Для того чтобы выполнить опыт, необходимо на панели параметров: 1) выбрать исследуемую жидкость; 2) указать значения радиуса шарика; 3) указать плотность материала шарика и, наконец, нажать на кнопку «Применить». После этого шарик начнет двигаться вниз, ко дну сосуда со скоростью, определяемой вязкостью жидкости, размерами шарика и его плотностью. Результаты эксперимента выводятся на экран в соответствующем окне. При повторении опыта и изменении значения входных параметров будет меняться и результаты эксперимента.

УДК 004.021

Студ. А.С.Федотов
Науч. рук. доц. В.В. Смелов
(кафедра информационных систем и технологий, БГТУ)

ОСНОВНЫЕ ПРИНЦИПЫ РЕАЛИЗАЦИИ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Одна из самых серьёзных проблем с традиционной аутентификацией с использованием имени пользователя и пароля – поддержка базы данных паролей. Независимо от того, зашифрована база паролей или нет, если злоумышленник знает, на каком сервере она находится и ему нужно узнать только пароль, то время, через которое он сможет прочесть данные, зависит чаще всего только от вычислительных возможностей его оборудования.

Вычислительная скорость работы процессоров с каждым годом увеличивается. «Метод грубой силы» – метод полного перебора паролей – становится особенно актуальным. К тому же, разработки вроде взлома паролей с помощью GPGPU (графического процессора общего назначения) и технология «радужных таблиц» предоставляют схожие возможности взлома паролей для злоумышленников. Взлом с помощью GPGPU, например, позволяет генерировать больше пятисот миллионов паролей в секунду при использовании оборудования, уровень, который соответствуют игровым ПК начального уровня. В зависимости от особенностей ПО, технология «радужных таблиц» может быть использована для взлома пароля из четырнадцати-символьного буквенно-цифрового пароля примерно за сто шестьдесят секунд. База паролей в большинстве случаев не сможет противостоять подобным методам взлома.

Существует три основных фактора для многофакторной аутентификации [1].

Первый тип – факторы знания – информация, которую знает пользователь. К этой категории можно отнести имена пользователей,

пароли, идентификационные номера, различного рода пин-коды, ответы на секретные вопросы и прочее. В настоящее время категорически не рекомендуется использовать пароли, длина которых меньше 8 символов. Также к общим рекомендациям можно отнести использование в пароле букв верхнего и нижнего регистра, цифр, специальных символов. Подобные пароли в сочетании с многофакторной аутентификацией обеспечивает весьма надёжную защиту.

Второй тип – факторы владения – любые предметы, которыми владеет пользователь. К этой категории относятся жетоны (токены) безопасности, удостоверение пользователя (с каким-либо секретным кодом), сим-карта мобильного телефона и так далее. Жетоны (токены) безопасности – физические средства, в аппаратную реализацию которых заложена функция генерация ключей, которые в дальнейшем используются для аутентификации [2].

По схеме работы жетоны подразделяются на:

– аппаратные – внешнее устройство, представляющее собой набор схем, с помощью которых происходит генерация кодов. Обычно такие жетоны представляют собой брелоки;

– программные – приложения, в которых происходит генерация кода. Обычно такие жетоны используются в мобильной аутентификации (например, приложение в смартфоне).

По способу подключения жетоны подразделяются на:

– контактные. Данный тип жетонов подключается к компьютеру в момент аутентификации, операционная система считывает значение из ключа и вставляет его в заранее подготовленное поле;

– бесконтактные. Данный тип жетонов обычно имеет дисплей, на котором отображается сгенерированная информация для аутентификации.

Среди контактных выделяют:

– смарт-карты (сим-карты) или USB-устройства со встроенными смарт-картами;

– ПК карта – спецификация на модули расширения, разработанная ассоциацией PCMCIA. Широко использовался в ноутбуках в основном для подключения сетевых карт, жёстких дисков, модемов [3];

– square — устройство для чтения кредитных карт через аудио разъём мобильного телефона iPhone.

Среди бесконтактных можно выделить:

– bluetooth-жетоны – обеспечивают аутентификация на расстоянии примерно 10 метров. Часто данный тип жетонов совмещён с USB-жетоном. Это сделано для тех случаев, когда устройство, требующее ау-

тентификацию, не поддерживает Bluetooth;

– NFC-жетоны – работают по стандарту NFC, обычно совмещены с Bluetoothдля обеспечения наилучшей связи.

Среди недостатков жетонов можно выделить следующее:

– возможность кражи или потеря жетона;

– перехват жетонов при использовании схемы «человек посередине» с дальнейшей попыткой расшифровки;

– брешь системы кодов. В 2012 году был опубликован эффективный способ получение секретного ключа (пин-кода) из жетона.

Третий тип – биометрические факторы [4]. Среди биометрических методов аутентификации можно выделить статические и динамические методы.

