Литература

1. Искусство управления информационной безопасностью. [Электронный ресурс]. – http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/obespechenie-zaschity-personalnyh-dannyh-v-subd-oracle.

2. Обзор технологий идентификации и аутентификации. [Электронный ресурс]. – http://www.infosecurity.ru/cgi-bin/mart/.

3. 10 шагов к обеспечению защищенности базы данных Oracle встроенными механизмами безопасности. [Электронный ресурс]. – https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/326445.php

УДК 004.056.5

Современные технологии аутентификации пользователей

Ковалькова И.А., Лабкович О.Н.
Белорусский национальный технический университет

Современная цифровая глобализация привела к возможности получать, хранить и передавать информацию без ограничений, но в то же время, большая часть этой информации нуждается в защите. Одним из самых важных видов защиты информации является ограничение доступа. В данном случае доступ получают те, кто имеет на это право, и это право может быть доказано посредством владения «ключом» – неважно, пароль это, или радужная оболочка глаза. [1]

Здесь необходимо обратиться к понятию аутентификации.

Аутентификация – это процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В зависимости от степени доверительных отношений, структуры, особенностей сети и удалённостью объекта проверка может быть односторонней или взаимной. В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения («да» или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдаёт, с другой стороны – для защиты трафика обмена «субъект - система» от злоумышленника. [2]

Существует очень большое количество технологий аутентификации, и все они обладают разной степенью удобства и надёжности. Основной

задачей при выборе технологии аутентификации является понимание функционирования того или иного способа, и итогом осознанного выбора будет успешный расчёт рисков. Такой анализ позволит выбрать наиболее удачный вариант защиты доступа от несанкционированного входа, и позволит сделать это наименее затратным путём.

Аутентификация по логину и паролю

Парольная аутентификация является самой распространённой, поскольку это самый простой и привычный способ. Пароли давно встроены в операционные системы и информационные сервисы. Однако необходимо признать, что использование паролей является довольно слабым средством проверки подлинности. Основным фактором надёжности пароля является его сложность. Но особенность человеческого мозга такова, что человек не в состоянии помнить уникальные, длинные и сложные пароли, которые считаются наиболее надёжными.

Часто пользователь выбирает в качестве пароля слова, которые много значат для него и потому их легко отгадать – дата дня рождения, имя близкого человека, кличка любимой собаки. К тому же, ввод пароля не так сложно подсмотреть. А иногда пользователи и вовсе сами дают пароль своим близким или друзьям. Есть также популярные пароли – например, использование рядом стоящих клавиш при создании пароля (qwerty, 123456), или часто используемые слова (admin). Одним из распространённых способов взлома паролей является подбор слов по словарю, поскольку очень часто пользователи используют то, что легко запомнить, с чем есть ассоциации – то есть какие-то слова. К тому же, часто пользователь использует один и тот же пароль для входа на многие сайты, таким образом, надёжность этого пароля сразу ощутимо снижается.

Отдельно стоит сказать о системах перехвата электронной информации, и программах, отслеживающих нажатие клавиш. Такие программы очень трудно отследить, а злоумышленник сразу получает доступ практически ко всей информации пользователя. Взлом пароля почты также может привести к неприятным для пользователя последствиям – система восстановления пароля часто не содержит никаких дополнительных мер безопасности, а потому под угрозой утечки информации окажутся все сайты и социальные сети, привязанные к данному почтовому ящику. Вся конфиденциальная информация уже не будет защищена – деловая переписка, фотографии из отпуска, учётные записи в личные кабинеты интернет-банка – все может оказаться публично доступным, либо быть использованным злоумышленником в своих целях. Это может нанести как репутационный, так и финансовый ущерб.

Аутентификация через социальные сети

Помимо общеизвестной комбинации логин/пароль для аутентификации, владельцы информационных систем имеют возможность установить более удобные технологии подтверждения подлинности пользователя. К примеру, получившая широкое распространение в последнее время технология аутентификации пользователей по аккаунтам социальных сетей, сокращает время на заполнение форм для создания новой учётной записи (регистрации), а также не требует повторного ввода комбинаций логина и пароля. Однако, встраивание данной технологии может потребовать некоторых усилий и затрат на услуги специалистов для интеграции нужных модулей или кодов в систему.

Аутентификация с использованием одноразовых паролей

Гораздо более строгим и надёжным методом проверки и подтверждении подлинности пользователя является использование двухфакторной аутентификации. В данном случае пользователь не только предъявляет системе свой идентификатор (логин, пароль, смарт-карту, e-mail), но и подтверждает свою личность дополнительно – это может быть, к примеру, PIN-код, или биометрические данные.

Каждому, кто хоть раз проводил денежные расчёты через Интернет, используя пластиковую карту, знакомо заполнение форм с последующим подтверждением личности с использованием одноразового пароля, высылаемого банком-эмитентом для подтверждения оплаты. Это вполне возможно реализовать на любом сайте, но при этом данный способ требует определённых затрат на интеграцию и обслуживание.

Это надёжный метод аутентификации, тем не менее, современные методы взлома позволяют хакерам обходить даже такие, казалось бы, сложные технологичные схемы.

Аутентификация с использованием цифрового сертификата

Ещё одним безопасным методом является использование цифрового сертификата, который может быть реализован в виде приложения для компьютера или иного устройства (планшета, телефона), либо сертификат может быть записан на физический носитель в виде смарт-карты, USB-токена или другого физического устройства. Сложно сказать, какой тип цифрового сертификата является более удобным в использовании. Физический носитель может быть утерян, но цифровой сертификат в виде приложения менее портативен. В любом случае, квалифицированный цифровой сертификат является подтверждением личности, который его использует, и таким аутентификатором практически невозможно воспользоваться несанкционированно, поскольку для получения доступа к

приложению с цифровым сертификатом, либо к физическому устройству часто дополнительно требуется знание кода доступа, то есть пин-кода. [1]

Все перечисленные технологии аутентификации имеют свои преимущества и недостатки, однако встраивание любого из них требует определённых временных и финансовых ресурсов.

Литература

1. Современные технологии аутентификации. [Электронный ресурс]. – https://www.trusted.ru/company/news/sovremennye-tekhnologii-autentifikatsii/.
2. Обзор технологий идентификации и аутентификации. [Электронный ресурс]. - http://www.infosecurity.ru/cgi-bin/mart/.

Особенности деятельности таможенных органов при увеличении объема интернет-торговли

Осипова П.Д., Бровка Г.М.
Белорусский национальный технический университет

Перед таможенными органами всего мира стоит задача всемерного содействия развитию торговли при одновременном сохранении и повышении результативности таможенного контроля. Данная двойственная задача не может быть эффективно решена без максимального использования современных таможенных технологий, необходимость применения которых обусловлена быстрым увеличением объема международного товарооборота, усложнением его структуры, ограничению кадровых ресурсов таможенных органов и желанием всех участников ВЭД свести к минимуму потери времени и материальных средств в ходе таможенного контроля. Исходя из этого можно сказать, что тема совершенствования информационных систем является более чем актуальной.

В Республике Беларусь электронная торговля рассматривается как путь к созданию прозрачного, высокоорганизованного рынка продукции, услуг и технологий. Сегодня в байнете более 2 000 Интернет-магазинов. Представлены практически все категории товаров и услуг. Реальный оборот Интернет- магазинов неизвестен. Однако известно, что приблизительно 95% платежей в интернете белорусские пользователи делают за услуги и