Модел. и анализ информ. систем. Т. **20**, № **4** (2013) 91–103

УДК 004.94

Новый подход к множественной аутентификации пользователя в современных разнородных информационных системах

Петров В.И., Комар М.С., Кучерявый Е.А.

Технологический Университет г. Тампере,
PO Box 527, FI-33101, Korkeakoulunkatu 10, Тампере, Финляндия
Ярославский государственный университет им. П.Г. Демидова,
150000 Россия, Ярославль, ул. Советская, д. 14

e-mail: vitaly.petrov@tut.fi, maria.s.komar@uniyar.ac.ru, yk@cs.tut.fi

получена 26 октября 2013

Ключевые слова: множественная аутентификация, беспроводные сети, безопасность информационных систем

Предлагается новый подход к множественной аутентификации пользователя в разнородных информационных системах. Описанное решение основано на применении беспроводных ключей — специальных устройств, которые идентифицируют пользователя посредством передачи запрашиваемой ключевой информации с использованием беспроводной связи. Ключевым свойством предложенного подхода является неинтерактивность: вместо двухсторонней аутентификации ключа и информационной системы для защиты данных, хранящихся на ключе, предлагается использование специального алгоритма шифрования. Разработанный алгоритм построен на комбинации стойких криптографических примитивов, что исключает возможность неавторизованным участникам системы читать данные других пользователей, даже при наличии физического доступа к памяти ключа. Указанный подход не требует вычислительной мощности или питания на стороне ключа и не вовлекает пользователя в процесс аутентификации, что позволяет использовать в качестве ключа USB носитель или пассивную NFC метку. Для доказательства корректности работы системы было разработано программное обеспечение, реализующее описанную систему аутентификации для технологий USB и NFC. Также было проведено качественное сравнение полученного решения с существующими аналогами.

1. Введение

За последние несколько лет значительно возросло количество информационных систем (ИС), с которыми человек взаимодействует в течение дня: персональные компьютеры, платежные терминалы, панели контроля доступа в здание, турникеты в общественном транспорте, и многое другое. Пропорционально росту количества

ИС растет и риск потери или кражи конфиденциальных сведений пользователя по причине технического сбоя или злонамеренных действий третьих лиц. Современный уровень развития систем информационной безопасности позволяет обеспечить должный уровень защиты личных данных пользователя и конфиденциальных сведений. Одной из наиболее важных задач в области защиты конфиденциальных данных является аутентификация пользователя. На сегодняшний день существует множество различных технологий аутентификации (одна из ключевых частей системы безопасности): одноразовые и многоразовые [1] пароли, PIN-коды [2], цифровые сертификаты [3], криптографические токены [4], биометрические системы [5] и т.д. В последние несколько лет начали набирать популярность системы, основанные на использовании графических паролей [6] и беспроводных ключей [7].

Однако наиболее совершенные подходы к обеспечению аутентификации не получили широкого распространения в силу того, что конечные пользователи отдают предпочтение не наиболее безопасным, а наиболее удобным в обращении системам. Более того, зачастую пользователь вынужден проходить процедуру аутентификации независимо в каждой из ИС, с которыми он взаимодействует, что требует существенных временных затрат и усилий на сохранение секретной информации для каждой ИС. Следовательно, это косвенно ведет к снижению общего уровня безопасности, так как пользователь будет стремиться всеми силами упростить для себя процедуру входа в систему (например, выберет один и тот же пароль для всех ИС).

Таким образом, крайне актуальной является задача создания безопасной, но в то же время удобной в использовании системы аутентификации пользователя в различных, не связанных друг с другом ИС. На сегодняшний день известно несколько подходов к созданию подобных систем, большинство из которых являются интерактивными, то есть так или иначе вовлекают пользователя в процедуру аутентификации либо реализуются с использованием сложных криптографических протоколов, требующих существенных вычислительных мощностей на стороне "ключа" — специального устройства для хранения и обработки идентификаторов пользователя в различных ИС, а значит, и соответствующего питания.

