OS Day 2022

Контроль работоспособности процессов посредством мониторинга размерностей

Данила Пучкин
Разработчик-исследователь

Игорь Сорокин
Руководитель группы системных исследований

kaspersky

Agenda

Актуальность проблемы

Метод контроля размерностей

Подходы к внедрению метода

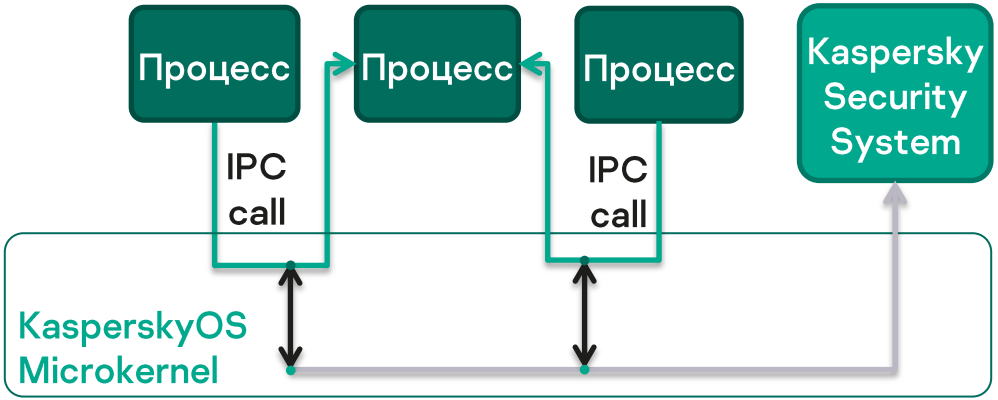
Agenda

Актуальность проблемы

Метод контроля размерностей

Подходы к внедрению метода

Базовые принципы KasperskyOS



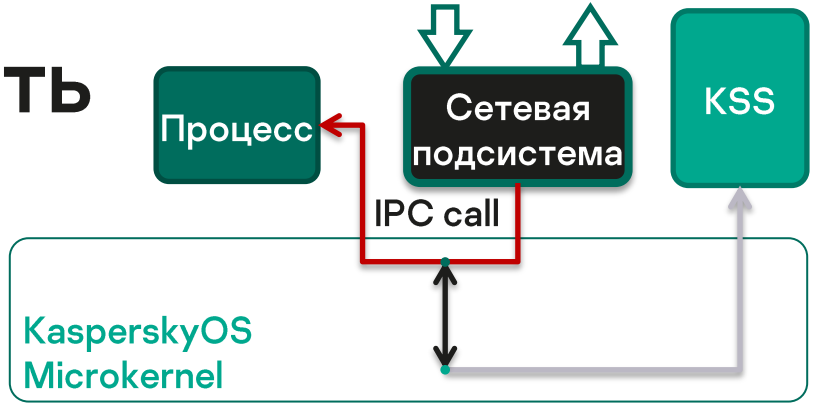
Микроядерная операционная система

Взаимодействие между доменами только по IPC-каналам

Изоляция приложений и их частей в отдельных доменах безопасности (MILS)

Контроль IPC-взаимодействий с помощью политик безопасности (Kaspersky Security System)

