УДК 004.056.52

Самофалов К.Г., чл.-кор. НАН Украины
Тубольцев А.А.
Ияд Мохд Маджид Ахмад Шахрури

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИДЕНТИФИКАЦИИ УДАЛЕННЫХ АБОНЕНТОВ МНОГОПОЛЬЗОВАТЕЛЬСКИХ СИСТЕМ

Национальный технический университет Украины "КПИ"

Проведен анализ факторов, влияющих на эффективность идентификации удаленных пользователей интегрированных систем. Основное внимание уделено повышению производительности идентификации. Разработана новая двухуровневая организация идентификации удаленных пользователей которая использует один цикл передачи между пользователями и системой. Предложенная схема не использует списка паролей зарегистрированных пользователей и операций поиска и соответственно не накладывает ограничений на число пользователей. Объем информации, используемой при идентификации в предложенной схеме, существенно меньше в сравнении с известными схемами

Введение

Многопользовательские системы играют важную роль в динамично расширяющейся интеграции информационных и вычислительных ресурсов. Такая интеграция позволяет повысить эффективность управления во всех сферах человеческой деятельности и является приоритетным направлением в развитии современных информационных технологий. Информационная интеграция охватывает широкий спектр систем обработки данных, включая компьютеризированные системы управления.

Развитие интегрированных систем обработки информации в значительной степени зависит от эффективности реализации в них функций защиты информации и разделения прав доступа к данным. Важное место в арсенале средств защиты интегрированных информационных и вычислительных ресурсов от несанкционированного доступа играет идентификация абонентов многопользовательских систем.

Расширение использования интегрированных систем хранения и обработки информации сопряжено с увеличением риска несанкционированного доступа к их ресурсам. Это обусловлено, с одной стороны, ростом технических возможностей для реализации несанкционированного доступа, а с другой – увеличением потенциальных выгод от такого доступа.

В этих условиях необходимо адекватное совершенствование всего арсенала средств, исключающих несанкционированный доступ к информационным и вычислительным ресурсам, в том числе и средств идентификации абонентов многопользовательских систем. Особую остроту в современных условиях приобретает проблема защиты от несанкционированного доступа к интегрированным системам компьютеризированного управления сложными техническими объектами. Для таких систем, к которым в полной мере можно отнести системы управления воздушным движением, возможность несанкционированного доступа связана со значительным риском техногенного и гуманитарного характера.

Таким образом, проблема повышения эффективности идентификации удаленных абонентов многопользовательских систем является актуальной и важной для современного этапа развития информационных технологий.

Критерии эффективности идентификации абонентов и анализ способов ее выполнения

Для получения несанкционированного доступа, нарушитель может выполнить чтение, перехват и подмену информации, используемой в процессе идентификации при ее передаче по открытых линиях. Кроме того, потенциальную опасность представляет возможность дос-

тупа к информации, используемой для предоставления прав доступа со стороны самой системы [2].

Эффективности идентификации удаленных абонентов пользователей определяется двумя факторами: устойчивостью к попыткам незаконного доступа (измеряется объемом затрат ресурсов, требующимися для такого доступа) и объем ресурсов, затрачиваемых для идентификации. Очевидно, что указанные факторы являются взаимосвязанными: чем выше уровень надежности идентификации абонента, тем сложнее ее процедура и тем больше ресурсов требуется для реализации процесса идентификации. С другой стороны, многопользовательские системы являются системами массового обслуживания и, соответственно, должны обладать производительностью, обеспечивающей возможность обработки запросов большого числа абонентов без существенных задержек. Фактически зависимость между рассматриваемыми факторами эффективности носит более сложный характер, поскольку результативность ряда способов незаконного доступа к ресурсам прямо зависит от времени идентификации абонентов [2]. Следовательно, высокая эффективность идентификации абонентов может быть достигнута только в рамках разрешения компромисса между надежностью и скоростью идентификации.

В основе большинства существующих систем идентификации удаленного абонента лежит концепция доказательства знания им какой-то информации. Соответственно, схема идентификации включает два этапа: регистрацию абонента, во время которой абонент обретает идентифицирующую информацию и собственно идентификацию, в рамках которой осуществляется проверка легальности доступа.

