Защита от несанкционированного доступа к информации

Защита паролем - первый этап по обеспечению безопасности информации на вашем компьютере.

Использование пароля позволяет вам защитить информацию на компьютере от:

- несанкционированного доступа (как от человека, включившего ваш компьютер без вашего разрешения, так и от попыток залезть к вам по сети);
- от некоторых (но очень немногих!) вирусов и троянских программ (главным образом также "хулиганящих" через сеть - локальную или Интернет).

Какой пароль выбрать?

1. пароль не должен легко раскрываться, подбор пароля должен быть максимально затруднен. В основе пароля не должно лежать ваше имя, дата рождения, кличка любимой кошки и т.п.
2. в Windows лучше всего защищены от взлома пароли длиной 7 или 14 знаков; кроме того, рекомендуется использовать в пароле сочетание букв, цифр и специальных символов (таких как подчерк, решетка, доллар, собака и т.п.), причем желательно, чтобы хотя бы один из этих символов присутствовал среди знаков пароля со второго по шестой.
3. рекомендуется использовать в паролях и строчные, и прописные буквы, причем примерно поровну и вперемешку.

Правила создания паролей:

1. Пароль не должен быть значимым словом или сочетанием слов какого-либо языка.
2. Не записывайте свой пароль в файле или на бумажке.
3. Не используйте один пароль для нескольких целей.
4. При наборе пароля, хотя он, как правило, на экране не отображается, следует всё же избегать чужих глаз.

Защита электронной почты

Подавляющее большинство электронной почты посылается через Internet или другие глобальные сети в виде простого текста, который можно прочесть. Закон о конфиденциальности электронных коммуникаций приравнивает вашу электронную почту к обычному телефонному звонку. Системные администраторы имеют все необходимые средства для чтения электронной почты на своей системе. Иногда им даже необходимо просматривать электронную почту, чтобы удостовериться, что система работает нормально.

Хакеры и любопытные отличаются тем, что владеют различными способами получения доступа к вашей почте, но обе эти категории не могут читать вашу почту, если она зашифрована. Если вам необходимо защитить секретную информацию используйте PGP (Pretty Good Privacy) для шифрования почты перед отправлением.

Шифрованные архивы

Программы-архиваторы, как правило, имеют опцию шифровки. Ею можно пользоваться для не слишком важной информации. Во-первых, используемые там методы шифровки не слишком надёжны (подчиняются официальным экспортным ограничениям), во-вторых, детально не описаны. Всё это не позволяет всерьёз рассчитывать на такую защиту. Архивы с паролем можно использовать только "для чайников".

На некоторых сайтах в Интернете вы можете найти "ломалки" для зашифрованных архивов. Например, архив ZIP взламывается на хорошем компьютере за несколько минут, при этом от пользователя не требуется никакой особой квалификации.

Шифровка в Word и Excel

Фирма Майкрософт включила в свои продукты некоторое подобие криптозащиты. Но это весьма законопослушная фирма, которая чётко соблюдает все экспортные ограничения США, да ещё и перестраховывается. Это не позволяет надеяться на стойкость такой защиты. К тому же, алгоритм шифровки не описан, что, как было показано выше, является показателем ненадёжности.

Кроме того, имеются данные, что Майкрософт оставляет в используемых криптоалгоритмах «чёрный ход». Если вам очень нужно расшифровать файл, пароль к которому утрачен (или враг не хочет говорить), можно обратиться в фирму. По официальному запросу, при достаточных основаниях они проводят расшифровку файлов Word и Excel.

Шифрованные диски (каталоги)

Шифровка – достаточно надёжный метод защиты информации на вашем жёстком диске. Однако если количество закрываемой информации не исчерпывается двумя-тремя файлами, то вам будет несколько сложно с ней работать: каждый раз нужно будет файлы расшифровывать, а после редактирования – зашифровывать обратно. При этом на диске могут остаться страховочные копии файлов, которые создают многие редакторы.

