KASPERSKY lab

МОДЕЛИ БЕЗОПАСНОСТИ И АРХИТЕКТУРНЫЕ ПОДХОДЫ К ИХ РЕАЛИЗАЦИИ В СИСТЕМАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Екатерина Рудина

Департамент защиты критической инфраструктуры

Перспективные технологии

ДЕПАРТАМЕНТ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

НАША РАБОТА И ПРОЕКТЫ

Участие в национальных и международных инициативах по обеспечению безопасности критической инфраструктуры

- Участник ENISA ICS Stakeholder Group
- Участник Industrial Internet Consortium
- Участник MILS Community в рамках EURO-MILS Project
- Работа с национальными методическими и нормативными документами (ФСТЭК)

Стандартизация

- Участник рабочей группы IEEE-SA P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)
- Участник в 362 ТК по стандартизации РФ «Защита информации»
- Работа с 22 ТК «Информационные технологии» и 306 ТК «Приборостроение» в рамках подготовки профильных стандартов

Работа с промышленными объектами и объектами критической инфраструктуры и разработка

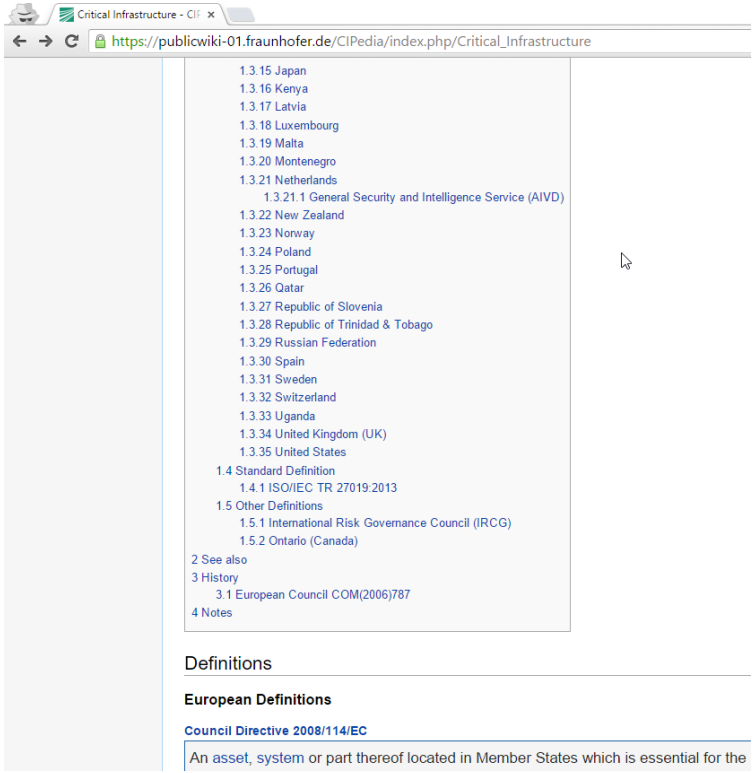
- Kaspersky Industrial Cyber Security - комплексное решение, включающее набор функциональных компонентов и защитных технологий, а также ряд экспертных сервисов.
- Подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется после полного обследования системы кибербезопасности промышленного объекта

ЦЕЛИ БЕЗОПАСНОСТИ
СИСТЕМ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ.

СИСТЕМЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

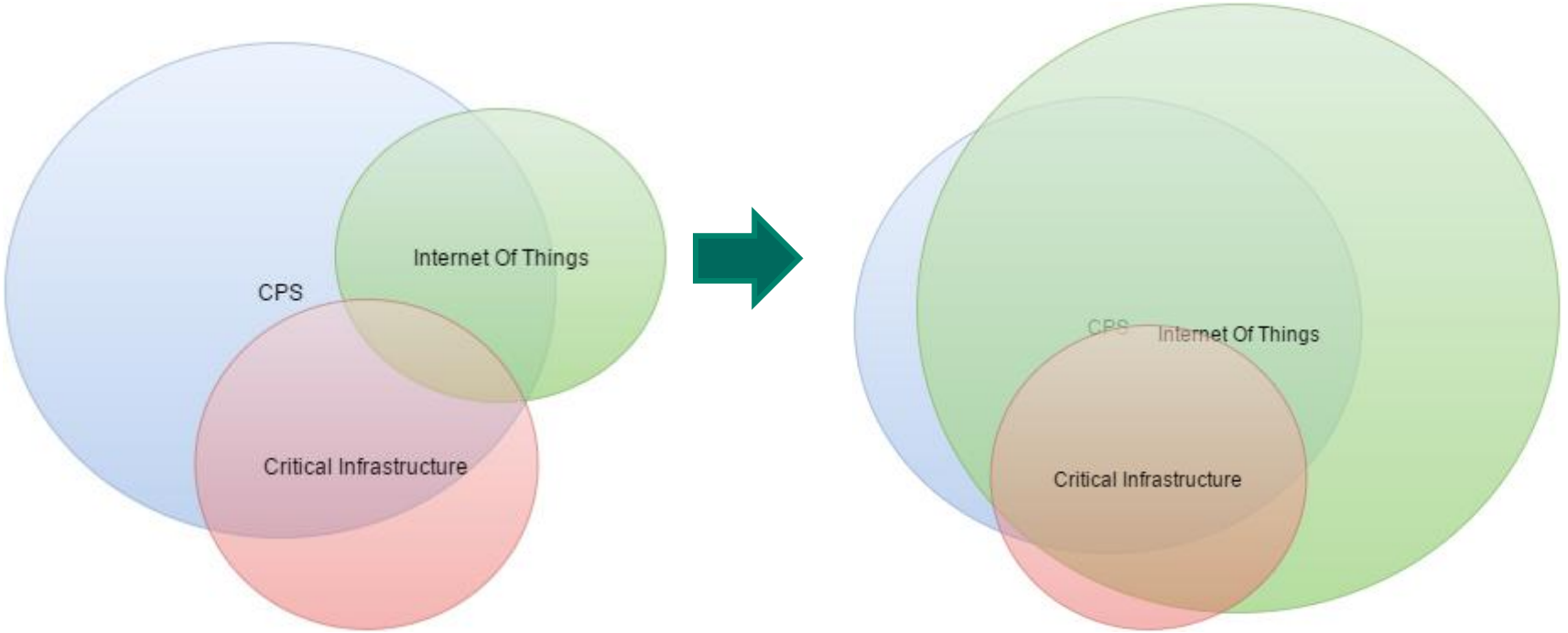
Критическая информационная инфраструктура Российской Федерации – совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка (далее – объекты критической информационной инфраструктуры Российской Федерации)

ЕЩЕ ОПРЕДЕЛЕНИЯ?



KASPERSKY lab

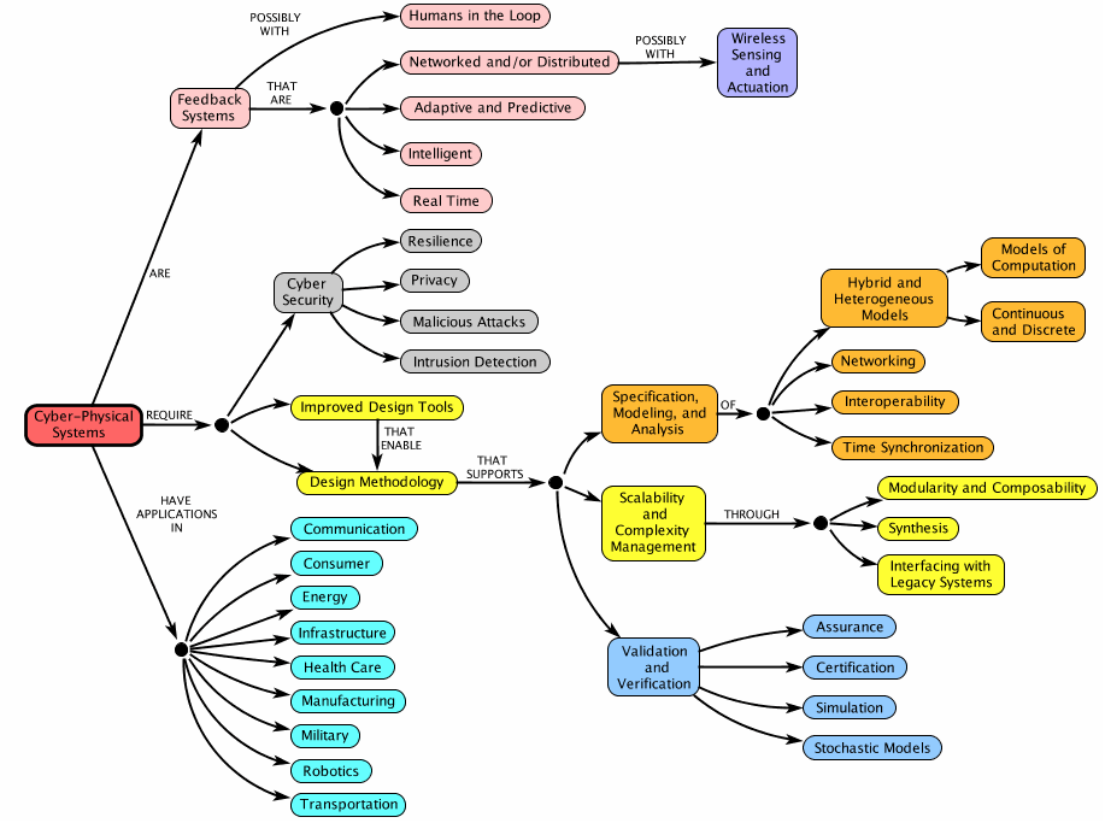
КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ



Cyber-Physical Systems – a Concept Map

See authors and contributors.

http://CyberPhysicalSystems.org



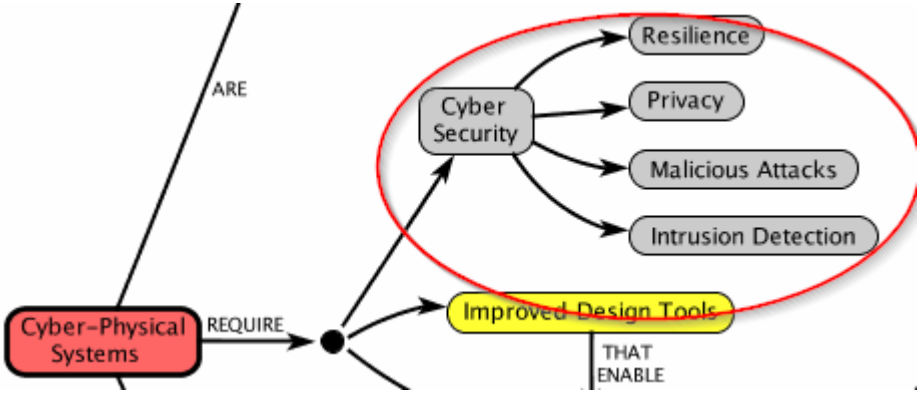
ПРЕДСТАВЛЕНИЕ АСПЕКТОВ БЕЗОПАСНОСТИ

Безопасность

- Функциональная безопасность
- Информационная безопасность

Основные проблемы

- Соотношение ФБ и ИБ
  - Взаимная зависимость и/или противопоставленность
- Аспекты ИБ
  - CIA – не подходит
  - AIC?
  - SRA (safety, resilience, availability)
  - ???



KASPERSKY lab

ЦЕЛИ БЕЗОПАСНОСТИ

(неполный, неконсистентный, и даже не типовой перечень :))

- **Функциональная безопасность (safety)**
- **Надежность (reliability)**
- **Жизнеспособность (resilience)**
- **Доступность (availability)**
- **Устойчивость к намеренным атакам (security) (да?!)**
- **Безаварийный отказ (fail-safety)**
- **Целостность ресурсов (integrity)**
- **Конфиденциальность личной информации (privacy)**
- **Надежность в широком смысле (dependability)…**

МОДЕЛИ БЕЗОПАСНОСТИ
ИХ ВОЗМОЖНОСТИ И ПРИМЕНЕНИЕ

МОДЕЛИ БЕЗОПАСНОСТИ

Два основных типа контроля доступа

- Дискреционный – произвольный контроль, возможность регулирования доступа «изнутри модели»
- Мандатный – принудительный контроль доступа, без возможности несанкционированного влияния на атрибуты доступа

Модель КД != модель безопасности

Модель безопасности это формальное представление политики безопасности, которая необязательно состоит только в КД (хотя формально может сводиться к КД)

МОДЕЛИ БЕЗОПАСНОСТИ

Применение решений преимущественно на основе мандатных моделей в обеспечении безопасности критической инфраструктуры

- Позволяет гарантировать нужные свойства системы (при условии корректной реализации)
- Свойства и функциональной, и информационной безопасности

Каким образом?