В данной статье предлагается конструктивное решение задачи создания неинтерактивной пассивной (не требующей вычислительной мощности на стороне "ключа", не требующей электропитания) системы аутентификации пользователя в нескольких не связанных между собой ИС. Ядром системы является новый алгоритм генерации ключей шифрования и расшифрования ключевых последовательностей, используемых для аутентификации. С помощью данного алгоритма возможно построение системы шифрования, при использовании которой ИС не может получить доступ к ключевым последовательностям других ИС. Аналогичным образом, Атакующий не может получить доступа к ключевым последовательностям ни одной из ИС даже при наличии физического доступа к носителю. Аутентификация возможна посредством практически любого протокола пакетной передачи данных (как проводного, так и беспроводного). В частности, система была реализована для технологий USB [8] и Near Field Communications (NFC, [9]).

Статья имеет следующую структуру: в разделе 2 рассматривается классификация существующих подходов к аутентификации пользователя в нескольких ИС. В разделе 3 описаны основные требования, выдвигаемые к системам аутентификации подобного класса. Разделы 4 и 5 посвящены базовой и улучшенной моделям

предлагаемой системы. Качественный анализ характеристик предлагаемого решения приводится в разделе 6. Основные результаты работы, выводы и направления дальнейших исследований обозначены в разделе 7.

2. Существующие подходы к аутентификации пользователя в нескольких ИС

В настоящее время существует множество подходов к созданию систем аутентификации пользователя в нескольких ИС [10],[11],[12],[13],[14], которые можно классифицировать по следующим принципам:

1. Использование единого идентификатора и единой ключевой информации во всех ИС, с которыми работает пользователь.

2. Использование различных идентификаторов, ключевых последовательностей и методов аутентификации в различных ИС.

3. Применение решений с участием доверенного посредника.

4. Применение решений с использованием унифицированного носителя с защищенным хранилищем идентификаторов и ключевых последовательностей для каждой из ИС:

   (a) Не интерактивные — пользователь не участвует в процедуре аутентификации;

   (b) Интерактивные — пользователь принимает непосредственное участие в процедуре аутентификации (выбирает ИС, вводит пин-код или пароль и т.д.)

Первый подход связан с использованием единой пары ”идентификатор – ключевая последовательность” во всех ИС, с которыми работает пользователь (см. рис. 1). Данный подход удобен для пользователя, так как отсутствует необходимость запоминать большое количество ключевых последовательностей. Однако предъявляя, например, документ, удостоверяющий личность, пользователь может раскрывать часть своих персональных данных системе, которая в них не нуждается. Также подобный подход ведет к необходимости хранить персональные данные о всех пользователях системы на стороне ИС, а следовательно, организовать их защиту. Кроме того, в случае раскрытия ключевой информации пользователя через уязвимость в одной из ИС, под угрозой оказываются все остальные системы.

Основной идеей следующего подхода, связанного с использованием уникальных идентификаторов для различных ИС, является создание уникальных пар ”идентификатор – ключевая последовательность” так, чтобы ни идентификаторы, ни ключевые последовательности в разных парах не повторялись (см. рис. 2). Типичными реализациями указанного подхода является использование различных ключей для доступа в различные помещения, или, например, именных дисконтных карт в фирменных магазинах. Подход является достаточно надежным, поскольку взлом одной ИС не приводит к появлению уязвимости в остальных. В то же время реализация

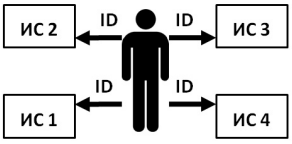

Рис. 1. Использование единого идентификатора

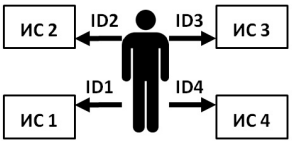

Рис. 2. Использование уникальных идентификаторов

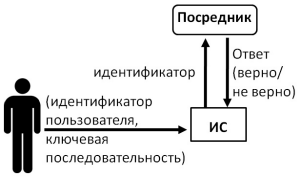

Рис. 3. Использование доверенного посредника

накладывает дополнительные ограничения на пользователя. Он вынужден в том или ином виде хранить идентификаторы и ключевые последовательности для всех ИС, с которыми работает (например, помнить множество неповторяющихся паролей).

