Сравнительная количественная оценка механизмов усиления защищённости микроядерных операционных систем для встроенных применений

Ефремов Д. В.
Институт системного программирования РАН,
Россия, 109004, г. Москва, ул. А. Солженицына, д. 25
efremov@ispras.ru

Постановка проблемы

Развитие встроенных и киберфизических систем обусловливает актуальность выбора архитектуры ядра операционной системы, обеспечивающей одновременно минимальный объём доверенной вычислительной базы и устойчивость к атакам на нарушение целостности и конфиденциальности. В последнее десятилетие наблюдается возвращение микроядерных архитектур ОС в сегмент встроенных систем: Fuchsia/Zircon корпорации Google, Fiasco.OC/L4Re в составе платформ для критически важных применений, исследовательский Redox на языке программирования Rust, классический GNU Hurd. Все указанные системы декларируют архитектурную изоляцию — межпроцессное взаимодействие на основе разрешений (capability-based IPC), вынесение драйверов в пространство пользователя, безопасность языка программирования — в качестве ключевого защитного свойства. Однако обоснованного количественного сопоставления подобных архитектур со зрелыми механизмами усиления защищённости монолитного ядра Linux в рамках единой методики до настоящего времени не проводилось. Общепринятого подхода к сравнению и количественной оценке таких разнородных систем как микроядерные и монолитные ОС в настоящее время нет, однако, это не означает, что сравнение в принципе невозможно. Количественные оценки позволят выявить сильные и слабые стороны различных архитектурных решений, так же как метрики сложности позволяют выделить фрагменты программного кода, которые несут в себе потенциальные проблемы, в том числе и проблемы безопасности.

Методика

В докладе будет представлена многомерная методика количественной оценки механизмов усиления защищённости ядер операционных систем, ориентированная на сопоставление систем различных архитектурных классов: монолитных и микроядерных. Методика охватывает несколько десятков механизмов защиты, сгруппированных в семь категорий: защита от повреждения памяти; контроль целостности потока управления; предотвращение утечек информации; разграничение привилегий; архитектурная изоляция; целостность и цепочка доверия; защита от спекулятивных атак. Оценка каждого механизма выполняется по совокупности параметров наличия, режима активации по умолчанию, силы реализации, архитектурной глубины и степени зрелости. Методика поддерживает настройку весовых коэффициентов категорий под различные модели угроз, в том числе модель, специфичную для встроенных применений, в которой повышен приоритет архитектурной компартментализации. Источниками первичных данных служат исходные тексты ядер, конфигурационные параметры сборки и результаты автоматизированного аудита защищённости. Методика применена к ядру Linux и четырём микроядерным операционным системам: Fuchsia/Zircon, Fiasco.OC/L4Re, Redox, GNU Hurd.

Основные результаты

Применение методики выявляет ряд устойчивых закономерностей. Архитектурная изоляция микроядер существенно повышает интегральную оценку защищённости при ориентации на встроенные применения: одно из исследованных микроядер опережает Linux в данной модели угроз, ещё два — приближаются к нему. Сильными сторонами рассмотренных микроядерных систем являются категории разграничения привилегий и архитектурной изоляции. Вместе с тем наблюдается системный пробел: даже наиболее зрелые микроядра уступают Linux в защите от повреждения памяти и в предотвращении утечек информации — в таких механизмах, как рандомизация расположения адресного пространства, контроль целостности стека и

запрет исполнения данных. Безопасность языка программирования Rust и модели доступа на основе разрешений представляют собой частные решения, не замещающие в полном объёме традиционных механизмов усиления защищённости. Полученная картина не позволяет признать какую-либо из рассмотренных архитектур безоговорочно превосходящей другие: выбор зависит от приоритетов модели угроз конкретной системы.

Содержание доклада

В докладе будут представлены общая схема предложенной методики и примеры обоснования весовых коэффициентов на основе известных распределений уязвимостей и моделей атакующего, детальная количественная матрица оценок исследованных операционных систем по семи категориям защиты, разбор сильных и слабых сторон каждой системы. Будут рассмотрены перспективные направления интеграции архитектурной изоляции с системными механизмами рандомизации расположения и контроля целостности стека, традиционно реализуемыми в монолитных ядрах, сценарии расчёта и предварительные оценки, полученные по предлагаемой методике.

Литература

1. Обзор механизмов усиления защищенности операционных систем и пользовательских приложений / Д. В. Ефремов [и др.] // Труды Института системного программирования РАН. — 2025. — Т. 37, № 3. — С. 325—354. — DOI: 10.15514/ISPRAS-2025-37(3)-23.
2. Evaluating Kernel Anti-Exploitation Capabilities: A Scalable and General Framework Based on Evaluatology / S. Chen [и др.] // Benchmarking, Measuring, and Optimizing – 16th BenchCouncil International Symposium, Bench 2024. Т. 15519. — Springer, 2025. — С. 127—143. — (Lecture Notes in Computer Science). — DOI: 10.1007/978-981-96-5032-3_8.
3. Comprehensive Formal Verification of an OS Microkernel / G. Klein [и др.] // ACM Transactions on Computer Systems. — 2014. — Т. 32, № 1. — 2:1—2:70. — DOI: 10.1145/2560537.
4. Attack Surface Metrics and Automated Compile-Time OS Kernel Tailoring / A. Kurmus [и др.] // Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS). — The Internet Society, 2013. — URL: https://www.ndss-symposium.org/ndss2013/attack-surface-metrics-and-automated-compile-time-os-kernel-tailoring.
5. A Survey on Systems Security Metrics / M. Pendleton [и др.] // ACM Computing Surveys. — 2017. — Т. 49, № 4. — 62:1—62:35. — DOI: 10.1145/3005714.