БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 26–35

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-1-26-35

АНАЛИЗ ПРОТОКОЛОВ БЕЗОПАСНОСТИ НА БАЗЕ СИСТЕМЫ РАСПРОСТРАНЕНИЯ ЛИЦЕНЗИРУЕМОГО КОНТЕНТА*

А.Д. АНИКИН[1], К.А. БИРЮКОВ[2], А.Б. АРХИПОВА[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: anikin.2020@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: k.biryukov.2020@stud.nstu.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*

В последние годы число кибератак значительно выросло. Большинство предприятий нуждается в надежной защите внутрикорпоративной сети. Системы предотвращения вторжений позволяют своевременно автоматически реагировать на угрозы различного рода, которые не могут быть идентифицированы с помощью файрволлов, антивирусов и других систем безопасности. На рынке представлено много компаний, предоставляющих свои сигнатуры правил для внедрения в системы предотвращения вторжений, разработанные производителями сетевого оборудования или персонального обеспечения. Существует необходимость сохранения конфиденциальности данных правил с реализацией возможности применения на устройствах коммерческих пользователей. Для этого разрабатываются системы распространения лицензионного контента на устройства потребителей. Однако необходимо обеспечивать высокий уровень безопасности подобных систем во избежание утечек секретных данных, предоставленных сторонними вендорами.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, Eltex Distribution Manager, безопасность, шифрование, система, правила, угрозы, конфиденциальность, ключ шифрования, проверка подлинности, контроль доступа, сигнатуры.

* Статья получена 16 февраля 2023 г.

ВВЕДЕНИЕ

Надежные системы обнаружения и предотвращения вторжений (Intrusion Detection System (IDS), Intrusion Prevention System (IPS)) становятся необходимостью, учитывая экспоненциально растущее число кибератак [1]. Системы обнаружения и предотвращения вторжений анализируют трафик на основе набора правил и реагируют согласно настроенным параметрам на сетевые атаки или аномалии [2].

Компании, специализирующиеся на кибербезопасности, создают инновационные технологии потокового сканирования и системы правил, предназначенные для обнаружения наиболее опасных и широко распространенных угроз. Positive Technologies на основе продукта Positive Technologies Expert Security Center и Лаборатория Касперского на базе инфраструктуры безопасности Kaspersky Security Network с поддержкой Kaspersky SafeStream II предоставляют наборы сигнатур, позволяющие обнаруживать вредоносное программное обеспечение во всех типах трафика [3, 4].

Работа системы IPS / IDS на маршрутизаторах ESR производства компании Eltex основана на сигнатурном анализе трафика. Наборы правил можно получать из открытых источников, таких как Suricata – системы обнаружения сетевых вторжений, которая использует наборы правил для отслеживания сетевого трафика и создает оповещения при обнаружении подозрительных событий [5]. Но более надежным источником сигнатур для систем IPS / IDS являются коммерческие поставщики. Для работы системы предотвращения вторжений на маршрутизаторе необходимо лицензировать устройство и получить правила коммерческих вендоров посредством настройки взаимодействия с централизованной системой распространения лицензируемого контента Eltex Distribution Manager (EDM).

1. ПОСТАНОВКА ЗАДАЧИ

- Рассмотреть алгоритмы взаимодействия системы EDM с пользовательским устройством.
- Провести анализ мер безопасности в случае реализации угроз в системе EDM.

2. СОСТАВ СИСТЕМЫ

Рассмотрим базовый состав компонентов системы.

- EDM Root – корневой сервис EDM, работающий на стороне компании Eltex. В его задачи входит взаимодействие с клиентскими устройствами и

пользовательскими сервисами EDM и передача на них запрошенного в рамках лицензий контента, предоставленного коммерческими вендорами [6].

- Клиентское устройство (маршрутизатор) является потребителем распространяемого EDM контента – правил лицензионных вендоров с использованием полученных сигнатур в работе системы IPS / IDS [6].

3. АЛГОРИТМЫ РАБОТЫ

I. Проверка подлинности

При подключении маршрутизатора к EDM необходимо провести его аутентификацию для подтверждения подлинности клиентского устройства и идентификации его в базе лицензионного менеджера. Алгоритм идентификации компонентов системы состоит из двух этапов: проверка подлинности Root-сервера и проверка подлинности клиентского устройства. Рассмотрим данные алгоритмы подтверждения оригинальности компонентов системы.

Проверка подлинности Root-сервера:

1) ESR генерирует уникальный код и шифрует его своим секретным ключом, получая соответствующую подпись устройства;
2) подпись передается Root-серверу в запросе аутентификации;
3) Root проверяет валидность данных ESR и действительность его лицензии;
4) Root расшифровывает специальным ключом и отправляет обратно уникальный код устройства;
5) ESR проверяет код, убеждаясь в подлинности Root-сервера.