Третий из перечисленных выше подходов связан с использованием доверенного посредника, который выполняет функции проверки корректности ключевой последовательности вместо подсистемы ИС и сообщает ИС только результат проверки: ”верно”/”не верно” (см. рис. 3). Типичными представителями систем, реализующих третий подход, являются приложения Google Wallet [10], Apple iWallet [11] и др. В общем случае использование доверенного посредника имеет тот же набор уязвимостей, что и использование единого идентификатора — появление ”единой точки отказа”[15]. Таким образом, реализация данного подхода не решает обозначенной выше задачи создания удобного и безопасного способа аутентификации.

Последним в списке стоит создание физического унифицированного носителя идентификаторов, заменяющего собой доверенного посредника. Сложности возникают с реализацией требования разделения доступа к ключевым последовательностям, хранящимся на носителе, между ИС. В существующих решениях данного класса широко применяются два способа решения указанной проблемы: либо двухсторонняя взаимная аутентификация носителя и ИС, либо интерактивный режим работы. В первом случае обычно используется один из известных протоколов, например Kerberos [16] или его модификации (см. рис. 4). Для реализации данного протокола на стороне носителя размещается вычислительное ядро небольшой мощности. Примерами такого подхода могут быть такие решения, как VeriChip [14] и codeREADr [12]

Рис. 4. Не интерактивный универсальный физический носитель идентификаторов

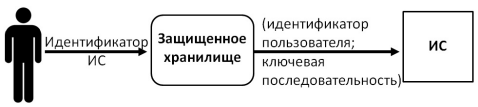

Рис. 5. Интерактивный универсальный физический носитель идентификаторов

К сожалению, большинство из решений класса 4a неприменимо для широкого круга задач. Этому способствуют низкая вычислительная мощность ядра носителя и необходимость использовать упрощенные версии протоколов с меньшей длиной ключа, в результате чего снижается уровень безопасности ИС. Дополнительные сложности возникают с электропитанием носителя, поскольку срок службы батарей на данном этапе не может быть неограниченным при решении подобных вычислительных задач.

Некоторое количество защищенных носителей информации для решения задачи разделения доступа к данным между ИС используют интерактивный режим (см. рис. 5). В частности, универсальная электронная карта [13] предлагает пользователю самому выбрать, к какой ИС он будет подключаться в данный момент каждый раз перед выполнением процедуры аутентификации. Несмотря на кажущуюся простоту и изящество данного решения, оно, как и в предыдущем случае, требует дополнительного оборудования на стороне носителя, а также заставляет пользователя совершать дополнительные действия каждый раз перед выполнением процедуры аутентификации. Таким образом, получившееся решение, являясь в должной мере безопасным, не является удобным для пользователя.

Обобщая анализ существующих решений, можно сделать вывод о том, что системы, обеспеченные вычислительными мощностями (класс 4a и 4b), успешно справляются с задачей аутентификации пользователя в системе и разделения доступа между ИС, а решения, не обеспеченные такими возможностями (классы 1–3), имеют достаточно ограниченный набор возможностей и не могут эффективным образом разделить доступ к ключевым последовательностям между ИС. К сожалению, системы класса 4b требуют участия пользователя в процедуре аутентификации, что не всегда удобно.

С учетом всего вышесказанного наиболее перспективным выглядит подход с использованием неинтерактивного хранилища идентификаторов (класс 4a), единственным существенным недостатком которого является необходимость в применении упрощенных версий криптографических примитивов, имеющих меньшую стойкость к атакам.