Работоспособность процессов



Вредоносному воздействию подвергаются взаимодействующие с внешним миром домены

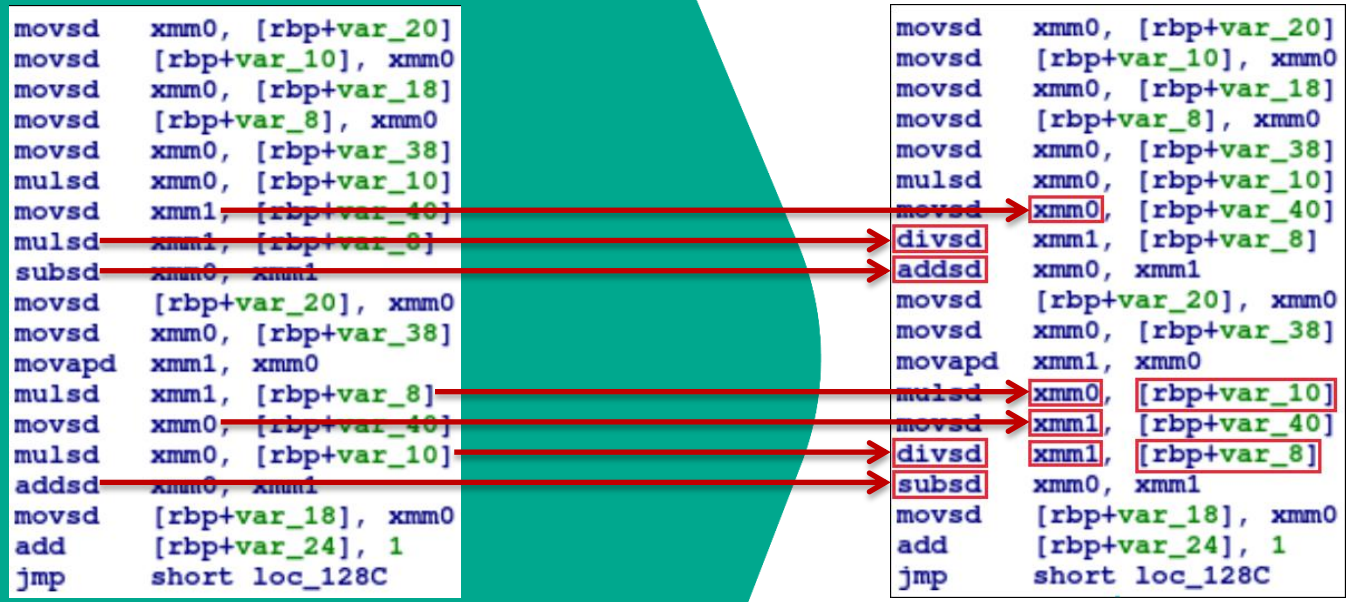
Вредоносное воздействие может распространяться при некорректных политиках

Компрометация может привести к нарушению работоспособности процессов

Возникает необходимость контроля работоспособности процессов

```
movsd   xmm0, [rbp+var_20]
movsd   [rbp+var_10], xmm0
movsd   xmm0, [rbp+var_18]
movsd   [rbp+var_8], xmm0
movsd   xmm0, [rbp+var_38]
mulsd   xmm0, [rbp+var_10]
movsd   xmm1, [rbp+var_40]
mulsd   xmm1, [rbp+var_8]
subsd   xmm0, xmm1
movsd   [rbp+var_20], xmm0
movsd   xmm0, [rbp+var_38]
movapd  xmm1, xmm0
mulsd   xmm1, [rbp+var_8]
movsd   xmm0, [rbp+var_40]
mulsd   xmm0, [rbp+var_10]
addsd   xmm0, xmm1
movsd   [rbp+var_18], xmm0
add     [rbp+var_24], 1
jmp     short loc_128C
```

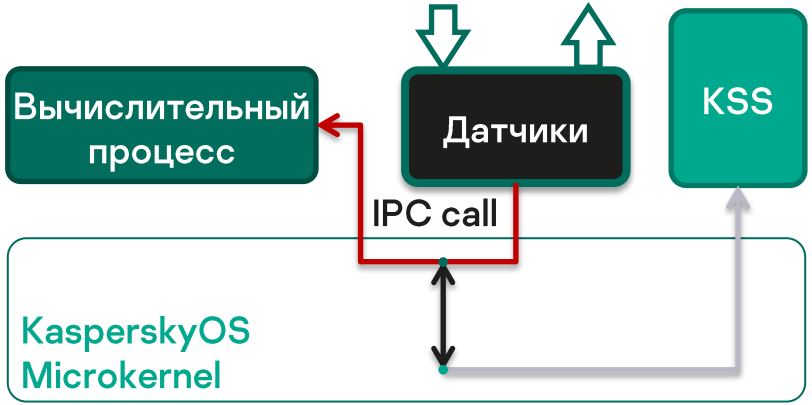
Исходный вычислительный алгоритм



Исходный вычислительный алгоритм

Модифицированные команды вычислений

Физические процессы



Контроль физических процессов связан с вычислениями

Расход газа в газопроводе:

$$Q = \frac{\pi}{4} \cdot \frac{T_0}{P_0} \cdot \sqrt{R_0} \sqrt{\frac{P_1^2 - P_2^2}{\lambda \cdot z \cdot \Delta \cdot T \cdot L} \cdot D^5}$$

Контроллеры производят вычисления на основе информации с датчиков

Управление оборудованием происходит на основе расчетов

Agenda

Постановка задачи

Метод контроля размерностей

Подходы к внедрению метода

```
for (int i = 1; i < power; i++)
{
        a_old = a_cur;

        b_old = b_cur;

        a_cur = a*a_old - b*b_old;

        b_cur = a*b_old + b*a_old;
}
```