К настоящему времени созданы и активно используется большое число протоколов идентификации удаленных абонентов [1, 2]. В большинстве систем [1] информация, связанная с предоставлением прав пользования ресурсами системы представлена в форме пароля пользователя. Обычно в системе имеется список паролей, в котором им сопоставляются перечни ресурсов, к которым возможен доступ. Практически все многопользовательские системы используют кроме имени пользователя закрытый пароль. При этом пароль выполняет функции аутентификации пользователя, входящего в систему. В системе *UNIX* [1] поиск выполняется по идентификатору пользователя, введенный им пароль шифруется с использованием модифицированного алгоритма *DES* и сравнивается с зашифрованным паролем, хранящимся в таблице. Такой способ идентификации уязвим для проникновения к идентифицирующей информации со стороны системы и не обеспечивает защиту от подбора пароля из списка наиболее часто используемых [1].

В более сложных протоколах идентификации удаленных абонентов используются несимметричные криптографические алгоритмы (алгоритмы с открытым ключом) типа *RSA, ElGamal* или *ECC*. Их недостатком является использование большого числа ключей, минимум двух пересылок по сети и необходимость в использовании операций поиска по ключу в процессе идентификации. Для идентификации абонентов используется также ряд специальных алгоритмов [1]. В основе всех этих алгоритмов лежит неразрешимая аналитически математическая задача, единственным способом решения которой является полный перебор, объем которого соответствует сложности *NP*-задачи. В основе большинства используемых на практике схем идентификации удаленных пользователей лежат труднорешаемые задачи теории чисел и комбинаторики [2]. Эти схемы также требуют нескольких пересылок идентифицирующей информации по сети между абонентом и системой. В работе [3] предложена схема идентификации, не требующая для идентификации операции множественного сравнения. Однако использование такой схемы не защищает от доступа легальных абонентов к недозволенным им ресурсам системы. Достоинством этой схемы является изменяемость идентифицирующей по-

сылки при каждом обращении к системы. Для этого используется вставка в посылку случайных строк символов, которые затем игнорируются системой.

Существенным недостатком большинства известных схем идентификации абонентов является малая производительность, связанная с выполнением нескольких сеансов обмена информацией, а также необходимостью операций поиска по ключу. Невысокая скорость идентификации существенно ограничивает количество абонентов и не позволяет реализовать повторные сеансы идентификации непосредственно в процессе информационного обмена с тем, чтобы воспрепятствовать технологии доступа к ресурсам путем "подмены легального абонента".

Целью работы является повышение эффективности идентификации удаленных абонентов многопользовательских систем за счет ускорения идентификации и уменьшения риска доступа к ресурсам посредством использования хранящейся в системе информации.

Анализ возможностей повышения эффективности идентификации абонентов

Высокая эффективность идентификации удаленных абонентов достигается как результат компромисса между противоречивыми требованиями. Сложность проблемы усугубляется невозможностью построения адекватной формальной модели действий стороны, производящей попытку несанкционированного доступа. В первом приближении, процедура идентификации должна удовлетворять следующим требованиям:

1. Организация хранения идентифицирующей информации таким образом, чтобы одна ее часть находилась у абонента, а другая – хранилась в системе и каждая из частей не была бы самодостаточной для доступа к ресурсам системы.

2. Пароль должен выбираться абонентом, не храниться в памяти, а вводиться при каждом сеансе и не быть достаточным для предоставления доступа к ресурсам.

3. Минимальное использование линий передачи данных – наиболее уязвимого места, с точки зрения незаконного проникновения к ресурсам системы;

4. Изменение идентифицирующей посылки абонента информации при каждом сеансе обращения к системе.

5. Объем сохраняемой в системе закрытой информации, которая используется для идентификации абонентов должен быть возможно меньшим.

6. Идентифицикационная информации при передаче по линии передачи данных должна шифроваться с использованием ключей, одинаковых для всех абонентов.

