УДК 004.056

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ СТРУКТУРАХ КОММЕРЧЕСКОГО ПРИМЕНЕНИЯ

Завадская Т.Е.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Цель – провести исследование возможности применения аппаратного и программного метода на практике для обеспечения целостности информации при использовании облачных технологий. На основе построенной математической модели обеспечения целостности информации в облачных структурах коммерческого применения, разработать алгоритм решения задачи обеспечения целостности информации в соответствии с математической моделью.

Модель ориентирована на обеспечение целостности данных. Базовые правила Модели обеспечения целостности формулируются следующим образом:

1. Простое правило чтения

Субъект с уровнем целостности x_s может читать информацию из объекта с уровнем целостности x_o тогда и только тогда, когда x_o преобладает над x_s.

2. Простое правило записи

Субъект с уровнем целостности x_s может писать информацию в объект с уровнем целостности x_o тогда и только тогда, когда x_s преобладает над x_o. Для первого правила существует мнемоническое обозначение No Read Down, а для второго – No Write Up.

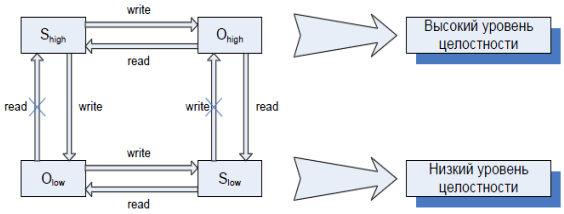

Рисунок 1 – Диаграмма информационных потоков для модели целостности

Отдельного комментария заслуживает вопрос, что именно понимается в модели под уровнями целостности. Действительно, в большинстве приложений целостность данных рассматривается как некое свойство, которое либо сохраняется, либо не сохраняется – и введение иерархических уровней целостности может представляться излишним. В действительности уровни целостности в модели необходимо рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот. Формальное описание модели полностью аналогично описанию модели Белла-ЛаПадулы. К достоинствам модели целостности следует отнести её простоту, а также использование хорошо изученного математического аппарата. В то же время модель сохраняет все недостатки, присущие модели Белла-ЛаПадулы (потенциальная возможность организации скрытых каналов передачи информации и т. д.).

Математическая постановка задачи

Исходные данные:

– A={a_1,a_2,…i…,a_n } – множество возможных актуальных классов угроз нарушения целостности информации в системе, N - число атак, определяемых классом угроз;

– B={b_1,b_2,…,b_m } – множество средств защиты от возможных угроз, M={1,2,…,m} – множество индексов средств защиты;

– T = [t_0,t_max] – рассматриваемый период функционирования. k_i,∀i∈N, k_i≥ 0 – среднее число реализации i-й угрозы на интервале T, определяются по данным статистики или с помощью экспертов;

– u_i, $\forall i \in N$ – средний ущерб от реализации i-й угрозы (атаки);

– c_j, $j \in M$ – стоимость j-го средства защиты;

– p_{ij}, $\forall i \in N$, $j \in M$, $[0,1]$ – вероятность (или нечеткая мера – возможность) предотвращения i-й атаки на целостность с помощью j-го средства защиты, определяется по данным статистики или с помощью экспертов.

Показатель качества выбора средств защиты. Введем булеву переменную $x_j \in \{0,1\}$, $\forall j \in M$, $x_j = 1$, если j-е средство защиты будет применяться в системе для защиты от тех или иных угроз нарушения целостности информации; $x_j=0$, в противном случае, т. е., если j-е средство не применяется.

Тогда $\boldsymbol{X}$ – вектор булевых переменных $\forall j \in M$. Введем показатель качества выбора средств защиты:

$$U(\boldsymbol{X}) = \sum_{i \in N} u_i k_i \{p_{ij} x_j\}, j \in M \qquad (1)$$

Ограничение.

$$\sum_{j \in M} c_j x_j \le C, \qquad (2)$$

где C – максимально возможные затраты, выделенные на защиту информации в АС.

Этим условием ограничивается стоимость выбранных средств защиты.

