Математическое и компьютерное моделирование:
материалы III Международной научной конференции
(Омск, 12 ноября 2015 г.). Омск, 2015. С. 183–184. УДК 004.056

С.В. Белим, Н.Ф. Богаченко, М.В. Шабанов

Омский государственный университет им. Ф.М. Достоевского,
г. Омск

МОДЕЛИ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ ОБЛАЧНЫХ СИСТЕМАХ

Актуальность задачи построения моделей безопасности для распределенных систем, в том числе с применением облачных вычислений обусловлена широким развитием данных систем на основе глобальной сети Интернет. Традиционные модели безопасности, рассчитанные для локальных систем, не могут применяться в облачных системах в тривиальном виде, так как наблюдается ряд проблем, связанных с отсутствием централизованной системы безопасности при их использовании. Наряду с этим крайне важно содержать в сохранности ценные данные, обеспечивая должную информационную безопасность и прежде всего контроль доступа к предоставляемым ресурсам. Использование распределенных вычислений влечет за собой массу возможностей для несанкционированных действий третьих лиц, в связи с чем в настоящее время существует необходимость как в модификации имеющихся моделей безопасности, так и в разработке новых подходов к моделированию подсистем безопасности для сведения к минимуму этих возможностей.

В соответствии с вышесказанным были проведены модификации моделей разграничения доступа: ролевой, мандатной и смешанной – для возможности использования их в системах типа «облако».

Рассмотрим виртуальную файловую систему, представляющую собой облако, в которой объекты образуют иерархическое дерево [2]. Наличие связи между объектами свидетельствует о возможности получить доступ (определенные права) из одной вершины к другой. Сопоставим каждому объекту O_i уникальный идентификатор id_i. Определим общий инициализирующий ключ системы k. Для каждой вершины с идентификатором id_m, являющейся потомком вершины с идентификатором id_n , вычислим ключ доступа $k_m = h(k_n||id_m)$, где $h()$ – «хорошая» хэш-функция.

Данный алгоритм позволяет получить доступ только к тем объектам, которые расположены по иерархии ниже, чем объект, на

© Белим С.В., Богаченко Н.Ф., Шабанов М.В., 2015

который субъекту выдан доступ. Ключи доступа к другим объектам не могут быть вычислены, так как это требует обращение хэш-функции. В данном случае идентификаторы объектов являются открытыми, что соответствует политике мандатного разграничения доступа. Дискреционная политика реализована с выдачей пользователю инициализирующий ключ k и списка разрешенных объектов дерева, имеющего открытую структуру. В смешанной политике субъекту выдается список разрешенных узлов и доступ к одному из объектов [1].

Для увеличения скорости работы используется предварительное распределение ключей, которое позволяет увеличить производительность при запросах от субъектов к объектам. Положим в основу схему предварительного ключевого распределения, которая получила название NHKP-схема (Non-Interactive Hierarchical Pairwise Key Predistribution Scheme with Multi-Level Key Establishment) [3]. Данная схема дает возможность иерархического предварительного распределения, при этом любая пара вершин может устанавливать соединение между собой без прямого взаимодействия. Использование схемы NHKP в облачных вычислениях предоставляет возможность достичь высокой вычислительной эффективности, маленьких издержек хранения и сопротивление к атакам типа сговор на всех уровнях иерархии.

Применение описанного алгоритма позволит решить проблему разграничения доступа в распределенных, в том числе географически, системах. Схема предварительного распределения ключей обеспечит быстрое установление связей между объектами системы, а алгоритм вычисления ключей с использованием хэш-функции в иерархическом дереве позволит просто, надежно и безопасно предоставлять доступ к объектам системы.

Литература

1. *Гайдамакин Н.А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Уральского университета, 2003.

2. *Ravi Mitra Reddy L., Harsha B.R.* File Access Control Through Access Tree And Attribute Based Encryption In Cloud Computing: A Survey // International Journal of Engineering Research & Technology. 2013. Vol. 2, Is. 4.

3. *Wang Q., Khurana H., Nahrstedt K.* Non-Interactive Hierarchical Pairwise Key Predistribution Scheme with Multi-Level Key Establishment. URL: `http://hdl.handle.net/2142/14459`.