ОБЩИЕ ВОПРОСЫ ЗАЩИТЫ МАГИСТРАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Голибжон Хайриддин Угли Кудратов
магистрант Ташкентского университета информационных технологий
Дилшод Эльмурадович Эшмурадов
доцент Ташкентского государственного технического университета
Маъмура Орифовна Ядгарова
Ассистент Бухарского инженерно-технологический института

https://doi.org/10.5281/zenodo.7433464

Аннотация. *В работе были рассмотрены организация безопасности в распределенных системах. Понятии надежности, конфиденциальности и целостности описаны как неотъемлемые части безопасности в компьютерных системах. Была иллюстрирована выделяемые типы угроз защите. Описаны три основных подхода организации защиты приложений.*

Ключевые слова*: авторизация, политика безопасности, системные объекты, шифрование, аутентификация, аудит, механизмы защиты*

GENERAL ISSUES OF PROTECTION OF THE BACKLINE COMPUTER NETWORKS

Abstract. *The work considered the organization of security in distributed systems. The concepts of reliability, confidentiality and integrity are described as integral parts of security in computer systems. The distinguished types of security threats were illustrated. Three main approaches to organizing application protection are described.*

Keywords*: authorization, security policy, system objects, encryption, authentication, audit, protection mechanisms*

ВВЕДЕНИЕ

Системы безопасности в распределенных системах можно разделить на две независимые части. Одним из них является связь между пользователями или процессами, которые могут находиться на разных машинах. Наиболее важным способом обеспечения безопасности связи является безопасный канал. Безопасные каналы и, в частности, аутентификация, целостность сообщений и конфиденциальность — это отдельные концепции для изучения.

Другой частью системы безопасности является авторизация, которая помогает гарантировать, что процессы получают доступ только к распределенным системным ресурсам, к которым они авторизованы. Авторизацию и контроль доступа можно рассматривать вместе. Помимо традиционных механизмов контроля доступа, мы также рассмотрим контроль доступа при работе с мобильным кодом, таким как агент.

Агенты изучения преференций пользователя должны быть когнитивными, только в такой реализации они могут выполнить поставленные перед ними задачи. Накопление и обработка знаний таких агентов осуществляется на основе базы знаний KB, например с применением онтологий. (Д.Э. ЭШМУРАДОВ, 2022)

Для безопасных каналов и контроля доступа нужны механизмы для работы с криптографическими ключами, а также механизмы для добавления и удаления пользователей из системы. Эти проблемы являются частью так называемого управления безопасностью. В отдельном разделе мы рассмотрим вопросы, связанные с управлением

криптографическими ключами, управлением безопасностью в группах и обработкой сертификатов, удостоверяющих право владельца на доступ к определенным ресурсам.

МЕТОДЫ

Безопасность в компьютерных системах тесно связана с понятием надежности. Неформально говоря, надежная компьютерная система — это та, услугам которой мы обоснованно доверяем. Надежность относится к доступности, надежности, безопасности и ремонтопригодности. Однако, если мы хотим доверять компьютерной системе, мы также должны учитывать конфиденциальность и целостность. Под конфиденциальностью мы понимаем владение компьютерной системой, в связи с чем доступ к содержащейся в ней информации ограничен кругом доверенных лиц. Целостность — это характеристика, указывающая на то, что изменения в системе могут быть сделаны только авторизованными людьми или процессами. Другими словами, незаконные модификации защищенной компьютерной системы должны быть обнаружены и исправлены. Основными компонентами компьютерной системы являются аппаратное обеспечение, программное обеспечение и данные.

Другой способ взглянуть на защиту в компьютерных системах — считать, что мы стараемся защитить службы и данные от угроз защиты (security threats) (рис.1.).

