

Архитектура и реализация KasperskyOS Kaspersky Security System

Андрей Духвалов

Руководитель Департамента Перспективных Технологий

Andrey.Doukhvalov@kaspersky.com

OSDay 2016, Иннополис

ТАК ЧТО ЖЕ ТАКОЕ БЕЗОПАСНАЯ ОС?

Принципы безопасности

- заложенные в архитектуру
- соблюдаемые при реализации и конфигурации системы

Реализация различных политик безопасности

- отвечающих потребностям всевозможных применений системы
- повторно используемых и сочетаемых между собой

Обеспечение высокой степени доверия

- к реализации системы путем проведения формальной оценки
- к реализации политики путем включения конфигураций в TCB

ЦЕЛЬ РАЗРАБОТКИ

Надежная платформа для разработки широкого спектра специализированных (программно-аппаратных) решений с высокими требованиями по информационной безопасности

СОДЕРЖАНИЕ

- Основные архитектурные решения
- Особенности реализации подсистемы безопасности
- Преимущества и ограничения

The background of the slide is a blue wireframe cityscape. It features several tall, rectangular buildings of varying heights, all constructed from a grid of white lines. The perspective is from a low angle, looking up at the structures. The lines are thin and white, creating a transparent, skeletal effect. The overall color scheme is a deep blue with white wireframe lines.

ОСНОВНЫЕ АРХИТЕКТУРНЫЕ РЕШЕНИЯ В KASPERSKYOS

Принципы безопасности в призме реализации

ДВА ПРИНЦИПА



В основе системы

Микроядерная архитектура, реализующая
разделение доменов безопасности

+

Выделенная подсистема безопасности,
предназначенная для вычисления политик

ПРИНЦИП 1



**Единый механизм
межпроцессного взаимодействия
(IPC)**

Реализуется на уровне ядра
Обеспечивает полноту контроля

МИКРОЯДРО

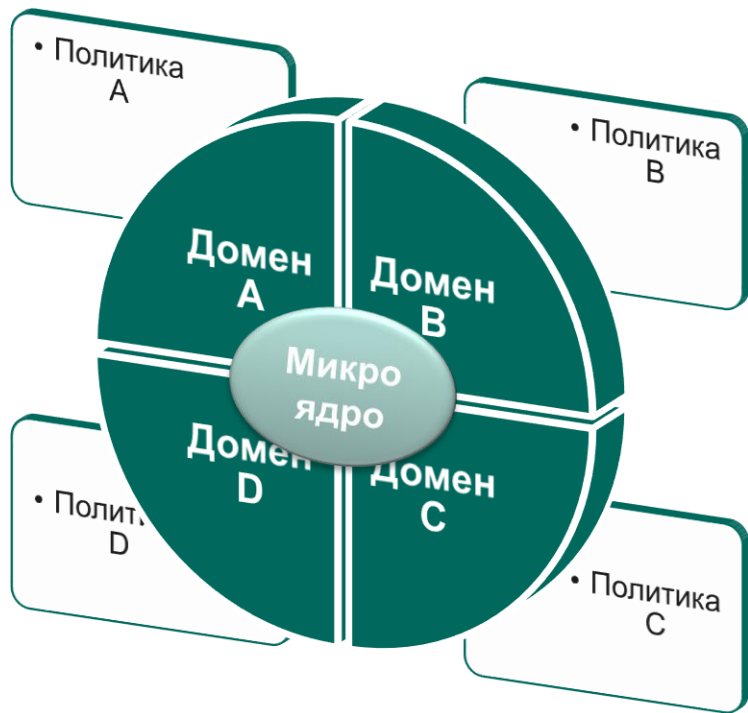


Реализует межпроцессное взаимодействие

Не существует способов взаимодействия в обход микроядра.

Взаимодействие синхронное (рандеву).

