архитектура взаимодействия МУС, сервера и клиентов показана на Рисунке 1. Мобильное устройство отправляет запрос в WTA с собственными мерами безопасности, которые дополнительно направляют запрос на монитор / сервер.

Рисунок 1 - Проектируемая архитектура системы мониторинга компьютерных сетей
Figure 1 - Designed System Architecture monitoring of computer networks

Сервер прослушивает запрос и предпринимает соответствующее действие или выдает запрос соответствующей рабочей станции (компьютерам) по компьютерной сети. Предлагаемая система мониторинга разделяет экран удаленной рабочей станции с помощью Wi-Fi. Захваченный экран - это снимок изображения и текущие процессы наблюдаемой системы (систем). Следствием восстановления состояния машины в таких частных сетях является проверка какой-либо службы, такой как воспроизведение / остановка воспроизведения, запись аудио / видео, выход из системы или завершение работы на клиентском компьютере. Эти интерактивные коммуникации между компьютерами и смартфоном маршрутизируются через сервер [3].

Приложению требуется доверенная платформа (как правило, сервер) для анонимного получения информации с компьютеров, подключенных по Wi-Fi. Работа разделена на два основных модуля: построение модели приложения для мониторинга приложений компьютерной сети и алгоритм шифрования. Для мониторинга и управления на уровне приложения требуется IP-адрес предполагаемой рабочей станции. Эффективная мера безопасности требуется при любом виде связи. Управление безопасностью приложения состоит из алгоритма симметричной безопасности, алгоритма потокового блочного шифра, который является быстрым и безопасным [3].

Построение модели приложения показано на Рисунке 2.

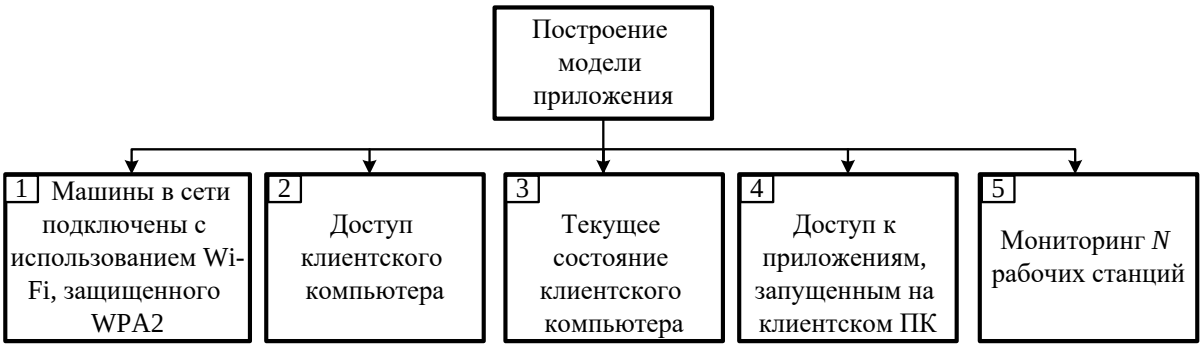

Рисунок 2 - Построение модели приложения
Figure 2 - Building an Application Model

Машины в сети подключены с использованием Wi-Fi защищенного WPA2. Каждый клиент является авторизованным пользователем в сети, обладающим групповым временным ключом. Сервер в сети обрабатывает и маршрутизирует все запросы, полученные МУС. Мобильное устройство отправляет запрос в приложение беспроводной телефонии (WTA) с собственными мерами безопасности, которое дополнительно направляет запрос на монитор / сервер. Сервер прослушивает запрос и предпринимает соответствующие действия или отправляет запрос соответствующему устройству по сети. Доступность клиентского компьютера: эмулятор МУС/ МУС используется для выбора одной из переключателей в макете для выполнения команды действия, выданной пользователем.

Текущее состояние клиентского компьютера. Таблицы базы данных, соответствующие операциям, обновляются с помощью IP-адреса (параметра) этого конкретного компьютера, и запрашиваемая служба выполняется. Приложение выполняет оконные операции, такие как получение текущих процессов, воспроизведение в VLC media player, открытие Internet Explorer, сохранение изображения, выключение системы.

Мониторинг N компьютеров: сервер сети получает текущее состояние с компьютера, запрошенного у МУС, по его IP-адресу. Таким образом, в сети может быть подключено n машин, где n> 1. Команды зондирования могут быть выданы и выполнены в течение промежутка времени, составляющего приблизительно 7 секунд. Таким образом, мониторинг более 1 машины достигается за один раз.

Алгоритм шифрования. Алгоритм основан на потоковом шифре, который реализует операцию XOR для генерации текста шифра с использованием значений блока подстановки.

