

клавиатурой в целях безопасности стандартная клавиатура блокируется.

VII Выводы

Проблема перехвата информации с помощью кейлоггеров стоит довольно остро. В мире существуют сотни подобных программ, которые могут быть несанкционированно установлены без ведома пользователя ПК. Многие вирусы и троянские программы имеют в своем составе модули для перехвата с клавиатуры. По итогам обзора можно сделать вывод, что существует комплексный подход, который позволит защитить персональные компьютеры от угроз данного вида. PrivacyKeyboard™ обеспечивает защиту от продуктов-шпионов большинства типов, причем делает это эффективнее других программ, которые используют сигнатурные базы для анализа.

Разработчиком программы PrivacyKeyboard™ является ООО "Центр информационной безопасности" (г. Запорожье, Украина). Доступна бесплатная версия для ознакомления, скачать которую можно по адресу: <http://www.bezpeka.biz/download.html>.

Литература: 1. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999. 2. «2001 AMA Survey: Workplace Monitoring & Surveillance: Summary of Key Findings» American Management Association http://www.amanet.org/research/pdfs/ems_short2001.pdf. 3. «Computer And Internet Surveillance in the Workplace: Rough Notes». Andrew Schulman, Chief Researcher, Privacy Foundation, US, 2001-2002 <http://www.sonic.net/~undoc/survttech.htm>. 4. «The Extent of Systematic Monitoring of Employee E-mail and Internet Use» Andrew Schulman, Chief Researcher, Privacy Foundation, US, 2001-2002 <http://www.sonic.net/~undoc/extent.htm>.

УДК 638.235.231

МОДЕЛЬ УГРОЗ, РЕАЛИЗУЕМЫХ АППАРАТНЫМИ РЕСУРСАМИ КОМПЬЮТЕРНЫХ СИСТЕМ

Валерий Горбачёв, Владимир Степаненко, Тарас Гриценко

Харьковский Национальный технический университет радиоэлектроники

Аннотация: Предлагается модель компьютерной системы, учитывающая угрозы реализуемые аппаратными ресурсами компьютерных систем.

Summary: In this clause the model of computer system which is taking into account threats sold hardware resources of computer systems is offered.

Ключевые слова: Информация, компьютерная безопасность, доступ.

Введение

В теории компьютерной безопасности формальное моделирование политики безопасности (ПБ) является одним из методов, который позволяет описывать различные аспекты безопасности и обеспечивать средства защиты формально подтвержденной алгоритмической базой.

Успешная разработка модели безопасности зависит от качества модели самой компьютерной системы (КС), от того, насколько полно удалось учесть все архитектурные особенности последней, а также угрозы компьютерной безопасности.

В работе предлагается субъектно-объектная модель аппаратных ресурсов КС [1, 2], охватывающая такой класс угроз, как аппаратные закладки (АЗ) [3].

I Основная часть

Определим АЗ как электронный компонент в интегральном исполнении, встроенный в интегральную схему при её проектировании и производстве, или выполненный в виде отдельной интегральной схемы и создающий угрозу безопасности информации своими не специфицированными функциями. В первом случае закладка является частью стандартного электронного компонента и изменяет его предполагаемые структуру и функции, во втором – сама является не специфицированным компонентом КС и изменяет предполагаемые структуру и функции самой КС. В работе будут рассмотрены АЗ, которые используют штатные каналы КС для передачи информации. В работе не будут рассматриваться все виды АЗ,

использующие в качестве каналов передачи информации каналы ПЭМИН.

Модель КС, связанная с реализацией ПБ и включающая модель угроз, реализуемых АЗ, во-первых, может быть абстрагирована с помощью понятий: объект, субъект, доступ и операции для пары «объект-субъект» [1]; во-вторых, в её основу может быть положена аксиома [1]: все вопросы безопасности информации описываются доступами субъектов к объектам.

Вышеупомянутым абстрактным понятиям поставим в соответствие следующие физические представления в среде КС.

Объект (O_j) – часть ресурсов системы, доступ к которым может контролироваться. Например, файлы, части файлов, программы, различные электронные компоненты (в том числе материальные носители информации).

Субъект (S_i) – элемент, способный осуществить доступ к объекту. Будем рассматривать такой элемент, как пару: ресурсы и доступ.

Доступ – категория субъектно-объектной модели, описывающая процесс выполнения операций субъектов над объектами. Множество возможных операций субъектов над объектами в системе будем обозначать через R . Очевидно, если операция доступа реализуется АЗ, то она должна иметь аппаратно-программную поддержку в виде некоторого канала.

Рассматривая АЗ как некоторый тип субъекта, который способен осуществить НСД, отметим следующие ее особенности.