Таким образом, актуальной является задача создания системы аутентификации класса 4a с использованием полноразмерных криптографических примитивов, а следовательно, и гарантированно высоким уровнем стойкости к возможным атакам. Базовое решение поставленной задачи приведено в разделе 4, а улучшенная версия системы, обладающая рядом существенных преимуществ по сравнению с аналогами, описана в разделе 5.

3. Основные требования к разрабатываемому решению

Прежде чем приступить к описанию предлагаемой системы, определим ряд понятий, которые будут использоваться в процессе изложения, а также выработаем набор требований к системе аутентификации в различных ИС. Общая схема сети, для которой разрабатывается система, представлена на рисунке 6. Объектами в сети являются Карты (защищенные носители информации), Документы, хранящиеся на

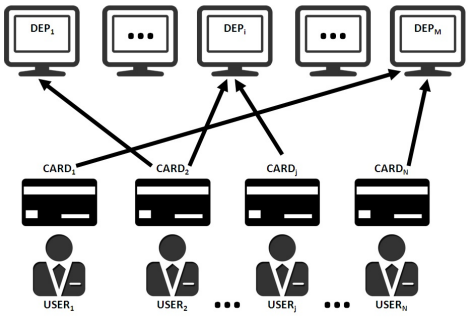

Рис. 6. Топология базовой системы

Картах (ключевые последовательности), а также Терминалы, умеющие считывать данные с этих карт.

- Документ — набор данных в формате, утвержденном Ведомством, доступных для чтения Пользователю (хранится на Карте) и соответствующему Ведомству.
- Карта — некоторое устройство хранения данных, не имеющее питания и не обладающее вычислительными способностями.
- Терминал — считывающее устройство для чтения, проверки, записи Документов на Карту.

Субъектами на схеме являются Пользователи и Ведомства.

- Пользователь — физическое лицо, владелец носителя (Карты).
- Ведомство — организация – участник системы, выдает Документы (ключевые последовательности) своего типа и может запрашивать их у любого Пользователя системы. Примерами Ведомств могут служить полиция, поликлиника, магазин.

С использованием предложенных обозначений, сформируем ряд требований к системе аутентификации во множестве ИС для указанной схемы сети.

1. Пользователь без каких-либо ограничений всегда может прочитать любой Документ, хранящийся на Карте.
2. Ведомство и его Терминалы могут читать относящиеся к своему Ведомству Документы с Карты любого Пользователя, при этом никаких дополнительных действий со стороны Пользователя для этой операции не требуется (не нужно в данный момент времени явно разрешать чтение именно этого Документа).
3. Пользователь не может читать Документы других Пользователей, хранящиеся на их Картах, даже при условии, что он получил физический доступ к памяти.
4. Ведомство не может получить доступ к Документам другого Ведомства, хранящимся на Карте Пользователя, даже при наличии физического доступа к памяти.

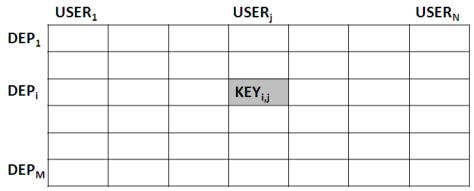

Рис. 7. Предлагаемый подход – шифрование каждого Документа Пользователя отдельным ключом

5. Пользователь не может создавать Документ/вносить изменения в Документ без явного согласия на это соответствующего Ведомства.

Убедимся, что выполнение указанных требований обеспечивает безопасность информации в случае потери или кражи Карты. Информационная безопасность складывается из конфиденциальности, целостности и доступности данных [17]. Доступность данных обеспечивается одновременным выполнением свойств 1 и 2. Конфиденциальность документов на Карте обеспечивается комбинацией свойств 3 и 4. Целостность — свойством 5. Таким образом, система, удовлетворяющая указанным требованиям, является безопасной. В последующих разделах приведено описание конкретной системы аутентификации, удовлетворяющей указанным требованиям.