Поэтому удобно использовать специальные программы (драйверы), которые автоматически зашифровывают и расшифровывают всю информацию при записи её на диск и чтении с диска.

Защита информации, хранящейся на iPhone, всегда очень актуальна. Вряд ли найдётся хоть один пользователь, который захотел бы, чтобы его личная переписка и прочие данные попали к посторонним людям. Несмотря на то, что единственным действенным способом защиты информации для большинства людей остаётся использование паролей, компания Precise Biometrics пошла дальше.

Устройство под названием Tactivo предназначено для защиты действительно важной информации, которой могут располагать государственные служащие и прочие лица «с доступом», и представляет собой некое подобие бампера с двумя способами аутентификации: с помощью отпечатка пальца и смарт-карты. Если второй способ более актуален для Соединённых Штатов, где подобные карты распространены во многих организациях, то аутентификация с помощью отпечатка пальца подойдёт всем.

Работает эта система так: на iPhone устанавливается приложение BioSecrets. К смартфону подключается Tactivo, которое включает в себя устройство считывания данных со смарт-карты на тыльной стороне, а также устройство для сканирования отпечатка пальца, расположенное в нижней части. Tactivo совместимо с iPhone 4 и 4S, а в скором будущем разработчики обещают создать аналогичное устройство для iPad. Сообщается о поддержке и будущих моделей смартфонов и планшетов Apple. Для разработчиков доступны инструменты, позволяющие интегрировать Tactivo со своими приложениями. Стоит это устройство $249, а приложение для его работы можно загрузить в App Store бесплатно.

Биометрическая защита информации

- Биометрические системы безопасности - системы контроля доступа, основанные на идентификации человека по биологическим признакам, таким как структура ДНК, рисунок радужной оболочки глаза, сетчатка глаза, геометрия и температурная карта лица, отпечаток пальца, геометрия ладони. Часто используются еще и уникальные динамические особенности человека - подпись и клавиатурный почерк, голос, походка

- Свойство изменяемости на протяжении длительного времени присуще и многим поведенческим характеристикам, таким, к примеру, как голос, походка, подпись, динамика печати на клавиатуре. Не каждая из перечисленных биометрических характеристик универсальна, то есть может быть измерена у любого человека. Например, по статистике около 5-7% населения нашей планеты не имеют (из-за возраста, расовой принадлежности, рода занятий и пр.) машинно-считываемых отпечатков пальцев.

- Одна из самых важных характеристик систем защиты информации, основанных на '"биометрических технологиях"', является высокая надежность, то есть способность системы достоверно различать биометрические характеристики, принадлежащие разным людям, и надежно "узнавать своих". В биометрии эти параметры называются ошибкой первого рода (FRR), когда система не узнала "своего", и ошибкой второго рода (FAR), когда система пропустила чужого, то есть приняла "чужого" за "своего". Подделать папиллярный узор пальца человека или радужную оболочку глаза практически невозможно. Так что возникновение «ошибок второго рода» (то есть предоставление доступа человеку, не имеющему на это право) практически исключено. Правда, здесь есть одно «но». Дело в том, что под воздействием некоторых факторов биологические особенности, по которым производится идентификация личности, могут изменяться. Ну, например, человек может простудиться, в результате чего его голос поменяется до неузнаваемости. Поэтому частота появлений «ошибок первого рода» (отказ в доступе человеку, имеющему на это право) в '"биометрических системах"' достаточно велика.

Любая биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;
- сравнение текущего шаблона с базой данных.