Постановка задачи

$$U(X) = \sum_{i \in N} u_i k_i \{p_{ij} x_j\} \to \max , j \in M, X \in \Delta_{доп}, \quad (3)$$

$$\Delta_{доп}: \sum_{j \in M} c_j x_j \le C,$$

здесь $\Delta_{доп}$ – множество допустимых альтернатив реализации средств защиты.

Из введенного показателя качества выбора средств защиты, который должен стремиться к максимуму и с учётом множества допустимых альтернатив реализации средств защиты, решением математической постановки задачи будет являться нахождение всех неизвестных компонент вектора $\boldsymbol{X}$ и выбор тех средств защиты b_j, для которых компонента вектора x_j равна 1.

В соответствии с разработанной математической моделью, необходимо разработать алгоритм, направленный на решение задачи обеспечения целостности информации в облачных структурах коммерческого применения.

Для того чтобы определить, какие средства защиты необходимы для максимальной степени защиты системы, необходимо рассмотреть классы атак.

В контексте облачных хранилищ можно разделить класс атаки на целостность на две:

– атака на облачное хранилище с целью нарушение целостности в облаке вне синхронизации, например, подмена файла;

– атака на облачное хранилище при синхронизации файлов, используя уязвимости мобильного устройства, канал связи или облачного хранилища.

Таким образом, разрабатываемое решение будет состоять из модуля проверки целостности файла, взаимодействующего с основным модулем облачного сервиса, обеспечивающего версионность файлов, авторизацию пользователей и так далее. Проверка целостности от динамических атак актуальна при записи файла из источника, при чтении файла актуальна проверка целостности от статических атак. Результаты проверки целостности файлов будут выводиться на консоль либо в графический интерфейс.

Согласно модели обеспечения целостности информации, источник с высоким уровнем целостности может писать в файлы как с высоким уровнем целостности, так и с низким. Если пришёл запрос от источника с низким уровнем целостности, программа должна ограничить источник, чтобы он имел возможность записывать в файлы с низким уровнем целостности. После записи в файл производится проверка целостности информации.

Литература

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: Логос, 2001. – 256 с.

2. Клементьев И.П., Устинов В.А. Введение в облачные вычисления // Интернет университет информационных технологий. – Режим доступа: http://www.intuit.ru/department/se/incloudc/. – Дата доступа 22.10.2016.

3. Li J., Wang Q., Wang C., Cao N., Ren K., Lou W. Fuzzy keyword search over encrypted data in cloud computing. Mini-Conf. IEEE INFOCOM, 2010, Digital Object Identifier 10.1109/INFOCOM.2010.5462196

4. Android vulnerabilities. – Режим доступа: https://www.androidvulnerabilities.com/. – Дата доступа: 15.09.2020.

УДК 681.326

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ В ОПЕРАЦИОННОЙ СИСТЕМЕ ANDROID

Карташова Ж.К.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

ОС Android за небольшой промежуток времени стала одной из самых популярных систем для всевозможных мобильных устройств. Ее используют как крупные производители с мировым именем, так и небольшие компании. Данная публикация посвящена анализу существующих решений в области защиты мобильных устройств, анализу алгоритмов управления доступом. Описаны программные и аппаратные требования для функционирования мобильной программы в операционной системе Android

На современном этапе развития все более активно в повседневную деятельность внедряются различные мобильные устройства. Уже несколько лет рынок мобильных устройств занимает лидирующие позиции по количеству пользователей, превосходя рынок персональных компьютеров. Учитывая возможности современных мобильных устройств перед разработчиками встают новые вопросы и проблемы в области обеспечения информационной безопасности. Для достижения этих целей мобильные устройства необходимо защищать от самых разных угроз.

Популярность использования мобильных устройств требует больших ресурсов для управления настройками и обеспечения информационной безопасности.

Разработанные для управления инфраструктурой мобильных устройств Mobile Device Management системы задают настройки соответствия политикам безопасности и настройки доступа в корпоративную сеть для всех одобренных мобильных устройств. При этом с их помощью осуществляется регистрация и мониторинг