**Что общего между шифрованием и линией Мажино?**

Алексей Лукацкий

В 1929–1934 гг., опасаясь военного вторжения со стороны Германии, французский военный министр Андре Мажино предложил построить систему неприступных укреплений по всей северо-восточной границе Франции – от Швейцарии до Бельгии. Эта система оборонительных укреплений длиной 380 километров, состоявшая из 5600 долговременных огневых сооружений, врытых на глубину до 30 метров, получила название “линия Мажино”. Охранял этот считавшийся неприступным рубеж двухсоттысячный гарнизон солдат. Однако в 1940 г., после того как генерал-фельдмаршал немецкой армии фон Бок обошел эти укрепления через Бельгию и взял Париж, линия Мажино пала.

К сожалению, сходная ситуация складывается сейчас и с шифрованием, которое преподносится как панацея от многих бед – от неусыпного ока государства, конкурентов, хакеров – всех любителей заглядывать в замочную скважину. Если данные спрятаны от посторонних глаз и, согласно математическим расчетам, на вскрытие шифра требуются сотни лет, то многие не без основания полагают, что этого вполне достаточно для безопасности данных. Но известно, “нормальные герои всегда идут в обход”.

На городских улицах нередко можно видеть банковские бронированные автомобили, перевозящие деньги в центральное хранилище. Закованные в броню машины, в недрах которых могут находиться баснословные ценности, – это точная аналогия шифрования информации. Но может быть, они перевозят обеды для сотрудников удаленного офиса? Однако не будем обсуждать вопрос соизмеримости стоимости защитных мер со стоимостью защищаемой информации и вспомним какой-нибудь гангстерский боевик, в котором грабители нападают на грузовики, перевозившие ценности. Как они это делают? Случаи грубого взрыва автомобиля или его угона с последующим безрезультатным и долгим вскрытием бронированной двери автогеном встречаются редко, и то происходят они только по причине неопытности преступников (или сценаристов). Более продвинутые грабители идут другим путем. Они либо заставляют самих инкассаторов открыть двери фургона, либо совершают свои опустошительные набеги в момент загрузки или выгрузки мешков с деньгами. В других фильмах бездарные злоумышленники безуспешно ищут нужную комбинацию тупым перебором, тогда как те, что посообразительнее, подсматривают верный код с помощью подзорной трубы. Эти сюжеты и подсказывают нам слабые места шифрования.

Вам приходилось слышать о взломе каких-либо шифров по причине слабой математики? И не просто о такой гипотетической возможности, а о реальном случае в каком-нибудь банке или военном ведомстве? Я – нет (если не брать в расчет слухи о том, что Кучма взломал шифры посольств стран НАТО, о чем сообщила “Новая газета” 30 сентября 2002 г.). Единственное, о чем мне доводилось слышать, – это о различных попытках полного перебора возможных ключей шифрования для распространенных алгоритмов шифрования (например, DES и RC5). Наиболее известный проект – distributed.net, направленный на привлечение свободных сетевых компьютеров для участия в распределенных вычислениях ключа шифрования. Даже для алгоритмов с длиной ключа в 64 бит время перебора составляет не менее трех лет, а современные алгоритмы используют ключи длиной 128 бит и более. Забегая вперед, скажу, что почти все известные случаи взлома шифров были осуществлены другими способами. Например, чтение засекреченных данных немецких военных во время второй мировой войны стало возможным потому, что к союзникам попала шифровальная машина “Энигма”. В других случаях ключи шифрования попадали в руки военных благодаря агентурным данным или иными путями (и, как правило, без применения математических методов).

