Использование capability-based security в ядрах операционных систем

Басков Евгений Сергеевич
ИСП РАН (109004, г. Москва,ул. А. Солженицына, дом 25.)
baskov@ispras.ru

Данный доклад посвящен применению подхода *capability-based security* в ядрах операционных систем (ОС). Этот подход заключается в реализации управления доступом к различным ресурсам ОС на основе системы *жетонов* (*capabilities*), использование которых нацелено на отказ от использования неявных прав доступа (ambient authority). Одним из важных результатов применения этого подхода является возможность вынесения большей части политик безопасности из ядра ОС в пользовательское пространство. Данная работа близка к теме конструктивной информационной безопасности, в данный момент совместно разрабатываемой ИСП РАН и Лабораторией Касперского.

В настоящее время *capability-based security* применяется во многих ядрах ОС, однако наблюдается большое разнообразие в выбранных способах реализации этого подхода. В связи с этим понятие *capability-based security* пока не получило четкого определения. К реализациям *capability-based security* относятся файловые дескрипторы UNIX-like ОС, фреймворки **Capsicum** и **Genode**, а также ряд микроядер, включающих в себя **Zircon**, **Mach**, **seL4** и **EROS**.

В докладе *capability-based security* сравнивается с более известным подходом на основе *Access Control List* (ACL) и представляется обзор наиболее интересных реализаций механизмов *capability-based security* в ядрах операционных систем. Формулируются ключевые особенности и понятия входящие в *capability-based security*, в том числе само понятие *capability* — неподделываемого локального идентификатора объекта ядра с прикрепленными к нему правами доступа и возможностью передачи доступа посредством механизмов межпроцессного взаимодействия.

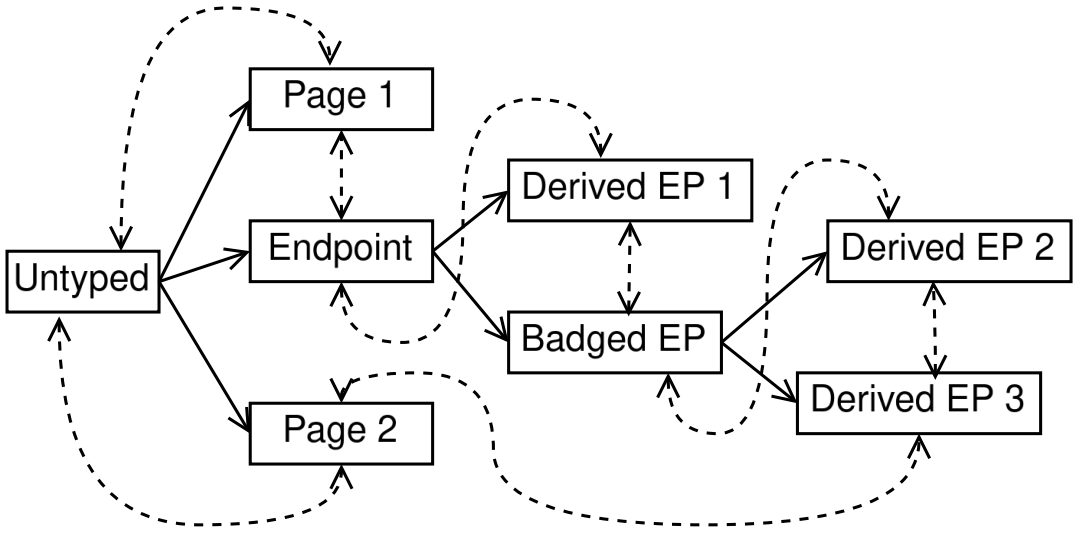

Рис. 1: Структуры данных capabilities в seL4

Также описывается ряд важных расширений базовых механизмов *capability-based security*, которые приводят к улучшению безопасности, предсказуемости и гибкости систем, построенных с использованием конкретных реализаций *capability-based security*. Изначальные реализации данного подхода имели ряд проблем с контролем распространения доступа и последующего отзыва раннее предоставленного доступа. Текущие реализации используют ряд различных расширений, которые устраняют эти проблемы. К другим аспектам реализации относится поддержка *ограниченных capabilities*, которые

предоставляют доступ к ограниченному кругу операций над объектом, описываемым *capability*, поддержку уникальных имен *capability* и наличие унифицированного интерфейса системных вызовов.