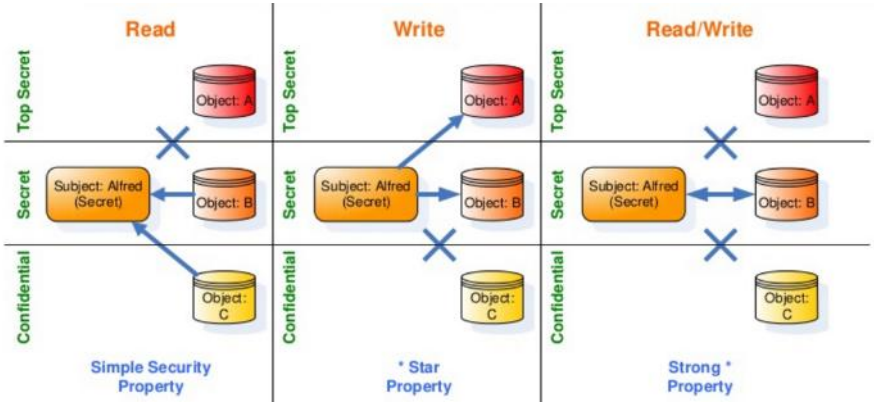
АКТУАЛЬНЫЕ МОДЕЛИ
ДЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛЕЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

МОДЕЛИ МАНДАТНОГО КД

Модель Белла-Лападулы

(конфиденциальность)

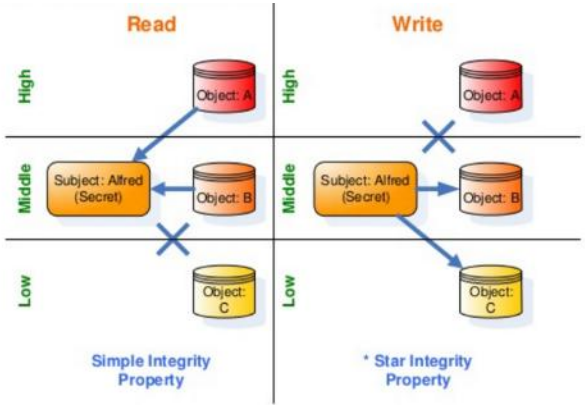
No Read Up, No Write Down



Модель Биба

(целостность)

No Read Down, No Write Up

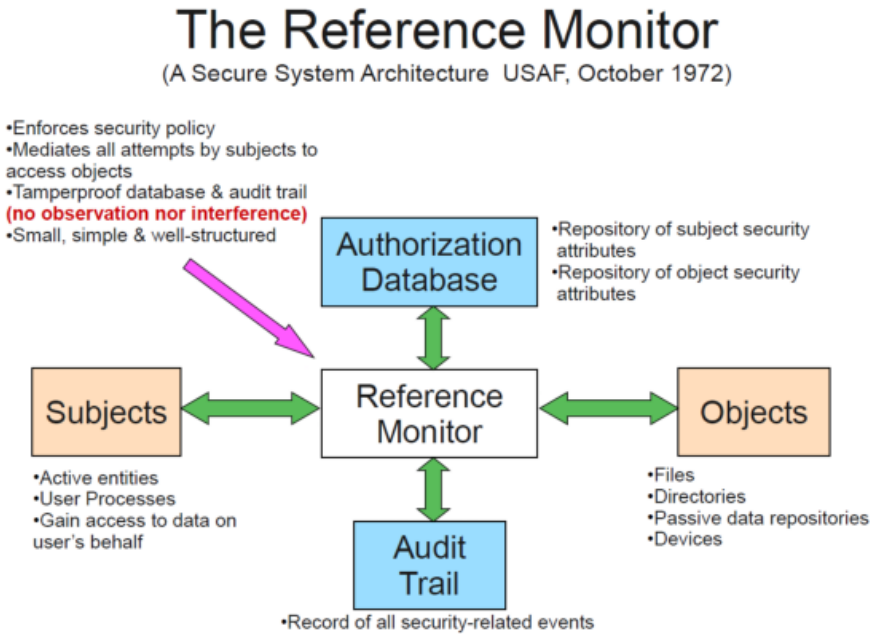


KASPERSKY lab

ЧТО НЕОБХОДИМО ДЛЯ ОБЕСПЕЧЕНИЯ КОРРЕКТНОЙ РАБОТЫ МОДЕЛИ

Монитор безопасности:

- Non-bypassable
- Tamperproof
- Verifiable

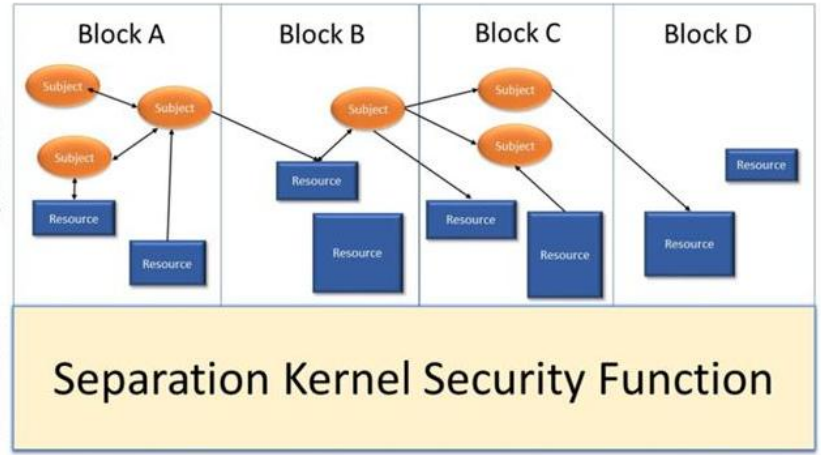


ЯДРО РАЗДЕЛЕНИЯ (SEPARATION KERNEL)

«Предельный случай» монитора безопасности

Задача ядра разделения (J.Rushby, 1981) - создать окружение, которое с точки зрения запускаемых в нем процессов неотличимо от распределенной системы

Каждый процесс в таком окружении считает, что может общаться с другими процессами только путем внешних коммуникаций

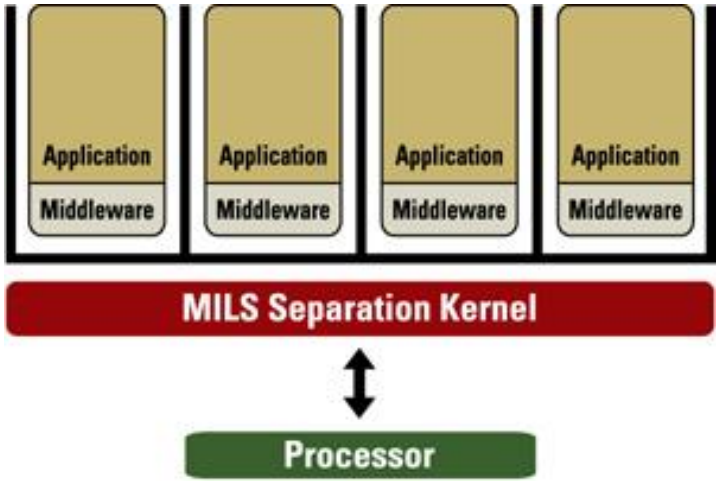


MILS SECURITY ARCHITECTURE

(**Multiple Independent Levels of Security)**

Ключевая идея: гарантии безопасности на уровне архитектуры

Основной принцип: разделение функций (separation of concerns)



KASPERSKY lab

ПОЧЕМУ ИМЕННО ЭТА МОДЕЛЬ АРХИТЕКТУРЫ КЛЮЧЕВАЯ ДЛЯ КРИТИЧЕСКИХ СИСТЕМ?