$[a\_old]^1 = [a\_cur]^1$

$[b\_old]^1 = [b\_cur]^1$

$[a\_cur]^1 = [a]^1[a\_old]^1$

$[a\_cur]^1 = [b]^1[b\_old]^1$

$[b\_cur]^1 = [a]^1[b\_old]^1$

$[b\_cur]^1 = [b]^1[a\_old]^1$

Вычислительные операторы задают уравнения размерностей

Уравнения связывают размерности левой и правой частей операторов

$$[a\_old]^1 = [a\_cur]^1$$
$$[b\_old]^1 = [b\_cur]^1$$
$$[a\_cur]^1 = [a]^1[a\_old]^1$$
$$[a\_cur]^1 = [b]^1[b\_old]^1$$
$$[b\_cur]^1 = [a]^1[b\_old]^1$$
$$[b\_cur]^1 = [b]^1[a\_old]^1$$

Логарифмирование приводит уравнения к линейному виду

$$1 \cdot \log[a\_old] = 1 \cdot \log[a\_cur]$$
$$1 \cdot \log[b\_old] = 1 \cdot \log[b\_cur]$$
$$1 \cdot \log[a\_cur] = 1 \cdot \log[a] + 1 \cdot \log[a\_old]$$
$$1 \cdot \log[a\_cur] = 1 \cdot \log[b] + 1 \cdot \log[b\_old]$$
$$1 \cdot \log[b\_cur] = 1 \cdot \log[a] + 1 \cdot \log[b\_old]$$
$$1 \cdot \log[b\_cur] = 1 \cdot \log[b] + 1 \cdot \log[a\_old]$$

Уравнения определяют зависимость между логарифмами размерностей

Метод контроля размерностей

Уравнение	a_old	a_cur	b_old	b_cur	a	b
1·log[a_old] - 1·log[a_cur] + 0·log[b_old] + 0·log[b_cur] + 0·log[a] + 0·log[b] = 0	1	-1	0	0	0	0
0·log[a_old] + 0·log[a_cur] + 1·log[b_old] - 1·log[b_cur] + 0·log[a] + 0·log[b] = 0	0	0	1	-1	0	0
-1·log[a_old] + 1·log[a_cur] + 0·log[b_old] + 0·log[b_cur] - 1·log[a] + 0·log[b] = 0	-1	1	0	0	-1	0
0·log[a_old] + 1·log[a_cur] - 1·log[b_old] + 0·log[b_cur] + 0·log[a] - 1·log[b] = 0	0	1	-1	0	0	-1
0·log[a_old] + 0·log[a_cur] - 1·log[b_old] + 1·log[b_cur] - 1·log[a] + 0·log[b] = 0	0	0	-1	1	-1	0
-1·log[a_old] + 0·log[a_cur] + 0·log[b_old] + 1·log[b_cur] + 0·log[a] - 1·log[b] = 0	-1	0	0	1	0	-1

Логарифмированные уравнения в совокупности задают однородную СЛАУ

Коэффициенты у логарифмов задают матрицу СЛАУ

Метод контроля размерностей

a_old	a_cur	b_old	b_cur	a	b
1	-1	0	0	0	0
0	0	1	-1	0	0
-1	1	0	0	-1	0
0	1	-1	0	0	-1
0	0	-1	1	-1	0
-1	0	0	1	0	-1

a_old	a_cur	b_old	b_cur	a	b
1	-1	0	0	0	0
0	1	-1	0	0	0
0	0	1	-1	0	0
0	0	0	0	1	0
0	0	0	0	0	1
0	0	0	0	0	0

Решение СЛАУ определяет зависимость между размерностями переменных

log[a_old] = log [a_cur] =
= log[b_old] = log[b_cur]

log[a] = log[b] = 0 => [a] = [b] = 1

Переменные a и b являются безразмерными

```
for (int i = 1; i < power; i++)
{
        a_old = a_cur;
        b_old = b_cur;
        a_cur = a*a_old - b*b_old;
        b_cur = a*b_old + b*a_old;
}
```

a_cur = a*a_old / b*b_old;

Вычисления производятся в цикле

На очередной итерации исполняется некорректное деление

Метод контроля размерностей

a_old	a_cur	b_old	b_cur	a	b
1	-1	0	0	0	0
0	1	-1	0	0	0
0	0	1	-1	0	0
0	0	0	0	1	0
0	0	0	0	0	1
-1	1	1	0	-1	1

$$-1 \cdot \log[a\_old] + 1 \cdot \log[a\_cur] + 1 \cdot \log[b\_old] + 0 \cdot \log[b\_cur] - 1 \cdot \log[a] + 1 \cdot \log[b] = 0$$

