ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ШИФРОВАНИЯ ОС LINUX

تأمين أنظمة تشفير نظام التشغيل لينوكس

Колбанов Григорий Павлович
Учащийся УО «Национальный детский технопарк»

Белоусова Елена Сергеевна
к.т.н., доцент кафедры защиты информации БГУИР

Научный руководитель

المشرف العلمي

Аннотация: *В работе рассмотрены уязвимости систем шифрования в ОС Linux, выполнен анализ методов защиты данных, включая LUKS и AES. Проведена модель кибератаки с использованием физического доступа к устройству и модификации initramfs. Предложены меры по повышению безопасности, включающие Secure Boot, TPM и Unified Kernel Image. Практические результаты подтверждают эффективность предложенных решений для защиты от компрометации шифрования.*

Ключевые слова: *Linux, шифрование, LUKS, AES, TPM*

الخلاصة : تتناول هذه الورقة البحثية نقاط الضعف في أنظمة التشفير في نظام التشغيل لينوكس وتحليل طرق حماية البيانات، بما في ذلك لوكس و AES. تم تنفيذ نموذج للهجوم الإلكتروني باستخدام الوصول المادي إلى الجهاز وتعديل إنيترامفس. تتضمن تحسينات الأمان المقترحة التمهيد الآمن، وTPM، وصورة النواة الموحدة. وتؤكد النتائج العملية فعالية الحلول المقترحة للحماية من اختراق التشفير.

الكلمات المفتاحية : لينكس، التشفير، LUKS، AES، TPM

د. ايلينا سيرجيفنا بيلوسوفا
أستاذ مشارك في قسم أمن وحماية المعلومات بجامعة بيلاروسيا الحكومية للاتصالات والمعلوماتية

جريجوري بافلوفيتش كولبانوف
طالب في تكنوبارك الوطنية للأطفال

Введение

Современные операционные системы (ОС), включая Linux, становятся важным инструментом защиты данных, однако с увеличением их использования возникают новые угрозы безопасности. Уязвимости в системах шифрования, особенно в процессе загрузки ОС, могут привести к утечке конфиденциальной информации. Исследование направлено на выявление этих уязвимостей и разработку мер по усилению защиты для повышения устойчивости систем к кибератакам.

Результаты и обсуждение

В ходе исследования была проведена оценка системы шифрования в ОС Linux, с акцентом на популярный дистрибутив Astra Linux [1]. Были выявлены уязвимости, связанные с процессом загрузки и шифрования данных, которые могут быть использованы нарушителями для обхода механизмов безопасности и получения доступа к зашифрованным данным. Основная угроза была связана с уязвимостью initramfs, которая предоставляет нарушителю возможность перехвата ключей шифрования при физическом доступе к устройству.

Для моделирования кибератаки был создан экспериментальный стенд с использованием виртуальных машин с ОС Astra Linux и полнодисковым шифрованием. В ходе кибератаки был продемонстрирован процесс модификации initramfs, что позволило перехватить ключ шифрования при следующей загрузке ОС. Эти действия доказали, что при отсутствии дополнительных мер защиты на этапе загрузки ОС, нарушитель может получить доступ к данным без необходимости взлома механизма шифрования.

В качестве мер для устранения выявленных уязвимостей были предложен способ модификации загрузочного процесса ОС Astra Linux. Было предложено использование загрузчика systemd-boot, интеграция с технологиями Secure Boot [2], Trusted Platform Module (TPM) [3], которые позволяют гарантировать целостность системы и защиту ключей шифрования. Внедрение формата Unified Kernel Image (UKI) [4], который объединяет все компоненты загрузки, включая initramfs, ядро и загрузчик, с цифровыми подписями, значительно повышает защиту системы.

Эксперименты, проведенные с использованием предложенных мер, показали их высокую эффективность: ОС не позволяет загружать модифицированные компоненты, что делает невозможным проведение кибератаки. Дополнительно, использование PIN-кода для защиты ключа шифрования в связке с TPM обеспечивает дополнительный уровень безопасности, снижая риски перехвата ключа при физическом доступе к устройству.

Заключение

В результате проведенного исследования были выявлены уязвимости в системах шифрования ОС Astra Linux, связанные с возможностью перехвата ключей шифрования через модификацию initramfs при физическом доступе к устройству. Для устранения этих уязвимостей предложены меры, включающие использование Secure Boot, TPM, systemd-boot и Unified Kernel Image (UKI), что значительно повышает защиту данных и предотвращает компрометацию системы. Экспериментальные результаты подтверждают эффективность предложенных решений для защиты от кибератак.