Во-первых, АЗ, являясь программно-аппаратными ресурсами КС, имеет одну и ту же среду существования, что и объекты. Более того, в пассивном состоянии АЗ является частью некоторого объекта.

Во-вторых, угрозы информации в КС могут исходить только от активного субъекта – АЗ, который в текущий момент времени владеет функцией управления ресурсами и, в общем случае, способный изменять состояния объектов.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты. Одним из результатов воздействия субъекта на объект могут быть порожденные в КС другие субъекты (или состояния системы), которые представляют угрозу для безопасности информации. В данном случае речь идет об инициализации АЗ и переводе ее в активное состояние.

Пары (S_i, O_j) связываются множеством разрешенных, с точки зрения системы защиты информации (ЗИ), операций R_i . Это множество определяется ПБ и является подмножеством всего множества R возможных операций для каждой пары. В то же время, пары (S_i, O_j) могут связываться множеством запрещенных, с точки зрения ПБ, операций R_k . Задачей ПБ является контроль и блокирование выполнения операций из множества R_k . Очевидно, что $R = R_i \cup R_k$.

Если учесть предположение о том, что АЗ может воспользоваться штатным каналом КС, т. е. каналом, который поддерживает операцию доступа из множества R_i , то $R_i \cap R_k = \emptyset$.

Здесь уместно рассмотреть понятие пользователя (злоумышленника). Он всегда связывается с частью системы (объектом), на которую направлены все его действия. Очевидно, что пользователь (злоумышленник) – это внешний по отношению к системе субъект, который может быть источником угроз. Рассматривая это понятие в рамках объектно-субъектного подхода, отметим следующие важные свойства пользователя (злоумышленника):

1. пользователь (злоумышленник) воспринимает объекты и получает информацию о состоянии КС через те активные субъекты, доступ к которым он имеет; таким образом, злоумышленник должен инициализировать субъект – АЗ и перевести его в активное состояние;

2. обобщая понятие субъекта КС, определенное выше, на пользователя (злоумышленника) отметим, что пользователь КС является внешним субъектом или субъектом внешней среды КС.

Анализ свойств субъектов, таких как АЗ и злоумышленник позволяет сделать следующие выводы относительно требований к модели КС, связанной с реализацией модели безопасности КС: необходимость учета возможностей субъектов изменять свойства и архитектуру КС; декомпозиция КС на субъекты и объекты должна быть априорно заданна и фиксирована; в любой заданный момент времени множество субъектов КС не пусто (в противном случае соответствующие моменты времени исключаются из рассмотрения и рассматриваются отрезки с нулевой мощностью множества субъектов).

Будем обозначать множество объектов в системе обработки данных через O , а множество субъектов в этой системе через S . Как было отмечено выше, каждый субъект в пассивном состоянии является объектом системы, поэтому $S \subseteq O$. Модель КС, связанную с реализацией ПБ и включающую модель угроз, реализуемых АЗ, можно представить в виде ориентированного размеченного графа, вершинами которого являются субъекты (S_i) и объекты (O_j). Каждой дуге такого графа поставлена операция доступа r_i ; $r_i \subseteq R$. Такая концептуальная модель представлена на рис. 1.

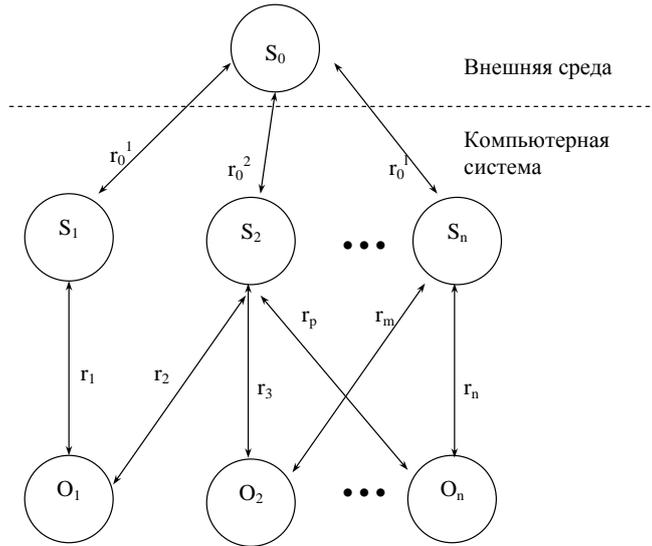


Рисунок 1 – Субъектно-объектная модель аппаратных ресурсов КС

Формализуем операцию доступа субъекта к объектам. В первую очередь специфицируем механизм порождения новых субъектов. Работу данного механизма можно продемонстрировать на следующем примере. Допустим некоторому процессу, протекающему в КС, необходимо прочитать определённые данные с накопителя на жёстком диске (HDD). Для этого процессор в некоторый момент времени (t), обращается к контролеру жесткого диска (IDE controller) с соответствующим запросом. В момент времени (t), процесс, инициирующий получение данных, является субъектом, а контроллер жёсткого диска объектом. При этом субъект изменяет содержимое внутренних регистров объекта, тем самым, изменяя его свойства и порождая новый субъект в КС. В следующий момент времени ($t+1$), порождённый субъект обращается к следующему объекту (непосредственно к контроллеру, управляющему механикой жёсткого диска) и передаёт ему соответствующие запросы, изменяя его структуру и тем самым, порождая новый субъект и т. д.