7. Распознавание легальных абонентов и сопоставление предоставляемых им прав доступа должно реализоваться разными механизмами защиты.

Приведенные требования весьма сложно удовлетворить в рамках одноуровневой схемы идентификации. Поэтому целесообразным представляется разнесение этапа установления легальности абонента и установления прав доступа его к ресурсам системы в рамках двух разных уровнях идентификации. Такое разнесение реализовано в рамках разработанной организации идентификации абонентов многопользовательских систем.

Разработка двухуровневой схемы идентификации абонентов многопользовательских систем

Сущность предложенной двухуровневой организации идентификации абонентов состоит в том, что на первом уровне производится установление легальности абонента без использования системной информации, привязанной к конкретному пользователю. На втором уровне, для идентификации абонента используются хранящиеся в системе данные, относящиеся к конкретному абоненту. Такой принцип использования идентифицирующей информации позволяет ускорить фильтрацию обращений к системе, связанных к попытками незаконного проникновения к ее ресурсам со стороны нелегальных пользователей.

В предлложенной организации идентификации абонентов многопользовательских систем используются симметричное $R=SCT(D, K)$ и несиммет-

ричное (с открытым ключом) $R=NSCT(D, K_D)$ криптографические преобразования (в качестве первого может, например, использоваться алгоритм *Rijndael*, а качестве второго–*RSA*). Через D обозначен блок данных до шифрования, а через R-после шифрования, K-ключ преобразования. Обратные преобразования обозначены как: $D=SCT^{-1}(R, K)$ и $D=NSCT^{-1}(R, K_R)$, $K_D \neq K_R$. Кроме упомянутых преобразований предлагаемая организация предполагает использование функции $P(X)$ перестановки битов кода X (через P^{-1} обозначено обратную перестановку, так, что $X=P^{-1}(P(X))$). При идентификации используется также необратимая функция $H(X)$ формирования хеш-сигнатуры кода X. В качестве такой функций может быть использован один из хеш-алгоритмов, например, *SHA*.

При регистрации абонента A, им произвольно выбирается мнемонический пароль P_A, который вводится абонентом при каждом сеансе обращения к системе. При регистрации, этот пароль P_A передается системе, где перемешивается с секретным постоянным кодом W: $K_A = P(P_A, W)$. Полученный в результате код K_A используется в качестве части ключа для преобразования универсального для всех абонентов системы секретного кода U во вторую часть пароля D_A абонента: $D_A= SCT(U, K_A)$. Вычисленная описанным способом часть пароля D_A перемешивается $D_A'=P(D_A)$ возвращается системой абоненту вместе с его номером N_A. В памяти системы выделяется область памяти, адресуемая кодом N_A. В этой области записываются ключи доступа абонента A к ресурсам системы. Генерируется случайная строка S, которая сохраняется в области памяти абонента A. Эта строка вместе с D_A и N_A возвращаются абоненту A.

Обмен регистрационной информации производится в зашифрованном виде. Для этого абонент с использованием открытого ключа K_D системы шифрует мнемонический пароль P_A и случайно выбранный абонентом сеансовый ключ K_C: $T_1=NSCT((P_A, K_c), K_D)$. Система с использованием закрытого открывающего ключа K_R восстанавливает коды P_A и K_c. С использованием полученного сеансового ключа K_C система шифрует сгенерированную часть D_A пароля абонента, его номер N_A и сохраненную строку S: $T_2=SCT((D_A, N_A, S), K_C)$.

Таким образом, после регистрации в закрытой памяти системы сохраняются общие для всех абонентов коды W и U. Кроме того, в общей памяти системы в области, адресуемой N_A сохраняется строка S и коды доступа к ресурсам.

Абонент сохраняет после регистрации в мнемонической памяти пароль P_A, кроме того, в компьютерной памяти хранится часть пароля D_A и принятая от системы строка S.

При обращении абонента к системе, выполняется *цикл его идентификации,* включающий следующую последовательность действий:

1. Абонент A вводит строку мнемонического пароля P_A, который конкатенируется со строкой S. Над результатом конкатенации выполняется хеш-преобразование H с получением новой строки $S'=H(P_A \mid S)$. Строка S' замещает в памяти ранее хранившуюся строку S.