К статическим методом биометрической аутентификации относятся:

– аутентификация по отпечаткам пальцев – самая распространённая биометрическая технология. Метод использует уникальность рисунка папиллярных узоров на пальцах людей;

– аутентификация по радужной оболочке глаза – работает на основе уникальности признаков и особенностей радужной оболочки глаза человека;

– аутентификация по сетчатке глаза – работает на основе уникальности рисунка кровеносных сосудов глазного дна;

– аутентификация по геометрии руки – работает на основе формы кисти руки. Сканируются такие параметры, как изгибы пальцев, их толщина, ширина, длина, расстояние между суставами и так далее;

– аутентификация по геометрии лица – довольно популярный способ аутентификации, основанный на измерении расстояний между глазами, бровями, губами, носом и другими частями лица, с последующим построение трёхмерной модели. Данная модель аутентификации широко применяется с системами видеонаблюдения в развитых странах.

К динамическим методам биометрической аутентификации относятся:

– аутентификация по голосу;

– аутентификация по рукописному почерку.

К дополнительным факторам многофакторной аутентификации относят:

– факторы местоположения – данный тип аутентификации приобрёл широкую популярность с распространением технологии GPS. Особую актуальность применение фактора местоположения

имеет в офисах — когда сотрудник работает с приложением постоянно из одного и того же места;

– факторы времени – текущее время часто рассматривается как дополнительный тип аутентификации. Данный тип аутентификации часто используется в совокупности с фактором местоположения. Так, к примеру, сотрудник, который получил доступ к приложению в двенадцать часов дня в США, не может через 15 минут получить доступ в России.

Часто используются следующие сценарии многофакторной аутентификации:

– оплата банковской картой – проведение картой через терминал и последующий ввод пин-кода;

– вход на веб-сайт с последующим вводом дополнительного одноразового пароля (OTP). Одноразовый пароль – автоматически сгенерированная последовательность цифр или совокупности цифр и букв. Данный пароль, как следует из названия, генерируется для одного сеанса аутентификации и обычно действует в течение небольшого промежутка времени (тридцать секунд). Популярностью пользуются мобильные приложения-аутентификаторы, которые через QR-код сканируют изображение, в котором зашифрована секретная последовательность, сгенерированная сервером. Далее это мобильное приложение раз в тридцать секунд генерирует новый код, основанный на секретной последовательности и, вероятно, каких-то дополнительных переменных (например, текущего штампа времени).

– загрузка VPN-клиента с действительной цифровой подписью и последующий вход в VPN перед получением доступа к сети;

– проведение картой через аппарат аутентификации, сканирование отпечатка пальца и ответ на секретный вопрос;

– подключение USB-жетона к ПК, который генерирует OTP и использует его для входа на сайт или в VPN.

ЛИТЕРАТУРА

1 The TechTarget network [Electronic resource] / multifactor authentication (MFA). – Mode of access: http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA. – Date of access: 21.03.2016

2 Wikipedia, the free encyclopedia [Electronic resource] / Security token. – Mode of access: https://en.wikipedia.org/wiki/Security_token. – Date of access: 21.03.2016.

3 Википедия – свободная энциклопедия [Электронный ресурс] / PCMCIA – Режим доступа:

https://ru.wikipedia.org/wiki/PCMCIA – Дата доступа: 21.03.2016.

4 Википедия – свободная энциклопедия [Электронный ресурс] / Биометрические системы аутентификации – Режим доступа: https://ru.wikipedia.org/wiki/Биометрические_системы_аутентификации – Дата доступа: 22.03.2016.

УДК 003.26+347.78

Магистрант Г.А. Язкулыев
Науч. рук. проф. д-р техн. наук П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ СИТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Информация стала одним из главных факторов исторического прогресса. Она имеет ключевое значение для успешного функционирования всех общественных и государственных институтов, адекватного поведения каждого отдельного человека. Без интенсивного обмена информацией, постоянной информационной связи с окружающим миром в принципе невозможна нормальная жизнедеятельность людей.

Диалектика развития, в том числе – в области информационных технологий (ИТ), характеризуется обострением противоречий, появлением проблем. К числу важнейших в области ИТ следует отнести проблему безопасности, которая напрямую касается обеспечения безопасности систем жизнеобеспечения людей, управления транспортом, производственными процессами, коммуникациями, вооруженными силами и других систем специального назначения (ССН). Большой класс таких систем предназначен для решения задач государственного управления, управления войсками и оружием, экологически опасными и экономически важными производствами и т.п. Они часто функционируют в условиях деструктивных воздействий, целью которых является разрушение информационных ресурсов, нарушение штатных режимов функционирования и, как следствие, срыв выполнения возложенных на такие системы функций. Это определяет необходимость организации защиты ИС СН от таких воздействий [1].

Политика безопасности при этом трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности описывает цели и задачи информационной безопасности (ИБ) на понятном пользователю языке и определяет направления работы подразделений ИБ. Политика безопасности зависит от:

- конкретных технологий обработки информации;