

Банк-клиент против хакеров: чья возьмет?

Текст: Алексей Синцов, ведущий аудитор по информационной безопасности компании «Digital Security»

Наверное, все банки, внедрившие системы дистанционного банковского обслуживания (ДБО), встречались с попытками перевода денег со счетов клиента без его ведома, то есть, фактически, воровства с применением информационных технологий.

Требуется защита и банкам, и их клиентам

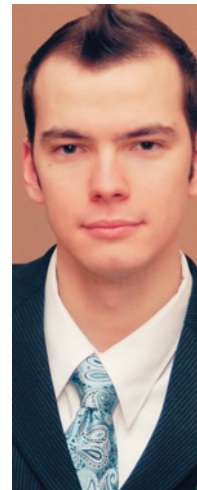
Самый популярный вектор атаки – на компьютер клиента банка с последующим хищением или использованием ключа его электронно-цифровой подписи (ЭЦП) и перехватом логина и пароля учетной записи в системе «интернет-банк». Причины популярности такого метода понятны: клиентов много, и многие из них могут быть защищены гораздо хуже банка, откуда следует, что определённый процент клиентов точно будет подвержен взлому. Ситуацию усугубляет использование однотипного программного обеспечения для доступа к ДБО.

Большинство банков не хотят тратить силы и средства на разработку собствен-

ной системы банк-клиент и покупают готовое ПО. Такой подход на руку хакерам, поскольку резко сокращает их трудозатраты – у большинства банков и их клиентов практически одинаковое программное обеспечение, поэтому применяется также универсальное вредоносное ПО для осуществления мошеннических операций.

Впрочем, не только клиентам требуется защита. Серверы банка тоже могут стать объектом хакерских атак не только инсайдеров, но и из внешнего мира, и могут быть использованы для атак на его клиентов. Таким образом, безопасность дистанционного банковского обслуживания – вопрос не только безопасности клиента и его электронно-цифровой подписи. В любом случае, бороться за безопасность

Алексей Синцов,
ведущий аудитор
по информацион-
ной безопасности
компании «Digital
Security»



нужно по двум фронтам: за клиента и за банк.

Как защитить клиента

Фактически банк не может влиять на безопасность клиента. Максимум, что обычно может сделать банк – это навязать клиенту USB-Token и выполнить привязку его IP-адреса. Кроме того, придумываются различные алгоритмы двухфакторной авторизации, вроде использования карточки одноразовых паролей или SMS-уведомлений.

Но, как показывает практика, хакеры также не стоят на месте. Уже известны случаи использования устройства USB-Token прямо с зараженной машины. Привязка IP-адреса также ничего не даёт: злоумышленник может действовать с зараженной машины из сети компании, чей IP-адрес разрешен для использования в системе.

Одноразовые пароли так же могут быть перехвачены. Например, если они передаются по сети GSM, можно заблокировать или клонировать SIM-карту (причем, прямо в офисе сотового оператора, используя, например, поддельную доверенность). Кроме того, существует воз-

Вопрос защиты информационных систем является сложным в силу отсутствия типизации этих систем

Павел Коростелёв, менеджер

по направлению ИБ компании «ТопС Бизнес Интегратор»

Закон о персональных данных предусматривает деление всех информационных систем, обрабатывающих персональные данные (ИСПДн) на 4 класса, в зависимости от типа ИСПДн, типа персональных данных, объема ИСПДн, наличия определенных технических и эксплуатационных характеристик.

Если собрать все эти факторы и пытаться защитить сразу всю информационную систему предприятия, то система защиты персональных данных получится очень дорогой. Поэтому на практике принято сегментировать информационные системы, обрабатывающие персональные данные, за пределы которых выходят только обезличенные данные, не требующие повышенной защиты рабочего места оператора.

Например, для CRM-системы компании федерального уровня со сложной территориально-распределенной системой нет необходимости держать в одном месте все персональные данные, а простое распределение данных по регионам значительно удешевит систему защиты. Имеет смысл разделить пользователей CRM на тех, кто может работать вне защищенного периметра ИСПДн (работая только с обезличенными или общедоступными данными), и тех, кому необходим полный доступ ко всем данным – к их рабочим местам будут предъявлены требования по защите информационных систем.

В целом же вопрос является очень сложным в силу отсутствия формализованных требований и, как следствие, типизации таких систем. Деление информационных систем, обрабатывающих персональные данные на классы условно, так как модель угроз (набор и степень угроз), у различных систем даже на одном предприятии может быть разной.

возможность перехвата данных GSM-сети, например, в моменты, когда шифрование отключено.

