ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ УЧЕБНЫХ ПРОГРАММ

Кручинин В.В.
ЛИСМО-ТУСУР

1. Анализ проблемной ситуации

Компьютерные учебные программы (КУП) - это программы, предназначенные для непосредственного использования в учебном процессе. Особенностью КУП по сравнению с другими является тот факт, что они могут контролировать уровень знаний в процессе обучения. Зачастую это является объектом взлома. Перечислим основные варианты взлома КУП:

1. Поиск эталонной информации с использованием специальных программ чтения двоичных файлов с целью поиска правильного ответа на вопрос или тестовое задание.
2. Создание специальных программ поиска эталонной информации.
3. Изменение информации в самой КУП.
4. Изменение программного кода КУП.
5. Вскрытие протоколов КУП.
6. Поиск и создание базы правильных ответов.

Рассмотрим каждый пункт более подробно. Поиск эталонной информации в коде самой программы или в специальном файле самый простой способ взлома, если КУП никак не защищена. В некоторых случаях, если кодирование является простым, этот способ также является эффективным способом взлома. Во втором случае пишут специальную программу, которая вместо ответа обучаемого, подставляет правильный ответ, зная опять же эталонную информацию.

В третьем случае, можно просто изменить сообщения, которые выдает КУП. Например, вместо «Ваша оценка 2», можно изменить цифру 2 на цифру 5, то получим «Ваша отметка 5».

В четвертом случае, происходит изменение программного кода. Изменение кода может быть осуществлено двумя способами: изменения файла образа программы и изменение кода программы в процессе исполнения. Во втором случае пишут специальную программу, которая обнаруживает КУП в оперативной памяти и изменяет определенные участки памяти.

Для КУП можно перечислить следующие участки кода, требующие защиты:

1. Программный код, который производит сравнение ответа обучаемого и эталона.
2. Программный код, который производит итоговое оценивание.
3. Программный код, который осуществляет отображение итоговой оценки.
4. Программный код, формирующий протокол.
5. Программный код, генерирующий список вопросов. В этом случае, существенно сокращается количество вопросов, которые может задавать КУП.

В пятом случае производится вскрытие и подделка протокола. Здесь вариантов может быть несколько. Первый вариант: вскрытие протокола и изменение полученных оценок. Второй – подделка реквизитов у протокола, имеющего хорошую оценку.

В шестом случае создается база вопросов с правильными ответами. У обучаемого в процессе экзамена имеется возможность найти вопрос из имеющегося списка и подставить правильный ответ.

2. Основные требования к защите информации в КУП

На основе имеющихся вариантов взлома перечислим основные требования к защите КУП от взлома:

1. КУП должна быть защищена от возможности несанкционированного изменения.
   1.1. Защита генерации списка вопросов.
   1.2. Защиты кода производящего оценивание ответа на вопрос.
   1.3. Защита кода, производящего итоговое оценивание.
   1.4. Защита кода, осуществляющего отображение итоговой оценки.
   1.5. Защита кода, производящего формирования протокола проведения экзамена.
2. Экзаменационные программы должны быть защищены таким образом, чтобы эталонный ответ нельзя было прочитать, механизм выставления оценки должен быть закрыт и по возможности количество вопросов, имеющихся в базе экзамена, должно быть достаточно большое (в идеале – бесконечное количество вопросов).
3. Протокол КУП должен быть защищен.

3. Основные варианты решения проблемы защиты

1. Проверка целостности КУП. Здесь можно предложить следующие варианты:

1) защита производится всей КУП;
2) защита только наиболее важных элементов КУП;
3) многоуровневая система проверки.

При этом схема защиты может быть следующей:

1) простейшая схема – проверка контрольной суммы (не помехоустойчива);
2) сжатие (кодирование) программы некоторым алгоритмом (раскрывается тогда, когда начинает выполняться программа); другой вариант – отдельные фрагменты программы работают с разными алгоритмами;
3) использование особенностей организации вычислительной системы, в этом случае КУП будет привязана к данному типу ЭВМ, в некоторых случаях это не желательно.

2. Защита важных элементов в КУП.

1) использование схем 1. применительно к некоторому участку программы;
2) в некоторых случаях замена текста на графическое представление;
3) многоуровневая система проверки – она предполагает, что существуют программы проверки i-го уровня.