Этапы алгоритма шифрования:

1. Рассчитать номер ключа:

– случайное число от 1024 до 999999;

– длина номера рассчитана;

– сумма ASCII-значений цифр числа вычисляется как цифра пароля = длина цифры (полученная на этапе b.) + Сумма ASCII-значения цифр (этап c).

2. Рассчитать параметры x0, x1, x2 и x3:

– x0 = сумма цифр в четных позициях пароля;

– x1 = сумма цифр в нечетных позициях пароля;

– x2 = произведение цифр кода доступа;

– x3 = (цифра пароля) мод (256).

3. Рассчитать параметры y0, y1 и y2. Для вычисления значения y0 необходимы параметры шифрования EP(1), EP(2), EP(3) и EP(4) [4]:

– y0 = EP(1) + EP(2) + EP(3) + EP(4).

4. Рассчитайте параметры z0, z1, z2 и z3:

– z0 = ((EP(1) [y2] XOR EP(2) [y2]) * x0) + y2;

– z1 = ((EP(1) [y1] XOR EP(3) [y1]) * x1) + y1;

– z2 = ((EP(1) [y0] XOR EP(4) [y0]) * x2) + y0;

– z3 = ((EP(2) [y2] XOR EP(3) [y2]) * x3) + y2.

5. Вычислите значения S-блока. Вычисление S-блока было показано в Таблице 2 [4].

Таблица 2 - Расчет S-блока
Table 2 - Calculation of S-block

(EP(1) XOR z0) * z0	(EP(1) XOR z1) * z0	(EP(1) XOR z2) * z0	(EP(1) XOR z3) * z0
(EP(2) XOR z0) * z1	(EP(2) XOR z1) * z1	(EP(2) XOR z2) * z1	(EP(2) XOR z3) * z1
(EP(3) XOR z0) * z2	(EP(3) XOR z1) * z2	(EP(3) XOR z2) * z2	(EP(3) XOR z3) * z2
(EP(4) XOR z0) * z3	(EP(4) XOR z1) * z3	(EP(4) XOR z2) * z3	(EP(4) XOR z3) * z3

6. Рассчитать параметр сообщения.

Параметр сообщения - номер ключа доступа (получен на шаге 1) + случайно сгенерированный ключ между 1024 и 9999 + среднее значение параметров x0, x1, x2 и x3 (получено на шаге 2) + среднее значение параметров y0, y1 и y2 (получено на шаге 3) + Среднее значение параметров z0, z1, z2 и z3 (получено на шаге 4).

7. Шифрование сообщений:

– переверните открытый текст, который необходимо зашифровать, чтобы получить частичное шифрование сообщений (PME1);

– выполните операцию PME1 сложение S-box [index] (полученную на шаге 5), чтобы получить частичное шифрование сообщений (PME2);

– выполните операцию параметра сообщения XOR PME2 (полученную на шаге 6), чтобы вычислить частичное шифрование сообщений (PME3);

– обратное двоичное / шестнадцатеричное значение PME3 для вычисления частичного шифрования сообщений (PME4);

– PME4 разбивается на группу из 8 битов и преобразуется в соответствующий символ ASCII для формирования зашифрованного текста и добавляется в файл вместе с разделителем текста [4].

Результаты

1. Модель приложения. Модель приложения запрашивает и выполняет соответствующее действие с очень низкой задержкой. Он поддерживает более поздние версии Android-смартфонов, что обеспечивает хорошую совместимость. Система может обслуживаться в будущем и любые атрибуты программного обеспечения могут быть изменены без каких-либо сложностей в программировании или интерфейсе. Были проверены проблемы совместимости для файла размера аудио, различного разрешения захваченных изображений, аудио форматов .mp*, .avi, браузеров для открытия сайта.

2. Алгоритма шифрования. IP-адрес шифруется и отправляется с МУС на сервер, где он расшифровывается. IP-адрес, передаваемый в качестве параметра пользователем МУС, зашифровывается в различный зашифрованный текст в каждом сеансе благодаря динамической генерации ключа.

3. Оценка эффективности. Мы измеряем производительность разработанной модели на разных уровнях. Во-первых, Personal Monitor Network расширила взаимодействие до «n» числа компьютерных машин с сервером в качестве единственной доверенной / аутентифицированной платформы для выполнения запроса с МУС. Во-вторых, производительность выхода из системы измерялась с помощью таймера, поскольку выполняется пакетный файл. Таблица 3 отображает время, затрачиваемое на выполнение функций через Wi-Fi. Процесс отслеживания состояния рабочей станции путем наблюдения за запущенными процессами занимает меньше времени. Производительность модуля Image Shot можно улучшить, сократив интервал между двумя последовательными захватами. Тем не менее, интервал времени установлен на 10000 мс, чтобы компенсировать задержку при извлечении его в системе МУС.