ЯДРО РАЗДЕЛЕНИЯ ДОМЕНОВ



Separation Kernel

Предназначено для эмуляции работы физически распределенной системы на одном процессоре (J.Rushby)

Реализация: микроядро/гипервизор

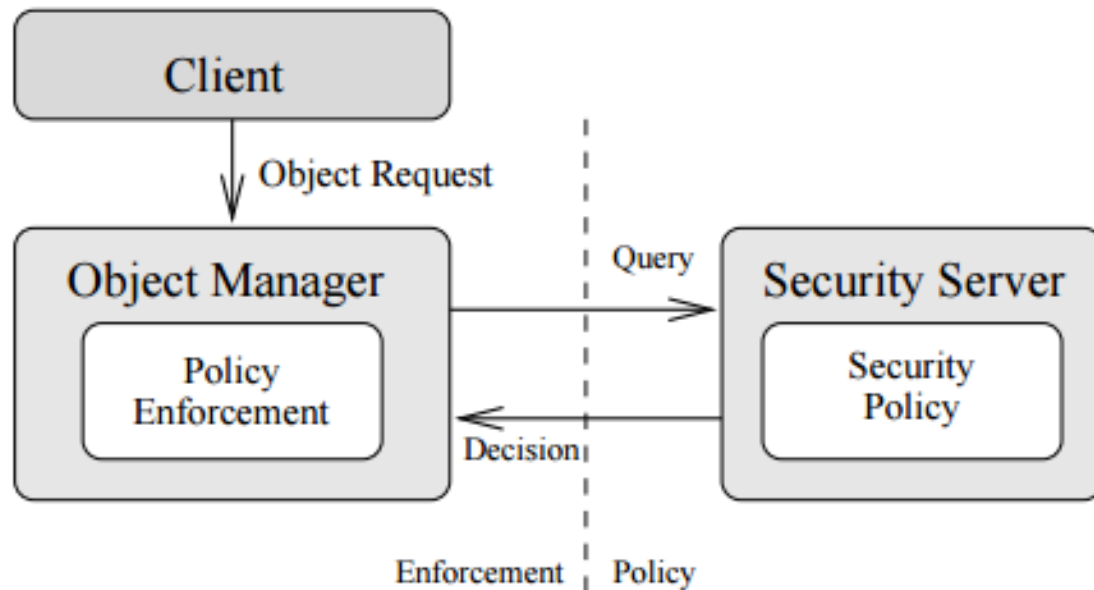
ПРИНЦИП 2



Выделенная подсистема безопасности

Гибкий контроль взаимодействия программных компонентов внутри информационной системы

АРХИТЕКТУРА БЕЗОПАСНОСТИ FLASK



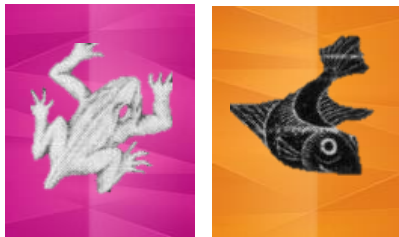
<https://www.cs.cmu.edu/~dga/papers/flask-usenixsec99.pdf>



ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ

Ядро гибкой и эффективной защиты

НЕОБХОДИМОСТЬ СУЩЕСТВЕННО РАЗЛИЧНЫХ ПОЛИТИК



Для каждого устройства, системы, сети

Своя область применения

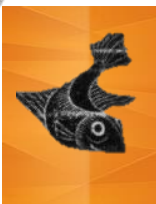
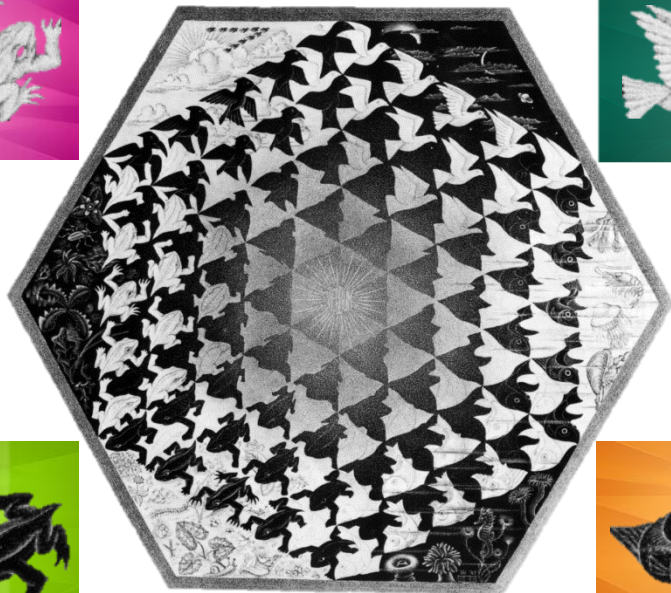
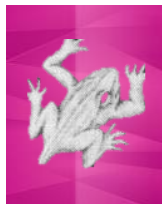
Свои цели

