УДК 04.056.53

МЕТОДИКА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ДИСТРИБУТИВА ОС LINUX С БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИЕЙ

Г.П. Колбанов
учащийся УО «Национальный детский технопарк»
grigoriy.kolbanov@gmail.com

Д.А. Романов
учащийся УО «Национальный детский технопарк»
dimromgomell@gmail.com

Е.С. Белоусова
Доцент кафедры защиты инфомации БГУИР, кандидат технических наук, доцент
belousova@bsuir.by

Г.П. Колбанов
Обучается в Гимназии №1 г. Витебска. Область научных интересов связана с информационной безопасностью, криптографией, разработкой программ и защищённых операционных систем.

Д.А. Романов
Обучается в Гомельском государственном областном лицее. Область научных интересов связана с искусственным интеллектом, машинным обучением, нейронными сетями и созданием программным продуктов.

Е.С. Белоусова
Окончила Белорусский государственный университет транспорта. Область научных интересов связана с областью информационной безопасность, разработкой и внедрением средств защиты инфомации в корпоративные сети организаций.

Аннотация. В статье рассматриваются современные подходы к повышению безопасности операционных систем (ОС), так как в условиях роста киберугроз необходимо применять комплексные меры защиты Linux-дистрибутивов, применяемых в критически важных объектах информатизации, обрабатывающих большие объемы данных. В процессе разработки нового дистрибутива ОС Secux Linux авторами статьи была разработана методика повышения безопасности подобный операционных систем на основе внедрения доверенной загрузки с верификацией initramfs, использования Secure Boot с собственными ключами, интеграции TPM и PCR sign policy.

Ключевые слова: Linux; Secure Boot, TPM, шифрование диска, изоляция приложений.

Введение. В условиях активного использования ОС Linux в системах обработки и хранения больших данных, в том числе и в критически важных объектах информатизации, необходимо применять комплексные меры по защите таких систем. В современных дистрибутивах Linux механизм загрузки системы имеет ряд уязвимостей, которые могут быть использованы нарушителями для обхода систем защиты ОС, включая компрометацию процесса расшифровки диска. Стандартная загрузка Linux в большинстве случаев основана на Shim, подписанном ключами Microsoft. Grand Unified Bootloader (GRUB), являясь основным загрузчиком, не выполняет проверку целостности загружаемых компонентов, включая initramfs – критический этап, отвечающий за расшифровку корневой файловой системы. В результате нарушитель может подменить initramfs, внедрив вредоносный код, способный перехватить пароль от зашифрованного диска.

Выбор методов повышения безопасности ОС Linux. К основным методам повышения относятся:

1 Обеспечение безопасности процесса загрузки. Рекомендуется использовать собственные ключи Secure Boot, отказаться от загрузчика GRUB в пользу systemd-boot.

2 Контроль целостности и TPM. Рекомендуется использовать аппаратную проверку целостности системы с использованием TPM [1].

3 Использование ядра linux-hardened – ядро Linux, ориентированное на безопасность, применяющее набор патчей для усиления защиты, чтобы уменьшить вероятность эксплуатации ядра.

4 Реализация полного шифрования диска с использованием LUKS (Linux Unified Key Setup).

5 Политики мандатного контроля доступа.

6 Использование Wayland в качестве графического сервера.

7 Изоляция приложений с помощью Flatpak.

8 Использование межсетевого экранирования (Uncomplicated Firewall, UFW).

9 Использование биометрической аутентификации.

Методика повышения безопасности дистрибутива ОС Linux. В процессе создания дистрибутива ОС Secux Linux были использованы все описанные выше методы повышения безопасности.

ОС Secux Linux – это современный дистрибутив на базе Arch Linux, разработанный для обеспечения максимального уровня безопасности на всех этапах работы системы. В Secux Linux есть возможность установки KIRTapp – программы, обеспечивающей биометрическую аутентификацию с распознаванием лица пользователя.