Однако это только так кажется, что шифр ломается исключительно специалистами-математиками с помощью сложных алгоритмических преобразований. На практике все гораздо прозаичнее, и ореол таинственности, которым себя окружают различные спецслужбы, сквозит прорехами – через них-то мы и заглянем в эти “тайны”. Можете ли вы запомнить ключ “cю}БТфР9” (0x63DE7DC154F4D039)? А ведь именно такой использовался в проекте distributed.net по взлому 64-битного алгоритма RC5. А вы сами применяете нечто подобное? Скорее всего, для ключа шифрования вы воспользуетесь гораздо лучше запоминаемым словом. Понимая это, злоумышленники концентрируются на иных, чем обычный метод “грубой силы”, способах проникновения за завесу тайны. Во-первых, они учитывают человеческий фактор. Зная, как пользователи выбирают пароли, злоумышленник может существенно сэкономить время. Человек – существо по природе ленивое, он не хочет утруждать себя процедурой выработки правильного ключа шифрования и тем более заниматься тестированием качества созданного им пароля. Мало того, пользователь даже если кто-то предложил ему надежный ключ, вряд ли будет запоминать комбинацию цифр и букв в верхнем и нижнем регистрах. В большинстве случаев он выберет для такого ключа свое имя, имя жены или любимой рыбки, название собственной компании, номер телефона или автомобиля и т. п. Или же возьмет какое-то слово, но и здесь его подстерегает ловушка. Несмотря на то, что комбинаций букв русского языка очень много, 17-томный “Словарь современного русского литературного языка” включает всего 120 480 слов (кстати, четырехтомный “Словарь живого великорусского языка” В. И. Даля содержит около 200 000 слов). Но много вы встречали моделей, которые оперируют всем этим многообразием? В “Словаре языка А. С. Пушкина” 21 290 слов, а современный взрослый образованный человек, как правило, обходится, по данным ученых, 10–12 тысячами слов. Осуществить их полный перебор не составляет большого труда даже для персонального компьютера средней мощности. А зная область интересов пользователя, ключ или пароль которого необходимо выяснить, число вариантов можно значительно сократить. Известна анекдотичная статистика – при запросе “Введите пароль:” около трети американских военных вводили слово…“пароль”. Количество возможных вариантов еще больше сокращается, если знать, что основная масса паролей вводится только в нижнем регистре без применения цифр, знаков препинания и иных символов. Ну и, наконец, в Интернете можно найти уже готовые списки самых распространенных паролей. Таким образом, спецслужбам нет нужды заниматься сложными алгоритмическими преобразованиями для взлома того или иного шифра. Достаточно знать основы человеческой психологии в применении к информационной безопасности.

Другой способ обойти криптографические препоны – проникнуть в шифровальное устройство, иными словами, внедрить в компьютер “троянца”, способного открыть доступ ко всей важной информации, включая пароли и ключи шифрования. Так, например, поступили в 1999 г. агенты ФБР, собирающие доказательства преступной деятельности мафиози Никодемо Скарфо, делающего деньги на нелегальном игровом бизнесе в Нью-Джерси. Этот субъект шифровал все компрометирующие файлы (по некоторым данным, с помощью известной программы PGP). Однако агенты ФБР оказались тоже не лыком шиты и внедрили на компьютер Скарфо клавиатурного шпиона, который регистрировал все нажатия клавиш, в том числе и в момент ввода пароля доступа к засекреченным данным. После этого ФБР смогло собрать необходимые улики, и в феврале 2002 г. Скарфо был осужден американским судом. Именно поэтому в инструкциях ко многим средствам криптографической защиты написано, что пользователь обязан обеспечить защиту своего компьютера и ключей. Но кто из считающих себя продвинутым пользователем читает документацию?

Эти два примера лишний раз показывают, что шифрование само по себе не решает проблем. Без дополнительных мер защиты (технических и организационных) применение шифрования лишь вводит вас в заблуждение. А нет ничего хуже чувства ложной безопасности. Вы будете думать, что ваши данные надежно скрыты от любопытных глаз, а на самом деле к ним смогут получить доступ все желающие.

В заключение хочу привести слова известного специалиста по информационной безопасности Юджина Спаффорда, сказанные им о шифровании: “Это похоже на перевозку в бронированном автомобиле кредитной карты от человека, живущего в картонной коробке, человеку, живущему на скамейке в парке”.