Своя политика безопасности

Своя степень принятия рисков

- связанная с доверием
- связанная со стоимостью защиты

УНИВЕРСАЛЬНАЯ ПОДСИСТЕМА БЕЗОПАСНОСТИ

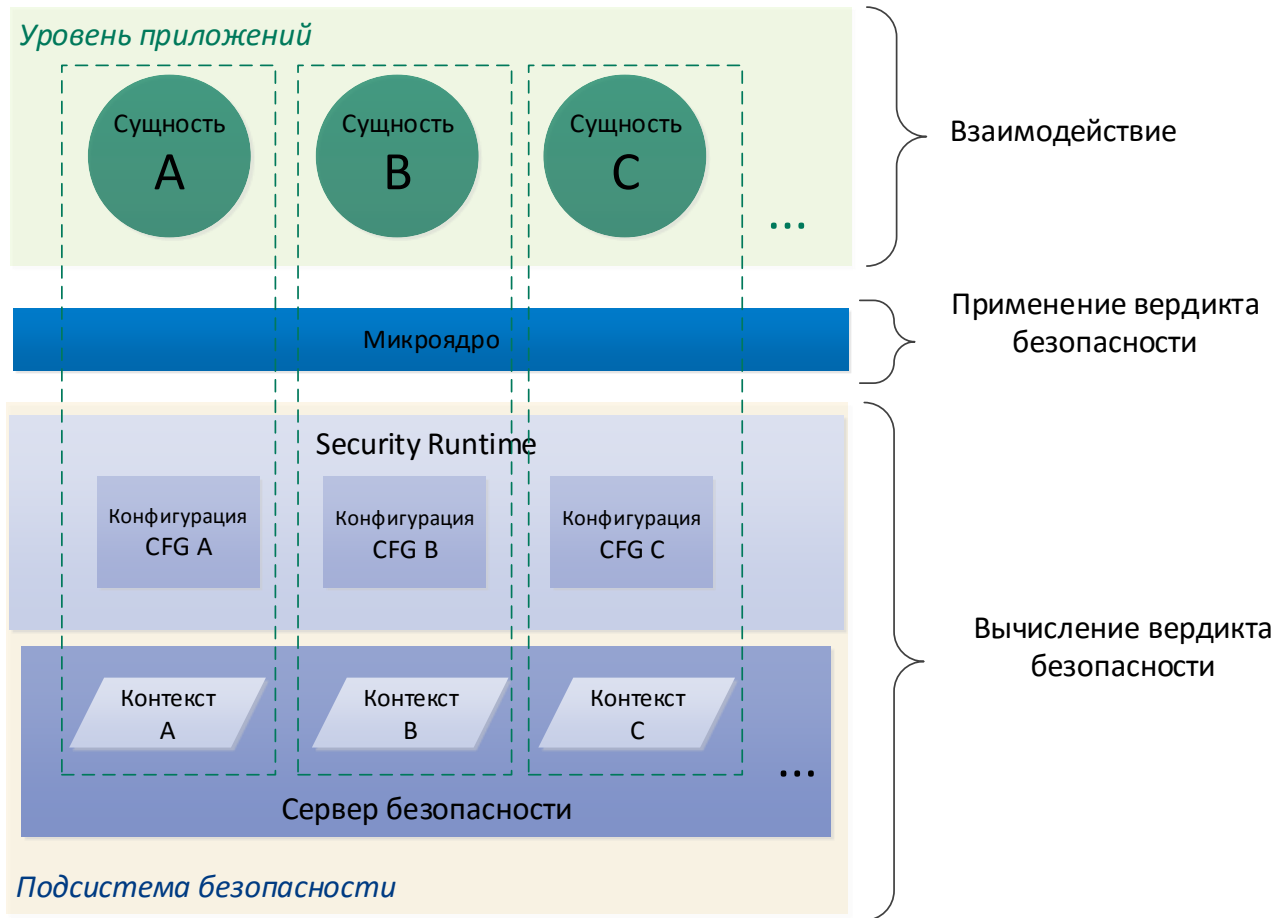


Реализация правил безопасности

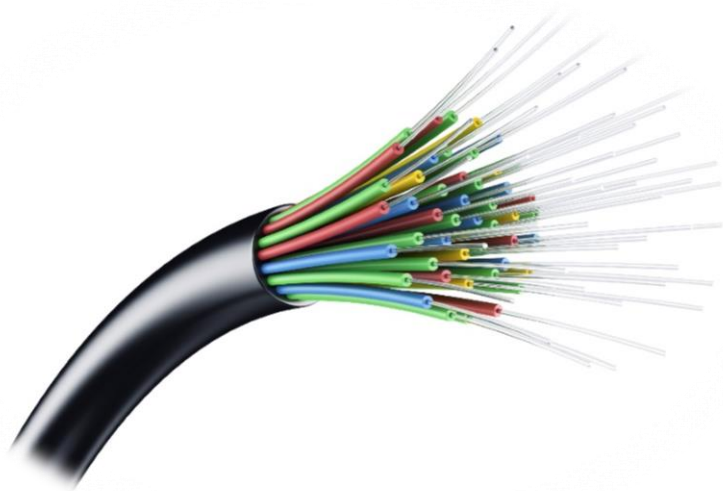
С возможностью комбинировать базовые и специализированные политики.

В соответствии с индивидуальными требованиями конкретной системы.

Без необходимости поддерживать ненужные механизмы и сложные конфигурации.



