АВРОРА
СВОЯ СИСТЕМА

Встраиваемая Аврора TEE для обеспечения динамической защиты от 0-day

Дмитрий Алехин

Инженер-разработчик, Открытая Мобильная Платформа

Обо мне

- Инженер-разработчик в ОМП
- Университет Иннополис (2021-2025)
- ИТМО, DevTools (2025-2027)

УНИВЕРСИТЕТ ИННОПОЛИС

ИТМО

О компании

- Офисы разработки в Москве, Санкт-Петербурге, Нижнем Новгороде и Иннополисе
- Дочерняя компания ПАО Ростелеком
- Сотрудничаем с ведущими университетами страны
- Участники opensource-проектов и организаций

О чем доклад

1. Обзор недавних уязвимостей
2. Проблематика защиты ОС
3. Комплексная защита

АВРОРА
СВОЯ СИСТЕМА

Обзор недавних уязвимостей

Статистика CVE в ядре Linux

С 2024 года Linux стал CNA (CVE Numbering Authority). В этом случае практически всем обнаруженным багам в ядре присваивается своя CVE

- **2024: 3887 CVE**
- **2025: 5530 CVE**
- **2026: …**

tuxcare.com/blog/linux-kernel-vulnerabilities-added-to-cisas-kev-catalog-cve-2024-53197-and-cve-2024-53150

https://commandlinux.com/statistics/linux-malware-vulnerability-statistics

Copy Fail (CVE-2026-31431)

“Одна логическая ошибка в authencesn, объединённая через AF_ALG и splice() в запись 4 байт в page cache — бесшумно эксплуатируемая на протяжении почти десятилетия”

https://copy.fail

Dirty Frag (CVE-2026-43284)

Локальная уязвимость, позволяющая повысить привилегии. Она возникает из-за <u>логической</u> ошибки при обработке фрагментов сетевых пакетов: при расшифровке ESP-пакетов в XFRM или в подсистеме RxRPC ядро выполняет запись в page cache файла, который был считан через splice в сетевой сокет. Далее эксплойт перезаписывает первые байты /usr/bin/su в page cache ELF-заглушкой, после чего вызывает execve("/usr/bin/su") для получения рута

Нарушено ответственное разглашение

https://github.com/V4bel/dirtyfrag

Fragnesia (CVE-2026-46300)

Эксплойт для локального повышения привилегий в Linux, который использует <u>логическую</u> ошибку в подсистеме XFRM ESP-in-TCP, использует аналогичный метод запуска /usr/bin/su, как у Dirty Frag