Помимо этого обозреваются наиболее интересные аспекты реализации *capability-based security* и связанных структур данных, которые влияют на накладные расходы, производительность, а также простоту применения реализаций механизмов, используемых в данном подходе. Рассматриваются реализации данного механизма в ядрах **seL4** и **EROS**, поскольку эти ядра имеют наиболее продвинутые и гибкие варианты механизмов *capability-based security* и используют данных подход в качестве основного механизма управления и контроля доступа к ресурсам ядра. Некоторые аспекты, такие как структура пространства имен *capabilities* описываются применительно к более широкому кругу реализаций.

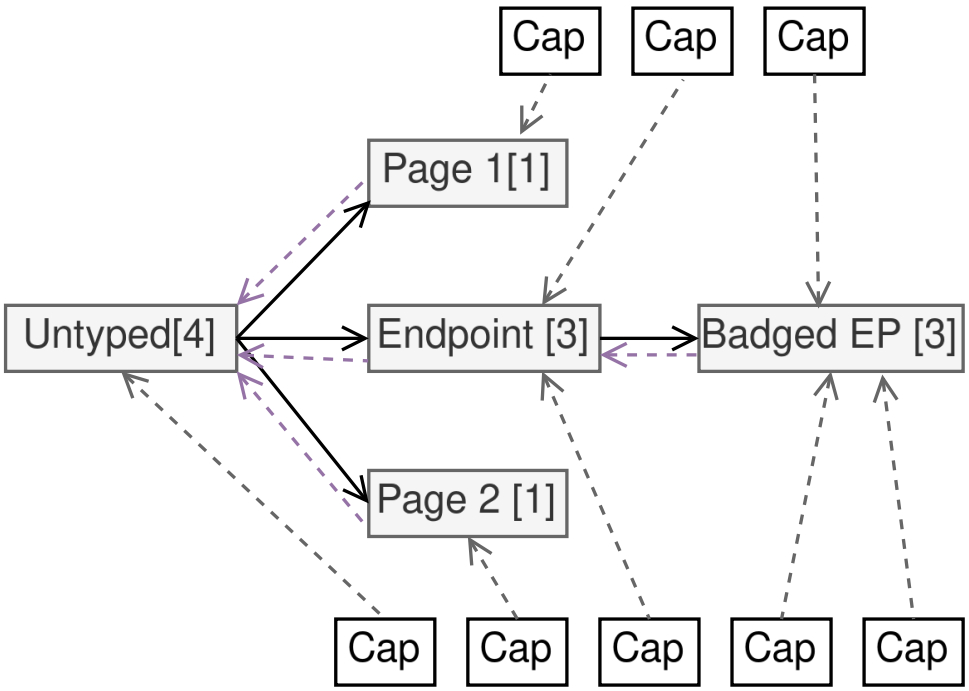

Рис. 2: Структуры данных capabilities в новом микроядре

В заключение к данному обзору представляется реализация механизмов *capability-based security*, которая используется в экспериментальном микроядре общего назначения, которое позволяет обеспечить достаточную гибкость и производительность для реализации интерфейсов **POSIX**, при этом минимизируя накладные расходы. Эта реализация имеет некоторые преимущества по сравнению существующими реализациями данного подхода применительно к микроядру общего назначения, поскольку остальные системы имеют меньшую гибкость, большую сложность или проблемы с масштабируемостью на современный системах, имеющих большое число процессорных ядер.