4. Базовая версия системы

Основной идеей разрабатываемого решения является применение комбинации криптографических примитивов, позволяющих зашифровать данные в памяти носителя таким образом, чтобы информационная система, выполняя аутентификацию пользователя, могла корректно интерпретировать только те ключевые последовательности, которые имеют отношение к данной ИС. Отметим, что предлагаемое решение основывается на использовании пассивного модуля памяти в качестве носителя информации. По причине отсутствия вычислительных мощностей на стороне носителя на подобных устройствах невозможно реализовать протокол двухсторонней аутентификации. Следовательно, выбранный способ шифрования данных должен быть достаточно надежным для предотвращения различных попыток взлома в случае утери или кражи носителя.

Достигнуть столь высокого уровня безопасности можно, например, шифрованием каждого документа каждого пользователя отдельным ключом (уникальным для каждого Документа, Пользователя и Ведомства, см. рисунок 7).

К недостаткам описанного решения стоит отнести тот факт, что Ведомству приходится хранить ключи для всех Пользователей, а Пользователю — ключи для всех Ведомств. Это достаточно безопасно, но неудобно для обеих сторон. К тому же подобная схема требует больших объемов памяти ($O(n \cdot m)$, где n — число Пользователей, а m — число Ведомств). Для того, чтобы сократить требуемый объем памяти, как на стороне Ведомства, так и на стороне Пользователя, необходимо разработать алгоритм генерации ключей шифрования для каждой пары ”Ведомство–Пользователь” на основе открытой информации и секретного ключа Ведомства, с

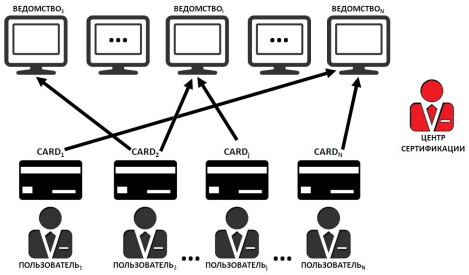

Рис. 8. Топология модифицированной системы

одной стороны, или открытой информации и секретного ключа Пользователя, с другой. Один из вариантов подходящего алгоритма описан в следующем разделе.

5. Модифицированная система, алгоритм мгновенной генерации ключей шифрования

В данном разделе описана модифицированная система аутентификации пользователя в нескольких ИС. Ключевым достоинством системы, по сравнению с базовой (см. Раздел 4), является снижение объемов требуемой памяти с $O(n \cdot m)$, где n — число Пользователей, а m — число Ведомств, до $O(1)$. Данная цель достигается с помощью описанного ниже алгоритма мгновенной генерации ключей шифрования Документов, специфичного для нашей системы. Для детального описания работы системы введем несколько обозначений.

- *Идентификатор Ведомства* DEP_i — публичный уникальный номер, однозначно идентифицирующий Ведомство в системе.
- *Идентификатор Пользователя* $USER_j$ — публичный уникальный номер, однозначно идентифицирующий Пользователя в системе.

В дополнение к схеме сети, представленной на рисунке 6, введем в рассмотрение дополнительного участника — "Центр Сертификации (ЦС)", который по уникальным идентификаторам Ведомств и Пользователей (DEP_i и $USER_j$ соответственно) выдает им секретные ключи: $DKEY_i$ для Ведомства и $UKEY_j$ для Пользователя. Модифицированная схема сети представлена на рисунке 8.

