УДК 004.457

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ДИНАМИЧЕСКОЙ НАСТРОЙКИ ПАРАМЕТРОВ КОНТРОЛЬНЫХ ГРУПП ПРОЦЕССОВ

Потапова П.А. (Университет ИТМО)
Научный руководитель – доцент Гирик А.В.
(Университет ИТМО)

Введение. Локальные отказы в обслуживании (LDoS) в операционных системах (ОС) могут быть вызваны истощением ресурсов процессами и представляют серьезную угрозу информационной безопасности. В ОС Linux присутствуют такие механизмы контроля процессов, как контрольные группы - cgroups: они предлагают распределение ресурсов системы, что может предотвратить сценарий LDoS. Внедрение машинного обучения для анализа метрик процессов, запущенных в ОС, позволяет делать управление через контрольные группы более гибким и адаптивным.

Основная часть. Механизм контрольных групп позволяет иерархически агрегировать процессы, а также их дочерние процессы, предписывая им специальное поведение. [1] Контрольные группы имеют параметры, которые планируют ресурсы и применяют ограничения для выделенных процессов. Несмотря на то, что самое популярное применение контрольных групп - это системы контейнеризации, были попытки их использования также для изоляции критически важных процессов [2] и повышения производительности дата-центров и облачных вычислений [3]. Однако возможность ограничения ресурсов, чье истощение или нерациональное использование может привести к LDoS (центральный процессор (CPU), память, количество дочерних процессов, ввод/ввыод), позволяет применить механизм контрольных групп и для противостояния угрозам информационной безопасности.

При использовании описанного выше подхода могут возникнуть сложности следующего характера:

- выявление процессов, чье поведение представляет угрозу информационной безопасности;
- определение ограничений для таких процессов перед применением механизма контрольных групп.

Методы машинного обучения позволяют преодолеть указанные сложности. Метод k-ближайших соседей является примером метрического алгоритма классификации и входит в десятку алгоритмов интеллектуального анализа данных, оказавших наибольшее влияние в исследовательском сообществе. [4] Он позволяет не только классифицировать процесс, основываясь на метриках, но и подбирать ограничения, устанавлеваемые в контрольной группе, на основе метрик, которые соответствуют процессам обучающей выборки с допустимым поведением.

Программная реализация такого подхода может использовать преимущества модульной архитектуры, где один модуль отвечает за применение машинного обучения, то есть принятие решения о классификации процесса, а другой реализует логику ограничения ресурсов для процесса, создающего потенциальную угрозу информационной безопасности.

Выводы. Применение контрольных групп в ОС Linux с алгоритмами машинного обучения обеспечивает новый подход к защите ОС от LDoS, позволяя реагировать на потенциальные угрозы информационной безопасности, динамически настраивая ресурсы. Это стратегический подход, совмещающий преимущества низкоуровнего контроля средствами ОС и интеллектуального анализа поведения процессов, что открывает путь к созданию более отзывчивых и устойчивых к угрозам систем.

Список использованных источников:

1. The Linux Kernel : сайт. – URL: https://www.kernel.org/doc/html/latest/admin-guide/cgroup-v2.html (дата обращения: 15.02.2024).
2. Reducing Memory Interference Latency of Safety-Critical Applications via Memory Request Throttling and Linux Cgroup / J. Kim, P. Shin, S. Noh [и др.] // 2018 31st IEEE International System-on-Chip Conference (SOCC). – 2018. – С. 215-220. DOI: 10.1109/SOCC.2018.8618555
3. Resource Isolation Method for Program'S Performance on CMP / T. Guan, C. Liu, Z. Xu [и др.] // Journal of Physics: Conference Series. – 2017. – Т. 910, № 1. – С. 1-7. DOI: 10.1088/1742-6596/910/1/012007
4. Top 10 algorithms in data mining / X. Wu, V. Kumar, J. Ross Quinlan [и др.] // Knowledge and information systems. – 2008. – № 14. – С. 1-37.

Потапова П.А. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись