За основу языка программирования AspectTalk взят диалект Little Smalltalk [3] языка Smalltalk. В него введён специальный тип данных — *метакласс*, элементы которого являются классами классов и позволяют программисту давать виртуальной машине дополнительные указания о функционировании объектной системы. Эти указания определяются в виде обработчиков операции посылки сообщения от объекта к объекту и наследуются метаклассами в иерархии наследования метаклассов. Граф иерархии наследования метаклассов является подграфом графа иерархии наследования классов. Данный подход позволяет избавиться от недостатков АОП, описанных в [4], а также упростить семантическую модель языка. Подробнее об AspectTalk можно прочитать в [5].

Виртуальная машина имеет стековую архитектуру с разделением стека данных и стека вызова процедур. Набор команд виртуальной машины включает операции управления стеком данных, а также операции над примитивными типами данных. Язык программ для виртуальной машины представляет собой польскую инверсную запись последовательности команд. Для реализации транслятора с AspectTalk в язык виртуальной машины построена грамматика класса LL(2).

Использование предложенных методов и средств позволит снизить затраты на внесение изменений в политики безопасности, а также повторно использовать реализации политик безопасности при разработке новых программных систем. Научная новизна работы состоит в модификации аспектно-ориентированного подхода в программировании, состоящей в специализации средств метаязыка, а именно: в классическом подходе они используются при написании аспекта совместно с операциями объединения, в предложенном подходе — при написании только соединительных модулей. Последнее упрощает процедуру повторного использования аспектов: в классическом подходе это требует переписывания заново самого аспекта, в предложенном подходе — переписывания только соединительного модуля, который, как правило, много проще присоединяемого аспекта.

ЛИТЕРАТУРА

1. *Elrad T., Aksit M. M., Kiczales G., et al.* Discussing aspects of AOP // Communications of ACM. 2001. October. V. 44. No. 10. P. 33–38.
2. *Kiczales G.* The Art of Meta-Object Protocol. The MIT Press, 1991. 345 p.
3. *Budd T.* A Little Smalltalk. Addison-Wesley, 1987. 280 pp.
4. *Bouraqadi N., Seriai A., Leblanc G.* Towards unified aspect-oriented programming // ESUG 2005 Research Conference. 2005. 22 p.
5. *Стефанцов Д. А.* Реализация политик безопасности в компьютерных системах с помощью аспектно-ориентированного программирования // Прикладная дискретная математика. 2008. №1(1). С. 94–100.

УДК 681.511:3

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ, УСТОЙЧИВЫЕ К АТАКЕ СГОВОРОМ

Р. С. Стружков, Т. М. Соловьёв, Р. И. Черняк

В настоящее время основным способом борьбы с пиратством в сфере цифровых технологий является внедрение в медиа-данные цифровых водяных знаков. В большинстве случаев водяной знак выбирается как произвольный идентификатор пользователя

или логотип какой-либо организации, а его стойкость обеспечивается лишь алгоритмом внедрения. Однако при таком выборе водяных знаков метод защиты оказывается малоэффективным против серьезных атак, направленных на полное или частичное удаление или изменение водяного знака. В частности, он абсолютно неустойчив к атаке сговором, а для систем с большим количеством пользователей, таких, как IPTV, это недопустимо.

В данной работе вводятся допустимые множества водяных знаков, использование которых позволяет противостоять атакам сговором, изучаются свойства и оцениваются количественные характеристики таких множеств с целью их построения и обсуждается проблема идентификации участников сговора по созданному ими ложному водяному знаку.

Под атакой сговором понимается следующее. Злоумышленник побитно сравнивает имеющиеся у него копии некоторого медиа-данного с различными водяными знаками в них и заключает, что биты, в которых сравниваемые данные различаются, суть биты водяного знака. Затем он эти биты устанавливает в некоторые значения так, чтобы полученный водяной знак, называемый *ложным*, не совпадал ни с одним из использованных при сравнении. Делая это, злоумышленник преследует одну из следующих двух целей: уничтожить водяной знак, т. е. сделать его распознавание невозможным, либо изменить водяной знак так, чтобы он идентифицировал какого-либо законопослушного пользователя.

