XACML – СТАНДАРТ УПРАВЛЕНИЯ ПОЛИТИКАМИ БЕЗОПАСНОСТИ.

Литвяков Е.В.
Российский Университет Дружбы Народов

В данной работе рассмотрены современные принципы безопасности бизнес ориентированных систем, с акцентом на управление политиками безопасности.
Ключевые слова: расширяемый язык контроля доступа, стандарты безопасности, информационная безопасность, компьютерная безопасность, безопасность компьютерных систем.

Введение

Ранее в связи со спецификой предприятий и бизнеса в целом безопасность концентрировалась на централизованных системах. Ключевые моменты безопасности основывалась на мандатных и дискреционных моделях. С развитием бизнеса и его масштабным ростом, с появлением в большей степени распределённых систем на предприятиях, появилась необходимость в полной модификации систем безопасности вплоть до переосмысления принципов безопасности в целом.

Была проделана огромная работа комитетами по стандартизации и рядом институтов и университетов запада по созданию портфеля стандартов чётко описывающих принципы безопасности распределённых систем до мельчайших деталей, в ряде организаций была начата работа над разработкой пакета системы безопасности отвечающей новым требованиям. Также были запущенны успешные коммерческие проекты направленные на предоставление услуг по развёртыванию системы на предприятиях заказчика.

Цель работы изучить и предоставить материал для дальнейшего развития нового мышления безопасности, положить начало изучению этого аспекта в нашей стране и основываясь на наработках зарубежных коллег разрабатывать и совершенствовать стандарт и его реализации, и в ближайшем будущем предоставить проект для поддержки российского бизнеса и государственных некоммерческих предприятий.

Безопасность организации от информационных утечек очень актуальна на сегодняшний день, информация стоит денег, и часть просочившихся с предприятия коммерческих данных может серьёзно ударить по доходам компании. Новые стандарты призваны для удовлетворения естественной потребности в надёжности и безопасности а самое главное соответствие современным реалиям. Так же реализации стандартов направлены на автоматизацию рутинного процесса аутентификации и авторизации, что повышает удобство в администрировании довольно больших предприятий.

Основные аспекты архитектур.

Стандарт XACML выделяет несколько сущностей для обеспечения аутентификации и авторизации в системе. Это PEP – точка применения правила, PDP – точка выбора правила, PAP – точка администрирования политик и PIP – информационная точка. Такое разделение позволяет выявить в системе самостоятельные элементы, основываясь на выполняемых ими функций и инкапсулировать их. Подобная архитектура обеспечивает прозрачность в системе и позволяет легко отслеживать и обеспечивать взаимодействие сущностей.

Точка PEP ответственна за обработку запроса от пользователя, который она делегирует точке PDP, и ожидает специфический ответ, который в конечном итоге преобразует в понятное для пользователя сообщение или событие.

Точка PDP отвечает за принятие решения о доступе к ресурсам, PDP получает всю информацию о соответствующем ресурсе, окружении и субъекте, и проверяет списки правил полученные от PAP точки.

Точка PIP ответственна за сбор соответствующих атрибутов необходимых для PDP и формирования для него соответствующего ответа. Это как уже упоминалось, атрибуты ресурса, атрибуты окружения и субъекта.

PAP – точка администрирования, обеспечивает наполнение списка политик информационной безопасности который будет рассматриваться при принятии решения PDP.

Для внедрения такого подхода на практике требуется дополнительное множество объектов и протоколов обеспечивающих взаимодействие элементов системы. В проекте Trusted Network Control от Trusted Computing Group такие объекты явно стандартизированы и включены в пакет программного обеспечения tnc@fhh. Архитектура проекта несколько сложнее архитектуры стандарта XACML.

Система разбивается на три уровня. Уровень доступа к сети, объединяющий компоненты отвечающие за подключение к сети и безопасность. Уровень оценки целостности, здесь осуществляется общая оценка целостности запроса доступа в отношении политик безопасности. И уровень измерения целостности, здесь осуществляется полный сбор информации, а так же проверка её на целостность. Каждый слой включает в себя часть компонентов отвечающих за определённую функциональность и обеспечивающих её. Все части архитектуры являются логическими обеспечивая тем самым гибкую физическую реализацию.

Сборка и конфигурация пакета tnc@fhh.

В реализации можно выделить ряд базовых модулей обеспечивающих основную функциональность системы в соответствии со спецификацией стандарта.

В ходе работы была собрана, и запущена реализация системы безопасности от Trusted Computing Group, были настроены компоненты системы для обеспечения работоспособных функций аутентификации и авторизации. Скачаны пакеты и исходники с официальных хранилищ проекта Trusted Network Connect группы TCG, собраны и скомпилированы библиотеки и сопутствующие заголовочные файлы проекта необходимые для работы системы. Установлен и скомпилирован сервер FreeRADIUS, выполнена его конфигурация для использования внутри туннеля безопасности TTLS. Сконфигурирован PEP компонент архитектуры проекта TNC используемый в качестве VPN шлюза.

Собран, скомпилирован и сконфигурирован компонент системы wpa_supplicant, а так же была выполнена компиляция компонента IMC и настроена его конфигурация для использования совместно с wpa_supplicant. Собран и скомпилирован компонент TNCS роли PDP архитектуры Trusted Network Connect и проведена его конфигурация, так же настроен сетевой экран в соответствии со спецификацией проекта. Собран, скомпилирован и сконфигурирован компонент TNCC роли AR архитектуры TNC.

Установлена последняя версия пакета Trust@FHH XACML PDP и выполнена его конфигурационная настройка – это ключевой момент в управлении политиками безопасности во всей системе. В этой работе была рассмотрена одна из ключевых частей в механизме безопасности, стандарт XACML, описывающий основные этапы аутентификации и авторизации в системе.

Для проверки работоспособности системы на машине был протестирован простой набор политик безопасности.

Выводы

В результате выполнения работы рассмотрены основные этапы обеспечения безопасности в распределённых системах. Рассмотрена специфика стандарта управления политиками XACML и раскрыты его базовые, основные элементы и принципы. Изучена архитектура проекта Trusted Network Connect и развёрнута его реализация под виртуальной машиной на операционной системе Ubuntu, позволяющая более детально

осознать и изучить процессы проходящие в системе и ощутить на практике преимущества применения стандарта управления политиками безопасности.

Литература

1. *OASIS.* eXtensible Access Control Markup Language (XACML) Version 3.0. – 2013. – URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf
2. *Trusted Computing Group.* TCG Trusted Network Connect TNC Architecture for Interoperability Version 1.5. – 2012. – URL: http://www.trustedcomputinggroup.org/files/resource_files/2884F884-1A4B-B294-D001FAE2E17EA3EB/TNC_Architecture_v1_5_r3-1.pdf
3. *Trust@HsH.* Architecture of tnc@fhh 0.4.x. Trust@HsH. – 2009. – URL: http://trust.f4.hs-hannover.de/2009/02/16/architecture-of-tncfhh-0.4.x.html
4. *OASIS.* XACML MAP Authorization Profile version 1.0. – OASIS. – 2013. – URL: http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.pdf

XACML – STANDART POLISY MANAGEMENT.

Litvyakov Y.V.
Peoples Friendship University of Russia

In this paper some modern principles of business-oriented security systems, with a focus on security policy management.

Keywords: extensible access control markup language, security standards, information security, computer security, computer systems security.