Таблица 3 - Производительность модуля приложения
Table 3 - Application Module Performance

Действие	Занятое время модуля (в секундах)
Наблюдение за ходом процесса	12,345
Получить снимок изображения	47,830
Открыть сайт	34,318
Прочитать файл	17,465
Воспроизвести аудио	23,492
Доступ к файлу Excel	06,321
Выйти (измеряется таймером)	38,100

Для чтения файла, воспроизведения аудио и открытия веб-сайта требуется время, указывающее, что компьютерная система может быть исследована практически сразу. Время выполнения функции выхода из системы больше, так как для этого требуется выполнение командного файла Windows.

Заключение

В целом, приложение работает без больших задержек и сбоев, когда в качестве сервера, клиента и контроллера выбран один ноутбук. Функциональность модулей - реализованы действия и запросы. Создав модель приложения в качестве отдельного прикладного проекта, сложность параллельных потоков была уменьшена, но увеличились накладные расходы на использование процессора. Результаты обновлялись без снижения производительности и отображалось в эмуляторе с использованием

макета. Форматы аудиофайлов - запускались в медиаплеере VLC. Размер аудиофайла не сыграл существенной роли. Функциональность файловой системы включает в себя чтение удаленного текстового файла. Модель в настоящее время может работать на 10 - 15 машинах одновременно, учитывая эффективность используемых машин (ноутбуков). Система может быть масштабирована. Алгоритм шифрования генерирует случайный ключ каждый раз из построенного блока замещения и находит другой зашифрованный текст для того же IP-адреса. Разработанный алгоритм обеспечивает решение недостатка WPA2 и использует s-box (аналогичный AES) для решения этой проблемы. Таким образом, между МУС и сервером в сети формируется надежное соединение для мониторинга или контроля клиентских рабочих станций.

ЛИТЕРАТУРА

1. Синицын Ю.И., Кунавин Д. А. *Модель системы мониторинга сетевой распределенной информационной инфраструктуры.* Физико-математические и технические науки как постиндустриальный фундамент эволюции информационного общества: сборник статей Международной научно - практической конференции (15 декабря 2017 г., г. Уфа). Уфа: АЭТЕРНА, 2017;1(1):127-129.
2. Синицын Ю.И., Витковский Н. Е. *Анализ методов управления трафиком в распределенных компьютерных сетях.* Проблемы эффективного использования научного потенциала общества: сборник статей Международной научно - практической конференции (10 декабря 2017 г., г. Челябинск). Уфа: АЭТЕРНА, 2017;1(1):21-24.
3. Синицын Ю.И., Кунавин Д. А. *Система мониторинга сетевой информационной инфраструктуры медицинского учреждения.* Norwegian Journal of development of the International Scienc. 2018;1(1):45-51.
4. Синицын Ю. И., Витковский Н. Е. *Мониторинг трафика в распределенной компьютерной сети* [Электронный ресурс] : свидетельство о гос. регистрации программы для ЭВМ. Правообладатель Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т".- № 2018614584 заявл. 07.05.2018 зарегистрировано в реестре программ для ЭВМ 26.06.2018.

REFERENCES

1. Sinitsyn Yu.I., Kunavin D.A. *Model of a monitoring system for network distributed information infrastructure.* Physical and mathematical and technical sciences as a post-industrial foundation for the evolution of the information society: a collection of articles of the International scientific and practical conference (December 15, 2017, Ufa). - Ufa: AETERNA, 2017;1(1):127-129. (In Russ)
2. Sinitsyn Yu.I., Vitkovsky N. Ye. *Analysis of traffic management methods in distributed computer networks.* Problems of the effective use of the scientific potential of society: a collection of articles of the International scientific and practical conference (December 10, 2017, Chelyabinsk). At 5 h. Part 4 / - Ufa: AETERNA, 2017;1(1):21-24. (In Russ)
3. Sinitsyn Y.I., Kunavin D. A. *Monitoring system of the network information infrastructure of a medical institution.* Norwegian Journal of development of the International Science 2018;1(1):45-51. (In Russ)
4. Sinitsyn Y. I., Vitkovsky N. E *Monitoring traffic in a distributed computer network* [Electronic resource]: certificate of state. registration of a computer program; copyright holder Feder. state budget. educate. institution of higher prof. Education "Orenburg. State

University" - No. 2018614584 decl. 05/07/2018 registered in the registry of computer programs 06/26/2018. (In Russ)

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Синицын Юрий Иванович, к.т.н, доцент кафедры Кафедра вычислительной техники и защиты информации, Оренбургский государственный университет, Оренбург, Российская Федерация.
e-mail: siniza1960@mail.ru

Tatyana N. Ivanilova Ph.D., Associate Professor, Department of Computer Engineering and Information Protection, Orenburg State University, Orenburg, Russian Federation.