Эссе по курсу "Защита информации",
кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Андреев Андрей. 113 гр.
9.04.2005

Особенности и проблемы электронного голосования

(The main issues and problems of electronic voting)

Введение

Термин электронное голосование описывает многие практические применения современных технологий. С некоторой точки зрения, в США уже давно используют электронное голосование, там продолжительное время работала система перфокартного голосования. Электронное голосования также может означать голосование с помощью компьютерного терминала или сенсорного экрана, эта технология была использована в США впервые в 1994 году. Мы будем рассматривать термин электронное голосование с точки зрения существующих в настоящий момент систем. Например, системы оптического сканирования, основанные на том, что избиратель отмечает (обводит) имя своего кандидата, затем бюллетень считывается с помощью оптического распознавания знаков (OMR). После окончания голосования результаты считываются из устройства OMR и распечатываются для наблюдения инспекторами, затем передаются по модему к центральной базе данных. Подобные системы осуществляют мгновенную запись голосов, которую можно использовать в подсчетах, но печать бюллетеней является сложной и дорогостоящей процедурой. Больше внимания, в силу их большего распространения, мы уделим сенсорным системам голосования (Touch-screen voting systems), известным также как системы прямой записи (DRE - direct recording electronic), они не работают с бумажными бюллетенями, при этом работают с различными языками, и обладают возможностью воспроизводить звуковую информацию. Системы голосования DRE изначально имеют несколько преимуществ перед традиционным бумажным голосованием, например, уменьшают число ошибок избирателей. Если система была качественно разработана, то она запрашивает подтверждение выбора в случае ошибки голосующего и делает невозможным «вбрасывание» нескольких бюллетеней за один раз. Также, DRE делает возможными выборы для людей с различными отклонениями, позволяя им голосовать без посторонней помощи. Однако есть и отрицательные стороны. Существует мнение, что в современных системах электронного голосования не выполняются даже минимальные требования безопасности. Открытыми остаются проблемы недозволенного расширения полномочий, неправильного использования криптографии, уязвимости сетей, слабого развития программного обеспечения. Кроме того, существует большая вероятность вмешательства инсайдеров (работников участков и пр.), способных не только изменить голоса, но и нарушить анонимность голосования, что является краеугольным камнем всей системы современных выборов. Сохранение анонимности бюллетеней необходимо, чтобы гарантировать безопасность избирателя, и чтобы сделать невозможным покупку голосов (не существует доказательств, кому именно избиратель отдал свой голос). Приходится констатировать, что действенными могут оказаться оба основных направления атак систем голосования - физический доступ к носителям информации и

«человек по середине» при передаче информации по некоторой сети. Также следует заметить, что программное обеспечение часто бывает написано исключительно на языке C++, и потому программисты должны быть чрезвычайно внимательны, чтобы сделать свой код неуязвимым для атак переполнения буфера и пр. Вышеперечисленные недостатки обнаружены, например, в машинах фирмы Diebold, используемых в 37 штатах США.
Итак, доверять ли подобным машинам? Считается, что ошибки «железа» в сенсорных системах приводят к неправильно подсчитанным голосам, и эти ошибки уже нельзя исправить. Говоря о программном обеспечении, стоит отметить, что многие системы содержат в себе закрытые участки кода, потому не подвержены внешнему тестированию. Некоторые производители скрывают результаты собственных исследований. Недостатки же программного обеспечения могут серьезно повлиять на исход выборов. Открытый программный код в системах голосования, причем на всех его стадиях, необходимая, но, увы, недостаточная мера защиты. На практике не существует систем, работающих по принципу «черных ящиков», код которых является промышленной тайной, исключающих возможность утечек. Большее число исследователей всегда уменьшает риск трюков, спрятанных в коде. Открытый программный код способствует организации групп разработчиков, занимающихся исключительно поиском и исправлением уязвимых мест. Если подобная потребность возникает во многих программных продуктах, тем более она есть в системах электронного голосования

Проверяемость
Т.к. сенсорные системы хранят результаты голосования только в цифровом виде, то не существует независимого метода проверки точности записи голосов, соответственно нельзя утверждать о надежности подсчета. Несмотря на криптографические исследования в области электронного голосования, наиболее жизнеспособным решением является оснащение избирательных машин «проверяемым избирателем листом учета» (audit trail). Для этого системы DRE, оснащенные принтерами, и обычные системы оптического сканирования будут предоставлять пользователю лист бумаги для проверки правильности выбора. Этот лист хранится в корзине бюллетеней и считается основной записью выбора голосовавшего. Избиратель сможет проверить, что его выбор зафиксирован верно, но не будет иметь собственной копии распечатанной записи. Здесь также есть свои недостатки – увеличение стоимости и длительности процедуры выборов, возможность сбоя принтеров. Другое предложение – результат будет находиться в защищенном лог-файле, который избиратель сможет посмотреть на экране сенсорной машины.