В результате происходит подтверждение подлинности Root-сервера, что позволяет избежать такой угрозы, как подмена Root-сервера, и дальнейшей компрометации данных лицензий.

Проверка подлинности клиентского устройства:

1) Root-сервер генерирует уникальный код и шифрует его сгенерированным ключом, получая специальную подпись;
2) подпись передается в ответ на запрос аутентификации в ESR;
3) ESR расшифровывает подпись своим ключом и отправляет полученное значение;
4) Root-сервер проверяет данные, убеждаясь в подлинности ESR.

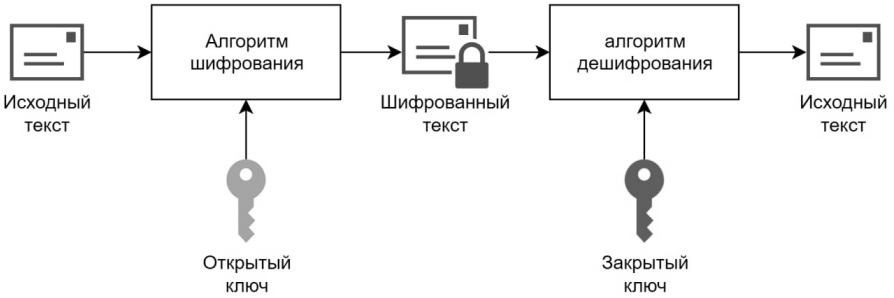
Ключи шифрования генерируются на основе уникальных параметров устройства с помощью алгоритма, разработанного компанией-производителем, благодаря чему обеспечивается уникальность данных значений и снижается вероятность компрометации ключей в результате попытки их генерации путем подделки данного алгоритма.

Таким образом, проверка подлинности каждого компонента системы позволяет свести к минимуму возможность фальсификации каких-либо компонентов системы и обеспечить сохранность правил, предоставленных вендорами.

II. Замена компонента системы

Однако возможна ситуация, когда компонент системы со стороны заказчика был заменен на новый, вследствие чего возникала необходимость актуализации ключей шифрования. Рассмотрим алгоритм работы системы в случае замены устройства.

Перед запросом клиентского устройства менеджером лицензий на получение правил производится проверка актуальности ключей для расшифровки получаемых данных. Проверяется актуальность ключа шифрования. В случае изменения ключа или вовсе его отсутствия в первую очередь выполняется обновление соответствующих данных, иначе клиентское устройство не сможет расшифровать полученные от Root правила. Так как используются симметричные алгоритмы шифрования для обмена ключами, которые уязвимы для модификации данных в канале связи, в том числе для атаки «Man-in-the-middle» (человек посередине), используются дополнительные методы односторонней или двусторонней аутентификации [7].



Алгоритм симметричного шифрования

Symmetric cryptographic algorithm

4. УГРОЗЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ В EDM

I. Перехват или подмена правил при передаче – реализация вышеупомянутой атаки «Man-in-the-middle» [8]

Методы предотвращения

1. Использование криптографического протокола обмена ключами при передаче контента.

2. Использование дополнительных методов односторонней или двусторонней аутентификации.

II. Компрометация алгоритмов генерации ключей ESR

Методы предотвращения

1. Реализация алгоритмов с учетом математической сложности декомпиляции данных. Сложность декомпиляции данных вызвана следующими особенностями [9].

1.1. Согласно архитектуре фон Неймана, данные и инструкции в памяти представляются в одинаковом виде. Следовательно, рассмотрев случайную последовательность байт из бинарного файла, будет невозможно однозначно прийти к выводу, что данный набор правил является инструкцией или данными. В случае, если процессор поддерживает разделение сегментов кода и данных, какая-то часть данных (например, таблицы ветвлений типа case) может всё равно остаться в сегменте кода.

1.2. Самомодифицирующийся код. Иногда программы могут использовать одни и те же адреса памяти для хранения исполняемого кода и данных, например, для экономии памяти, шифрования кода [10].

1.3. Идиомы. Идиома – это последовательность инструкций, которая формирует логическую единицу, действие, которое не является просто использованием первичного назначения используемых инструкций [11].

2. Осуществление контроля доступа к документации и исходникам прошивок.

3. Запрет удаленного доступа к критически важным системам.

III. Разведка – различные попытки определить алгоритм шифрования и авторизации [12]

Методы предотвращения

1. На Root-сервере IP-адрес автоматически блокируется в случае фиксации с этого IP-адреса большого количества обращений за отведенный интервал времени, в которых указаны неизвестный серийный номер или мак-адрес.

2. Блокировка IP-адреса в случае обнаружения попыток перебора.

IV. Расшифровка полученных правил на устройстве с легальной подпиской

Методы предотвращения

1. Шифрование правил для их дальнейшего хранения с использованием оптимальных с точки зрения криптостойкости и затратности по памяти и времени алгоритмов [13].