ТИПИЗИРОВАННЫЕ ВЗАИМОДЕЙСТВИЯ



Уникальное свойство KOS

Типизация в рамках единого канала согласно IDL-описаниям

Политики безопасности применяются в соответствии с типом взаимодействия

КОНФИГУРАЦИИ БЕЗОПАСНОСТИ

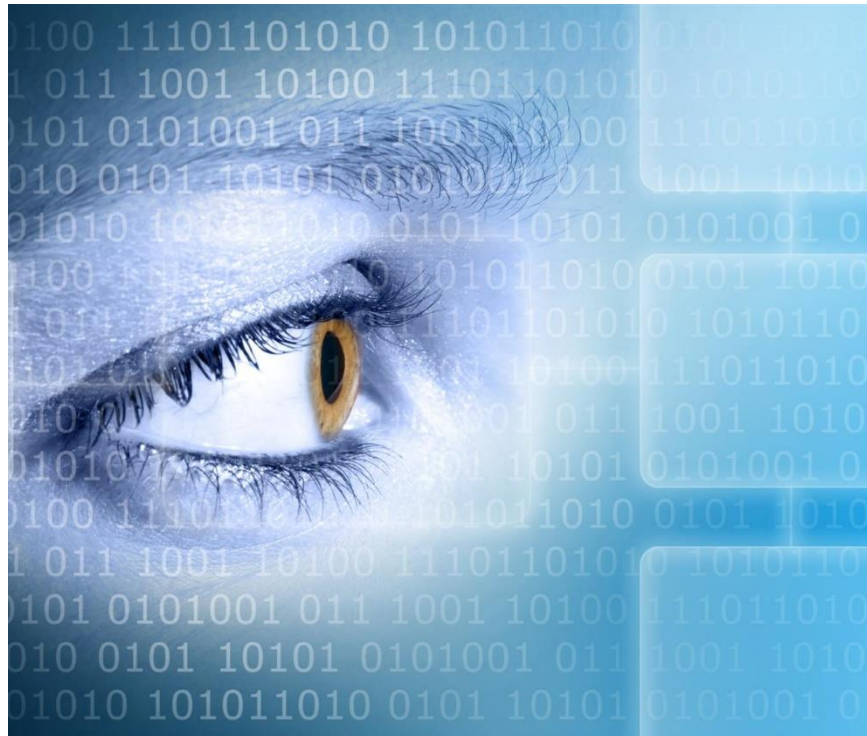


Определяют использование политик

Связывают типы взаимодействий и политики безопасности

Определяют реакцию на события безопасности

ВИДЫ СОБЫТИЙ БЕЗОПАСНОСТИ



Вызов подсистемы безопасности

В случае одного из событий:

- Запуск сущности (процесса)
- Обращение к сущности по IPC
- Вызов интерфейса безопасности



ПРЕИМУЩЕСТВА И ОГРАНИЧЕНИЯ KASPERSKYOS

Известные на данный момент

ПРЕИМУЩЕСТВО: ПОЛНОТА КОНТРОЛЯ



На всех уровнях

На уровне архитектуры:

принцип полноты перекрытия (IPC)

На уровне реализации:

открытый дизайн (компонентная модель)

На уровне конфигурации:

принцип безопасных умолчаний (default deny)

ПРЕИМУЩЕСТВО: ГИБКОСТЬ КОНТРОЛЯ



На всех уровнях

На уровне архитектуры:
расширяемый сервер безопасности

На уровне реализации:
типизация межпроцессного взаимодействия

На уровне конфигурации:
большое количество событий, поддающихся
конфигурации

ПРЕИМУЩЕСТВО: ВЕРИФИЦИРУЕМОСТЬ



На всех уровнях

На уровне архитектуры:

Микроядерная архитектура, выделенное TCB

На уровне реализации:

Компонентная модель для приложений

На уровне конфигурации:

Декларативный язык конфигураций

ПРЕИМУЩЕСТВО: ПОДДЕРЖКА МАНДАТНОГО КОНТРОЛЯ ДОСТУПА



На всех уровнях

На уровне архитектуры:

Выделенная подсистема безопасности, обеспечивающая различные политики

На уровне реализации:

Прозрачный для приложений контроль на уровне внешних интерфейсов

На уровне конфигурации:

Жесткая конфигурация, включенная в TCB

ПРЕИМУЩЕСТВО: ОБЯЗАТЕЛЬНАЯ РАЗМЕТКА И КОНФИГУРАЦИЯ



На всех уровнях

На уровне архитектуры:

Жестко заданные конфигурации приложений

На уровне реализации:

Приложение без конфигурации его допустимого поведения не может функционировать.

На уровне конфигурации:

Аппаратные и прикладные ресурсы должны быть помечены атрибутами безопасности.

НЕДОСТАТОК: ОГРАНИЧЕНИЯ ЕДИНОГО ИРС



Обратная сторона полноты контроля

- Неполная POSIX совместимость
- Вопросы контроля доступа к ресурсам
- Вопросы производительности

НЕДОСТАТОК: ОГРАНИЧЕНИЯ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ



Обратная сторона гибкости контроля

- Трудности корректного выбора политик (выход за пределы модели – отказ)
- Жесткие конфигурации
- Вопросы кэширования вердиктов

НЕДОСТАТОК: СЛАБАЯ СВЯЗНОСТЬ СИСТЕМЫ



**Обратная сторона поддержки
мандатного контроля и строгого
определения безопасности**

Фактически две независимые системы

- среда выполнения приложений
- среда принятия решений

синхронизация которых требует серьезной
работы

ОСНОВНЫЕ ОСОБЕННОСТИ KASPERSKYOS

Архитектура на основе разделения доменов

- следствие единого IPC
- позволяет усилить информационную и функциональную безопасность

Выделенная подсистема безопасности

- реализует всевозможные политики безопасности
- политики повторно используются и сочетаемы

Обеспечение высокой степени доверия

- микроядро и компонентная модель упрощают верификацию
- конфигурации безопасности являются частью TCB

Архитектура и реализация KasperskyOS Kaspersky Security System

Андрей Духвалов

Руководитель Департамента Перспективных Технологий

Andrey.Doukhvalov@kaspersky.com

OSDay 2016, Иннополис