Процедура голосования
Машины DRE, вообще говоря, полностью исключают бумажные бюллетени из процесса голосования. Как и при традиционном голосовании, для того чтобы начать процесс голосования, избиратель должен иметь карточку избирателя, обычно, карты избирателя выдаются на избирательном участке в день выборов. Получив свою карту (PIN, смарт-карту или другой токен), избиратель вставляет ее в устройство чтения, терминал проверяет правильность карты, и выводит изображение бюллетеня на экран. После этого, машина DRE обычно показывает итоговый выбор голосующего, предоставляя ему последнюю возможность внести изменения. Если выбор подтверждается, результат записывается на терминал, а карта голосования становится недействительной. Этот шаг предотвращает возможность повторного голосования, недействительная карточка возвращается работникам участка, которые перепрограммируют ее для следующего пользователя. Бюллетень считается «вброшенным», и избиратель может быть свободным. В настоящее время используются различные способы аутентификации избирателя – в некоторых требуется кредитная карточка

и/или существенная персональная информация, но во всех случаях, идентификация является своего рода ключом для доступа к голосованию. Тем не менее, этот ключ не должен присутствовать в последующих шагах процесса электронного голосования. Ключ выдается электронной машиной голосования (возможно со специальным интерфейсом для людей с дефектами зрения), в случае если избиратель испортит бюллетень, он будет помечен как испорченный, отправлен на согласование, а избирателю будет выдан новый ключ. После произведения требуемых процедур голосования, создается некоторая запись выбора избирателя, или на бумаге, или на электронных носителях информации (или на их комбинации). Эта запись выбора становится «вброшенным бюллетенем» (cast ballot).

Небезопасноть смарт-карт.

Таким образом, секретность ключа голосования (Voting Token) – секретность смарт-карты. Вообще говоря, намерение построить безопасную систему с помощью смарт-карт уже вызывает интерес, поскольку само по себе использовании последних не предполагает безопасности системы. Одним из наибольших преимуществ смарт-карт, скажем перед обычными магнитными картами, является то, что они могут выполнять криптографические операции внутри, при том с физически защищенным ключом. Но из-за недостатка криптографии, нет безопасной аутентификации в смарт-картах для терминалов голосования. Другими словами, ничто не мешает злоумышленнику создать собственную, самодельную смарт-карту. Если злоумышленник знает протокол между терминалом и картой, единственным препятствием для массового производства самодельных карт является то, что каждый терминал должен удостовериться в правильности программирования смарт-карты. Но при помощи инсайдерской информации (проверочные данные терминалов доступны для обозрения и с других участков для работников голосования), и в силу того, что многие данные повторяются для разных терминалов, вся необходимая информация является, вообще говоря, доступной. Тем самым можно заполнить большое число бюллетеней, не оставляя следов. Критики утверждают, что индустрия сенсорных машин не торопится использовать новые разработки в области электронной безопасности, при этом представители властей на выборах не достаточно в ней компетентны. Улучшить ситуацию может традиционный для Запада метод – сертификация и стандартизация, в данном случае – сенсорных машин голосования.

Рассмотрим более подробно атаки, использующие смарт-карты. Избиратель начинает процесс голосования, вставив смарт-карточку в терминал. Если карточка активирована, терминал принимает голос избирателя и дезактивирует карточку, меняя определенное 8-битное значение на смарт-карте (например, «1» – карточка для голосования, «8»- проголосовавшая карточка). Если злоумышленник будет обладать самодельной действующей картой, то она может быть запрограммирована игнорировать это действие терминала. Следовательно, по одной карте можно проголосовать несколько раз. При этом, несмотря на несогласованность числа проголосовавших людей и полученных голосов система не сможет отличить настоящие голоса от незаконных. Другое направление атаки - после голосования, вместо того чтобы возвратить «проголосовавшую» карточку работнику участка, злоумышленник может вернуть фальшивую карту, которая запишет то, каким образом она была перепрограммирована, и выдаст эту информацию следующему голосующему. Также он может просто подключить «подслушивающее» устройство и проследить сообщения, которыми обменивается терминал с картой. Устройство, активирующее смарт-карту, включает в себя интерфейс, используемый персоналом. Природа этого интерфейса ограничивает типы закодированной информации. Кодирование времени голосования на смарт-карту, намеренное или в виде побочного эффекта процесса записи файлов, есть потенциальное направление атак. Тем более, электронные машины голосования также знают время, поэтому не обязательно хранить эту