В общем, варианты имеются. Наилучшая стратегия защиты – предотвратить вторжение на машину клиента, принудив его проводить грамотную политику поддержания информационной безопасности. Если рабочая станция с «банк-клиентом» будет отделена межсетевым экраном от локальной сети, если доступ с этой рабочей станции возможен только на IP-адрес банка, если удалить с этого компьютера все ненужное ПО и не держать USB-Token постоянно включенным в компьютер, то это снизит риски практически до минимума.

Уязвимости на банковской стороне

Обеспечение безопасности банковских серверов системы банк-клиент, казалось бы, задача несложная: необходимо лишь правильное использование межсетевого экрана, настройка ДМЗ, парольной политики, регулярные обновления ОС и сервисов. Но, увы, этого недостаточно. Как показала наша многолетняя практика анализа защищённости ДБО, программное обеспечение, используемое банками, содержит уязвимости, приводящие как к возможности атаки на клиентов, так и к компрометации базы данных системы «Банк-клиент». Причём уязвимости характерны для всех систем ДБО.

При атаках из сети Интернет известны две типовые модели поведения нарушителя. «Классический хакер» сканирует сервисы, ищет устаревшую версию используемого ПО, слабости и уязвимости в системе аутентификации, и, конечно же, уязвимости в доступных web-приложениях – самом слабом, по статистике, звене системы дистанционного банковского обслуживания. Но от такого нарушителя достаточно легко защититься, да и обнаружить его деятельность также не является проблемой. Гораздо опаснее вторая модель, когда нарушитель является законным пользователем системы, когда у него есть своя учетная запись, свой счёт и все права на него. Вот только в отличие от обычного пользователя он пытается

исследовать систему в надежде найти уязвимости.

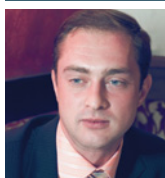
Cross-Site Scripting

По статистике, самый популярный класс уязвимостей, – это «Cross-Site Scripting» (XSS). Такая уязвимость позволяет атакующему влиять на генерируемое содержимое web-страницы системы интернет-банк. Таким образом, злоумышленник может использовать ресурс банка для атаки на клиента, например, изменив страницу так, как если бы она выглядела при аутентификации в системе. То есть, пользователь увидел бы, что домен принадлежит банку, что это страница его родного интернет-банка, только он не аутентифицирован. Если клиент введёт данные своей учетной записи, то они будут

отправлены злоумышленнику, так как код страницы им подделан.

Такая атака называется «Фишинг» (Phishing) и обычно используется для хищения данных учетной записи путем покупки злоумышленником похожего домена и вывешивания на главную страницу копии дизайна страницы аутентификации системы «Банк-клиент». Однако в сочетании с уязвимостью XSS эта атака становится более опасной, так как домен и IP-адрес действительно принадлежат банку. Кроме того, XSS уязвимости могут использоваться для атаки на ПО клиента с целью использовать уязвимость в браузере или ActiveX-надстройке для браузера, вследствие чего у клиента будет установлено вредоносное ПО.

Как правило, для использования XSS



Мы пока не готовы полноценно войти в мировое информационное сообщество

Юрий Черкас, руководитель отдела технической защиты информации компании ReignVox

К сожалению, вопрос защиты информации является одним из самых актуальных на сегодняшний день и не только для систем ДБО. На мой взгляд, основная проблема состоит в том, что наше общество, в большинстве своём, ещё не готово полноценно войти в мировое информационное сообщество.

Причина заключается в том, что рядовой пользователь систем ДБО, как правило, далек от проблем информационной безопасности. Он задумывается об элементарных правилах защиты информации только тогда, когда инцидент уже произошел – таков, к сожалению, наш менталитет – кстати, в отличие от банков, деятельность которых контролируется государством.

Банки хорошо справляются с обеспечением приемлемого уровня безопасности информации, чему способствует качество подготовки кадров: не секрет, что службы безопасности многих банков сформированы из бывших сотрудников компетентных органов, которые располагают необходимыми знаниями по защите информации. В отличие от них, далеко не каждый человек, умеющий работать на персональном компьютере, хоть сколько-нибудь задумывается о том, как защищен его компьютер от вредоносных программ. Поэтому банку гарантировать защиту информации на клиентских компьютерах практически невозможно, даже если клиент и использует предоставленное им специализированное программное обеспечение. Пользователям ДБО часто не хватает элементарной бдительности. К примеру, они просто не обращают внимание на тот факт, что после ввода правильных данных аутентификации эти же данные могут запрашиваться повторно, хотя, казалось бы здравый смысл подсказывает, что здесь что-то не так.

Способы и методы атак компьютерных злоумышленников будут развиваться, как и способы обычного воровства. Если вставить во входную дверь «хитрый» замок, то рано или поздно его все равно откроют. Поэтому, в первую очередь, банкам необходимо развивать и поддерживать у своих клиентов навыки выполнения элементарных норм безопасности – не оставлять токены, не вводить дважды правильные пароли, быть просто внимательными.