Исполнение одинаковых операторов не добавляет в систему новых уравнений

Исполнение подмененной команды задает новое уравнение

Метод контроля размерностей

a_old	a_cur	b_old	b_cur	a	b
1	-1	0	0	0	0
0	1	-1	0	0	0
0	0	1	-1	0	0
0	0	0	0	1	0
0	0	0	0	0	1
-1	1	1	0	-1	1

a_old	a_cur	b_old	b_cur	a	b
1	0	0	0	0	0
0	1	0	0	0	0
0	0	1	0	0	0
0	0	0	1	0	0
0	0	0	0	1	0
0	0	0	0	0	1

log[a_old] = log [a_cur] =
= log[b_old] = log[b_cur]

log[a] = log[b] = 0

Переменные a и b являются безразмерными

Условие нарушения корректности
Переменная, изначально имевшая размерность, в ходе проведения вычислений становится безразмерной

log[a_old] = log [a_cur] =
= log[b_old] = log[b_cur] =
= log[a] = log[b] = 0

Все переменные являются безразмерными

Ограничения метода

Метод контролирует только команды по изменению состояния переменных и не контролирует значения переменных

Невозможность обнаружения модификаций, сохраняющих систему размерностей

_____ a_cur = a*a_old - b*b_old;

_____ a_cur = a*a_old + b*b_old + b*b_old;

Отсутствует контроль значений переменных

Невозможность обнаружения семантических ошибок управляющих операторов

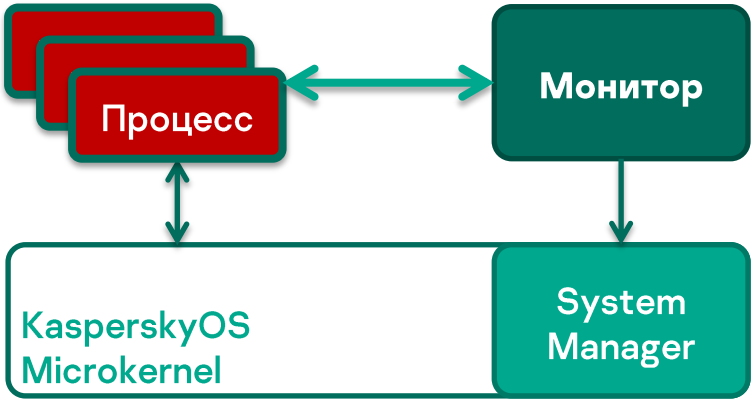
Agenda

Постановка задачи

Метод контроля размерностей

Подходы к внедрению метода

Архитектура решения



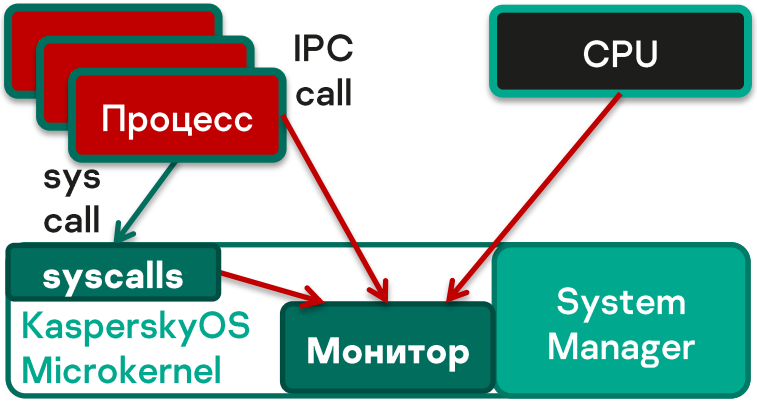
Предусматривается монитор контроля размерностей