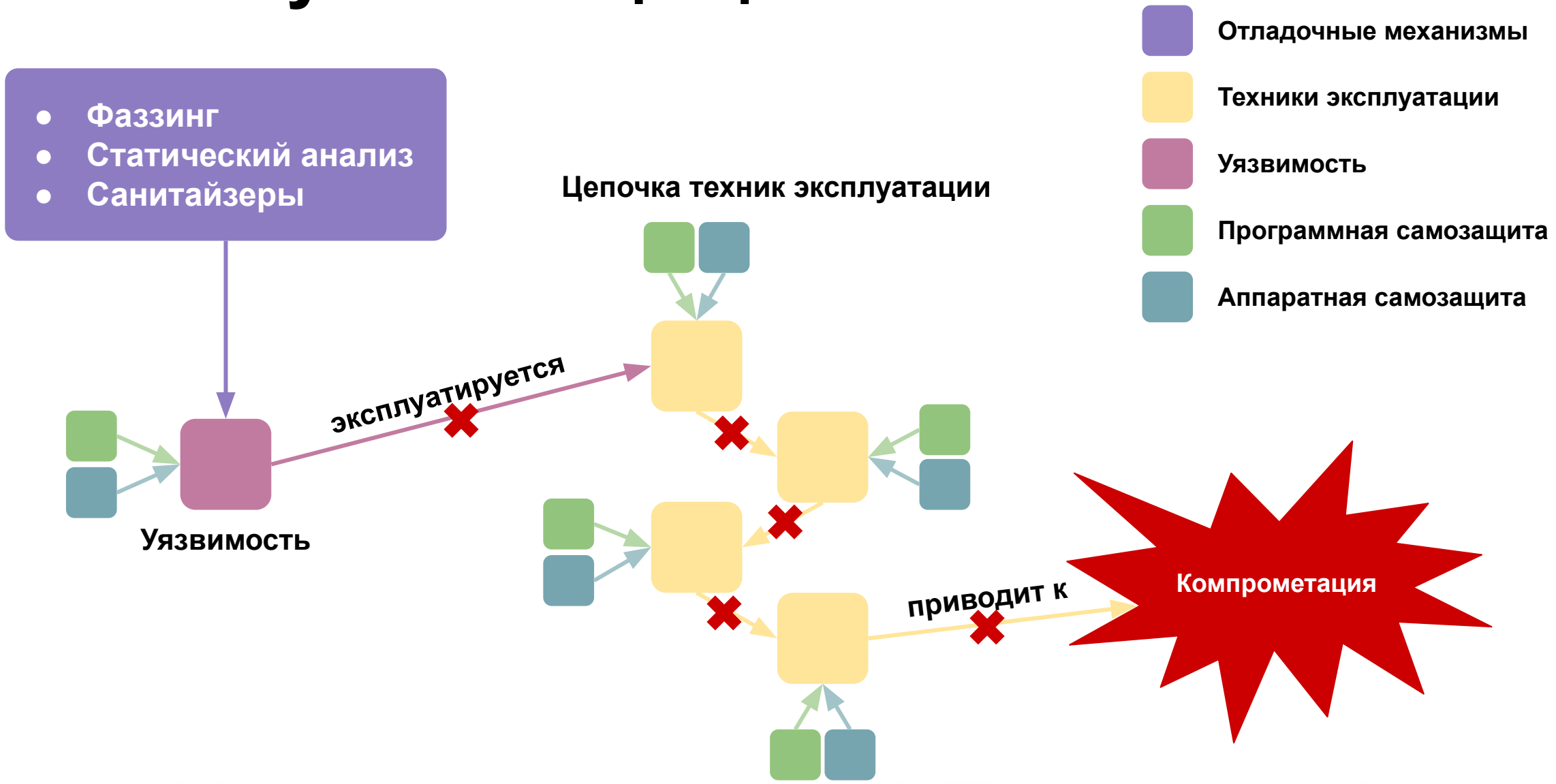
https://github.com/v12-security/pocs/tree/main/fragnesia

Я нашел 0-day
в ядре.
Не устал?

АВРОРА
СВОЯ СИСТЕМА

Проблематика защиты ОС

Как атакуют и защищают ОС



Помогают ли самозащиты?

- **Обход ARM PAC (2022)**
  pacmanattack.com
- **Обход ARM MTE (2025)**
  github.blog/security/vulnerability-research/bypassing-mte-with-cve-2025-0072
- **Обход KASLR на aarch64**
  googleprojectzero.blogspot.com/2025/11/defeating-kaslr-by-doing-nothing-at-all.html