2. Абонентом выполняется конкатенация мнемонического пароля P_A, второй части пароля – D_A', номера N_A и строки S'. Результат конкатенации шифруется открытым закрывающим ключом K_D системы: $T=NSCT((P_A, D_A', N_A, S'))$. Полученный код T отсылается в систему.

3. Многопользовательская система принимает идентифицирующий код T, посланный абонентом A и, используя свой секретный открывающий ключ K_R, выполняет дешифрацию компонент принятого кода: $P_A, D_A', N_A, S'=NSCT^{-1}(T)$.

4. Обратной перестановкой битов система восстанавливает исходный код $D_A=P^{-1}(D_A')$ и вычисляет код ключа K_A путем перемешивания с секретным постоянным кодом W: $K_A = P(P_A,W)$.

5. С использованием полученного ключа K_A выполняется обратное криптографическое преобразование над кодом D_A: $R=SCT^{-1}(D_A,K_A)$. Если результат равен хранящемуся в систему постоянному для всех абонентов коду U, то есть если $R=U$, то принимается решение о легальности

абонента A. В противном случае, в доступе отказано.

6. Если установлен факт легальности абонента A, то выполняется идентификация прав доступа абонента A к оговоренным ресурсам системы. Для этого из области памяти системы, адресуемой кодом N_A считывается строка S_A. Выполняется конкатенация полученного от абонента мнемонического пароля P_A со считанной из памяти строкой S_A. Над результатом конкатенации выполняется хеш-преобразование H с получением новой строки $S_A'=H(P_A | S_A)$. Полученная в результате хеш-преобразования строка S_A' сравнивается со строкой S'', полученной от абонента. Если эти строки совпадают, то есть S_A' =S', то абоненту предоставляется право использовать ресурсы системы, обозначенные в области памяти N_A. В этом случае строка S' замещает в памяти ранее хранившуюся строку S_A в области памяти, адресуемой N_A. Если $S_A' \neq S'$, то возникшая ситуация классифицируется, как попытка доступа легального пользователя к ресурсам, доступ к которым не оговорен при его регистрации. Соответственно, в доступе отказано и замещения кода строки в области, адресуемой N_A не производится.

Таким образом, предложенная организация реализует двухуровневую схему идентификации абонентов многопользовательских систем. На первом уровне со стороны системы используются только три секретные кода: открывающий ключ K_R, и произвольно выбираемые при инициализации системы коды W и U, одинаковые для всех абонентов. На первом уровне признаком того, что абонент является зарегистрированным является совпадение результата описанного в пп.4-5 преобразования с секретным, единым для всех пользователей кодом U, а не результатом совпадения с элементами списка идентификационной информации, как это реализовано в известных схемах идентификации удаленных пользователей [1,2]. Это обуславливает высокую скорость идентификации удаленных пользователей, причем особенно важным является то, что время идентификации не зависит от их количества. При этом многократно уменьшается объем хранящейся в системе секретной информации, что упрощает техническую реализацию закрытой памяти.

На втором уровне идентификация осуществляется путем сравнения строк, сгенерированной абонентом и системой. Это обеспечивает изменчивость идентифицирующей информации для каждого из сеансов обращения к системе. Анализ отказов в доступе при реализации второго уровня идентификации позволяет эффективно выявлять попытки незаконного доступа к ресурсам системы и осуществлять, на этой основе, мониторинг ее безопасности.

Предложенная организация идентификации использует только один цикл передачи идентифицирующей информации от абонента к системе. Это уменьшает риск незаконного проникновения в систему путем внедрения в процессе передачи. Кроме того, снижается использование важного для систем коллективного доступа ресурса – линии передачи.

