УДК 004.056

НАЗВАНИЕ ДОКЛАДА

Капустин А. Е. (ИТМО)
Научный руководитель – инженер Савков С. В. (ИТМО)

Введение. Современные технологии виртуализации и контейнеризации, в основном, ориентированы на облачную и серверную инфраструктуру. Большинство решений разрабатываются с упором на управление множеством контейнеров, чтобы обеспечить удобство оркестрации и взаимодействия в сложных распределенных системах. Однако, в области пользовательской безопасности существует значительный дефицит специализированных инструментов для изолированного выполнения недоверенного кода.

Существующие решения, такие как FireJail, обладают широким функционалом, что в некоторых случаях является недостатком, так как увеличивает сложность кода, потенциальные уязвимости и накладные расходы. Дополнительно, использование SUID-бита в подобных инструментах создает дополнительные риски эскалации привилегий, что делает их менее безопасными. Существуют и другие средства контейнеризации, такие как Docker, LXC и Bubblewrap. Однако, Docker и LXC ориентированы в первую очередь на создание изолированных сред для сервисов и приложений в инфраструктурных целях. Bubblewrap, в свою очередь, является более близким аналогом предлагаемого подхода. Он не требует дополнительных привилегий, но не предусматривает готовых предустановленных профилей для различных приложений, что делает его эксплуатацию менее удобной для конечных пользователей.

В связи с этим возникает необходимость разработки нового программного обеспечения, которое обеспечивает безопасное выполнение недоверенного кода без использования привилегированных операций и лишней функциональности.

Основная часть. Предлагаемое решение представляет собой легковесное программное обеспечение, ориентированное на простоту и безопасность изолированного запуска недоверенного кода. Оно основывается на использовании технологий, которые предоставляет ядро Linux, таких как namespaces и seccomp, что позволяет ограничить доступ выполняемого процесса к ресурсам системы, минимизируя потенциальные угрозы. Далее перечислены ключевые архитектурные особенности данного решения:

1) Отсутствие использования привилегированных операций (например, SUID-бита), что минимизирует риски эскалации привилегий.
2) Минимальный набор функциональности, направленный исключительно на изоляцию запускаемого кода – не увеличивает кодовую базу и, как следствие, уменьшает поверхность атак.
3) Простота развертывания и эксплуатации – поскольку пользователи зачастую отдают предпочтение удобству перед дополнительными мерами безопасности.

Выводы. Разработка и внедрение легковесного непривилегированного инструмента для изоляции процессов позволяет удовлетворить потребность в обеспечении пользовательской безопасности. Практическое использование такого решения позволит:

1) Уменьшить риски компрометации основной системы при запуске недоверенных программ, загруженных из различных непроверенных источников.
2) Предложить альтернативу сложным и тяжеловесным решениям, которые не всегда оправданы для конечного пользователя.

Список использованных источников:

1. Bubblewrap [Электронный ресурс] // GitHub. – URL: https://github.com/containers/bubblewrap (дата обращения: 15.02.2025).
2. Firejail [Электронный ресурс] // GitHub. – URL: https://github.com/netblue30/firejail (дата обращения: 15.02.2025).