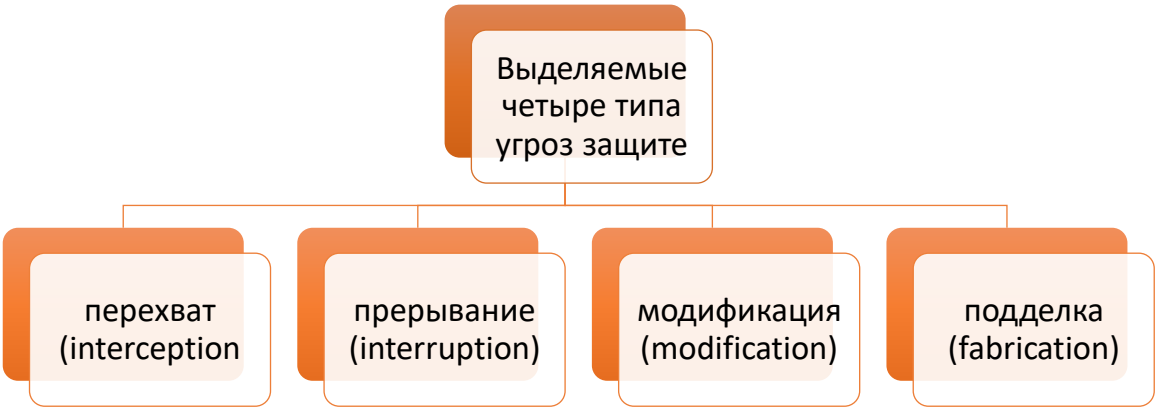

Рис.1. Угрозы защиты (security threats)

Простое утверждение о том, что система должна быть способна противостоять всем типам угроз безопасности, не является методом построения безопасных систем. Во-первых, должны быть описаны требования к защите, т. е. правила защиты. Политики безопасности детализируют разрешенные и запрещенные действия для объектов системы. Термин «системные объекты» включает пользователей, службы, данные, компьютеры и т. д. После того, как у нас есть правила безопасности, мы можем сосредоточиться на механизмах безопасности, обеспечивающих соблюдение этих правил. Наиболее важными из них являются шифрование; аутентификация; авторизация; аудит.

В программе Anaconda доступна оболочка для программирования на языке Python, который в свою очередь является одним из самых мощных решений проблемы построения

статистического анализа. На данном языке программирования можно проводить извлечение и сортировку данных, вести статистику и систематизировать полученные данные. (Эшмурадов Д.Э., 2021).

В распределенную систему, да впрочем и в любую компьютерную систему, должны быть встроены механизмы защиты, при помощи которых можно будет реализовать различные правила защиты. При реализации служб защиты общего назначения следует учитывать несколько моментов. (Таненбаум Эндрю, 2006).

Для организации защиты приложений (в том числе распределенных приложений) можно использовать три основных подхода, представленных на рис. 2. Первый вариант заключается в защите данных, непосредственно связанных с приложением. Второй вариант — это защита путем точного указания того, кто и как может использовать операции доступа к данным или ресурсам. Третий вариант — сосредоточиться непосредственно на пользователе и обеспечить доступ к приложению только определенным людям, независимо от операций, которые они будут выполнять.

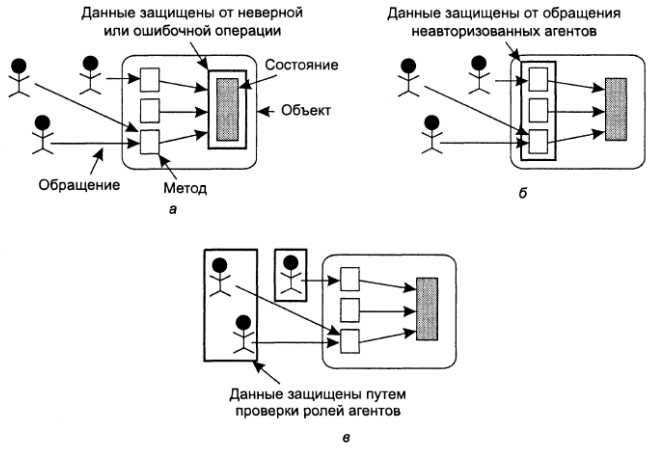

Рис. 2. Три подхода к противодействию угрозам защите. Защита от неверных операций (а). Защита от неавторизованных обращений (б). Защита от неавторизованных пользователей (в)

Важным моментом при проектировании систем защиты является решение о том, сколько уровней защиты должно быть. Уровень соответствует логической организации системы. Например, компьютерные сети часто являются многоуровневыми в соответствии с эталонной моделью, в которой есть отдельные слои для приложений, задач среднего уровня, служб и ядра операционной системы. Если объединить многоуровневые структуры компьютерных сетей и распределенных систем, то получится схема, показанная на рис. 3.

Рис. 3. Логическая многоуровневая организация распределенных систем

Принципиально (рис. 3.) многоцелевые услуги отделены от услуг связи. Это разделение очень важно для понимания многоуровневого механизма безопасности в распределенных системах и особенно для понимания доверия. Разница между доверием и защитой очень важна. Система может быть безопасной, а может и не быть, особенно с учетом различных возможностей, но мнение заказчика о безопасности системы — это вопрос доверия. Уровень, на котором размещен механизм защиты, зависит от доверия клиента к защите служб на этом уровне.

