М. В. Дубовицкая

ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ОБЕСПЕЧЕНИЕМ АНОНИМНОСТИ СТОРОН – УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА

Введение

Обеспечение анонимности пользователей различных интернет-сервисов становится актуальной задачей, эффективными инструментами для решения которой являются протоколы «забывающей» передачи, доказательства с нулевым разглашением, анонимные электронные удостоверения и «электронные деньги». Существующие на данный момент системы не обеспечивают полной анонимности пользователей одновременно с контролем доступа (когда провайдер услуг не знает не только кто, но и к чему именно в данный момент обращается, однако он уверен, что тот, кто это делает, обладает правами и/или, когда речь идет о покупке, достаточной суммой денег на счету). В данной работе анализируются требования к построению подобных систем, а также наиболее эффективные инструменты для их построения.

1. Требования к системам анонимной аутентификации пользователей

Все больше и больше операций в нашей повседневной жизни осуществляются через Сеть: сервисы мигрируют из бумажного мира в цифровой. Люди предоставляют свои персональные данные различным провайдерам онлайн-услуг, будучи при этом уверенными в том, что разглашение небольшого количества персональной информации не может впоследствии отразиться на них негативным образом. Однако при активном пользовании интернет-услугами они раскрывают гораздо больше информации о себе, чем им кажется. Можно получить полную картину действий пользователя: осуществляемые электронные транзакции, местонахождение, персональные данные, анализируя запросы и взаимодействие пользователей с различными веб-сайтами и базами данных. Поэтому обеспечение анонимности пользователей является важной задачей. Однако для защиты конфиденциальной информации, такой как медицинские или финансовые данные, необходимо обеспечить контроль доступа, чтобы быть уверенными, что только авторизованные пользователи получают доступ к информационным ресурсам, что, казалось бы, противоречит требованию анонимности пользователей и осуществляемых ими транзакций.

Поэтому для обеспечения конфиденциальности персональных данных пользователей одновременно с контролем доступа к информации необходимо, чтобы все электронные транзакции могли выполняться без разглашения большего количества информации о пользователе, чем это необходимо. Т. е. пользователь должен лишь подтвердить тот факт, что он имеет право на доступ к тем ресурсам, которые он запрашивает, не предоставляя своих персональных данных, а также информации о том, к каким именно данным или сервисам он в тот или иной момент обращается.

Для решения таких задач используются анонимные сертификаты [1—3], протоколы «забывающей» передачи [4—8], доказательства с нулевым разглашением и системы «электронных денег». Если рассматривать систему провайдера базы данных (медицинской, финансовой, патентной и т. д.), обеспечивающего *полную анонимность пользователей одновременно с контролем доступа*, то можно определить следующие требования к подобной системе:

– *обеспечение контроля доступа:* только авторизованные пользователи могут получить доступ в систему;

– *анонимность самого пользователя:* пользователи известны в системе под псевдонимами, провайдер услуг не получает от пользователя никакой его персональной информации — только доказательство того, что у пользователя есть права для доступа в систему для конкретного случая (категории, типа услуг);

– *анонимность действий пользователя:* провайдер не знает, к какой именно информации (услугам) обращается пользователь;

– *несвязность:* невозможность найти соответствие между псевдонимом и его обладателем, а также между двумя транзакциями с использованием одного псевдонима в случае регламентированных действий пользователя;

– *возможность раскрытия анонимности:* в случае несанкционированных действий пользователя его анонимность может быть раскрыта;

– *возможность аннулирования и отзыва анонимных электронных сертификатов (удостоверений);*

– *неподдельность:* другие пользователи не могут подделывать анонимные сертификаты, дающие право на доступ к данным и услугам, а также подделывать электронные «монеты»;

– *трассируемость*: трассируемость означает, что пользователь не может получить такое электронное удостоверение, что тот, кто его выдал, не сможет установить владельца или сможет установить его, но не сможет корректно доказать это.

2. Системы анонимных электронных удостоверений

Для обеспечения анонимности пользователей служат системы анонимных электронных удостоверений (anonymous credential systems). Существуют два основных типа участников в системе: пользователи и организации. Организации могут предлагать различные сервисы. Для предоставления этих сервисов организации требуют, чтобы пользователи выполняли определенные условия. Эти условия могут включать в себя уплату налога, выполнение какого-нибудь отношения или доказательство обладания правами от какой-либо доверенной организации. Организации знают пользователей только по псевдонимам. Разные псевдонимы одного пользователя не могут быть связаны друг с другом и с самим пользователем.

Цифровые электронные удостоверения, выпускаемые одной организацией и заверенные ею, дают права пользователю, на чей псевдоним они были выпущены, на доступ к различным данным и сервисам. Пользователь может доказать другой организации (которая знает его под другим псевдонимом) свое владение таким электронным удостоверением без разглашения каких-либо дополнительных сведений (кроме того факта, что он владеет данным удостоверением) — анонимно «предъявить» его. Электронное удостоверение может быть «предъявлено» различное количество раз. В связи с этим выделяют три типа электронных удостоверений [2]:

– многократно предъявляемые удостоверения (multiple-show credentials): могут быть использованы бесконечно много раз, причем все случаи предъявления не связаны друг с другом или с организацией, выпустившей их;

– однократно предъявляемые удостоверения (one-show credentials): могут быть использованы анонимно только один раз, при повторном использовании анонимность аннулируется;

– предъявляемые ограниченное число раз (limited- или k-show credentials (для $k > 1$)): могут быть показаны анонимно до k раз, затем анонимность аннулируется.

Первая такая система была предложена в 1985 г. [1]. Позже предлагались различные версии таких систем, но наиболее эффективной является система анонимных цифровых удостоверений, предложенная Каменишем и Лысянской [2, 3], которая позволяет использовать многократно предъявляемые удостоверения и раскрывать анонимность пользователей при их несанкционированном поведении. В данной системе используется схема цифровой подписи, предложенная этими же авторами, которая основана на проблеме дискретного логарифмирования [3].

3. Протоколы «забывающей» передачи

Протокол «забывающей» передачи, предложенный Рабином [4] и усовершенствованный Эвеном и Брассардом, заключается в том, что пользователь получает выбранное им из m сообщений отправителя сообщение, при этом (а) отправитель не знает ничего о выборе получателя, (б) пользователь, в свою очередь, не может получить никакой информации о каком-либо из остальных (m – 1) сообщений отправителя. Наиболее эффективной является схема, предложенная Каменишем, Невеном и Шелатом [5], являющаяся адаптивной версией протокола, в котором пользователь может получить до k записей по своему выбору. Базовая форма данного протокола не накладывает никаких ограничений ни на пользователей, ни на доступ к определенным записям в базе. Однако существуют усложненные версии протокола с различными вариантами осуществления контроля доступа.

Аиелло и Рейнголд [6] предложили вариант протокола (priced oblivious transfer), где каждой записи в базе ставится в соответствие цена, а зашифрованный баланс пользователя уменьшается на величину цены запрашиваемой записи после каждого запроса. Таким образом, пользователь может получать доступ к базе по протоколу «забывающей» передачи, до тех пор пока его баланс положителен. Другим примером усложненного протокола «забывающей» передачи является протокол «условной забывающей передачи», предложенный Ди Крещенцо и Островским [7], в котором доступ к записи в базе предоставляется пользователю лишь в том случае, когда его секрет удовлетворяет некоторому предикату. Протокол «ограниченной забывающей» передачи [8] также определяет права доступа для пользователей, однако ни один из этих протоколов не обеспечивает анонимности для пользователей.

