ПАРОЛЬНАЯ АУТЕНТИФИКАЦИЯ (ОДНОРАЗОВЫЕ, МНОГОРАЗОВЫЕ ПАРОЛИ)

Славенко Д.С.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Парольная аутентификация – это процедура проверки подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов. Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. [1]

Аутентификация нужна для доступа к: соцсетям, электронной почте, интернет-магазинам, форумам, интернет-банкинг и платёжным системам.

Аутентификация по многоразовым паролям.

Один из способов аутентификации в компьютерной системе состоит во вводе пользовательского идентификатора, в просторечии называемого «логином» и пароля – неких конфиденциальных сведений. Достоверная пара «логин – пароль» хранится в специальной базе данных.

Простая аутентификация имеет следующий общий алгоритм:

1) Субъект запрашивает доступ в систему и вводит личный идентификатор и пароль.

2) Введённые неповторимые данные поступают на сервер аутентификации, где сравниваются с достоверными.

3) При совпадении данных с достоверными аутентификация признаётся успешной, при различии – субъект перемещается к 1-му шагу. [2]

Аутентификация по одноразовым паролям.

Заполучив однажды многоразовый пароль субъекта, злоумышленник имеет постоянный доступ к взломанным конфиденциальным сведениям. Эта проблема решается применением одноразовых паролей. Суть этого метода в том, что пароль действителен только для одного входа в систему, при каждом следующем запросе доступа требуется новый пароль. Реализация механизма аутентификации по одноразовым паролям может осуществляться как аппаратно, так и программно.

Существуют следующие технологии использования одноразовых паролей:

1) Использование генератора псевдослучайных чисел, единого для субъекта и системы. То есть, сгенерированный субъектом пароль может передаваться системе при последовательном использовании односторонней функции или при каждом новом запросе, основываясь на уникальной информации из предыдущего запроса.

2) Использование временных меток вместе с системой единого времени. В качестве примера такой технологии можно привести SecurID. Она основана на использовании аппаратных ключей и синхронизации по времени. Аутентификация основана на генерации случайных чисел через определённые временные интервалы. Уникальный секретный ключ хранится только в базе системы и в аппаратном устройстве субъекта. Когда субъект запрашивает доступ в систему, ему предлагается ввести PIN-код, а также случайно генерируемое число, отображаемое в этот момент на аппаратном устройстве. Система сопоставляет введённый PIN-код и секретный ключ субъекта из своей базы и генерирует случайное число, основываясь на параметрах секретного ключа из базы и текущего времени. Далее проверяется идентичность сгенерированного числа и числа, введённого субъектом.

3) Использование базы случайных паролей, единой для субъекта и для системы. Эта технология основана на единой базе паролей для субъекта и системы и высокоточной синхронизации между ними. При этом каждый пароль из набора может быть использован только один раз. Благодаря этому, даже если злоумышленник перехватит используемый субъектом пароль, то он уже будет недействителен. По сравнению с использованием многоразовых паролей одноразовые пароли предоставляют более высокую степень защиты. [4]

Использование пароля в качестве аутентификационного фактора, наверное, ещё очень долго будет являться наиболее распространённым способом решения задач определения подлинности. Простота реализации и логическая ясность принципов функционирования делают системы парольной аутентификации самыми популярными. И хотя существует множество угроз данной схеме авторизации (подбор пароля, анализ трафика, повторное воспроизведение запроса на аутентификацию), она используется в большинстве информационных систем, а задачи защиты от перечисленных угроз решаются обычно комплексом мер, одно из центральных мест в которых занимает криптографическая защита. [3]

Литература

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.- СПб.: Изд-во СПбГУЭФ, 2010.- 267 с.

2. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса "Основы информационной безопасности". - Интернет Университет Информационных Технологий, 2010г.

3. Сабанов А.Г. Аутентификация как часть единого пространства доверия / Электросвязь. 2012. №8, с.40-44.

4. Сабанов А.Г. Обзор технологий идентификации и аутентификации / "Документальная электросвязь" 2006., №17, с.23-27.

ОБЩАЯ ХАРАКТЕРИСТИКА АППАРАТОВ ФЛЮОРОСКОПИЧЕСКОГО ТИПА КАК СРЕДСТВ ПОИСКА ПРИ ТАМОЖЕННОМ ДОСМОТРЕ

Сладикова Я.С.
Научный руководитель: д.т.н., доцент Голубцова Е.С.
Белорусский национальный технический университет

Под досмотрово-поисковой техникой понимается комплекс технических средств, используемый для поиска объектов, обнаружение которых органолептическим методом затруднено или невозможно.

Досмотровая флюороскопическая установка – это специальная аппаратура, предназначенная для таможенного досмотра методом просвечивания объектов таможенного контроля с целью выявления в них и их содержимом любых видов предметов таможенных правонарушений и их признаков.

Главной особенностью данного класса досмотровых установок является использование специального флюороскопического экрана для отображения результатов просвечивания контролируемого объекта. Свечение, возникающее под воздействием внешнего облучения и исчезающее в течение короткого времени после окончания воздействия, называют **флюоресценцией.** Поэтому установки, использующие такой экран, называют **флюороскопами.**

Флюороскопические системы эффективно используются для решения задач обеспечения безопасности, в том числе для решения антитеррористических задач.

Объектами применения флюороскопических установок являются ручная кладь и сопровождаемый багаж пассажиров, несопровождаемый багаж пассажиров и среднегабаритные грузовые упаковки, крупногабаритные грузы, а также международные почтовые отправления.

В флуороскопических системах изображение формируется целиком, при необходимости усиливается и наблюдается оператором установки. При