Позволяет обеспечить и функциональную, и информационную безопасность

Для функциональной безопасности:

- Возможность обеспечить свои свойства исполнения в каждом домене (real-time, изоляция ресурсов и т.п.)
- Исключение взаимного (в том числе случайного) влияния процессов в разных доменах
- Возможность более простой проверки и верификации системы с разделением доменов
- Возможность дублирования функций безопасности для критических объектов (SIS)

Для информационной безопасности

- Возможность реализации междоменного взаимодействия по заданным правилам
- Исключение влияния процессов в доменах на вердикт безопасности (мандатный КД)

ПРОБЛЕМЫ
РЕАЛИЗАЦИИ МОДЕЛЕЙ БЕЗОПАСНОСТИ

ПОЧЕМУ ТАК СЛОЖНО СДЕЛАТЬ КАЧЕСТВЕННЫЙ SK?

Требования на поверку оказываются слишком высокими

Non-bypassable: не должно существовать любых способов обойти. То есть это самый низкоуровневый механизм в системе

- доверие к аппаратной части?
- как реализовать высокоуровневые политики и правила?

Tamperproof: без малейшего намека на доверие к способам связи в системе, в том числе между системными компонентами, и между системными и прикладными компонентами

- как реализовать доверенные части middleware и прикладных процессов?
- Как избежать проблем типа TOCTOU

Verifiable

- формализация целей верификации
- сложность процесса формальной верификации ПО

АРХИТЕКТУРНЫЕ
И ТЕХНОЛОГИЧЕСКИЕ ПОДХОДЫ
К РЕАЛИЗАЦИИ МОДЕЛЕЙ БЕЗОПАСНОСТИ

РЕАЛИЗАЦИЯ MILS

Принципы MILS оказываются применимы и полезны практически в любых типах систем и решений

- Операционные системы реализующие MILS
- Определенным образом сегментированные вычислительные сети (возможно с применением специальных устройств однонаправленной передачи)
- Автоматизированные системы в том числе с физической изоляцией компонентов

Области применения: авионика, автомобильные системы, системы коммуникаций, системы промышленной автоматизации, медицинские системы, системы поддержки железнодорожной автоматики…

НЕДАВНИЙ СЛУЧАЙ

Основная задача, которую решали исследователи

Очень упрощенно:

Как преодолеть изоляцию между развлекательным (entertainment) модулем и общей шиной (CAN) модулей управления (safety critical ECU) и вызвать тем самым какие-либо физические последствия

- Каналы связи между модулями есть, чем «умнее» автомобиль, тем их, как правило, больше
- Как сделать так чтобы их нельзя было использовать со злым умыслом?

РЕАЛИЗАЦИЯ SEPARATION KERNEL

«Второе дыхание» концепция получила с развитием аппаратной виртуализации

SK на основе гипервизора:

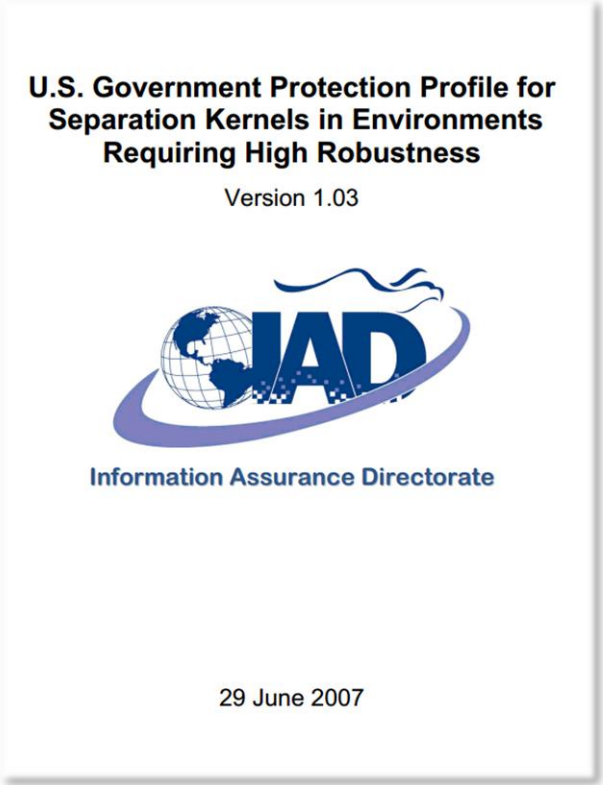
- Позволяет удовлетворить основные требования к SRM
- Подходит для встраиваемых решений
- Safety: Позволяет запустить в разных доменах системы общего и специального назначения (например, в одном домене систему реального времени, в другом Linux) - safety
- Security: Позволяет в разных доменах запустить системы в разными требованиями к ИБ («корпоративный» и «личный» режим на мобильном устройстве с гарантиями конфиденциальности и целостности)