Обозначим как $KEY_{i,j}$ ключ шифрования, которым зашифрованы Документы ведомства DEP_i на Карте пользователя $USER_j$. Теперь для создания алгоритма генерации ключей необходимо построить функции $F_{DEP_i}(USER_j)$ и $G_{USER_j}(DEP_i)$ такие, что выполняется следующее свойство (Формула 1):

$$F_{DEP_i}(USER_j) = G_{USER_j}(DEP_i) = KEY_{i,j}. \tag{1}$$

Наконец, предложим следующий алгоритм генерации ключей шифрования:

Алгоритм вычисления ключей шифрования

Пусть a — некоторое число, которое известно только центру сертификации — секретный ключ системы (Master Secret Key, MSK)[18], c — некоторое число, известное всем участникам системы, а операция $mod\ c$ означает получение остатка

от деления на c. Тогда секретные ключи Пользователей и Ведомств предлагается строить по следующим формулам:

$$UKey_j = a^{USER_j} mod\ c; \tag{2}$$

$$DKey_i = a^{DEP_i} mod\ c; \tag{3}$$

Затем, согласно формуле (1), будем вычислять ключ шифрования Ведомства i для Пользователя j ($KEY_{i,j}$) на стороне Ведомства по следующей формуле:

$$KEY_{i,j} = DKey_i^{USER_j} mod\ c; \tag{4}$$

На стороне Пользователя $KEY_{i,j}$ вычисляется аналогичным образом:

$$KEY_{i,j} = UKey_j^{DEP_i} mod\ c. \tag{5}$$

Конец алгоритма

Используя формулы (2) и (3), легко показать, что правые части уравнений (4) и (5) равны одному и тому же числу — $a^{DEP_i * USER_j} mod\ c$. Таким образом, ключ шифрования конкретного документа не зависит от того, на чьей стороне происходит генерация ключа: Пользователя или Ведомства, а зависит лишь от пары идентификаторов DEP_i, $USER_j$ и секретного ключа системы MSK.

Таким образом, описанная в разделе система удовлетворяет свойству (1), при этом требует всего $O(1)$ ячеек памяти для работы. Качественный анализ безопасности и удобства использования системы приведен в разделе 6.

6. Качественный анализ характеристик предлагаемой системы

В данном разделе представлен качественный анализ таких характеристик предлагаемой системы, как безопасность, надежность и удобство использования. Стойкость разработанного решения базируется на выборе в качестве алгоритма шифрования одного из высокозащищенных блоковых шифров, например AES-256 [19] или IDEA [20]. Также можно показать, что для указанного решения выполняются первые 4 требования из раздела 3. В частности, свойство 1 следует из равенства 5 — Пользователь, зная свой секретный ключ и публичный уникальный номер Ведомства, может расшифровать все Документы, хранящиеся на Карте. Свойство 2 обосновывается через 4, так как Ведомство, зная свой секретный ключ и публичный уникальный номер Пользователя, может расшифровать все Документы, принадлежащие ему, не привлекая к этому Пользователя. Свойство 3 также вытекает из формул 4 и 5, так как при попытке злоумышленника расшифровать данные другого Пользователя, ему не будет известен ни секретный ключ этого Пользователя (т.к. он не хранится на карте), ни секретные ключи Ведомств, также в получении этих ключей ему будет отказано центром сертификации, несмотря на то, что $USER_j$ и DEP_i публично доступны. Подобные рассуждения верны и для свойства 4 – при попытке расшифровать данные, принадлежащие другому Ведомству, злоумышленнику не

будут известны ни секретные ключи Пользователей, ни секретный ключ другого Ведомства. К сожалению, для данной системы не выполняется свойство 5, что не влияет на безопасность решения для аутентификации пользователя в ИС, однако в то же время не позволяет использовать аналогичный подход для создания защищенного хранилища документов (например, удостоверений личности, банковских реквизитов и т.д.). Указанное ограничение может быть снято в процессе дальнейшей модификации системы.

Корректность описанного подхода была продемонстрирована на примере двух программных реализаций системы: на основе USB-ключей [8], а также с использованием технологии NFC [9].

В сравнении с существующими аналогами, например codeREADr [12] или Универсальной Электронной Картой (УЭК, [13]), предлагаемая система обладает целым рядом преимуществ. В частности:

- Вся информация о Пользователе хранится локально на Карте, а не в некой глобальной базе данных. Таким образом значительно снижается риск взлома системы.

- Для работы с системой каждому из участников требуется всего один секретный ключ (в УЭК, например, их четыре [13]).