Обобщенно все методы защиты от муляжей отпечатка пальца можно разделить на две группы:

- 1. **Технические –** методы защиты, реализованные либо на уровне программного обеспечения, работающего с изображением, либо на уровне считывающего устройства. Рассмотрим их подробнее:

- ***защита на уровне считывающего устройства***: заключается в том, что в самом сканере реализован алгоритм получения изображения, который позволяет получить отпечаток пальца только с живого пальца, а не с муляжа, например, так работают оптоволоконные сканеры;

- ***защита по дополнительной характеристике***: суть данного метода заключается в получении с помощью сканирующего устройства некоторой дополнительной характеристики, по которой можно принять решение является ли предоставленный идентификатор муляжом. Например, с помощью ультразвуковых сканеров можно получать информацию о наличии пульса в пальце, в некоторых оптических сканерах с высоким разрешением можно определить наличие на изображении частиц пота и т.д.;

- ***защита по предыдущим данным***: на некоторых сканерах – отпечаток последнего прикасавшегося к нему пальца остается на его поверхности, чем можно воспользоваться при изготовлении муляжа. На этот случай защищаются с помощью хранения нескольких последних изображений со сканера (для каждого производителя это число разное) с которыми в первую очередь сравнивается любое новое изображение. А так как дважды приложить абсолютно одинаково палец к сканеру нельзя, при любом совпадении принимается решение о применения муляжа.

2. **Организационные** – суть эти методов заключается в организации процессов аутентификации, таким образом, чтобы затруднить или исключить возможность использования муляжа. Вот эти методы:

- ***Усложнение процесса идентификации***. Метод заключается в том, что в процессе регистрации отпечатков пальцев в системе на каждого пользователя регистрируется несколько пальцев (в идеале все 10). После этого непосредственно в процессе аутентификации у пользователя запрашиваются для проверки несколько пальцев в произвольной последовательности, что значительно затрудняет вход в систему по муляжу;

- ***Мультибиометрия или многофакторная биометрия***: для аутентификации используется несколько биометрических технологий, например отпечаток пальца и форма лица или сетчатка глаза и т.д.

- ***Многофакторная аутентификация***: суть метода проста – использовать для усиления защиты совокупность методов аутентификации, например биометрию и смарт-карты.

Биометрическая идентификация по рисунку лица

- Системы распознавания по форме лица являются встроенными компьютерными программами, которые анализируют изображения лиц людей в целях их идентификации. Программа берет изображение лица и измеряет такие его характеристики, как расстояние между глазами, длина носа, угол челюсти, на основе чего создается уникальный файл, который называется "шаблон". Используя шаблоны, программа сравнивает данное изображение с другими изображениями, а затем оценивает, насколько изображения являются похожими друг на друга. Обычными источниками изображений для использования при идентификации по лицу являются сигналы от телекамер и ранее полученные фотографии, наподобие тех, что хранятся в базе данных водительских удостоверений. Но согласно исследованиям от снимков с зернистым изображением или старых фотографий, типа тех, которые хранятся в личных делах, будет очень мало пользы.

- На практике, при использовании систем распознавания лиц в составе стандартных электронных охранных систем, предполагается, что человек, которого следует идентифицировать, смотрит прямо в камеру. Таким образом, система работает с относительно простым двумерным изображением, что заметно упрощает алгоритмы и снижает интенсивность вычислений. Но даже в этом случае задача распознавания все же не тривиальна, поскольку алгоритмы должны учитывать возможность изменения уровня освещения, изменение выражения лица, наличие или отсутствие макияжа или очков. Объем баз данных при использовании стандартных персональных компьютеров не превышает 10000 изображений.

Распознавание голоса

- Распознавание голоса — это технология, которая позволяет использовать голос в качестве идентификационного устройства. Распознавание голоса может использоваться для диктовки текста компьютеру или для отдачи команд (таких как открытие определенных программ, сворачивание меню, сохранение данных).

  Применения технологии распознавания голоса, используемые на протяжении долгого времени, предполагали произнесение каждого слова отдельно. Это позволяло машине определить, где кончается одно слово и где начинается другое. Такие применения технологии распознавания голоса все еще встречаются для управления компьютерными системами.