Монитор оповещает ОС о нарушении работоспособности процессов

Монитор анализирует получаемую информацию о командах

Анализ производится с помощью метода контроля размерностей

Программный монитор



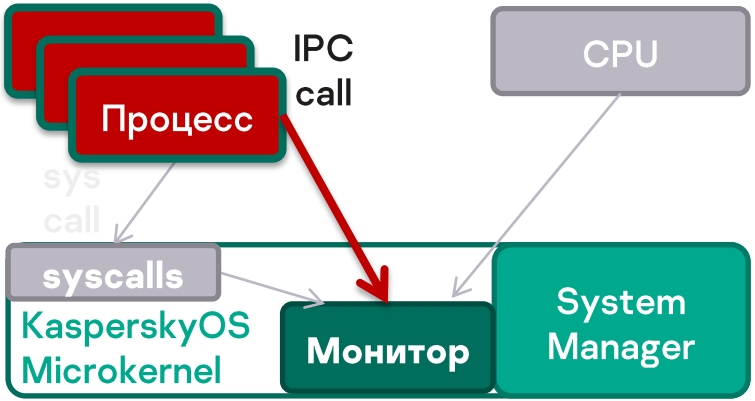
Процесс-монитор является доверенным

Возникает проблема источника информации

Источники информации

- Контролируемые процессы
- Операционная система
- Аппаратное обеспечение

Информация от процесса



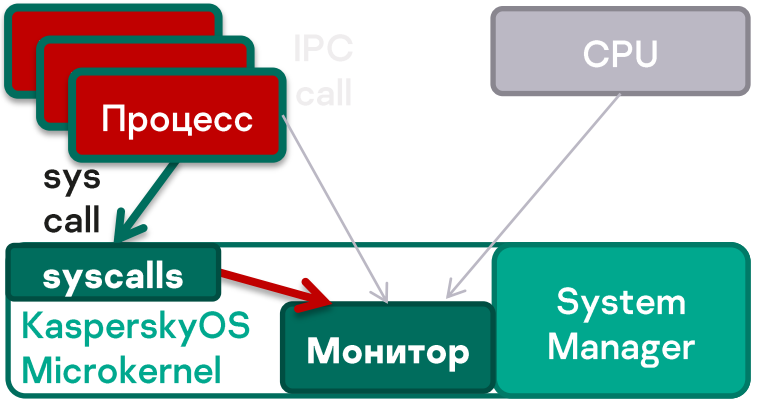
Контролируемые процессы оповещают монитор

Оповещение посредством механизма IPC

Возникает проблема доверия к получаемой информации

Требуется атомизация команд и оповещения

Информация от ОС



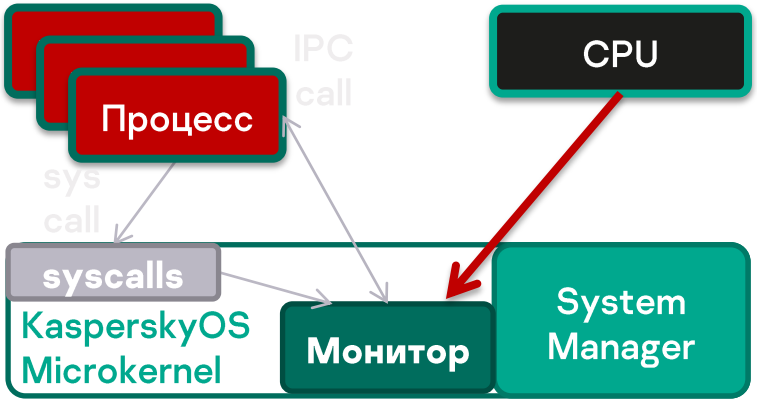
Системные вызовы атомизируют вычисления и оповещение

Монитор имеет доступ к информации о системных вызовах

Процесс производит вычисления посредством системных вызовов

Возникает падение производительности

Информация от CPU



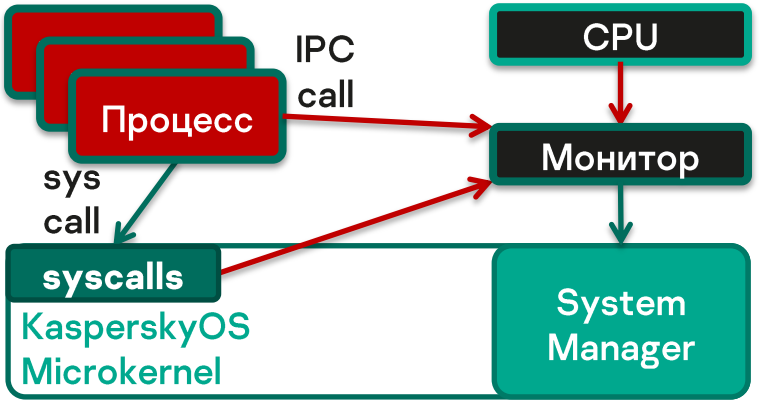
Информация о выполненных командах получается аппаратно

Монитор имеет доступ к исполняемым CPU командам

Монитор анализирует получаемую информацию о командах

Требуется специализированное АО для доступа к командам

Аппаратный монитор



Монитор выступает в качестве отдельного устройства

Источники информации могут быть теми же

Не всегда возможно использовать дополнительное устройство

Требуется проектирование устройства

Примите участие в коротком опросе

Спасибо за внимание!

Данила Пучкин — **Разработчик-исследователь** — **Danila.Puchkin@kaspersky.com**

Игорь Сорокин — **Руководитель группы системных исследований** — **Igor.Sorokin@kaspersky.com**

kaspersky