также индуцированный им полугрупповой гомоморфизм $\eta : \Gamma \to \Gamma_1$. Рассмотрим произвольное отображение $g : Y \cup \{x\} \to \Gamma$, ограничение которого на *Y* (обозначим его тоже буквой *g*) удовлетворяет равенству $g \circ \eta = f$. Пусть $x^g = a$. Тогда, так как $\Gamma \models W_1 x = W_2 x$, для любого $u \in pr_1 \Gamma$ имеем $(u, u_1) \in W_1^g a$ и $(u, u_1) \in W_2^g a$ или $(u, u_2) \in W_1^g$, $(u_2, u_1) \in a$, $(u, u_3) \in W_2^g$, $(u_3, u_1) \in a$, т.е. $u_2 - u_3 \in \ker a$. Поскольку $x \notin Y$, в качестве *a* можно брать любой элемент из Γ, откуда $u_2 - u_3 \in \bigcap_{a \in \Gamma} \ker a = \ker \Gamma$. Факторизуя *V* по ker Γ и учитывая, что для слова *W* в алфавите *Y* выполняется (по определению *g*) равенство $W^g \eta = W^f$, получим для любого $\upsilon \in Coim \Gamma$ справедливо равенство $\upsilon W_1^f = \upsilon W_2^f$. Ввиду произвольности отображения f теорема доказана.

Следствие. Пусть $\Gamma \subseteq LR(V)$ – полугруппа, W_1 W_2 – непустые слова и $x \notin C(W_1 W_2)$. Если $\Gamma \models xW_1 = xW_2$, $\Gamma[\ker \Gamma + pr_2 \Gamma] \models W_1 = W_2$.

Теорема 3. Пусть $\Gamma \subseteq LR(V)$ – полугруппа, W_1 и W_2 – непустые слова и $x \notin C(W_1 W_2)$. Если $\Gamma \models xW_1 = xW_2$, то $\Gamma[pr_2 \Gamma] \models W_1 = W_2$.

Доказательство. Пусть на Γ выполняется тождество $xW_1 = xW_2$.

Тогда ${}^t\Gamma \models \overline{W_1} x = \overline{W_2} x$ и, по теореме 2, ${}^t\Gamma[Coim\, {}^t\Gamma] \models \overline{W_1} = \overline{W_2}$. Но из теоремы 1 и второго равенства (5) следует, что

${}^t\Gamma[Coim\, {}^t\Gamma] = {}^t(\Gamma[{}^tCoim\, {}^t\Gamma]) = {}^t(\Gamma[pr_2 \Gamma])$, откуда $\Gamma[pr_2 \Gamma] \models W_1 = W_2$. Теорема доказана.

Следствие. Пусть выполняются условия теоремы 3. Тогда, если $y \notin C(W_1 W_2)$, $y \neq x$, $\Gamma \models xW_1 y = xW_2 y$, то $\Gamma[(\ker \Gamma + pr_2 \Gamma) / \ker \Gamma] \models W_1 = W_2$.

Список литературы

1. Наумик, М.И. Полугруппа линейных отношений / М.И. Наумик // Доклады НАН Беларуси. – 2004. Т. 48, № 3. – С. 34–37.
2. Бирюков, А.П. Многообразия идемпотентных полугрупп / А.П. Бирюков // Алгебра и логика. – 1970. – Т. 9, № 3,. – С. 255–273.
3. Коряков, И.О. Линейные полугруппы идемпотентов / И.О. Коряков // Исследования по современной алгебре. – 1978. – Т. 11, № 3. – С. 54–96.

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ КОНТЕНТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ АРХИТЕКТУРЫ КЛИЕНТ-СЕРВЕР

В.В. Новый
Витебск, УО «ВГУ им. П.М. Машерова»

В настоящее время большинство информационных систем строится на основе клиент-серверной или распределенной архитектуры. При этом для некоторых видов информационных систем особую роль играет защита контента от несанкционированного доступа или модификации информации. Одним из типов подобных систем являются приложения для проведения автоматизированного тестиро-

вания, как входящие в состав систем управления обучением, так и выполненные в виде отдельных приложений. В данной статье основной темой рассмотрения является безопасность клиентской части и особенности защиты контента и системы от несанкционированного использования, в том числе и от раскрытия ответов теста. Вопрос безопасности системы, полностью расположенной на стороне клиента рассматриваться не будет, так как при этом имеется полный доступ не только к клиентской части и каналу передачи данных, но и к серверной части приложения.

Результаты и их обсуждение. Клиент-серверная тестирующая система разделяется на такие части как сервер, на котором хранится база вопросов и реализуется основная логика программы, клиентская программа, выполняющая предоставление информации клиенту и отправку ответа клиента на верификацию, и канал связи.

Уязвимости серверной части здесь не будут рассматриваться, так как они в значительной мере зависят от безопасности программного обеспечения отличного от самой тестирующей системы (серверной операционной системы, Web-сервера, сервера базы данных и т.д.).