В результате нарушений безопасности информации банки теряют прибыль, а население – деньги. Но это вовсе не означает, что нужно отказываться от удобных нам новых видов сервисов и услуг. Просто следует осознать, что нужно детально разобраться, как ими пользоваться, подобно тому как не стоит садиться за руль, не сдав на права.

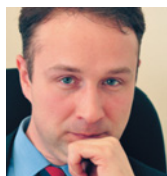
уязвимости необходима помощь человека (человеческий фактор), так как злоумышленник должен спровоцировать переход жертвы на специально сформированную гипер-ссылку в домене системы ДБО. Выглядеть URL такой ссылки может так: «bank-client.moibank.ru/login.asp?color=SESSION_CODE%3a%3b%3c». Атака скрыта в последовательности сим-

волов параметра color. Отметим, что у жертвы может не возникнуть подозрения, так как домен принадлежит его банку.

SQL-инъекция

Другой популярной уязвимостью является возможность SQL-инъекции. Эта уязвимость гораздо опаснее XSS, но встречается практически также часто.

Она позволяет злоумышленнику общаться с базой данных системы интернет-клиент в обход правил системы, что, в итоге, может привести к утечке (или в некоторых случаях – к изменению) базы клиентов, их счетов, номеров пластиковых карт, платежных поручений, паролей от системы, и т.п. к злоумышленнику. Все это возможно, потому что часто обеспечение безопасности и разделения доступа лежит на web-приложении, имеющем единственную учетную запись в базе данных. Когда злоумышленник эксплуатирует SQL-инъекцию, то он обходит все уровни защиты web-приложения и работает с базой данных под учётной записью web-приложения, вследствие чего у него появляется доступ ко всем таблицам системы. Кроме того, критичная информация в базе данных не всегда шифруется.



Превентивные механизмы противодействия угрозам информационной безопасности в системах ДБО

*Кривилёв Михаил, заместитель коммерческого директора
ООО «Банк Софт Систем»*

При использовании современных систем ДБО банкам необходимо принимать во внимание целый арсенал потенциальных угроз и выработать адекватные превентивные или детектирующие меры противодействия им. На сегодняшний день потенциальные атаки на системы ДБО сводятся к нескольким типам. Это атаки на клиентскую часть ДБО, использующие невозможность создания доверенной среды на компьютере конечного пользователя — клиента банка, атаки на банковскую часть системы ДБО извне и атаки на банковскую часть системы ДБО изнутри с использованием инсайдеров внутри банка. Каковы популярные на сегодня меры противодействия данным атакам?

Наиболее популярны атаки на клиентскую часть ДБО. Причиной является невозможность средствами самой системы ДБО обеспечить достаточный уровень защиты клиентского рабочего места, которое для банка по определению не является «доверенной средой». Злоумышленник, используя технические средства, методы социальной инженерии или элементарное несоблюдение пользователем системы правил эксплуатации получает как клиентскую идентификационную информацию, так и доступ к носителям ключевой информации. После этого отправка финансовых распоряжений от лица клиента является делом техники.

Единственной действенной мерой является использование комбинации превентивных и детектирующих мер: одноразовых сеансовых ключей (на скрэтч-картах или с применением аппаратных генераторов сеансовых ключей для VIP-клиентов) для дополнительной авторизации финансовых транзакций и аппаратных токенов для обеспечения более надежного хранения ключевой информации. Детектирующие меры — информирование клиента о поступившем от его лица финансовом распоряжении посредством sms (предпочтительно) или e-mail сообщений.

Безусловно, не следует забывать и про традиционные организационные мероприятия, а также использование на стороне клиента средств антивирусной защиты, но, к сожалению, выполнение клиентом рекомендаций банка находится вне зоны банковского контроля.

Потенциально интересным, но не используемым пока в России, направлением развития средств защиты от атак на клиентскую часть ДБО является использование специализированных рабочих мест системы ДБО на защищенных аппаратных платформах. Только набирают популярность специализированные программные продукты защиты от финансового мошенничества (Fraud Detection System), обладающие как сигнатурными, так и статистическими механизмами обнаружения подозрительных транзакций.

Для обеспечения адекватного уровня защиты финансовых транзакций, проходящих через системы ДБО, необходимо рассматривать системы ДБО в комплексе с прочими ИТ-системами банка, разрабатывать целостную модель угроз и регулярно подвергать ее ревизии. Базируясь на разработанной модели угроз, банку необходимо определить адекватный перечень организационных и технологических мер для предотвращения (противодействия) угрозам, поддерживать в актуальном состоянии и регулярно доводить до сведения всех заинтересованных лиц (включая клиентов-пользователей системы ДБО) относящиеся к их деятельности нормативные документы (политика безопасности, регламенты, инструкции и т.п.), проводить тренинги персонала банка и контролировать знание и следование нормативным документам, проводить просветительскую работу с клиентами банка, требовать от них исполнения нормативных документов при работе с системами ДБО.

