Технічні науки

УДК 004.056.55

Шемрикович Ангелина Дмитриевна

студент

Харьковского национального университета радиоэлектроники

Шемрікович Ангеліна Дмитрівна

студент

Харківського національного університету радіоелектроніки

Shemrikovych Anhelina

Student of the

Kharkiv National University of Radioelectronics

Олейник Александр Александрович

ассистент кафедры Программной инженерии

Харьковский национальный университет радиоэлектроники

Олійник Олександр Олександрович

асистент кафедри Програмної інженерії

Харківський національний університет радіоелектроніки

Oliynyk Oleksandr

Assistant of the Software Engineering Department

Kharkiv National University of Radioelectronics

СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАЗРАБОТКЕ ИГРОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЗАСОБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РОЗРОБЦІ ІГРОВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

INFORMATION SECURITY BEST PRACTICES IN GAME SOFTWARE DEVELOPMENT

Аннотация. *Сфера разработки игрового программного обеспечения активно развивается в сегодняшнее время. Игровое ПО имеет в своей структуре и сложные алгоритмы, и высоконагруженные многопользовательские сервера, и системы транзакций. Современные игры нацелены на длительное удержание игрока, поэтому применяют различные методики, тем самым привлекают пользователей проводить много времени в игре, нарабатывать прогресс и даже делать финансовые вложения для получения дополнительных привилегий в игровом мире. Важную роль в разработке игрового ПО занимает безопасность данных продукта и его пользователей, поскольку любая утечка данных или незаконное их использование может нанести как финансовый, так и моральный ущерб пользователям и компании-разработчику.*

Ключевые слова: *безопасность данных, алгоритмы шифрования, игры, разработка игрового программного обеспечения.*

Анотація. *Сфера розробки ігрового програмного забезпечення активно розвивається сьогодні. Ігрове ПЗ має у своїй структурі і складні алгоритми, і високонавантажені розраховані на багато користувачів сервери, і системи транзакцій. Сучасні ігри націлені на тривале утримання гравця, тому застосовують різні методики, тим самим залучають користувачів проводити багато часу у грі, напрацьовувати прогрес і навіть робити фінансові вкладення для отримання додаткових привілеїв в ігровому світі. Важливу роль у розробці ігрового ПЗ займає безпека даних продукту та його користувачів, оскільки будь-який витік даних або незаконне їх використання може завдати як фінансової, так і моральної шкоди користувачам та компанії-розробнику.*

Ключові слова: *безпека даних, алгоритми шифрування, ігри, розробка ігрового програмного забезпечення.*

Summary. *The sphere of gaming software development is actively developing today. Gaming software has in its structure and complex algorithms, and highly loaded multi-user servers, and transaction systems. Modern games are aimed at long-term retention of the player, therefore, they use various methods, thereby attracting users to spend a lot of time in the game, make progress and even make financial investments to obtain additional privileges in the game world. An important role in the development of gaming software is played by the safety of product data and its users, since any data leak or illegal use of it can cause both financial and moral damage to users and the developer company.*

Key words: *data security, encryption algorithms, games, game software development.*

Основными рисками, которым подвергается безопасность игрового программного обеспечения являются: фальсификация виртуальных товаров или данных и хаккинг (трояны и искусственный взлом системы).

Поскольку получить виртуальные предметы в играх обычным способом сложно и отнимает много времени, компании-разработчики добавляют функционал подключаемых модулей и ресурсов, которые с помощью команд подтягиваются из сервера. Данный функционал необходим для тестирования разработанного продукта отделом качества. Подключаемый модуль представляет собой автономную программу, которая либо искажает прогресс, добавляя игроку указанное количество игровых ресурсов, либо же имитирует действия реального пользователя, тем самым продвигая персонажа по игровым уровням. Из-за отсутствия передовых технологий защиты от подключаемых модулей, некоторые игровые компании сталкиваются с переполнением подключаемого программного обеспечения, что приводит к потере игроков и экономическому ущербу для компании. Кроме того при должном умении злоумышленники могут находить в бинарных файлах программы

необходимые данные для выкачки подобных модулей с сервера. Таким образом, подключаемые модули стали целью тщательного исследования игровыми разработчиками и инженерами по информационной безопасности.