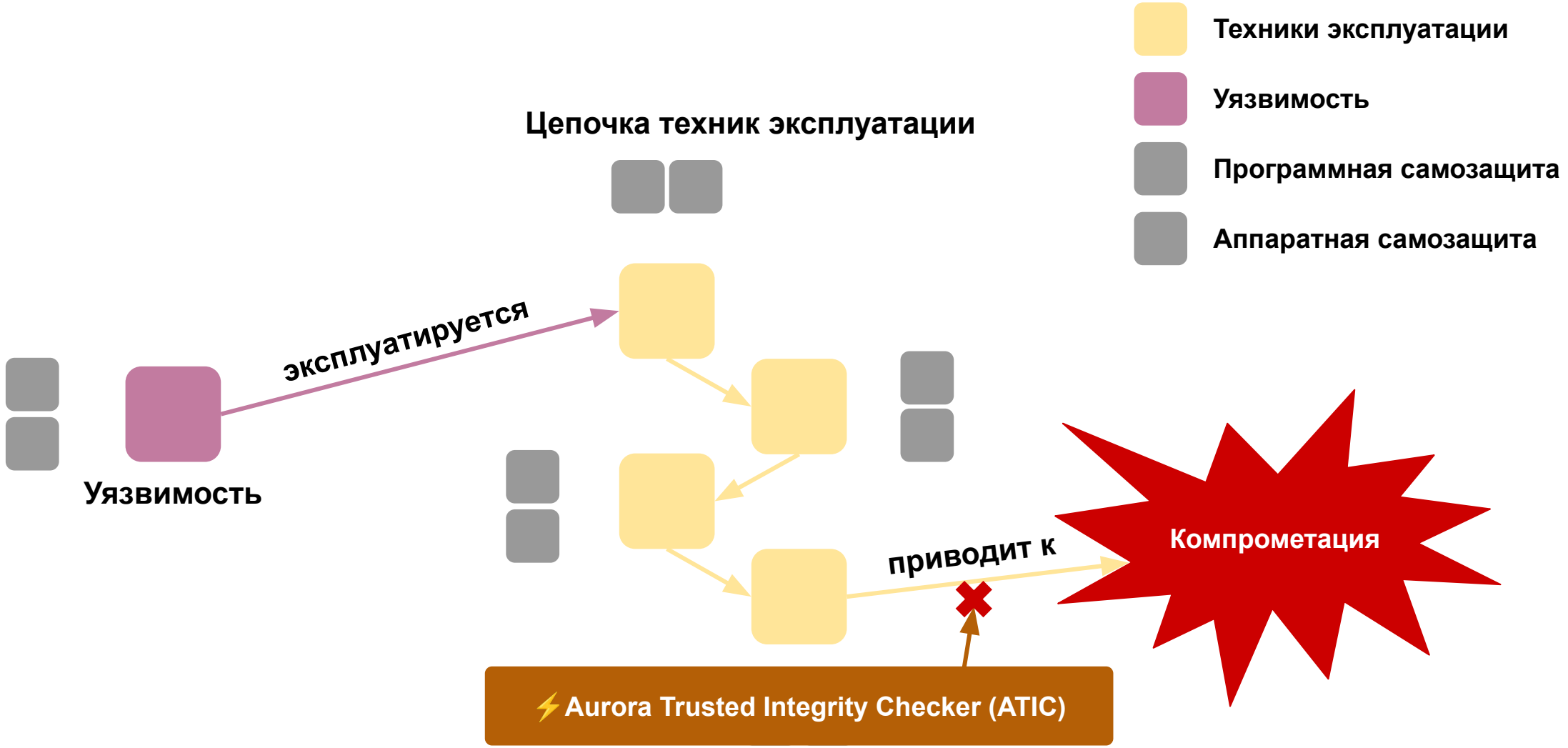
- **Обход Memory Integrity Enforcement на Apple M5**
  https://blog.calif.io/p/first-public-kernel-memory-corruption

KillSwitch

- Позволяет отключать функции ядра, в которых нашли уязвимость
- Принудительно возвращает ошибку
- Полезно для тех, у кого нету защиты от 0-day атак в реальном времени
- Написан с использованием ИИ

