редных членов последовательности чисел при помощи РГПЧ, сплошными жирными линиями – перемещение данных с их спецобработкой.

Таким образом, в соответствии с предоставленными исходными данными, проведенным анализом этих данных и выбранной аппаратной платформой реализации был разработан протокол прозрачного шифрования данных для организации сеансов передачи данных по защищенному каналу связи «земля–борт». Данный протокол определяет архитектуру построения МОИ, место генерации, тестирования и хранения, процедуры выбора и режимы смены ключевой информации при обработке передаваемых и принимаемых данных.

Библиографический список

1. Шаранок, А. С. Аппаратная реализация алгоритмов шифрования на элементной базе ПЛИС / А. С. Шаранок // Актуальные проблемы безопасности информационных технологий : сб. науч. ст. ; ред. О. Н. Жданов, В. В. Золотарев, А. В. Шахматов ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2008.

2. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : ИПК Изд-во стандартов, 1996.

3. Винокуров, А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы x86 [Электронный ресурс] / А. Винокуров. Электрон. дан. Режим доступа: http://re-tech.narod.ru/inf/crypto/gost.htm. Загл. с экрана.

4. Столингс, В. Криптография и защита сетей: принципы и практика / В. Столингс. 2-е изд. М. : Изд. дом «Вильямс», 2001.

5. Потехин, Д. С. Разработка систем цифровой обработки сигналов на базе ПЛИС / Д. С. Потехин, И. А. Тарасов // М. : Радио и связь, 2007.

K. M. Voloshchuk, T. A. Chalkin

TRANSPARENT ENCRYPTION PROTOCOL FOR DATA TRANSMITTED VIA «SURFACE-TO-BOARD» CHANNEL

The organization of the Transparent data encryption protocol designed for the data transmission via the secure «surface-to-board» channel is described in this paper. This protocol determines the place of key information generation, testing location, key information selection and change procedures while data-processing operation.

Keywords: transparent data encryption protocol, «surface-to-board» channel, data processing module.

УДК 004.056.53:519.873

Е. С. Семенкин, М. А. Стюгин

ЗАЩИТА ОТ ИССЛЕДОВАНИЯ И ЕЕ ПРИМЕНЕНИЕ В СИСТЕМАХ БЕЗОПАСНОСТИ

Рассматривается информационное взаимодействие нарушителя и защищаемой системы в виде стереотипных схем исследования, предлагается метод снижения эффективности атаки путем искусственного повышения разнообразия атакуемой системы, описывается задача автоматизации проектирования систем безопасности.

Ключевые слова: информационное взаимодействие с нарушителем, стереотипные схемы, снижение риска в системах безопасности.

С давних времен человечество пыталась упростить как свою жизнь, так и способы ее поддержания. Простота – признак гениальности, а порядок – залог успеха. Однако такой подход эффективен до тех пор, пока дело не доходит до серьезных конфликтов, где единственный способ преобладать – это сделать свой уникальный шаг к цели. В таком конфликте каждый исследует своего противника, и чем проще и стереотипнее этот противник, тем он беззащитнее от атак конкурента (нарушителя).

Информационный обмен. Любая активная деятельность сопровождается получением, передачей и анализом информации. Такой информационный обмен происходит всегда. Схематично его можно изобразить следующим образом (рис. 1).

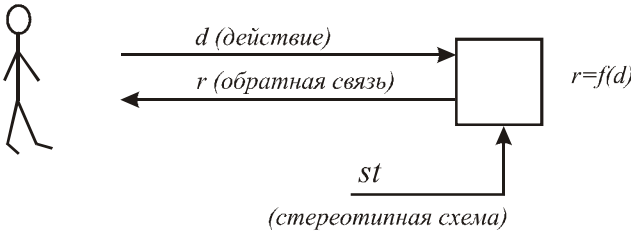

Рис. 1. Схема информационного обмена

Совершая некие действия (d), субъект наблюдает ответную реакцию объекта (r). Значение r интерпретируется в соответствии с внутренней структурой объекта. Это означает, что субъект имеет некую информацию об объекте и предполагает, как объект будет реагировать на его действия. Эту информацию об объекте субъект получает в результате применения стереотипной схемы (st) взаимодействия с объектом. Стереотипная схема является исходной моделью, в рамках которой субъект определяет структуру объекта (выполняет интерпретацию информации r). Таким образом, представленная схема исследования аналогична модели исследования «черного ящика» [1].