2. Запрет Root-доступа на устройство [14].

3. Защита прошивки цифровой подписью, что затрудняет установку неофициальных прошивок с возможностью компрометирования алгоритмов шифрования [15].

V. Подделка подписки – существует одно устройство с легальной подпиской, остальные устройства пытаются имитировать легальное

Методы предотвращения

1. Для генерации ключа используются уникальные параметры устройства.

2. Ограничение числа IP-адресов, с которых возможна авторизация для одного конкретного устройства. Если для устройства, успешно проходящего аутентификацию, фиксируется превышение лимита изменения IP-адресов за отведенное время, то эта персональная лицензия автоматически отзывается.

5. ИНСТРУКЦИИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Несмотря на весьма исчерпывающий набор протоколов противодействия различным видам угроз, нельзя исключать возможность компрометации алгоритма генерации ключей. На этот случай компанией была разработана следующая инструкция реагирования на данный инцидент.

1. Разрабатывается версия EDM с поддержкой нового и старого протокола.

2. Разрабатываются прошивки ESR с поддержкой нового протокола.

3. Проходит стандартная процедура тестирования версии EDM.

4. Обновляется продукт на стороне компании.

5. Производится информационная рассылка клиентам о необходимости обновления прошивок на устройствах.

6. Выпускаются новые версии прошивок ESR и EDM.

7. Отключается поддержка старого (скомпрометированного) протокола на ESR.

ЗАКЛЮЧЕНИЕ

Система передачи лицензируемого контента имеет широкий спектр протоколов безопасности на случай реализации различных угроз. Рассмотренные алгоритмы аутентификации компонентов системы распространения лицензируемого контента реализованы на высоком уровне безопасности. Протоколы передачи данных спроектированы с учетом возможности противодействия большинству самых распространенных видов атак. А в случае компрометации алгоритмов шифрования у компании имеется инструкция реагирования на данный инцидент.

СПИСОК ЛИТЕРАТУРЫ

1. *Chaudhuri A.* For the public sector, cyber resilience has never been more important / World Economic Forum. – 2022. – 18 July. – 13 p.

2. *Abdelkarim A.A., Nasereddin H.H.O.* Intrusion prevention system // International Journal of Academic Research. – 2011. – Vol. 3, N 1. – P. 432–433.

3. Positive Technologies: web-сайт. – URL: https://www.ptsecurity.com/ru-ru/services/ (дата обращения: 10.03.2023).

4. Kaspersky: web-сайт. – URL: https://www.kaspersky.ru/safestream2 (дата обращения: 10.03.2023).

5. Suricata: website. – URL: https://suricata.readthedocs.io/en/latest/what-is-suricata.html (accessed: 10.03.2023).

6. Eltex Distribution Manager (EDM). Руководство по эксплуатации. Версия ПО 1.1.

7. *Alenezi M.N., Alabdulrazzaq H.K., Mohammad N.Q.* Symmetric encryption algorithms: review and evaluation study // International Journal of Communication Networks and Information Security. – 2020. – Vol. 12, N 2. – P. 256–272.

8. Revisiting man-in-the-middle attacks against HTTPS / V. Kampourakis, G. Kambourakis, E. Chatzoglou, C. Zaroliagis // Network Security. – 2022. – Vol. 2022, N 3. – DOI: 10.12968/S1353-4858(22)70028-1.

9. *Щеглов К.Е.* Обзор алгоритмов декомпиляции // Исследовано в России. – 2001. – Ст. 116. – С. 1143–1158.

10. *Аветисян К.Р., Аидру А.В*. Применение принципов динамического полиморфизма при компиляции приложения с целью повышения его криптостойкости // Вестник Московского университета МВД России. – 2016. – № 2. – С. 213–215.

11. *Khanna T.* Rule-based pre-processing of idioms and non-compositional constructions to simplify them and improve black-box machine translation: Thesis / International Institute of Information Technology. – Hyderabad, 2021. – 62 p.

12. *Авдошин С.М., Савельева А.А.* Криптоанализ: современное состояние и перспективы развития // Информационные технологии. – 2007. – № S3. – С. 1–32.

13. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish / P. Patila, P. Narayankarb, D.G. Narayan, S.M. Meena // Procedia Computer Science – 2016. – Vol. 78. – P. 617–624.

14. *Ferraiolo D.F., Kuhn D.R.* Role-based access controls // 15th National Computer Security Conference, Oct. 13–16, 1992. – Baltimore, 1992. – P. 554–563.

15. Interrupt.memfault: website. – URL: https://interrupt.memfault.com/blog/secure-firmware-updates-with-code-signing (accessed: 10.03.2023).