https://linuxsecurity.com/features/linux-runtime-killswitch

Как атакуют и защищают ОС

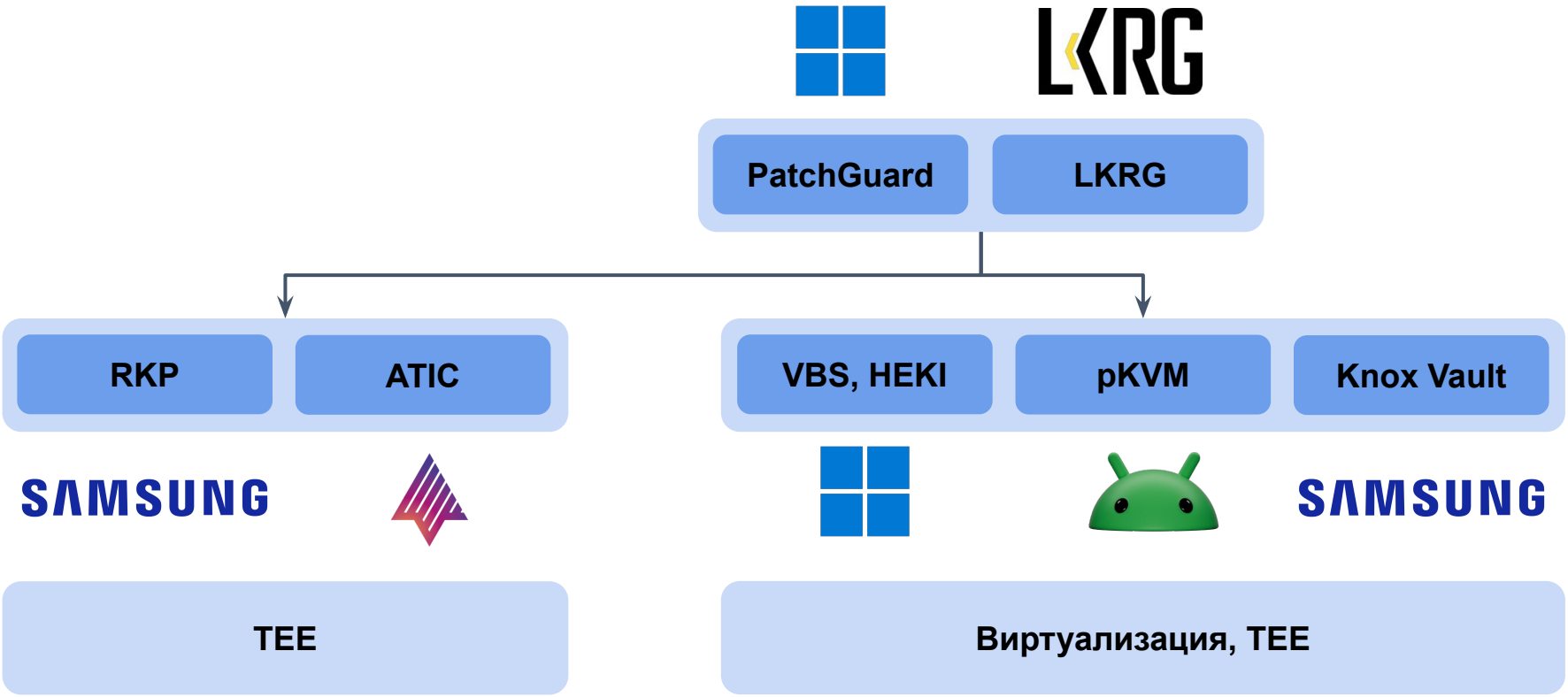


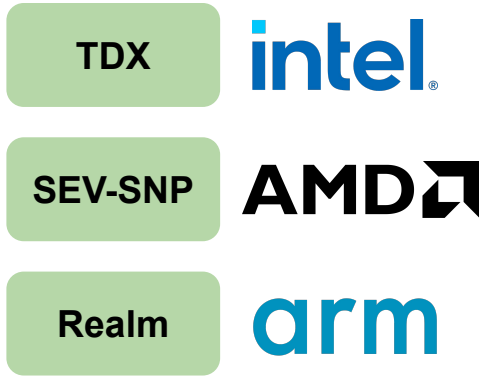
АВРОРА
СВОЯ СИСТЕМА

Комплексная защита

Aurora Trusted Integrity Checker

Индустриальные решения





Защита в реальном времени

Trusted Computing

Aurora Trusted Integrity Checker

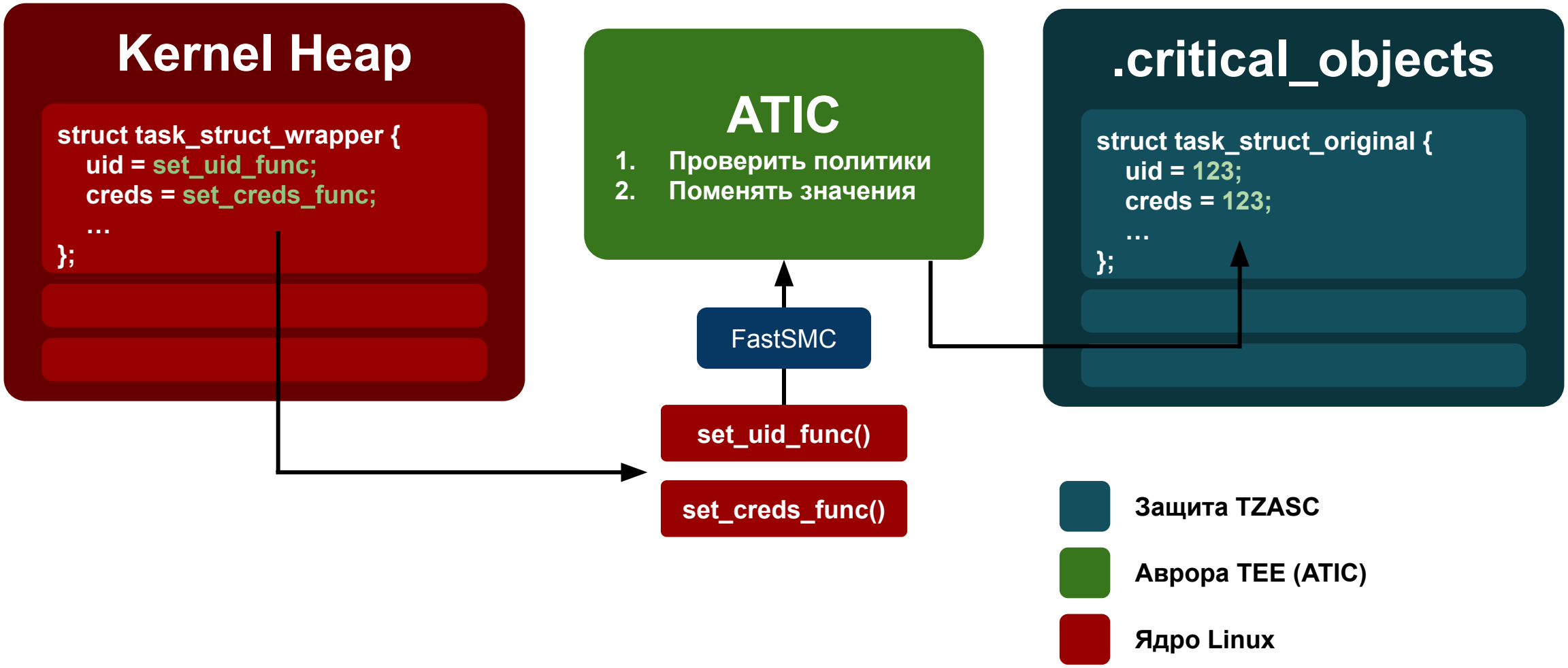
Механизм защиты ядра Linux из-под Аврора ДСИ (TEE)