ТРЕБОВАНИЯ COMMON CRITERIA

Профиль защиты

Описывает требования в системам на SK

Может применяться для сертификации (создания заданий по безопасности) платформы разделения: операционных систем, систем на основе гипервизора



РЕАЛИЗАЦИЯ SEPARATION KERNEL

Системы на Separation Kernel

- Green Hills
  - Multivisor
- Wind River
  - Wind River® VxWorks® MILS Platform
- Lynx
  - LynxSecure
- SYSGO
  - PikeOS
- Muen Project
  - Muen Separation Kernel

Практически все на основе гипервизора некотрые на основе паравиртуализации

Почти все “в комплекте” с RTOS

- KasperskyOS

НЕРЕШЕННАЯ ПРОБЛЕМА

Для SK на уровне гипервизора с аппаратной поддержкой

Non-bypassable: done

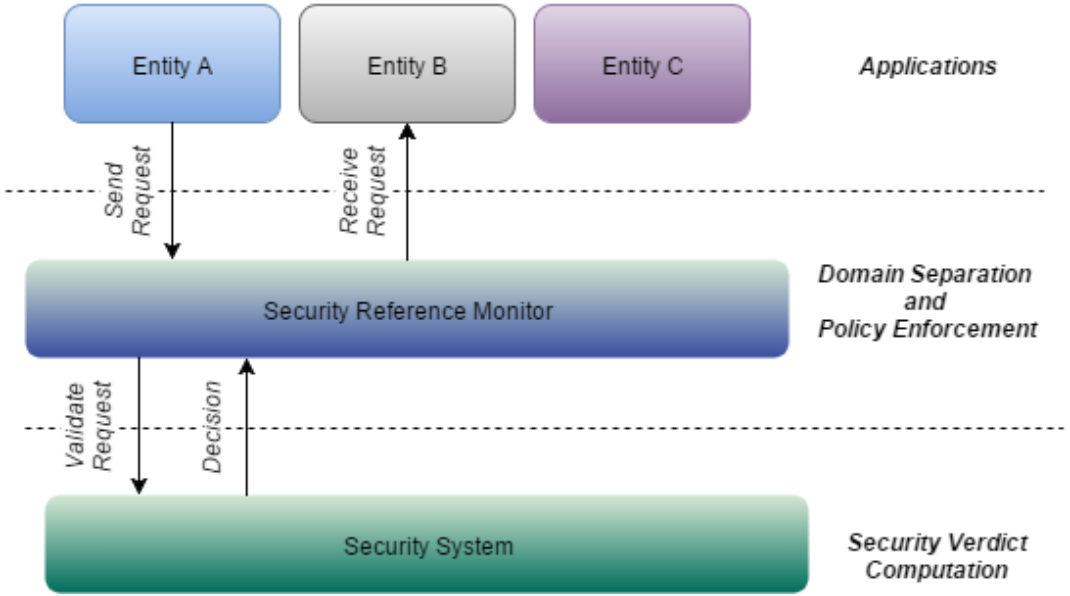
- **как реализовать высокоуровневые политики и правила?**
- *Не утяжеляя гипервизор*
- *Сохраняя семантику политик*

John Rushby, 1981 (снова)