Всю деятельность по данной схеме можно условно разделить на исследование и контроль. Контроль – это отслеживание обратной реакции r. Если она не согласуется с ожидаемым значением, то субъект вынужден перейти к исследованию. При исследовании субъект не знает заранее обратной реакции, но фиксирует ее для нахождения структуры объекта, т. е. функции $r = f(d)$.

Процесс исследования. В любых антагонистических конфликтах, в том числе и в системах безопасности, любым активным действиям предшествует исследование системы. Его можно не выделять как отдельный этап управления в конфликтной ситуации, но учитывать его необходимо, так как любые действия (контроль) совершаются с учетом неких представлений об объекте.

В качестве очень простого примера можно рассмотреть ввод символов с клавиатуры. Действием здесь будет ввод символов на клавиатуре, а обратной реакцией символы, отображаемые на экране монитора. В качестве стереотипной схемы здесь берется тождество между вводимым и отображаемым символом (рис. 2).

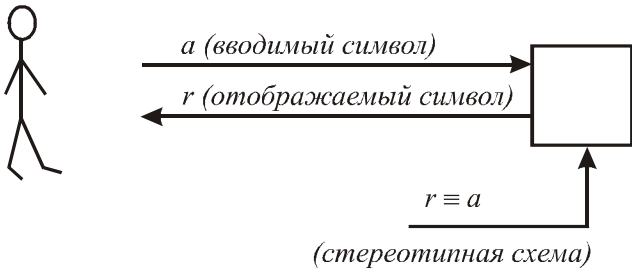

Рис. 2. Пример простейшей стереотипной схемы

Это взаимодействие – контроль, так как субъект предполагает реакцию системы. Допустим теперь, что произошел отход от стереотипной схемы, например, кто-то перемешал клавиши на клавиатуре. Символы на клавиатуре теперь не соответствуют тем, что появляются на экране. Это склонит субъекта к исследованию – необходимо найти (неизвестную) стереотипную схему (функциональную зависимость $r = f(a)$). Но такое исследование, в свою очередь, может быть проведено только в рамках некоторой новой стереотипной схемы, которой, например, может быть предположение о существовании взаимнооднозначного соответствия между вводимым и отображаемым символом. Это соответствие и должно быть установлено в ходе исследования (рис. 3).

С учетом новой стереотипной схемы объект исследуется, как черный ящик, и с использованием некоторых методов (например, перебора вариантов) определяется функция $r = f(a)$. Если на клавиатуре всего n символов, то необходимо перебрать $(n - 1)$ значений для установления зависимости.

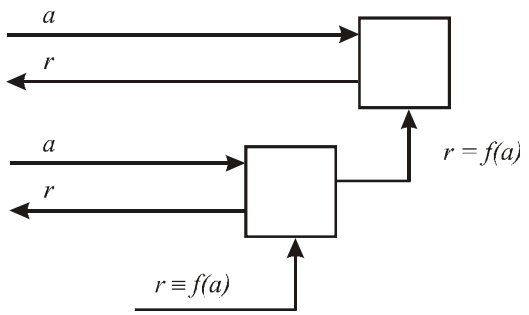

Рис. 3. Новая стереотипная схема
$r = f(a)$ – устанавливается вид функции f

Представим теперь, что снова произошел отход от стереотипной схемы путем ввода в зависимость дополнительного параметра, например, порядка вводимого символа – b. Теперь между вводимым и отображаемым символом нет взаимнооднозначного соответствия – если символ набирается первым, то он отображается иначе, нежели в ситуации, когда он вводится вторым или третьим. Поскольку значение r невозможно интерпретировать с помощью найденной ранее функции, выполняется переход к исследованию для установления зависимости в рамках новой стереотипной схемы – предположения, что зависимость между вводимым символом и отражаемым по-прежнему функциональная, но значение этой функции зависит от одного параметра (рис. 4).