4. Протокол анонимной «забывающей» передачи с разграничением доступа

Описанные выше протоколы не реализуют одновременно большую часть требований (п. 1), однако являются хорошими инструментами для построения системы, удовлетворяющей практически всем предъявленным выше требованиям. Подобная система позволяет использовать анонимные цифровые удостоверения и «электронные деньги» в протоколе «забывающей» передачи и обеспечивать таким образом полную анонимность для пользователей и разграничение доступа. Каждая запись в базе данных имеет свои атрибуты (категории, уровень доступа, цена) и пользователи получают подписанные удостоверяющим центром анонимные цифровые удостоверения (и/или кошельки) для доступа к записям в базе. После этого, используя протокол «забывающей» передачи и доказательства с нулевым разглашением, пользователи анонимно авторизуются и получают доступ к записи, при этом не предоставляя базе данных никакой информации о своем запросе. Такая система может использоваться провайдерами медицинских, финансовых и патентных баз данных, где не только важна анонимность самих пользователей, но также и анонимность самих запросов к базе.

СПИСОК ЛИТЕРАТУРЫ:

1. *Chaum D.* Security without identification: transaction systems to make big brother obsolete // Communications of the ACM. 1985. № 28 (10). P. 1030–1044.
2. *Camenisch J. and Lysyanskaya A.* Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation // EUROCRYPT 2001. LNCS. Springer Verlag, 2001. P. 93–118.
3. *Camenisch J. and Lysyanskaya A.* Signature schemes and anonymous credentials from bilinear maps // Advances in Cryptology — CRYPTO 2004. Vol. 3152 of LNCS. Springer Verlag, 2004. P. 56–72.
4. *Rabin M.* How to exchange secrets by oblivious transfer. Harvard Aiken Computation Laboratory, 1981.
5. *Camenisch J., Neven G., Shelat A.* Simulatable adaptive oblivious transfer // EUROCRYPT 2007. Vol. 4515 of LNCS. Springer-Verlag, 2007. P. 573–590.
6. *Aiello W., Ishai Y., Reingold O.* Priced oblivious transfer: How to sell digital goods // EUROCRYPT 2001. Vol. 2045 of LNCS. Springer-Verlag, 2001. P. 119–135.
7. *Di Crescenzo G., Ostrovsky R., Rajagopalan S.* Conditional oblivious transfer and timed-release encryption // EUROCRYPT'99. Vol. 1592 of LNCS. Springer-Verlag, 1999. P. 74–89.
8. *Herranz J.* Restricted adaptive oblivious transfer // Cryptology ePrint Archive, Report 2008/182, 2008. URL: http://eprint.iacr.org/.

С. Д. Жилкин

МЕТОДЫ ПОСТРОЕНИЯ МОДЕЛЕЙ ШТАТНОЙ РАБОТЫ ПО И АЛГОРИТМЫ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПО

Введение

Среди нынешних задач сферы компьютерной безопасности остро стоит проблема выявления событий некорректной работы программного обеспечения. На текущий момент обозначены многие способы решения этой задачи. Данная статья в общих чертах обозначает методы выявления некорректной и аномальной работы ПО с помощью математического аппарата нейронных сетей.

Так как нейронные сети успешно используются для угадывания образов, на которые они были натренированы [1], основная идея предлагаемого решения задачи заключаются в сравнении заранее заданных (эталонных) моделей поведения ПО с их реальным поведением. Результат сравнения двух образов посредством нейронных сетей является вероятностью совпадения этих образов [1]. По величине этой вероятности (а также некоторым дополнительным характеристикам нейронной сети) можно говорить об аномальном поведении программы. Таким образом, решение проблемы выявления аномалии поведения с помощью нейронных сетей подразумевает выполнение следующих шагов: а) построение модели поведения программы, б) постоянное сравнение запускаемых экземпляров программы с эталонной моделью.

1. Построение модели поведения ПО

Для начала опишем, что представляет собой модель поведения ПО с точки зрения нейронной сети. Нейронная сеть — это набор слоев с так называемыми нейронами. Каждый нейронный слой связан с последующим некой активационной функцией и множеством коэффициентов и смещений. Каждый нейрон принимает на вход множество значений (координат), вычисляет свой выход по активационной функции и передает получившееся значение в следующий слой. В зависимости от способов передачи результатов активационной функции по нейронным слоям нейронные сети делятся на различные классы. В данной статье речь будет идти о билинейном персептроне, каждый