информацию на карте. Кодировать в ключе следует только тип бюллетеня и округ. Также, смарт-карта должна быть подписана соответствующим аппаратным обеспечением во избежание подделок. Также, кроме обычных карт голосования, существуют карты администрирования (administrator card) и карты завершения (ended card), с их помощью работник участка завершает процесс голосования. Обнаружив подобную карту, терминал проверяет PIN, затем просит подтвердить окончание выборов, в случае согласия, результаты выборов записываются на переносную флэш-память или могут быть переданы на главный сервер. Если злоумышленник обладает подобной картой, он может досрочно завершить выборы, или получить доступ к дополнительным функциям управления. Заметим, что PIN пересылаемый со смарт-карты на терминал является открытым текстом, следовательно, любой, знающий этот протокол может получить права администратора. Даже не зная протокола, но, имея доступ к существующей карте администратора, злоумышленник может получить PIN за несколько итераций, если он знает, что код передается в коротком сообщении открытым текстом, посылаемым с карты. Другими словами, он может последовательно посылать каждые 4 байта из открытого текста карты.
Впрочем, уязвимы не только смарт-карты. Каждый раз, когда заполняется бюллетень, машина голосования добавляет как минимум в один лог-файл сообщение, содержащее время создания и признак того, что бюллетень был заполнен. Если временная метка связана с содержимым бюллетеня, то такая информация становится очень чувствительной к атакам. Также, каждый голос записывается последовательно в файл записи голосов. Этот факт позволяет взломщику, такому как работник участка с доступом к записям голосов, легко связать голосовавших с их голосами, что является одной из главнейших угроз правильности выборов.

Безопасность бюллетеней.
Номера бюллетеней (ballot-Ids), не должны нести никакой информации о порядке поданных голосов. Существующая модель использует модуль получения случайных чисел для изменения порядка номеров бюллетеней. Он использует проверенный алгоритм Mersenne Twister с периодичностью 2 19937 – 1. Применение в нем хорошего источника действительно случайных чисел – таких как первые несколько байтов из /dev/random в современных системах Linux – предотвратит атаки дублирующие последовательности номеров бюллетеней. Однако, выбранный разработчиками генератор (линейный генератор) не является криптографически безопасным. Более того он использует в качестве входных данных статическую информацию, связанную с терминалом и выборами.
Перед началом выборов, терминалы получают параметры бюллетеня (“ballot definition”). Для каждый выборов они содержит все от цвета фона экрана и информации о кандидатах, до настроек имени пользователя и пароля в PPP (point to point protocol), если результаты передаются с помощью диал-ап соединения. Эти данные, увы, не шифруются.Таким образом, параметры бюллетеня являются еще одним способом узнать практически всю информацию, необходимую для имитации настоящего терминала с помощью диал-ап соединения. Конечно, для этого злоумышленнику придется создать ID терминала, который иногда не проверяется на конечном сервере. Проблема безопасности проявится в много большем масштабе, если эти данные передаются просто по сети. Если злоумышленник знает структуру параметров бюллетеня, то он может перехватить и изменить данные настроек бюллетеня в процессе их передачи. К тому же многие поля являются простыми для опознания и изменения, включая имена кандидатов, которые передаются простым ASCII текстом. Тем самым легко изменить видимую последовательность имен кандидатов, и избиратели будут отдавать голоса не за своего кандидата.

Существует два способа загрузить в терминал данные начальной конфигурации выборов – с помощью съемного носителя (флэш-память) или через сетевое соединение. Терминалы могут потенциально связываться через небезопасные телефонные линии или даже беспроводные Интернет соединения, так что даже неизощренный злоумышленник может произвести атаку типа «человек посередине» («man-in-the-middle»). Протоколы, по которым терминалы голосования соединяются с центральной базой данных для передачи конфигурационной информации и, самое важное, итоговых результатов выборов, не используют криптографических методов аутентификации конца соединения, и не используют проверки целостности переданных данных. Если терминалы используют Интернет соединение, то злоумышленник, способный перехватывать пакеты истинного терминала может узнать достаточно информации (например, IP адрес конечного сервера) для того, чтобы имитировать его работу. В версиях, в которых избирательные терминалы никогда не подсоединяются к сети или телефонной линии, физическая транспортировка карт флэш-памяти от терминала к центральной системе подсчетов является аналогом сети с неавтоматическими переносами файлов, значит, подобные системы также уязвимы к атаке «человек в середине». Таким образом, сетевые атаки являются наиболее опасными в разработке систем электронного голосования.