Важным достоинством предложенной организации является то, что в ее рамках достигается разнесение информации, используемой при идентификации: выбранный абонентом мнемонический пароль P_A не сохраняется в компьютерной памяти, что исключает несанкционированный доступ к нему; однако подбор этого пароля неэффективен в силу того, что сам по себе он позволяет получить доступ к ресурсам системы. Дополнительная часть пароля D_A хранится в преобразованном виде D_A' только в компьютерной памяти абонента. Общая для всех абонентов часть пароля W хранится в закрытой памяти системы. Это не позволяет абоненту, которому не известны коды D_A и W, равно как и функция P перестановки установить код U.

Для проникновения в систему нелегального пользователя, последний должен знать пароль P_A, соответствующий ему код D_A, номер N_A и код строки S. Разрядность D_A и P_A равна 256 (при использовании в качестве симметричного преобразования *Rijndael*), длина S больше 256. Оче-

видно, что успешный подбор указанных компонент маловероятен.

Для получения доступа легального пользователя к недоступным для него ресурсам необходимо также подобрать связанные между собой необратимыми преобразованиями коды P_A, D_A, N_A и S. В случае проникновения к общей памяти системы можно получить коды строк S и номер области памяти, что не позволяет реализовать доступ извне: для этого надо подбирать коды P_A и D_A.

Выводы

В результате анализа факторов, определяющих эффективность идентификации абонентов многопользовательских систем сформулированы требования к ее организации. Предложена двухуровневая организация идентификации абонентов, удовлетворяющая этим требованиям. Ее достоинствами является высокий уровень защищенности, обеспечиваемый двумя уровнями анализа идентифицирующей информации, а также высокая производительность, достигаемая за счет использования только одной пересылки. В отличии от известных схем идентификации, определение легальности абонента производится без обращения к области памяти, связанной с абонентом. Это позволяет ускорить идентификацию и сократить объем секретной информации до трех кодов: K_R, W и U, общих для всех абонентов, что упрощает реализацию специальной защищенной памяти.

Предложенная организация идентификации удаленных абонентов может быть использована как в многопользовательских компьютерных системах, так и в сетевых интегрированных системах коллективного доступа.

Список литературы

1. *Столлингс В.* Криптография и защита сетей: принципы и практика. – М.: Изд. дом. "Вильямс". – 2001 – 621 с.

2. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК. – 2002. – 655 с.

3. *Эль-Хами Ияд.* Методы повышения эффективности аутентификации удаленных пользователей интегрированных систем обработки информации // Вісник Національного технічного університету України "КПІ". Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+". – № 36. – 2001. – С. 30 – 40.

видно, что успешный подбор указанных компонент маловероятен.

Для получения доступа легального пользователя к недоступным для него ресурсам необходимо также подобрать связанные между собой необратимыми преобразованиями коды P_A, D_A, N_A и S. В случае проникновения к общей памяти системы можно получить коды строк S и номер области памяти, что не позволяет реализовать доступ извне: для этого надо подбирать коды P_A и D_A.

Выводы

В результате анализа факторов, определяющих эффективность идентификации абонентов многопользовательских систем сформулированы требования к ее организации. Предложена двухуровневая организация идентификации абонентов, удовлетворяющая этим требованиям. Ее достоинствами является высокий уровень защищенности, обеспечиваемый двумя уровнями анализа идентифицирующей информации, а также высокая производительность, достигаемая за счет использования только одной пересылки. В отличии от известных схем идентификации, определение легальности абонента производится без обращения к области памяти, связанной с абонентом. Это позволяет ускорить идентификацию и сократить объем секретной информации до трех кодов: K_R, W и U, общих для всех абонентов, что упрощает реализацию специальной защищенной памяти.

Предложенная организация идентификации удаленных абонентов может быть использована как в многопользовательских компьютерных системах, так и в сетевых интегрированных системах коллективного доступа.

Список литературы

1. *Столлингс В.* Криптография и защита сетей: принципы и практика. – М.: Изд. дом. "Вильямс". – 2001 – 621 с.

2. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК. – 2002. – 655 с.

3. *Эль-Хами Ияд.* Методы повышения эффективности аутентификации удаленных пользователей интегрированных систем обработки информации // Вісник Національного технічного університету України "КПІ". Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+". – № 36. – 2001. – С. 30 – 40.