Самой распространённой проблемой со стороны пользователей являются трояны. Трояны с функцией записи с клавиатуры могут подключаться ко всей операционной системе или назначенному девайсу ввода данных и записывать нажатия клавиш и последовательность действий пользователя, а затем отправлять записанную информация о пароле и данных текущего устройства ввода на сервер, для входа в учетную запись взломанного пользователя. Трояны с возможностью мониторинга сетевых данных могут анализировать пароль учетной записи в онлайн-играх. Поскольку запрос на вход в онлайн-игру отправляется на сервер, то если установить трояна для мониторинга сетевых данных на неконтролируемом компьютере в той же локальной сети, он сможет отслеживать, когда пользователь вводит пароль для входа в систему, и записывать эти данные для взлома.

Не менее важной проблемой является и недостаточная безопасность серверов, где хранятся важные данные. Часто из-за открытых сетевых портов, использования интернет-протоколов без шифрования или же при отсутствии VPN подключений у разработчиков, злоумышленники получают доступ не только к готовым частям игрового продукта, а и к исходному коду, полной базе данных пользователей и самого продукта.

Чтобы устранить угрозы информационной безопасности в игровом ПО, используются системы шифрования данных, которые используют протокол SSL. Для шифрования потоков компании-разработчики чаще всего прибегают к алгоритму RC4. Для шифрования пакетов применяются всемирно известные алгоритмы, такие как AES, DES и 3DES. Алгоритм RSA и DSA обычно используется для секретного обмена и цифровой подписи,

иногда используется при шифровании данных. Алгоритм DH применяют для обмена ключами.

Чтобы обеспечить безопасность сетевой информации в игровом ПО активно внедряется распределенная аутентификация. В прошлом режим централизованной аутентификации единой системы имел большой недостаток в надежности и безопасности. Этот режим мог не аутентифицировать пользователя из-за сбоев в сети, а также легко мог быть взломан в открытой сети. Теперь же аутентификация может быть распределена по разным серверам, а затем интегрировать результаты оценки систем, в которых расположены эти серверы, для аутентификации пользователей по сетевой идентичности, чтобы избежать возможной неверной оценки идентичности в исходном едином централизованном режиме аутентификации. Криптографические методы, используемые в распределенных системах аутентификации, представляют собой пороговую криптографию. Используются две стратегии пороговых паролей: одна – это пороговая криптосистема с открытым ключом, а другая – пороговая подпись. Пороговая криптосистема с открытым ключом имеет много общего с криптосистемами с открытым ключом, используемыми в прошлом, но она использует стратегию распределенного дешифрования. При шифровании несколько серверов используют один и тот же открытый ключ, и каждая система имеет закрытый ключ, который можно использовать для его расшифровки. Когда учетная запись расшифровывается, каждый субъект получает выходное значение операции, используя свой собственный закрытый ключ, а также информацию, которая представляет его действительность.

Чтобы избежать простоев сервера и рисков кибербезопасности для работы игры, можно использовать несколько стратегий конфигурации высокопроизводительных серверов для решения проблемы, их называют тремя шлюзами. Входной шлюз в основном используется для сетевой связи

между игроком и клиентом при входе в систему, а также для шифрования, дешифрования и проверки данных связи клиента и сервера входа. Игровой шлюз в основном используется для сетевой связи между игровым сервером и клиентом во время игры, он шифрует, дешифрует и проверяет данные связи, сгенерированные между игровым сервером и клиентом, и анализирует пользовательские данные предыдущий клиент, чтобы отфильтровать пакет с ошибкой. Игровой сервер в основном используется для работы с игровой логикой. С точки зрения архитектуры программного обеспечения, эти системы могут использовать подсистемы и субмодули игрового сервера. для коллективной обработки и управления логикой игрового мира.

Подводя итоги, можно сделать вывод, что с активным развитием отрасли разработки игрового программного обеспечения развивается и отрасль, связанная со взломами и использованием чужих данных. Поэтому применение практик информационной безопасности является чуть ли не самой важной задачей при разработке игрового ПО.

Литература

1. Klimburg A. National Cyber Security Framework Manual (NATO CCD COE Publications), 2012.
2. Wang Y. Psychological Considerations on "Plug-in" in Online Games [D]. University of Suzhou, 2013.
3. Luo L. Study on Security Protection of User's Personal Information in Social Networks [J]. Journal of Library and Information Sciences. 2012. № 14. P. 36-40.
4. Xu Y.L. Information Security Solutions for Online Games [J]. Computer Knowledge and Technology, 2005.

5. Pascal M. Handbook of Science and Technology for Homeland Security. Classes of Vulnerabilities and Attacks. Wiley, New York (2007) Google Scholar.
6. Perlroth N. A Tough Corporate Job Asks One Question: Can You Hack It? New York Times Online 20, July 2014.