После голосования результаты копируются на диск и отправляются в центральную базу данных, потому важно гарантировать безопасность информации, хранимой на терминалах.. Согласно существующим стандартам, каждый терминал должен сохранять полное число бюллетеней, когда-либо «вброшенных» в него. Этот счетчик является еще одним способ гарантировать, что число обработанных бюллетеней на каждом терминале верное. Однако этот счетчик просто сохраняется как целочисленное значение в системной директории терминала, этот метод увеличения счетчика является небезопасным, причем криптографической контрольной суммы недостаточно для его защиты, злоумышленник с возможностью изменения и чтения счетчика сможет вернуть счетчику его прежнее значение. Единственным решением может быть хранение счетчика на защищенном аппаратном ключе (token), но это повлечет за собой серьезные изменения в архитектуре существующих систем голосования. В отличие от другой информации, сохраненной на терминале, запись голосов и контрольный журнал учета являются зашифрованными, и контрольная сумма вычисляется перед записью на устройство-носитель. К сожалению, обе эти процедуры не выполнены согласно установленным, безопасным методикам.

Все данные на устройстве хранения терминала зашифрованы используя однократный, жестко закодированный ключ DES («F2654hD4»). Однако, значение ключа не является случайно сгенерированным. Известно, что значение ключа в коде программы источника – плохая идея, если таким же образом скомпилированная программа используется на каждом терминале, то атакующий с доступом к коду источника, или даже с одним из образов программы, может узнать ключ и таким образом изменить записи голосов. Даже если управление ключом будет улучшено, проблемы останутся. Например, ключи DES могут быть получены простым перебором за относительно не большое время. DES должен быть заменен на тройной DES или, что лучше, на AES. Перед шифрованием вычисляется проверка с помощью циклического избыточного кода (16-битная CRC) для простого текста. После этого эта CRC сохраняется вместе с зашифрованным текстом в файле и проверяется после расшифровки данных и их чтения. Обычной же практикой является, наоборот, предварительное шифрование данных, а после вычисление основанной на ключе криптографической контрольной суммы. Мишенью вероятной атаки являются сами записи голосов - возможность изменения файла с записью голосов, сохраненной на устройстве. Из-за слабого шифрования злоумышленник может получить доступ к этому файлу, и произвести столь угодно много голосов, причем они будут неотличимы от настоящих голосов. Подобная атака не оставляет

следов. Она может быть замечена позднее, сравнением содержания флэш-памяти терминала с данными, переданными по сети, хотя сами накопители могут быть объектом атаки. Сетевые же атаки можно предотвратить с использованием стандартных криптографических методов, например, SSL/TLS.

Конкретно: Россия.

В России уже в течение 10 лет разрабатывается система электронного голосования ГАС "Выборы". Нижний уровень системы, на котором вводится основной объем информации, - территориальные избирательные комиссии, верхний – Федеральный центр информатизации при Центральной избирательной комиссии РФ.

Несмотря на некоторые, вполне плодотворные решения и планомерное развитие системы вот уже в течение десяти лет, использовать ее в качестве основной системы голосования не видится возможным. Также нельзя не отметить огромное отставание от американских аналогов, например, сенсорные системы рассматриваются пока только как возможный эксперимент. На данный момент, на участках производится автоматическое считывание информации с избирательных бюллетеней с учетом отметок, внесенных избирателями, подсчет поданных за кандидатов голосов, регистрация результатов на магнитном и бумажном (лента) носителях. Отличие результатов ручной и автоматической обработки бюллетеней составляет не более 0,05% от общего количества подсчитанных голосов. Информация передается с помощью ведомственной электронной почты, преимущественно по обычным телефонным линиям, поэтому нет непосредственного доступа к базе данных более высокого уровня, что является не очень эффективным, зато безопасным решением. Доступа к сети Интернет, безусловно, нет. Применяется защита от внешнего доступа с помощью аппаратных ключей, а также регулярно меняющихся паролей. Действия пользователей протоколируются. К сожалению, шифрование информации и электронная подпись не используются, потому, несмотря на то, что злоумышленнику требуется пароль доступа, а случаи ошибочного ввода фиксируются, результаты ГАС «Выборы» не должны иметь юридической силы.