Ошибки бизнес логики

Третий класс ошибок – ошибки бизнес-логики системы, которые приводят к нарушению её функционирования, а иногда и к прямым денежным потерям. Описание таких ошибок не формализовано, и их поиск нельзя автоматизировать. Примером такой ошибки может быть ситуация, когда при конвертации валюты скрипт генерирует курс и просит пользователя ввести сумму, которую он хочет обменять. Далее пользователь вводит сумму, и на сервер отправляются данные – курс, сумма и требуемая валюта. Если при этом не происходит дополнительной проверки курса, то злоумышленник может поменять курс по своему усмотрению, из-за чего конвертация может пройти с неправильным курсом.

Кроме того, многие системы ДБО предполагают использование на клиентской части надстроек ActiveX для проставления электронно-цифровой подписи на платежные поручения. Это программное обеспечение также подвержено ошибкам.

Мы провели исследование трех ActiveX компонентов от различных систем интернет-банкинга и убедились в наличии там таких ошибок. Три из трех содержали уязвимость переполнения буфера, что могло привести к прямому выполнению кода и, как следствие, к за-

ражению клиентского компьютера. Две из трех надстроек позволяли через манипуляцию доступными методами писать и читать произвольные файлы на машине клиента. Таким образом, можно было бы считать ключи ЭЦП (если клиентом не использовался USB-Token) или установить в автозагрузку вредоносное ПО. К счастью, некоторые производители оперативно реагируют на найденные нами уязвимости и добросовестно их исправляют. Однако это ПО всегда модифицируется и обновляется, и поэтому со временем такие ошибки могут всплыть вновь.


Точка кипения

В целом по результатам наших работ по анализу защищенности систем ДБО в 2009 году нами было обнаружено две уязвимости типа «SQL-инъекции», шесть уязвимостей типа «XSS», три уязвимости переполнения буфера в «ActiveX», два небезопасных метода в «ActiveX». И это только в трех «коробочных» системах ДБО, не привязанных к конкретному банку. Проблема усугубляется тем, что злоумышленники также могут

проводить подобные исследования, ведь большинство систем ДБО доступно в режиме демо-версии, а ActiveX-элементы можно установить с сайта любого банка. Кроме того, для некоторых банков компании-разработчики пишут специализированные, спроектированные под их нужды версии ПО. В таком коде также могут быть ошибки, которых нет в стандартной версии. Поэтому такие версии необходимо анализировать отдельно.

Таким образом, для обеспечения безопасности ДБО на стороне клиента необходимо применить серьезные организационные меры. Для обеспечения безопасности серверной части системы необходимо применять четкие требования к ПО, которое использует банк. Например, для платежных приложений, используемых для работы с банковскими картами, существует обязательный стандарт безопасности «PA DSS». Этот стандарт разработан регулятором в лице «PCI SSC», куда входят крупнейшие международные платежные системы (VISA, MasterCard, JSB, «American Express», и т.д.). Этот стандарт требует проведения неза-

висимого анализа безопасности приложения, проводимого сертифицированными компаниями, таким образом, безопасность ПО, выпускаемого разработчиками, заметно повышается. Особенно если аудит безопасности не превращается в формальную процедуру, а содержит серьезные проверки, включающие в себя поиск уязвимостей, анализ процедур разработки, используемых средств шифрования и т.д. Для систем дистанционного банковского обслуживания таких стандартов не существует, однако независимый анализ защищенности систем банк-клиент необходим как самим банкам, так и разработчикам этих систем.

В настоящий момент ситуация приближается к критической отметке – «точке кипения». Инциденты информационной безопасности, связанные с системами дистанционного банкинга, происходят все чаще, и если отношение к этому вопросу не изменится, то в ближайшее время мы придем к ситуации, когда пользователи будут отказываться от услуг ДБО, что уже происходит в некоторых банках. 



ВСЬ СПЕКТР РЕШЕНИЙ ДЛЯ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ



«CORREQTS»

автоматизация фронт-офиса банка



«ДБО BS-Client»

дистанционное банковское обслуживание юридических лиц



«ДБО BS-Client. Частный Клиент»

дистанционное банковское обслуживание физических лиц



«Расчетный Центр Корпорации (РЦК)»

управление корпоративными финансами



«Единая Точка Контакта»

организация приёма платежей

Узнайте больше о новых продуктах и услугах BSS на семинаре 2 июня!
Регистрация открыта на сайте BSS