- Система не требует наличия ни вычислительных мощностей, ни источника питания на стороне ключа, что значительно снижает стоимость конечных устройств и упрощает взаимодействие с ними. Стоит отметить, что для чтения данных с карты Пользователь использует свой терминал.

- Основные операции в системе: аутентификация, добавление/удаление пользователя в ИС, добавление/удаление ИС имеют минимальную вычислительную сложность (несколько операций шифрования/расшифрования), занимают объем памяти, ограниченный сверху $O(1)$, а главное, могут быть выполнены в реальном времени (для добавления новой ИС в УЭК, например, необходимо перевыпустить BCE карты).

- Система не требует специализированного интерфейса для взаимодействия карты с ИС, а может работать поверх практически любого протокола как проводной, так и беспроводной связи (USB, Wi-Fi [21], Wireless USB [22], NFC и др.)

Таким образом, описанная в работе система аутентификации является дешевым, масштабируемым, надежным, безопасным и удобным в использовании решением. Более того, при дальнейшем усовершенствовании системы возможно расширение сферы ее применения для обеспечения защищенного хранения документов.

7. Заключение

С ростом уровня информатизации общества задача защиты конфиденциальных данных пользователя является все более важной. Одним из элементов системы защиты данных является безопасный, надежный и, немаловажно, удобный в использовании

механизм аутентификации. На сегодняшний день существует множество подходов к аутентификации пользователя, однако очень малый класс систем позволяет обеспечить аутентификацию одновременно в нескольких не связанных друг с другом ИС удобным для пользователя образом. В связи с чем в статье поставлена и успешно решена задача создания безопасной, но в то же время удобной в использовании системы аутентификации пользователя в неограниченном числе разнородных ИС, от домашнего компьютера до платежного терминала.

Основными особенностями системы являются использование беспроводных ключей, а также матричный способ выбора ключей шифрования для каждой пары "Пользователь – ИС" таким образом, что каждая из сторон в состоянии независимо сгенерировать ключ на основе своего секретного ключа и открытой информации. С использованием указанного ключа производится расшифрование секретной последовательности, выбираемой на стороне ИС и однозначно аутентифицирующей пользователя.

К преимуществам описанного подхода стоит отнести малый объем занимаемой памяти ($O(1)$), высокую скорость работы (для выполнения аутентификации требуется всего одна операция расшифрования), возможность использования в качестве ключа любого носителя информации без вычислительной мощности и без питания, а также применение простого протокола обмена информацией между носителем и ИС, способного работать поверх практически любого современного стандарта пакетной передачи данных, как проводного (например, USB, реализация описана в [8]), так и беспроводного (например, NFC, реализация описана в [9]).

Для доказательства работоспособности системы было разработано программное обеспечение, реализующее описанную выше систему аутентификации. Реализация системы и ее успешное тестирование на разработанном стенде показали работоспособность предложенной математической модели, а также позволили оценить удобство использования и быстродействие предлагаемого решения. Данная система представляет собой альтернативу существующим системам аутентификации и, являясь в достаточной мере безопасной, оказывается дешевой и удобной в использовании. Более того, при наличии дополнительного механизма обеспечения целостности данных, хранящихся на Карте, описанная в работе система может использоваться для более широкого круга задач, чем аутентификация пользователя, например, для создания защищенного хранилища конфиденциальных документов.