Программное обеспечение – общее на базе СУБД Oracle на платформе Windows, специальное программное обеспечение – отечественные разработки на платформе MS-DOS. Перед выборами все программное обеспечение устанавливается с нуля. Аппаратное обеспечение – компьютеры фирмы Compaq. Аппаратно-программные средства защиты – защита от несанкционированного доступа, криптографическая защита информации в каналах связи, контроль целостности и подлинности электронных документов, антивирусная защита. По традиции особенности этих средств защиты засекречены, что влечет за собой описанные в начале эссе недостатки. Стоит отметить степень защиты от злоумышленника-оператора (инсайдера) – его работа контролируется наблюдателями, в процессе ввода автоматически проверяются контрольные соотношения между числовыми данными протокола, при несовпадении которых выдается сообщение об ошибке, после ввода данные распечатываются и проверяются, только после этого передаются по электронной почте. В целях уменьшения влияния человеческого фактора на результат выборов апробируется комплекс обработки избирательных бюллетеней, но повсеместно еще не используется код избирателя, который, возможно, появится в паспортах нового образца – как уже говорилось, система активно разрабатывается и развивается.

Итоги

Несомненно, следует проводить подсчеты результатов и их опубликование отдельно по каждому округу, и лишь после этого проводить глобальное суммирование по стране. Однако, самым уязвимым местом любой системы голосования являтся доступ к итоговым данным, случай масштабной коррумпированности, когда речь идет о контроле над потоком уже

обобщенной информации, поступающей из избирательных участков в ЦИК. Такой контроль позволял бы перераспределять очередность поступления данных из участков с перевесом в пользу одного из кандидатов, что позволяло бы формировать на основе предварительных данных мнение о перевесе конкретного кандидата. Парироваться подобное действие может организацией пересылки данных с уведомлением о получении, с пересылкой уникальных для каждого сообщения числовых последовательностей (контролльных сумм), в которые включены параметры даты и времени транзакции. Также подобный контроль, вроде «транзитного сервера», позволял бы злоумышленнику корректировать данные из участков. Однако при этом необходима дополнительная информация об участках, где появляется "запас мертвых душ" и обратный поток данных для подгонки протоколов участков. Потому это возможно только при массированном участии персонала избирательных участков в подтасовке результатов.

Заключение

Несмотря на то, что системы электронного голосования находят все большее распространение (США, Англия, возможно, Австралия), существует слишком много проблемных вопросов, касающихся корректности и анонимности их работы. Есть серьезные трещины в безопасности: избиратели могут легко «вбросить» большое количество голосов без возможности это проследить после, функции администратора могут быть выполнены рядовыми избирателями, а атаки инсайдеров, таких как работники участков, могут носить глобальный характер. Для тестирований создаются проверочные машины «взлома» голосования (Hack-a-Vote), упрощенные DRE машины, которые изначально проектировались для демонстрации того, насколько просто внедрить троянский вирус в систему голосования.
Несмотря на выше перечисленные недостатки, лоббисты электронных систем голосования продолжают утверждать об их относительной безопасности.

Ссылки

[1] Electronic Voting
Rebecca Mercury
http://www.notablesoftware.com/evote.html

[2] E-voting Security
By Avi Rubin
Johns Hopkins University
Department of computer science
http://www.avirubin.com/vote/

[3] The Open Voting Consortium (OVC)
http://www.openvotingconsortium.org/

[4] Verified Voting America
http://www.verifiedvoting.org/

[5] Privacy Issues in an Electronic Voting Machine
Arthur M. Keller, UC Santa Cruz and Open Voting Consortium;
David Mertz, Gnosis Software, Inc.mertz@gnosis.cx

Joseph Lorenzo Hall, UC Berkeley School of Information Management and Systems
jhall@sims.berkeley.edu
Arnold Urken, Stevens Institute of Technology aurken@stevens.edu
http://gnosis.cx/publish/voting/privacy-electronic-voting.pdf

[6] Black Box Voting
http://www.blackboxvoting.com/

[6] Black Box Voting
http://www.blackboxvoting.com/

[7] Александр Калинин: ГАС "Выборы" - это ERP для избирательной системы России
http://www.cnews.ru/newcom/index.shtml?2004/04/21/158088