- Предназначен для предотвращения особо сложных атак на ядро Linux, включая 0-day уязвимости
- Нацелен на контроль целостности ядра Linux (Runtime Kernel Integrity)
- Уже в продакшене (версия 1.0)

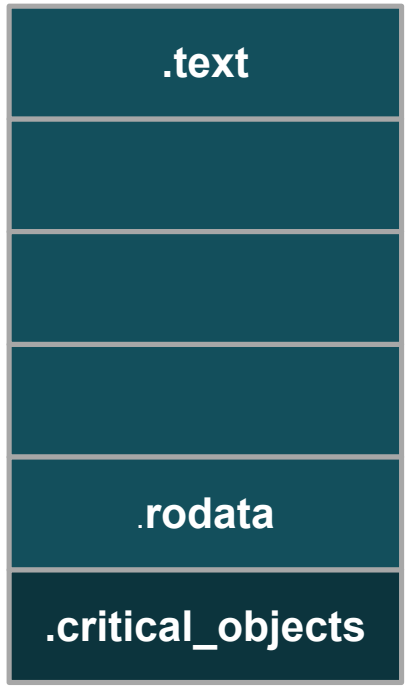
Когда ATIC должен срабатывать?

1. Периодическое прерывание по доверенному таймеру (расположен в TEE)
2. Подсистема контроля динамических объектов
3. Хуки критически важных функций ядра (через TEE Probes)