Список литературы

1. *Dan Griffin. Safer Authentication with a One–Time Password Solution // MSDN. 2008. Magazine 5.*

2. *ПИН-код ПЛАС №122. 2007*

3. *Цифровой сертификат //URL: www.authority.ru/scdp/page?als=504349*

4. *Криптографический токен //URL: www.rsa.com/rsalabs/node.asp?id=2133*

5. *Biometrics research Group – What is biometrics? //URL: http://biometrics.cse.msu.edu/info/index.html*

6. *Biddle R., Chiasson S., van Oorschot P.C. Graphical Passwords: Learning from Fisrt Generation, Technical Report TR-09-09 / School of Computer Science, Carleton University, Ottawa, Canada, 2009.*

7. *Беспроводной ключ от ПК //URL: http://www.rohos.ru/2011/05/security-performances-with-wireless-pc-lock/*

8. *Комар М. Защищенное хранилище документов: выпускная квалификационная работа бакалавра. Ярославль, 2013. (Komar M. Zashchishchennoe khranilishche dokumentov: vypusknaya kvalifikatsionnaya rabota bakalavra. Yaroslavl, 2013 [in Russian]).*

9. *Petrov Vitaly, Komar Maria, Koucheryavy Yevgeni. A Lightweight Many-to-Many Authentication Protocol for Near Field Communications // 21st IEEE International Conference on Network Protocols, Goettingen, Germany.*

10. *Google Inc. – Google Wallet //URL: www.google.com/wallet/ 26.05.2011*

11. *Apple iWallet //URL: www.patentlyapple.com/patently-apple/tech-nfc/ 11.06.2013*

12. *codeREADr project //URL: www.codereadr.com/, 2009-2013*

13. *Универсальная электронная карта //URL: http://www.uecard.ru/, 2010 – 2013*

14. *VeriChip //URL: www.positiveidcorp.com/. 2013*

15. *Single point of failure //URL: www.techopedia.com/definition/4351/single-point-of-failure-spof*

16. *Kerberos: The Network Authentication Protocol //URL: http://web.mit.edu/kerberos/*

17. *ГОСТ Р ИСО/МЭК 17799-2005 (GOST R ISO/MEK 17799-2005 [in Russian]).*

18. *Терехов А.Н.,Тискин А.В. Криптография с открытым ключом: от теории к стандарту // Программирование. 1994. №5 (сентябрь-октябрь). С. 17–22. (Terekhov A.N.,Tiskin A.V. Kriptografiya s otkrytym klyuchom: ot teorii k standartu // Programmirovanie. 1994. No 5. S. 17–22 [in Russian]).*

19. *Advanced Encryption Standard //URL: csrc.nist.gov/publications/fips/fips197/fips-197.pdf*

20. *Xuejia Lai and James Massey. A Proposal for a New Block Encryption Standard // EUROCRYPT. 1990.*

21. *WiFi Alliance //URL: http://www.wi-fi.org/*

22. *Wireless USB Specification //URL: http://www.businesswire.com/news/home/20100929005516/en/Wireless-USB-1.1-Specification*

A Novel Approach to Many-to-Many User Authentication in Different Information Systems

Vitaly Petrov, Maria Komar, Yevgeny Koucheryavy

Tampere University of Technology,
PO Box 527, FI-33101, Korkeakoulunkatu 10, Tampere, Finland
P.G. Demidov Yaroslavl State University
Sovetskaya, 14, Yaroslavl, 150000, Russia

Keywords: authentication, wireless networking, information systems security

In this paper, we propose a novel approach to many-to-many user authentication in heterogeneous information systems. The described solution is based on the use of wireless keys – special devices that identify the user by transmitting the requested key information over a wireless network. The key feature of the proposed approach is noninteractive operating mode that allows to use a special encryption algorithm instead of two-way authentication. The algorithm is built on the basis of existing cryptographic primitives that prevents unauthorized system participants from getting access to the data of other users, even with physical access to the memory of the key. This approach does not require computational power or the battery on the key side and does not involve the user in the authentication process that allows implementing a method on passive NFC tags. To proof the concept, software implementation of the described system was developed and a qualitative comparison of the resulting solutions with existing analogues was conducted.

Сведения об авторах:

Петров Виталий Игоревич,
Технологический университет г. Тампере, Финляндия, научный сотрудник
Комар Мария Сергеевна,
Ярославский государственный университет им. П.Г. Демидова, магистрант
Кучерявый Евгений Андреевич,
Технологический университет г. Тампере, Финляндия, профессор