На основе опыта полученного при разработке дистрибутива ОС Secux Linux была сформирована методика повышения безопасности ОС Linux, которая включает следующие этапы:

1 Шифрование диска с помощью LUKS. Многие дистрибутивы позволяют это сделать при установке. Используйте LUKS 2 и функцию формирования ключа Argon2id [2].

2 Установка системы, ядра linux-hardened, apparmor, ufw. AppArmor должен запускаться при каждом включении устройства по этому добавим его в параметры запуска cmdline. Для применения профилей apparmor необходимо включить автоматический запуск сервиса apparmor [3].

3 Настройка генерации UKI. Для этого дистрибутив Secux Linux настраивает mkinitcpio, редактирует cmdline и создает политику подписи PCR.

4 Использование собственных ключей Secure Boot. Для этого Secux Linux использует утилиту sbctl. Настройте автоматическую подпись загрузочных программ (sbctl sign --save). Если ваше устройство не поддерживает замену ключей Secure Boot, то используйте SHIM и собственные ключи Machine Owner Key (MOK).

5 Настройка разблокировки диска с помощью TPM и программы Security Manager (интегрирован в Secux Linux).

6 Использование Wayland.

Заключение. Разработанная методика повышения безопасности дистрибутива ОС Linux была реализована в созданном дистрибутиве Secux Linux. Тестирование Secux Linux показало, что применяемые комплексные меры защиты такие как проверка загрузки, использование TPM, усиленное ядро, шифрование, мандатный контроль доступа и изоляция приложений, позволяет минимизировать риски компрометации системы. Описанная методика повышения безопасности может использоваться для любых дистрибутивов ОС Linux.

Необходимо отметить, что дистрибутив Secux Linux включает в себя все описанные методы повышения безопасности, которые полностью активируются при установке ОС. Использование ОС Secux Linux с системой биометрической аутентификации KIRTapp в

критических важных объектах информатизации позволяет минимизировать риск утечки конфиденциальных данных.

Список литературы

[1] Arthur W., Challener D., Goldman K. A Practical Guide to TPM 2.0. USA: Apress, 2015. – 392 pp.

[2] Dodis Y., Shrimpton E. T. Advances in Cryptology. USA: Springer, 2022. – 828 pp.

[3] Donald A. Tevault Mastering Linux Security and Hardening. United Kingdom, Packt Publishing, 2023. – 652 pp.

Авторский вклад

Колбанов Григорий Павлович – выбор методов повышения безопасности ОС Secux Linux, реализация и тестирование методов повышения безопасности ОС Secux Linux, составление методики повышения безопасности ОС Linux.

Романов Дмитрий Алексеевич – выбор методов биометрической аутентификации, реализация и внедрение системы биометрической аутентификации в ОС Secux Linux.

Белоусова Елена Сергеевна – постановка цели, формулировка задач исследования, координирование процесса разработки дистрибутива ОС Secux Linux, функциональное тестирование дистрибутива ОС Secux Linux.

METHOD OF INCREASING THE SECURITY OF THE LINUX OS DISTRIBUTION WITH BIOMETRIC AUTHENTICATION

G.P. Kolbanov
Student of the Educational Institution «National Children's Technopark»

D.A. Romanov
Student of the Educational Institution «National Children's Technopark»

E.S. Belousova
Associate Professor of the Informational Security Department of BSUIR, PhD of Technical Sciences, Associate Professor

Abstract. The article discusses modern approaches to improving the security of operating systems (OS), since in the context of growing cyber threats it is necessary to apply comprehensive measures to protect Linux distributions used in critical IT facilities that process large volumes of data. In the process of developing a new OS distribution Secux Linux, the authors of the article developed a technique for improving the security of such operating systems based on the implementation of trusted boot with initramfs verification, using Secure Boot with its own keys, integrating TPM and PCR sign policy.

Keywords: Linux, Secure Boot, TPM, Disk Encryption, Isolation.