В третьем случае необходимо предусмотреть защиту всех этапов:

1) генерацию вопросов;
2) оценивание вопроса;
3) итоговое оценивание;
4) отображение результатов экзамена.

3. Разделение процесса проведения экзамена и оценивания. В этом случае производится разделение процесса проведения экзамена на два этапа: этап проведения опроса – специальная программа производит опрос обучаемого и формирование протокола с его ответами (на данном этапе не присутствуют эталонные ответы) и этап оценивания – производится без участия обучаемых. В данном варианте защиты требует:

1) процесс генерации вопроса;
2) процесс формирования протокола, в этом случае важно, чтобы протокол не был фальсифицирован, вместо протокола истинного не был подставлен протокол с хорошей отметкой, полученный ранее.

Подобный подход может быть реализован в сети Интернет: экзамен разделяется на две части: серверная и клиентская. Клиентская часть обеспечивает ввод ответа и передачу на сервер. Серверная часть обеспечивает анализ ответа на вопрос, производит оценивание, запись результатов в базу данных и передачу результатов оценивания клиенту.

4. Использование функций свертки. Защиту эталонов(правильных ответов) можно осуществить методом, предложенным в устройстве для контроля знаний «Символ». В данном методе используется специальный набор функций свертки. Функция свертки обеспечивает перевод некоторой строки символов в число. Тогда для всех эталонов подбирается функция свертки, которая преобразует эталон в число. Так что в КУП хранятся функции свертки и соответствующие числа. При вводе ответа на вопрос, строка введенная обучаемым также свертывается, при этом используется та же функция свертки. Далее полученное число сравнивается с тем, что хранится в КУП в виде эталона и на основании сравнения делается вывод о правильности ответа.

Данный метод имеет ряд недостатков. Первый из них – функции свертки неоднозначны. Т.е. есть некоторое подмножество строк, разных, которые могут теоретически иметь одно и тоже число свертки. Второй недостаток заключается в том, что при вычислении эталонных чисел необходимо использовать автоматизированный режим подбора функций свертки. Т.е. обязательно должен быть эксперт по подбору функций сверток для данного эталонного ответа.

5. Использование генераторов. Как правило, количество вопросов в КУП заранее фиксировано и имеет достаточно небольшой объем (в ТМЦДО каждый компьютерный экзамен содержит около 100 вопросов).

Опыт подсказывает, что довольно скоро подготавливаются правильные ответы на все вопросы. Выход из создавшегося положения состоит в том, что создаются специальные программы – генераторы вопросов или тестовых заданий. Кроме того, есть специальная программа – решатель тестовых заданий. Тогда процесс экзамена будет следующий: случайно генерируется список тестовых заданий, эти задания выдаются обучаемому, в процессе решения обучаемый вводит ответы на решенные тестовые задания. Программа эти тестовые задания решает самостоятельно и сравнивает ответ, полученный от обучаемого, со своим ответом. Если совпадает, то ответ правильный, если нет – то неправильный.

Такой подход легко реализовать для естественнонаучных дисциплин, когда тестовое задание можно сформулировать в виде задачи. Например, дано напряжение и сила тока, нужно найти значение сопротивления. В этом примере можно сделать генератор тестовых заданий с бесконечным числом заданий. Для каждого входного параметра генерируется вещественное число. И составляется программа для вычисления результата (по закону Ома). Далее сформулированная задача выдается обучаемому, он ее решает, вводит ответ, программа вычисляет свой ответ и сравнивает. В результате сравнения ставит отметку. Что касается дисциплин гуманитарного характера, здесь генератор вопросов построить значительно сложнее.

4. Защита КУП от просмотра отладчиками

Общепризнанно, что если программа защищена от всякого рода отладчиков, то 90% программистов перестанут пытаться ее взламывать. Поэтому желательно в программе КУП предусматривать эту защиту. Как правило, программисты вставляют фрагменты кода, который производит определенные преобразования с системным стеком.

В последних версиях OS Windows имеются функции (Например, IsDebugBreaset), которые позволяют обнаружить работу программы в режиме отладки.

Перечисленные проблемы и пути решения не являются полными, однако описывают круг проблем, связанных с защитой компьютерных учебных программ.