Защита динамических объектов



Защита TZASC



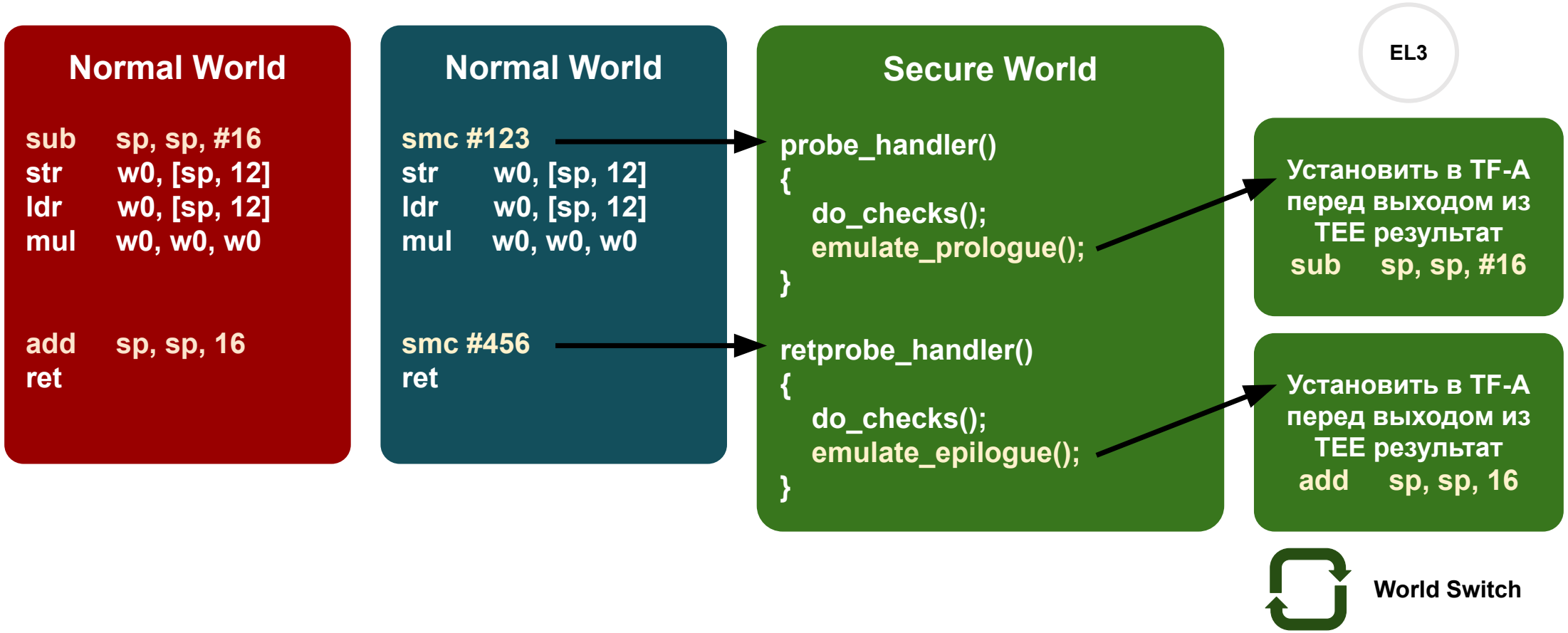
TZASC

Накладываем аппаратный “фаервол” (TZASC), который на физическом уровне запрещает запись данных в регионы кода и критических данных (.critical_objects) ядра

Политики при защите процессов

1. Проверки привилегий SELinux, AppArmor (иных LSM)
2. Проверки “опасных” настроек (perf_paranoid, yama_ptrace_scope, jit_enabled и т.д.)
3. Доверенный список приложений, которым разрешено взаимодействовать с SUID-бинарниками

TEE Probes


Normal World
sub sp, sp, #16
str w0, [sp, 12]
ldr w0, [sp, 12]
mul w0, w0, w0
add sp, sp, 16
ret
Normal World
smc #123
str w0, [sp, 12]
ldr w0, [sp, 12]
mul w0, w0, w0
smc #456
ret
Secure World
probe_handler()
{
do_checks();
emulate_prologue();
}
retprobe_handler()
{
do_checks();
emulate_epilogue();
}
EL3
Установить в TF-A перед выходом из TEE результат
sub sp, sp, #16
Установить в TF-A перед выходом из TEE результат
add sp, sp, 16
World Switch

Заключение

- Ожидаем увеличение количества CVE, в том числе 0-day
- Учащение случаев нарушения ответственного разглашения
- Стандартные меры реагирования на инцидент будут дополняться механизмами немедленной нейтрализации угроз
  - Отключение уязвимых компонентов (например, KillSwitch)
  - Комплексная защита (ATIC, RKP и другие)