Предлагается следующий подход к противодействию этой атаке.

При атаке сговором злоумышленник может различить и уничтожить без потери качества медиа-данного лишь те биты водяного знака, которые различаются в имеющихся у него копиях медиа-данного. В связи с этим водяной знак необходимо внедрять в одинаковые позиции во всех копиях любого медиа-данного.

Отходя от деталей внедрения, под водяными знаками будем понимать булевы векторы некоторой размерности n и их множество обозначать W_n или W, если размерность векторов в нём несущественна. Для того чтобы противостоять атаке сговором, предлагается в качестве последнего использовать такое подмножество $W \subset \{0,1\}^n$, называемое *допустимым*, которое удовлетворяет условию: каждому подмножеству $P \subseteq W$ минимальный интервал $I(P)$ в $\{0,1\}^n$, его покрывающий, сопоставляется взаимно-однозначно, т. е. если $P_1, P_2 \subseteq W$ и $P_1 \neq P_2$, то $I(P_1) \neq I(P_2)$, и, кроме того, если $|P| > 1$, то $I(P) \neq P$. В этом случае злоумышленник, проводящий атаку сговором, имеет копии некоторого медиа-данного с водяными знаками в некотором $P \subseteq W$ с $|P| \geqslant 2$ и получает копию этого медиа-данного с ложным водяным знаком w, выбирая его произвольно из множества $I(P) \setminus P$. Для такого w верно $w \notin W$, ибо иначе $I(P) = I(P \cup \{w\})$, что противоречит допустимости W.

Таким образом, при атаке сговором на водяные знаки из допустимого множества невозможно получить ложный водяной знак, который идентифицировал бы невиновного пользователя.

Тем самым противодействие атаке сговором на водяные знаки, защищающие медиапродукцию от пиратства, сводится к построению больших допустимых множеств булевых векторов некоторой размерности. В этой связи полезно изучить предварительно свойства и установить количественные характеристики таких множеств, что, собственно, и делается далее.

Обозначим $k(I)$ размерность (количество переменных компонент векторов) интервала I в $\{0,1\}^n$.

Утверждение 1. $k(I(P)) \geqslant |P|$ для любого $P \subseteq W$ мощности $|P| > 2$ и допустимого W.

Утверждение 2. Для любых допустимых множеств W и W' в $\{0,1\}^n$ если $W \subseteq W'$, то $|W'| \leqslant |W| + n - k(I(W))$.

Утверждение 3. Мощность любого допустимого множества W_n не больше n.

Отсюда следует, что количество всех допустимых множеств векторов в $\{0,1\}^n$ не превосходит числа $\sum_{i=1}^{n} C_{2^n}^i$.

Пусть $O_1(a)$ обозначает окружность радиуса 1 вокруг булева вектора a в пространстве $\{0,1\}^n$, т. е. $O_1(a) = \{x \in \{0,1\}^n \colon d(x,a) = 1\}$, где $d(x,y)$ — расстояние Хэмминга между булевыми векторами x и y.

Утверждение 4.

1) $O_1(a)$ — допустимое множество;
2) всякое допустимое множество мощности n имеет вид $O_1(a)$.

Ввиду утверждения 3 это значит, что все допустимые множества векторов в $\{0,1\}^n$ наибольшей мощности суть $O_1(a)$ для $a \in \{0,1\}^n$, и их количество равно 2^n.

Два интервала будем называть *эквивалентными*, если их множества внутренних (переменных) компонент совпадают. Все интервалы размерности 0 являются эквивалентными по определению. Пусть также $E(W) = \{I(P) \colon P \subseteq W, |P| > 1\}$.

Утверждение 5. Для любого допустимого множества W все элементы в $E(W)$ попарно не эквивалентны.

Подмножества W и W' в $\{0,1\}^n$ будем называть эквивалентными, если $|W| = |W'|$ и для каждого интервала любого одного из множеств $E(W)$ и $E(W')$ найдётся эквивалентный ему интервал в другом. Если W и W' допустимые, то по утверждению 5 последнее соответствие устанавливается единственным образом. Заметим также, что любое множество, эквивалентное допустимому, также допустимо. Непосредственно проверяется, что для любого n все допустимые множества $O_1(a) \subset \{0,1\}^n$ образуют класс эквивалентности.