К сожалению, простых механизмов реализации правил защиты часто бывает недостаточно. Поэтому для аутентификации на уровне пользователя может как минимум потребоваться знание криптографических ключей и определенных механизмов, таких как сертификация, хотя многие службы безопасности полностью автоматизированы и прозрачны для пользователя.

В других случаях само приложение может быть достаточно сложным, а введение защиты еще больше усложняет его. Примером приложения, содержащего сложные протоколы безопасности, являются цифровые платежные системы, которые мы рассмотрим далее в этой главе. Сложность цифровых платежей часто связана с тем, что для совершения платежа необходимо взаимодействие нескольких участников. В этих случаях важно, чтобы базовые механизмы реализации протоколов были относительно простыми и понятными. Простота вызовет доверие у пользователей, работающих с приложением, и, что более важно, разработчики смогут убедить в отсутствии «дыр» в системе безопасности.

ЗАКЛЮЧЕНИЕ

При обсуждении вопросов безопасности в распределенных системах можно вернуться к примеру клиентов и серверов. На практике построение безопасной распределенной системы, в частности, сводится к двум основным моментам. Первым из них является установление безопасного соединения между клиентом и сервером. Безопасная связь требует аутентификации взаимодействующих сторон, а также гарантирует целостность сообщений и, возможно, их конфиденциальность. Связь серверов внутри группы также можно рассматривать как частный случай этой проблемы.

Второй момент — способ авторизации. Как сервер, получающий запрос от клиента, может знать, что клиент имеет право пересылать этот запрос для обработки? Авторизация связана с проблемой контролируемого доступа к ресурсам, которую мы подробно

рассмотрим в следующем разделе. Здесь мы сосредоточимся на защите связи в распределенных системах.

Идея защиты связи между клиентами и серверами может быть выражена в терминах организации между взаимодействующими сторонами защищенного канала. Безопасные каналы защищают отправителей и получателей от перехвата, изменения и подделки сообщения. Обычно нет необходимости вводить защиту от прерывания связи. Сообщения защищены от прослушивания за счет гарантированной конфиденциальности: безопасные каналы гарантируют, что содержащиеся в них сообщения не могут быть подслушаны злоумышленниками. Сообщения защищены от модификации или подделки с помощью протоколов взаимной аутентификации и целостности сообщений.

REFERENCES

1. Андрюшкевич Сергей Константинович, Журавлев Сергей Сергеевич, Золотухин Евгений Павлович, Ковалев Сергей Протасович, Окольнишников Виктор Васильевич, Рудометов Сергей Валерьевич Разработка системы мониторинга с использованием имитационного моделирования // Проблемы информатики. 2010. №4. URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-monitoringa-s-ispolzovaniem-imitatsionnogo-modelirovaniya (дата обращения: 23.11.2022).
2. Семенов Александр Сергеевич Разработка системы мониторинга показателей качества электроэнергии горных предприятий // Технические науки – от теории к практике. 2012. №11. URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-monitoringa-pokazateley-kachestva-elektroenergii-gornyh-predpriyatiy (дата обращения: 23.11.2022).
3. Хуторов В. С., Беленькая М. Н. Основные проблемы и цели мониторинга базы данных средствами субд Oracle // T-Comm. 2013. №7. URL: https://cyberleninka.ru/article/n/osnovnye-problemy-i-tseli-monitoringa-bazy-dannyh-sredstvami-subd-oracle (дата обращения: 23.11.2022).
4. Исаев Е. А., Корнилов В. В., Тарасов П. А. Научные компьютерные сети—проблемы и успехи в организации обмена большими объемами научных данных //Математическая биология и биоинформатика. – 2013. – Т. 8. – №. 1. – С. 161-181.
5. Львович И. и др. ПРОБЛЕМЫ ПРОЕКТИРОВАНИЯ И ОПТИМИЗАЦИИ КОМПЬЮТЕРНОЙ СЕТИ //European Science. – 2022. – №. sge09-01. – С. 38-61.
6. Цыбин В. В., Шукуров А. Г., Эшмуратов Д. Э. Современные методы диагностики бортового радиоэлектронного оборудования //Материалы республиканской научно-технической конференции" Проблемы развития аэрокосмической отрасли Республики Узбекистан» Ташкент, Узбекистан. – 2007. – С. 131-134.
7. Эшмурадов Д. Э., Элмурадов Т. Д., Тураева Н. М. Автоматизация обработки аэронавигационной информации на основе многоагентных технологий //Научный вестник Московского государственного технического университета гражданской авиации. – 2022. – Т. 25. – №. 1. – С. 65-76.