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;

— IEEE 802.11i (Draft 3), в котором предлагается протокол WPA, использующий контроль целостности сообщений, генерацию динамических ключей шифрования, а также увеличенные длины векторов инициализации алгоритма RC4. Сегодня также известны уязвимости в данном протоколе;
— IEEE 802.11i (WPA2, 2004 г.). Его механизмы являются наиболее безопасным решением на сегодняшний день, для шифрования трафика используется алгоритм AES.

В процессе исследования проводилось пассивное сканирование эфира при помощи свободно распространяемых утилит (Kismet, airodump-ng). Основные выводы делались на основе служебных фреймов Beacon и Probe Response. Передаваемые в сетях данные, а также координаты точек доступа не сохранялись. Была собрана информация по следующим показателям:

— используемые механизмы шифрования (WEP, WPA, WPA2 или никакой);
— рассылка идентификатора сети;
— использование настроек по умолчанию;
— производители оборудования;
— состав сетей (количество точек доступа);
— стандарты передачи данных (частотный диапазон, скорость передачи, радиус действия);
— загруженность частотных каналов.

На основе собранных материалов получены следующие данные о защищенности беспроводных сетей г. Томска:

— 71 % сетей используют шифрование, однако в большинстве используются механизмы WEP и WPA, которые в той или иной степени могут быть скомпрометированы;
— большая часть сетей представлена лишь одной точкой доступа, что говорит об активном использовании беспроводных технологий частными лицами;
— для 8 % сетей не удалось определить производителя оборудования, что может быть связано с ручным изменением параметров оборудования;
— добровольная рассылка идентификатора сети включена в 88 % сетей, из них 22 % используют идентификатор по умолчанию.

Сравнение полученных результатов с результатами аналогичных исследований в других городах (см., например, [1 – 3]) показало, что общая ситуация в Томске соотносится с общемировыми показателями.

ЛИТЕРАТУРА

1. http://www.securitylab.ru/analytics/270874.php
2. http://www.securelist.com/ru/analysis?pubid=204007548
3. http://www.securelist.com/ru/analysis/204007540/Wardriving_v_Varshave

УДК 004.773.5

МЕТОД ЗАЩИТЫ ЦИФРОВОЙ ВИДЕОИНФОРМАЦИИ ПРИ ЕЁ ПЕРЕДАЧЕ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Е. В. Щерба

Неотъемлемым атрибутом большинства видеосистем становится использование потоковой передачи видеоинформации по компьютерным сетям. Но при передаче информации по открытому каналу связи неизбежно встает задача её защиты. Наиболее часто