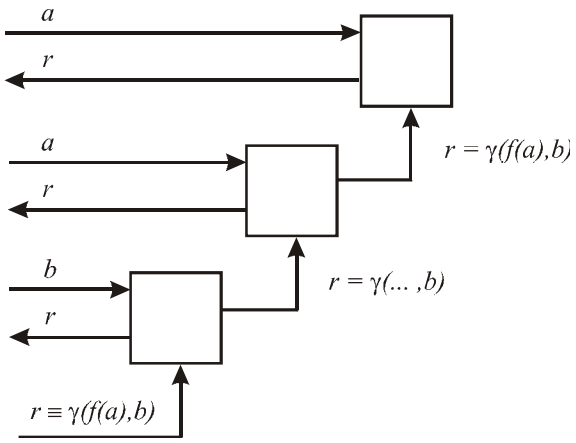

Рис. 4. Стереотипная схема с одним параметром

В результате исследования мы находим исходную стереотипную схему, которая уже имеет вид $r = \gamma(f(a), b)$. Если параметр b имеет m значений, то для исследования черного ящика нам теперь необходимо перебрать $(nm - 1)$ значений.

Из рассмотренного примера видно, что стереотипные схемы необходимо разделять по количеству параметров, на которых она определяется. Если субъект не знает эти параметры, то соответственно, не может исследовать систему. Она будет представлять для него хаос. Вводя в данном примере еще один параметр, например время, можно добиться того, что непосвященный субъект просто не увидит никакой зависимости между символа-

ми на клавиатуре и теми, что отображаются на экране. Интерпретация для него будет невозможной, а работа системы – хаотичной.

Информативность обратной связи. Вводя такой хаос в систему, можно затруднить нарушителю какие-либо действия на «нашей территории», т. е. так же, как и в конкурентной борьбе, сохранять свою «невидимость» для конкурентов. В любой системе есть пространство для таких усложнений, т. е. для хаоса. Главное здесь – научиться самому с ним справляться. Тогда он будет создавать проблемы только для нарушителя.

Рассмотрим еще один пример из области атак на компьютерные сети. Здесь нарушитель, прежде чем осуществить контроль, как правило, вынужден просканировать сеть с целью определения IP-адресов хостов, а также открытых портов, запущенных служб и пр. (рис. 5). То есть он сразу переходит к исследованию в рамках стереотипной схемы – взаимнооднозначное соответствие между IP-адресами и хостами в сети (st_1).

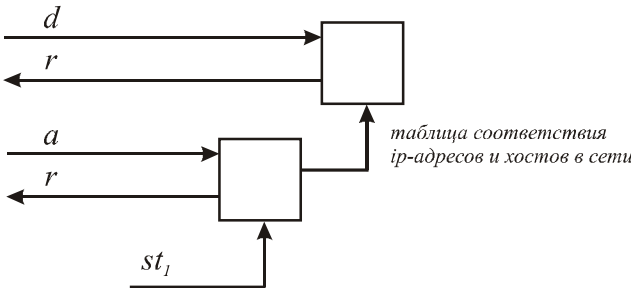

Рис. 5. Простейшая стереотипная схема при атаке на компьютерные сети

От этой стереотипной схемы можно отойти, вводя, например, еще один параметр – номер порта, по которому идет попытка соединения. То есть отдельный компьютер в сети не имеет своего IP-адреса. Адреса в сети как бы «размыты». Данное техническое решение не столько сложно в реализации, сколько нестандартно. Никаких противоречий в работе служб при такой настройке не будет, хотя настроить «стандартное» оборудование на такую работу, конечно, невозможно. Исследование теперь возможно только в рамках новой стереотипной схемы – предположении о взаимнооднозначном соответствии между номером порта отдельного хоста и IP-адресом в сети (st_2) (рис. 6).

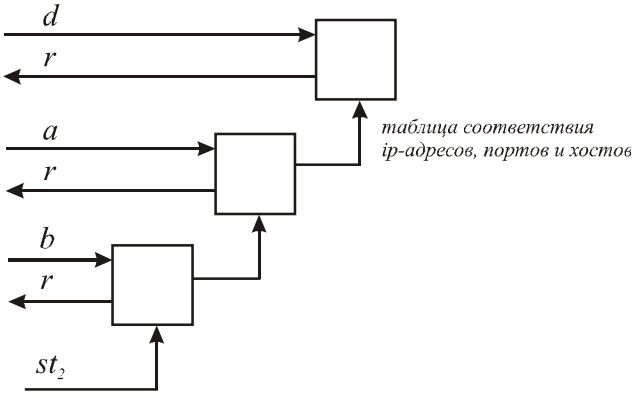

Рис. 6. Новая стереотипная схема при атаке на компьютерные сети

В этом примере, как и в предыдущем, субъект может исследовать черный ящик, только если обратная связь (r) является информативной, т. е. канал контроля выбран правильно. Можно настроить файрвол и запретить сканирование в сети – это будет равносильно тому, что, как и в предыдущем примере, на экране (для ввода пароля, например) не будут отображаться символы. Исследование здесь будет невозможно, а значит, будет необходимо искать новый канал обратной связи. Однако можно поступить и иначе: в предыдущем примере на экране отображаются именно вводимые символы, а реально в системе записываются другие. В случае с атакой на сеть аналогом является такое действие, когда вместо файрвола ставится HoneyPot и выполняется имитация хостов по IP-адресам, которых на самом деле нет. Исследование системы в этом случае было бы гораздо сложнее. Эта сложность объясняется тем, что здесь уже наблюдается неинформативность самой информативной обратной связи. Чтобы это понять, необходимо учитывать, что поиск такого информативного канала – это тоже процесс исследования, который можно представить в виде такого же черного ящика. То есть исследование идет в два этапа.

Затраты на исследования. Основной ресурс, затрачиваемый на исследование, – это время. Ориентируясь на этот показатель, можно говорить о возможности исследования противником системы и совершения им адекватных действий. Оценить это время можно, конечно, только экспериментальным путем. Затраты времени могут быть бесконечно большими (нарушитель воспринимает процессы в системе как хаотичные и не может установить взаимосвязи) или предельно малыми (последовательный анализ черного ящика с точно определенными параметрами).

Как принято в анализе систем безопасности, будем ориентироваться на наихудший для защищающегося случай (являющийся предельно оптимистичным вариантом для атакующего), когда субъект, исследующий систему, затрачивает предельно мало времени, т. е. точно знает параметры и диапазон входных и выходных значений каждого черного ящика. И (что очень существенно) не затрачивает время на поиск самих черных ящиков.

Как уже упоминалось выше, когда речь шла об информативной обратной связи, исследование может проходить в несколько этапов. Например, в случае подбора пароля (назовем это действие a), если нет информативной обратной связи, то необходимо ее найти (действие b). Кроме того, для получения информативной обратной связи по действию b, возможно, необходимо исследовать еще одну систему – действие c:

$$c \to b \to a.$$

Эту последовательность можно продолжать бесконечно. То есть можно также бесконечно склонять исследователя к поиску информативной обратной связи, без которой исследование невозможно.

На каждое действие необходимо затратить некоторое время. Обозначим его как t_x:

$$c \to b \to a.$$

$$T_c\, t_b\, t_a$$

В свою очередь, время, затрачиваемое на каждое действие, есть произведение количества итераций, которые необходимо свершить на время каждой итерации:

$$t_x = n_x \cdot \Delta t_x .$$

При поиске информативной обратной связи время итерации будет кратно времени исследования системы на более «низком» уровне:

$$\Delta t_b \propto t_a ,$$

$$\Delta t_c \propto t_b .$$

То есть

$$t_b = n_b \cdot n_a \cdot \Delta t_a \cdot k ,$$

где k – это коэффициент (больший единицы), который характеризует время, затрачиваемое на «переориентирование» между исследованием двух систем. Однако мы будем считать его равным единице, так как рассматриваем максимально пессимистичный для защищающегося вариант. Полное время, затрачиваемое на исследование, равно времени исследования первой системы, т. е. время первого действия

$$T = t_c = n_c \cdot n_b \cdot n_a \cdot \Delta t_a .$$

Это может показаться парадоксальным, так как действие *c* совершается первым. Но этот процесс неразрывен и действие *c* заканчивается тогда, когда исследована вся система. Нельзя говорить о получении информативной обратной связи, пока не получен конечный результат. Возвращаясь к примеру с паролем, это можно проиллюстрировать следующим образом. На экране отображаются не те символы, которые вводятся, т. е. необходимо искать их в другом месте (действие *b*). Можно анализировать данные в памяти, сигналы, передаваемые в сеть, прерывания процессора и т. д. И каждый раз для проверки информативности обратной связи необходим возврат к подбору пароля (действие *a*). И только когда пароль уже подобран, действие *b* будет закончено.

Возьмем три очень простых черных ящика с взаимнооднозначным соответствием между входами и выходами (единственный параметр). Входов у каждого ящика 10; время, затрачиваемое на итерацию по последнему ящику – 1 мин. Тогда полное время, необходимое на исследование системы (оптимистичный вариант) равно

$$T = (10-1)\cdot(10-1)\cdot(10-1)\cdot 1 \text{ мин} = 729 \text{ мин}.$$

Снижение риска и издержек в системах безопасности. Как уже было показано, в качестве прикладной области защиты от исследования можно рассматривать снижение риска в системах безопасности или издержек, связанных с ее построением. Риск от преднамеренных атак можно снизить путем затруднения исследования системы безопасности со стороны нарушителя. Увеличивая время, необходимое на атаку, можно снизить риск вплоть до нуля (если время на исследование несоразмерно велико, как, например, в существующих криптографических алгоритмах с открытым ключом). Делается это путем поиска стереотипных схем и отхода от них при организации процессов в системе. Введя такую базу путей отхода от стереотипных схем, можно рассматривать их как параметры при постановке задачи оптимизации риска от преднамеренных атак с учетом издержек на построение системы безопасности.

Для поддержки данных технологий при проектировании систем безопасности и продвижении их на рынок разрабатывается программа автоматизированного проектирования. Она имеет по каждому классу атак (атаки по акустическому каналу, социальной инженерии, сетевые атаки и т. д.) динамичную базу стереотипных схем (рис. 7) и по каждой стереотипной схеме множество вариантов приведения ее в диссонанс.

База стереотипных схем, конечно, не статична. Специалист по безопасности может ее пополнять и сам. После этого он исключает из списка неприемлемые для него процедуры приведения стереотипных схем в диссонанс (экономически дорогие, нецелесообразные с точки зрения реализации, неэтичные с его точки зрения) и по оставшимся процедурам программа рассчитывает их оптимальную комбинацию с точки зрения снижения риска.

Рассмотрим простейший вариант. Допустим, что при проектировании известны n стереотипных схем атаки. Известны также m способов приведения стереотипных схем в диссонанс. О каждом j-м способе приведения в диссонанс известно, что его эффективность против i-й стереотипной схемы атаки определятся числом c_{ij}, $i = 1,\ldots, n, j = 1, \ldots, m$, а уровень затрат ресурсов на его реализацию – числом $r_j, j = 1, \ldots, m$. В этом случае задача формирования эффективного набора способов приведения

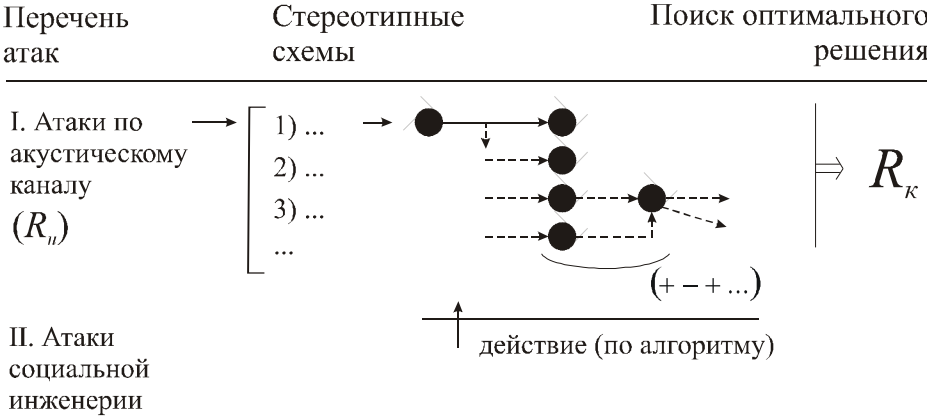

Рис. 7. База стереотипных схем автоматизированной системы проектирования систем безопасности

стереотипных схем в диссонанс может быть формализована в виде известной задачи о рюкзаке:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}x_j \to \max,\ \sum_{j=1}^{m} r_j x_j \le R,$$

или, альтернативно, в виде

$$\sum_{j=1}^{m} r_j x_j \to \min,\ \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}x_j \ge C,$$

где R – имеющийся запас ресурсов на реализацию системы; C – минимальный требуемый уровень эффективности; x_i – переменная принятия решения, равная единице, если i-й способ приведения стереотипных схем в диссонанс включается в формируемый набор, и равная нулю в противном случае. Решение данной задачи является чисто технической проблемой.

В более сложных случаях существует не один ресурс, затрачиваемый на реализацию защиты, и эффективность определяется не одним числом (или вообще не числом). Более того, возможны конфликты между способами защиты, когда использование одного способа исключает или изменяет эффективность применения другого. Возможно также, что эффективность и затраты ресурсов одного и того же способа защиты будут разными для различных способов атаки. Все это может значительно усложнить постановку задачи выбора эффективного варианта, приводя к нелинейным многокритериальным задачам оптимизации с разношкальными переменными и алгоритмически заданными функциями. Решение такой задачи уже не является чисто технической проблемой, но, тем не менее, вполне может быть осуществлено с помощью современного алгоритмического аппарата оптимизации [2].

Библиографический список

1. Эшби, У. Р. Введение в кибернетику / У. Р. Эшби. М. : КомКнига, 2006.

2. Семенкин, Е. С. Метод обобщенного адаптивного поиска для синтеза систем управления сложными объектами / Е. С. Семенкин, В. А. Лебедев. М. : МАКС Пресс, 2002.

E. S. Semenkin, M. A. Styugin

PROTECTION AGAINST INVESTIGATION AND APPLICATION IN SECURITY SYSTEMS

Informational interaction of a violator and a protected system in the form of stereotypic investigation schemes is considered. The attack effectiveness decreasing method based on artificial increase of the system diversification is suggested. Security systems design automation problem is described.

Keywords: informational interaction with a violator, stereotypic schemes, risk reducing in security systems.

УДК 004.056

И. А. Капчинский, П. В. Ковалев, А. Н. Лайков, С. Н. Гриценко

К ВОПРОСУ ФОРМИРОВАНИЯ МУЛЬТИВЕРСИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С УЧЕТОМ РЕСУРСНЫХ ОГРАНИЧЕНИЙ

Рассматривается методология мультиверсионного программирования, которая обеспечивает гарантию того, что ошибки одной из версий программного обеспечения не приведут к нарушению процесса управления сложными объектами, для которых характерны жесткие требования по надежности и автономности функционирования.

Ключевые слова: оптимизация, надежность, мультиверсионное программирование.

Проблеме формирования программных комплексов (ПК), проектируемых на основе принципов программной избыточности, в настоящее время уделяется значительное внимание. Проблематика проектирования программных комплексов с использованием методологии мультиверсионного программирования рассматривалась в работах А. Авижиениса, Н. Ашрафи, О. Бермана, М. Катлер, Дж. Ву, К. Яо, Р.К. Скотта, Д. Мак Аллистера, К. Е. Гросспитча и мн. др. [1–5]. Разрабатываются новые методы оптимизации версионного состава программного комплекса, новые системы формирования структуры программного комплекса, однако не достаточно внимания уделяется разработке методик формирования структуры мультиверсионного программного комплекса с учетом временных и ресурсных ограничений [1]. Основной задачей формирования мультиверсионного программного обеспечения является оптимизация версионного состава программного комплекса. В качестве критерия оптимизации обычно выбирают надежность комплекса.

В научных исследованиях, например, в работе [2] уже рассматривалось введение ограничений на ресурсы и время выполнения программы, но предложенный алгоритм требует больших вычислений и сложен в реализации. Кроме того, если временные ограничения вводятся