Утверждение 6. Мощность любого класса эквивалентности допустимых множеств векторов в $\{0,1\}^n$ не меньше 2^n.

В доказательстве этого утверждения показывается, как по любому допустимому множеству можно построить ещё, как минимум, $2^n - 1$ эквивалентных ему других допустимых множеств с линейной сложностью построения одного множества.

При обнаружении ложного водяного знака w в копии некоторого медиа-данного возникает задача идентификации создавших его участников атаки сговором, состоящая в вычислении подмножества водяных знаков, из которого атакой сговором получен этот знак, т. е. такого $P \subseteq W$ (или непустой его части), что $w \in I(P) \setminus P$. Ввиду возможности пересечения минимальных интервалов, покрывающих различные подмножества булевых векторов, эта задача может иметь несколько решений — «подозреваемых» подмножеств в W. В этом случае среди последних выбираются все минимальные по включению (их множество обозначается $M(W,w)$), и из них, рассматриваемых в порядке неубывания мощности, находится настоящий «нарушитель» путём «следственных мероприятий».

Качество допустимого множества W можно оценить по его *характеристическому вектору* $H(W) = H_1(W)H_2(W)\dots H_m(W)$, где $m = |W|$ и для любого $i = 1, \dots, m$

$$H_i(W) = \max_{P \subseteq W, |P|=i} \left(\max_{w \in (I(P) \setminus P)} |M(W, w)| \right).$$

В случае, если $H_i(W) = 1$ для $i = 1, \dots, t$ и некоторого $t \leqslant m$ и атака сговором проводится группой из t или менее пользователей, т. е. ложный водяной знак w построен по некоторому множеству $P \subseteq W$ мощности $|P| \leqslant t$, то непустая часть этого P вычисляется по w однозначно и, следовательно, некоторые участники этого сговора идентифицируются знаком w безошибочно.

Допустимое множество водяных знаков W называется *разделимым*, если для любых различных подмножеств $P_1, P_2, \dots, P_k \subset W$ верно

$$\bigcap_{i=1}^{k} P_i = \varnothing \Rightarrow \bigcap_{i=1}^{k} I(P_i) = \varnothing.$$

В случае разделимого множества W решением задачи идентификации участников сговора по ложному водяному знаку w является множество $\acute{P} = \bigcap_{P \in Q} P$, где $Q = \{P \subset W \colon |P| > 1, w \in I(P) \setminus P\}$.

Утверждение 7. Длина векторов в разделимом множестве W не меньше, чем $2^{|W|-1} - 1$ — количества разбиений множества W на два блока.

Эта оценка является существенным препятствием для практического применения разделимых множеств: чтобы обеспечить водяными знаками из разделимого множества хотя бы 100 пользователей, потребуются булевы векторы, длина которых не меньше $2^{99} - 1$.

УДК 004.732

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ г. ТОМСКА

М. И. Цой

На сегодняшний день существует множество стандартов, описывающих беспроводные сети. По своим возможностям современные беспроводные технологии практически не уступают традиционным проводным. Особое внимание разработчики уделяют вопросам безопасности, поскольку специфика беспроводной связи порождает ряд проблем, которых лишены проводные сети. Целью работы является проведение исследования защищенности беспроводных локальных сетей WiFi (семейство стандартов IEEE 802.11) в городе Томске: сбор данных и их анализ, позволяющий сделать выводы о состоянии их безопасности.

Наиболее известными стандартами, описывающими механизмы обеспечения безопасности в сетях WiFi, являются:

— IEEE 802.11, предполагающий использование алгоритма RC4 для шифрования данных и алгоритма CRC32 для контроля их целостности в протоколе WEP. В настоящее время известно множество уязвимостей как в алгоритме RC4, так и в его реализациях в WEP, поэтому последний не обеспечивает приемлемой степени защиты;