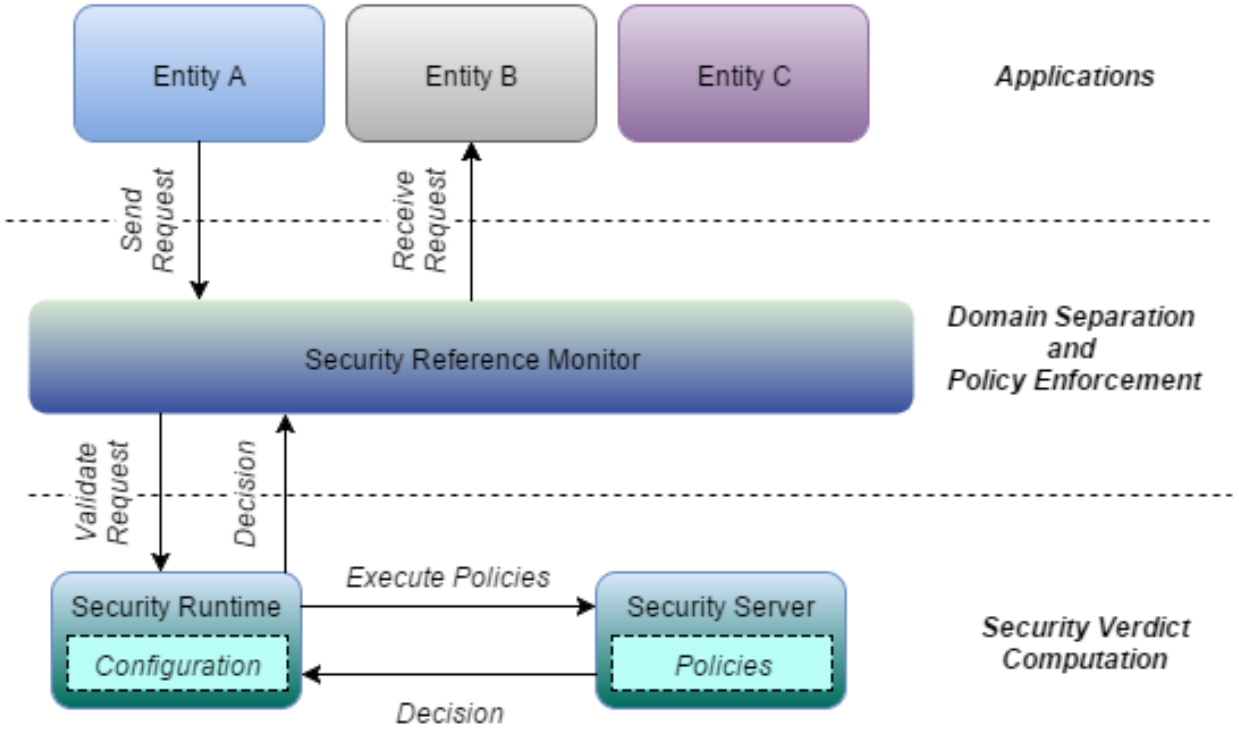
Policy enforcement is not the concern of a security kernel

АРХИТЕКТУРА FLASK

Выделенный сервер безопасности



ВАРИАНТ РЕАЛИЗАЦИИ FLASK



ВОЗМОЖНЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

Необязательно «классические» мандатные модели БЛМ и Биба

- Domain and type enforcement
- Object capabilites
- Flow (states flow enforcement)
- Role-base access control
- Multilevel security
- Темпоральные логики
  - Linear Temporal Logic (UNTIL, NEXT)
  - Past Time LTL (SINCE, PREV)
  - Metric Past Time LTL (SINCE, PREV), Metric LTL (SINCE, UNTIL)

ПРОЕКТИРОВАНИЕ БЕЗОПАСНЫХ РЕШЕНИЙ ДЛЯ СИСТЕМ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

КРАТКОЕ ОПИСАНИЕ

Подробное – тема для отдельной лекции (и не одной)

Изучение области и потребностей	Изучение области и моделирование угроз
Формирование требований функциональности	Формирование требований безопасности
Описание проектных решений (учитывающих потребности области, валидация в отношении нужной функциональности)	**Описание проектных решений (учитывающих домены безопасности, их связи, валидация в отношении требований безопасности)**
Реализация	Реализация функций безопасности
Тестирование	Тестирование безопасности
Деплоймент, сопровожение, обучение, использование	Усиление, конфигурирование, обучение, аудитб багтрекинг

КЛЮЧЕВЫЕ ФАКТОРЫ БЕЗОПАСНОСТИ

Моделирование угроз

и проектирование на основе моделей безопасности с гарантированными свойствами

- Ключевым фактором всех аспектов безопасности решения является правильное проектирование на основе детальной модели угроз
- Фактически любые меры и практики безопасности (статический и динамический анализ кода, тестирование безопасности, тестирование на проникновение, усиление, аудит) на этапах жизненного цикла после формирования проектных решений являются компенсирующими
- Однако это не делает их необязательными!

ВОПРОСЫ?

АО «Лаборатория Касперского»
Ленинградское шоссе 39А/3
Москва, 125212, Россия
тел.: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab