Интеграция средств гранулярного контроля безопасности поведения приложений в ОС Линукс

Выполнил: Фёдор Сахаров
Научный руководитель: Гамаюнов Д. Ю.

Лаборатория вычислительных комплексов ВМК
МГУ имени М.В.Ломоносова

Москва, 2011

Постановка задачи

Цель:

Расширение метода контроля поведения приложения, основанного на использовании политик, для увеличения гранулярности при контроле поведения приложений.

Задача:

Разработка и реализация средства гранулярного контроля поведения разбитого на состояния приложения со стороны ядра Линукс.

Для достижения указанной цели необходимо:

- Составить обзор существующих систем безопасности уровня ядра ОС.
- Разработать набор инструментов для разметки приложений контрольными точками.
- Разработать подсистему ядра Линукс, способную переключать профиль SELinux приложения при изменении состояния.
- Провести испытание средства на уязвимом приложении.

Обзор систем безопасности уровня ядра ОС.

В данной работе был сделан обзор 4 систем безопасности уровня ядра ОС. Критерии обзора:

- Реализованные модели безопасности.
- Возможность изменять матрицу доступа в процессе исполнения.
- Динамическая смена контекстов.
- Классы вредоносных действий, предотвращаемых системой.

Обзор показал, что ни одна из существующих систем безопасности уровня ядра ОС не предоставляет возможности динамически изменять контекст приложения.

Анализ поведения приложения с использованием контрольных точек

Для решения поставленной задачи была реализована система, позвляющая изменять контекст безопасности приложения в зависимости от его внутреннего состояния. Реализованная система отвечает следующим требованиям:

- Наблюдение и изменение контекстов производится «прозрачно» для приложения.
- Наблюдаемое приложение не модифицируется.

Изменения ядра ОС Линукс

Основная версия ядра ОС Линукс не позволяет динамически изменять контексты безопасности приложения.
Для решения поставленной задачи были внесены следующие изменения в ядро Линукс:

- Возможность динамически изменять контексты приложений из модулей ядра
- Возможность отслеживать события запуска новых процессов в системе

Контрольные точки

Контрольной точкой считается адрес в сегменте кода виртуального адресного пространства приложения.
Для наблюдения за попаданием исполнения на контрольные точки были использованы подсистемы utrace и uprobes ядра Linux.
Данные системы позволяют:

- Отслеживать события попадания исполнения на контрольные точки
- Отслеживать системные вызовы и другие события в наблюдаемом приложении

Результаты

Результаты

- Проведен обзор существующих систем безопасности уровня ядра ОС.
- Были внесены изменения в ядро Линукс, позволяющие производить динамическую смену контекстов в приложении.
- Реализован модуль ядра, позволяющий контролировать поведение приложений с использованием контрольных точек и изменять контекст безопасности наблюдаемых приложений в зависимости от их внутреннего состояния.
- Проведено испытание реализованного модуля на модельном примере уязвимого приложения.

Спасибо за внимание. Вопросы?