  Современные применения данной технологии позволяют пользователю быстро и слитно произносить текст. Новые системы могут распознать 160 слов в минуту, позволяя преобразовывать непрерывную речь в узнаваемый текст и форматировать его.

  Идентификация по голосу происходит по следующей схеме: система сравнивает образец голоса, представленного в цифровой форме, с так называемым «голосовым отпечатком», хранящимся в базе данных. Голос является уникальной биометрической характеристикой человека и может использоваться для подтверждения его личности

- Распознавание речи связано с тем, что было сказано, что и является главным отличием от верификации, связанной с тем, кто именно говорит. Системы голосовой идентификации не зависят от какого-либо языка или словаря. Человек может сказать что угодно и на каком угодно языке, что делает эти системы идеальными для международного использования.

  Весь процесс занесения данных занимает несколько минут. Система предлагает ответить на несколько простых вопросов, например, ваше имя, отчество, фамилия или дата рождения. Ответы становятся идентификационными фразами, которые позднее будут использоваться для идентификации человека. Неважно, что скажет человек, главное, как он это скажет; вопросы могут быть самыми разными, главное, чтобы ответ был хорошо знаком человеку, и он бы смог воспроизвести его в любую минуту. Для каждого вопроса пользователь произносит четыре раза свой ответ. Ответ должен состоять как минимум из трех слогов и длиться больше секунды для того, чтобы создать «голосовой отпечаток». Записанные ответы накладывают друг на друга, убирают посторонний шум и через несколько секунд «голосовой отпечаток» готов. Затем система таким же образом поступает с другими вопросами и ответами (системы безопасности предлагают делать несколько таких «голосовых отпечатков»). Через несколько минут создаются «голосовые отпечатки», которые будут применяться каждый раз, когда человек будет проходить через службу безопасности.

Идентификация по радужке глаза

- В последнее время все большую и большую популярность приобретает использование в качестве рабочего признака радужной оболочки глаза. И, если задуматься, в этом нет абсолютно ничего удивительного. Дело в том, что радужная оболочка — элемент достаточно уникальный. Во-первых, она имеет очень сложный рисунок, в ней много различных элементов. Поэтому даже не очень качественный ее снимок позволяет точно определить личность человека. Во-вторых, радужная оболочка является объектом довольно простой формы (почти плоский круг). Так что во время идентификации очень просто учесть все возможные искажения изображения, возникающие из-за различных условий съемки. Ну и, наконец, в-третьих, радужная оболочка глаза человека не меняется в течение всей его жизни с самого рождения. Точнее, неизменной остается ее форма (исключение составляют травмы и некоторые серьезные заболевания глаз), цвет же со временем может измениться. Это придает идентификации по радужной оболочке глаза дополнительный плюс по сравнению со многими биометрическими технологиями, использующими относительно недолговечные параметры, например геометрию лица или руки.

- Кстати, у идентификации личности по радужной оболочке глаза есть еще одно серьезное преимущество. Идентификация по радужной оболочке глаза полностью избавлена от ошибок первого и второго рода. В ней соотношение ошибок первого и второго родов является одним из лучших на сегодняшний день. Для примера можно привести несколько цифр. Исследования показали, что при вероятности возникновения ошибки первого рода в 0,001% (отличный уровень надежности) вероятность появления ошибок второго рода составляет всего лишь 1%.

  Но все же рассматриваемой технологии есть и недостатки. Первым из них является относительно высокая стоимость оборудования. Действительно, для проведения исследования нужна как минимум камера, которая будет получать начальное изображение. А стоит это устройство гораздо дороже, чем, например, сенсор отпечатков пальцев. Кроме того, она требует довольно много места для размещения. Все это ограничивает область использования идентификации личности по радужной оболочке глаза. На сегодняшний день она применяется в основном в системах допуска на различные объекты как гражданского, так и военного назначения.

СПАСИБО ЗА ВНИМАНИЕ!