Аникин Андрей Дмитриевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные сети. E-mail: anikin.2020@stud.nstu.ru

Бирюков Кирилл Андреевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные сети. E-mail: k.biryukov.2020@stud.nstu.ru

Архипова Анастасия Борисовна, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование в информационной безопасности. E-mail: arhipova@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-1-26-35

Analysis of security protocols based on the licensed content distribution system*

A.D. Anikin[1], K.A. Biryukov[2], A.B. Arkhipova[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: anikin.2020@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: k.biryukov.2020@stud.nstu.ru*
[3] *Novosibirsk State Technical University, Karl Marx Prospekt, 20, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*

In recent years, the number of cyberattacks has increased significantly. Most enterprises need reliable protection of the intracorporate networks. Intrusion prevention systems allow timely and automatic response to threats of various kinds that cannot be identified by firewalls, anti-viruses and other security systems. Many companies are represented on the market, providing their signatures to implement intrusion prevention systems developed by manufacturers of network equipment or personal security. There is a need to preserve the confidentiality of these rules with the implementation of the possibility of application on devices commercial users. That's why systems for the distribution of licensed content to consumer devices are being developed. However, it is necessary to ensure a high level of security of such systems, to avoid leaks of classified data provided by third-party vendors.

Keywords: Intrusion Detection System, Intrusion Prevention System, EDM, security, encryption, system, rules, threats, confidential, encryption key, authentication, access control, signatures

REFERENCES

1. Chaudhuri A. *For the public sector, cyber resilience has never been more important*. World Economic Forum, 2022, 18 July. 13 p.

2. Abdelkarim A.A., Nasereddin H.H.O. Intrusion prevention system. *International Journal of Academic Research*, 2011, vol. 3, no. 1, pp. 432–433.

3. *Positive Technologies*. Website. (In Russian). Available at: https://www.ptsecurity.com/ru-ru/services/ (accessed 10.03.2023).

4. *Kaspersky*. Website. (In Russian). Available at: https://www.kaspersky.ru/safestream2 (accessed 10.03.2023).

5. *Suricata*. Website. Available at: https://suricata.readthedocs.io/en/latest/what-is-suricata.html (accessed 10.03.2023).

* *Received 16 February 2023.*

6. *Eltex Distribution Manager (EDM)*. User manual. Version 1.1.

7. Alenezi M.N., Alabdulrazzaq H.K., Mohammad N.Q. Symmetric encryption algorithms: review and evaluation study. *International Journal of Communication Networks and Information Security*, 2020, vol. 12, no. 2, p. 256–272.

8. Kampourakis V., Kambourakis G., Chatzoglou E., Zaroliagis C. Revisiting man-in-the-middle attacks against HTTPS. *Network Security*, 2022, vol. 2022, no. 3. DOI: 10.12968/S1353-4858(22)70028-1.

9. Shcheglov K.E. Obzor algoritmov dekompilyatsii [Overview of decompilation algorithms]. *Issledovano v Rossii = Investigated in Russia*, 2001, art. 116, pp. 1143–1158.

10. Avetisyan K.R., Aidru A.V. Primenenie printsipov dinamicheskogo polimorfizma pri kompilyatsii prilozheniya s tsel'yu povysheniya ego kriptostoikosti [Application of the principles of dynamic polymorphism at compilation of the appendix on purpose increase of its cryptofirmness]. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2016, no. 2, pp. 213–215.

11. Khanna T. *Rule-based pre-processing of idioms and non-compositional constructions to simplify them and improve black-box machine translation*. Thesis. International Institute of Information Technology. Hyderabad, 2021. 62 p.

12. Avdoshin S.M., Savelieva A.A. Kriptoanaliz: sovremennoe sostoyanie i perspektivy razvitiya [Cryptanalysis: current state and future trends]. *Informatsionnye tekhnologii = Information Technologies*, 2007, no. S3, pp. 1–32.

13. Patila P., Narayankarb P., Narayan D.G., Meena S.M. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, 2016, vol. 78, pp. 617–624.

14. Ferraiolo D.F., Kuhn D.R. Role-based access controls. *15th National Computer Security Conference*, Baltimore, Oct. 13–16, 1992, pp. 554–563.

15. *Interrupt.memfault.* Website. Available at: https://interrupt.memfault.com/blog/secure-firmware-updates-with-code-signing (accessed 10.03.2023).

Для цитирования:

Аникин А.Д., Бирюков К.А., Архипова А.Б. Анализ протоколов безопасности на базе системы распространения лицензируемого контента // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 26–35. – DOI: 10.17212/2782-2230-2023-1-26-35.

For citation:

Anikin A.D., Biryukov K.A., Arkhipova A.B. Analiz protokolov bezopasnosti na baze sistemy rasprostraneniya litsenziruemogo kontenta [Analysis of security protocols based on the licensed content distribution system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 26–35. DOI: 10.17212/2782-2230-2023-1-26-35.