المقدمة

أصبحت أنظمة التشغيل الحديثة، بما في ذلك لينوكس، أداة مهمة لحماية البيانات، ولكن مع تزايد استخدامها، تنشأ تهديدات أمنية جديدة. يمكن أن تؤدي الثغرات الأمنية في أنظمة التشفير، وخاصة أثناء عملية تمهيد نظام التشغيل، إلى تسرب المعلومات السرية. ويهدف البحث إلى تحديد هذه الثغرات وتطوير تدابير تقوية لزيادة قدرة الأنظمة على الصمود في وجه الهجمات السيبرانية.

النتائج والمناقشة

قامت الدراسة بتقييم نظام التشفير في نظام التشغيل لينوكس، مع التركيز على توزيع أسترا لينكس الشهير [1]. تم تحديد الثغرات الأمنية المتعلقة بعملية تحميل البيانات وتشفيرها والتي يمكن للمهاجمين استغلالها لتجاوز آليات الأمان والوصول إلى البيانات المشفرة. كان التهديد الرئيسي مرتبطًا بثغرة انيترامفس التي تسمح للمهاجم باعتراض مفاتيح التشفير عند الوصول الفعلي إلى الجهاز.

لمحاكاة هجوم إلكتروني، تم إنشاء إعداد تجريبي باستخدام آلات افتراضية بنظام التشغيل أسترا لينكس وتشفير القرص الكامل. أثناء الهجوم الإلكتروني، تم توضيح عملية تعديل ملف انيترامفس، مما جعل من الممكن اعتراض مفتاح التشفير أثناء عملية تمهيد نظام التشغيل التالية. وقد أثبتت هذه الإجراءات أنه في حالة عدم وجود تدابير أمنية إضافية في مرحلة تمهيد نظام التشغيل، يمكن للمتسلل الوصول إلى البيانات دون الحاجة إلى اختراق آلية التشفير.

كإجراء لإزالة الثغرات الأمنية التي تم تحديدها، تم اقتراح طريقة لتعديل عملية تمهيد نظام التشغيل أسترا لينكس. تم اقتراح استخدام محمل الإقلاع سستيميدبوت، والتكامل مع تقنيات الإقلاع الآمن [2] ووحدة النظام الأساسي الموثوقة (TPM) [3]، والتي تسمح بضمان سلامة النظام وحماية مفاتيح التشفير. يؤدي تقديم تنسيق صورة النواة الموحدة (UKI) [4]، والذي يدمج جميع مكونات التمهيد، بما في ذلك انيترامفس، والنواة، ومحمل الاقلاع، مع التوقيعات الرقمية، إلى تحسين أمان النظام بشكل كبير.

وقد أظهرت التجارب التي أجريت باستخدام التدابير المقترحة كفاءتها العالية: لا يسمح نظام التشغيل بتحميل المكونات المعدلة، مما يجعل من المستحيل تنفيذ هجوم إلكتروني. بالإضافة إلى ذلك، فإن استخدام رمز PIN لحماية مفتاح التشفير بالاشتراك مع وحدة النظام الأساسي الموثوقة (TPM)، يوفر مستوى إضافيًا من الأمان، مما يقلل من خطر اعتراض المفتاح أثناء الوصول الفعلي إلى الجهاز.

الخاتمة

وبنتيجة البحث الذي تم إجراؤه، تم تحديد نقاط ضعف في أنظمة التشفير لنظام التشغيل أسترا لينكس ، مرتبطة بإمكانية اعتراض مفاتيح التشفير من خلال تعديل انيترامفس أثناء الوصول الفعلي إلى الجهاز. ولمعالجة هذه الثغرات الأمنية، تم اقتراح تدابير تشمل استخدام الاقلاع الآمن ووحدة النظام الأساسي الموثوقة (TPM)، وانظمة الاقلاع و صورة النواة الموحدة (UKI) مما يحسن بشكل كبير من حماية البيانات ويمنع اختراق النظام. وتؤكد النتائج التجريبية فعالية الحلول المقترحة للحماية من الهجمات الإلكترونية.

Литература المراجع والمصادر

1. Лидер российского рынка операционных систем приходит в Беларусь // Экономическая газета – 2023. – URL: https://neg.by/novosti/otkrytj/lider-rossiyskogo-rynka-operatsionnykh-sistem-prikhodit-v-belarus/.
2. Безопасная загрузка // Документация Microsoft – 2023. – URL: https://learn.microsoft.com/ru-ru/windows-hardware/design/device-experiences/oem-secure-boot.
3. Спецификация TPM // Документация Trusted Computing Group – 2015. – URL: https://trustedcomputinggroup.org/resource/tpm-library-specification/.
4. Unified Kernel Image // Документация Arch Linux – 2020. – URL: https://wiki.archlinux.org/title/Unified_kernel_image.