Уязвимости канала связи могут быть использованы для модификации передаваемых данных, перехвата трафика, которым обменивается клиентская и серверная части тестирующей системы. Вопросы безопасности канала данных достаточно хорошо решаются шифрованием трафика между клиентской и серверной частями системы.

Наиболее интересными являются вопросы построения клиентского приложения тестирующей системы. Оно наиболее уязвимо, так как содержит свободно доступную клиентскую часть программы, не ограничивает возможности доступа к вспомогательному ПО, например, браузеру, возможности манипулирования уже расшифрованным трафиком и т.д.

Из принципов построения систем безопасности известно, что система, основывающаяся на секретности используемых алгоритмов, не будет являться безопасной. Поэтому основным способом защиты является минимизация информации, доступной клиентской части программы.

Клиентская часть тестирующей системы в общем случае решает такие задачи как предъявление вопроса теста пользователю тестирующей системы, получение его ответа и отправка ответа серверной части. При этом серверной части необходимо идентифицировать как пользователя, так и вопрос, на который пользователь отвечает. Если система использует постоянные идентификаторы и имеется возможность доступа к базе вопросов, например, пробное тестирование, то потенциально имеется возможность сбора базы вопросов, использования экспертного метода для подготовки ответов на них и автоматизации ответа на вопросы теста. Это может быть сделано как на уровне канала связи, получая трафик тестирующей системы и отвечая ей, так и на уровне клиента, встраиваясь в клиентскую часть или реализуя вспомогательное приложение (возможно взаимодействие через буфер обмена и т.д.).

Решением этой проблемы является использование для идентификации вопроса из базы некоторой случайной величины или ее комбинации с сеансовым ключом.

Предельным случаем этого варианта является идентификация вопроса по его тексту. В качестве решений этой проблемы можно предложить два варианта: использование нетекстового формата для представления вопроса и/или ответов и «полиморфные» вопросы и/или ответы. Первый вариант может реализоваться представлением контента в виде изображения, или с использованием технологии

флеш или silverlight. Кроме того для относительной устойчивости от автоматического распознавания текста вопроса, расположенного на картинке или во flash-ролике, он должен содержать элементы затрудняющие машинное распознавание, подобные используемым в настоящее время в CAPTCHA-тестах. Второй вариант реализации требует предварительного составления базы синонимов для составления вопросов или чрезмерного усложнения системы элементами семантического анализа текста. Поэтому второй вариант ограничен количеством возможных комбинации синонимов или вариантов перестановки слов, сохраняющих смысловое значение вопроса и ответов на него.

Кроме того, возможна модификация клиентской части тестирующей системы, делающая вмешательство в эту систему более затруднительным, например, с помощью add-ins модуля к браузеру. Это решение также является частичным, так как легко обходится получением выводимого программой изображения с последующим его распознаванием.

Заключение. Таким образом, на основе рассмотренных вопросов могут быть сформулированы следующие рекомендации при разработке и использовании клиент-серверных тестирующих систем: по возможности минимизировать количество информации передаваемой клиентской части тестирующей системы, использовать случайные величины для идентификации вопросов теста, использовать нетекстовое представление вопросов и ответов теста. В случае использования существующей системы применять в финальном варианте теста альтернативную формулировку вопросов по сравнению с пробным тестированием.

О СВОЙСТВАХ РАДИКАЛОВ И ИНЪЕКТОРОВ ДЛЯ КЛАССОВ ХАРТЛИ

М.Г. Семенов
Витебск, УО «ВГУ им. П.М. Машерова»

Все рассматриваемые группы являются конечными. В определениях и обозначениях мы следуем [1,2].

Пусть $\sum = \{\pi_i : i \in I\}$ – семейство попарно различных подмножеств множества $\mathbb{P}$ такое, что $\mathbb{P} = \bigcap_{i \in I} \pi_i$. Функцию $h : \sum \to \{\textit{классы Фиттинга}\}$ будем называть функцией Хартли или *H*-функцией [3]. Класс Фиттинга H назовем классом Хартли [3], если $\mathsf{H} = \bigcap_{i \in I} h(\pi_i)\mathsf{E}_{\pi_i'}\mathsf{E}_{\pi_i}$ для некоторой *H*-функции h. В этом случае мы будем говорить, что H определяется локально *H*-функцией h. Функцию h будем называть приведенной, если $h(\pi_i) \subseteq \mathsf{H}$ для всех *i* из *I*.

Особый интерес для нас будут представлять *H*-функции h, обладающие следующим свойством: $h(\pi_i) \subseteq h(\pi_j)\mathsf{E}_{\pi_j'}$ для всех *i* и *j* из *I* ($i \neq j$). Возникает следующий вопрос: для каких классов Хартли существуют функции, обладающие свойством, описанным выше? Ответ на данный вопрос дает