Для формализации механизма порождения новых объектов воспользуемся следующими определениями [1].

Определение 1. Объект O_i называется источником для субъекта S_k , если существует субъект S_j , в результате воздействия которого на объект O_i в компьютерной системе возникает субъект S_k .

Определение 2. Субъект S_j , порождающий новый субъект из объекта O_i , в свою очередь, называется активизирующим субъектом для субъекта S_k ; S_k назовем порожденным объектом.

Теперь введем обозначение: $Create(S_j, O_i) \rightarrow S_k$, которое означает, что из объекта O_i порожден субъект S_k при активизирующем воздействии субъекта S_j . $Create$ назовем операцией порождения субъектов (рис. 2).

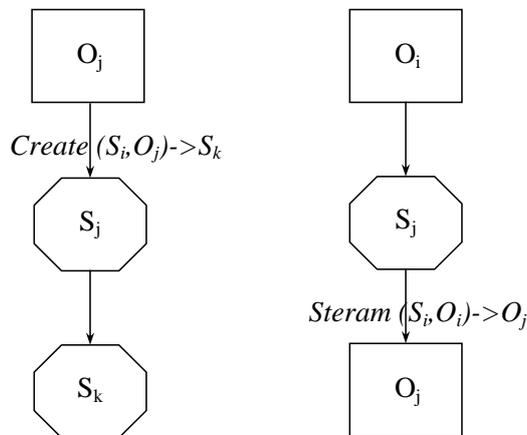


Рисунок 2 – Интерпретация операции порождения субъекта и понятия потока с помощью графа

Операция Create задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов с пустым множеством. На физическом уровне операция Create означает, что субъект S_j , обладая управлением и ресурсами, может передать S_k часть ресурсов и управление (активизация). Заметим также, что в КС действует дискретное время и фактически новый субъект S_k порождается в момент времени $t+1$ относительно момента t , в который произошло воздействие порождающего субъекта на объект-источник.

Очевидно, что операция порождения субъектов зависит как от свойств активизирующего субъекта, так и от содержания объекта-источника.

Считаем, что если $Create(S_j, O_i) \rightarrow \text{NULL}$ (конструкция NULL далее обозначает пустое множество), то порождение нового субъекта из объекта O_i при активизирующем воздействии S_j невозможно.

Свойство АЗ быть активной реализуется не только в выполнении действий над объектом с целью создания нового субъекта, но и с целью чтения или записи данных в объект. В общем случае необходимо отметить, что поскольку объекты КС по определению являются пассивными, то для выполнения аппаратной закладкой всех описанных выше действий, необходимо существование потоков информации от субъекта к объекту (в противном случае невозможно говорить об изменении объектов). Так как данный поток иницируется и реализуется субъектом – АЗ, это означает, что операция порождения потока локализована в субъекте – АЗ и отображается состоянием его функционально ассоциированных с ней объектов.

Поток информации между объектом O_m и объектом O_j всегда должен быть связан с некоторой операцией над объектом O_j , реализуемой субъектом S_j и зависящей от O_m . Поток информации от объекта O_m к объекту O_j обозначим как $Stream(S_j, O_m) \rightarrow O_j$. При этом будем выделять источник (O_m) и получатель (приемник) потока (O_j). Из данного определения также следует, что поток всегда иницируется (порождается) субъектом.

Очевидно, что с помощью приведенного определения операции Stream над объектами O_m и O_j формализуется операции доступа субъекта S к объекту O_j для записи в него данных из O_m или наоборот. Отметим, что в частном случае операция Stream может создавать новый объект или уничтожать его. Операции порождения субъектом потока, а также порождения субъектов назовем операциями доступа.

Понятие доступа является одним из основополагающих в теории защиты информации, поскольку разрешение или запрет доступа для заданных множеств субъектов и объектов в конечном итоге определяет безопасность КС.

Выводы

В работе предложена субъектно-объектная модель аппаратных ресурсов КС, охватывающая такой класс угроз, как аппаратные закладки (АЗ), а также определена операция доступа для АЗ. Полученные результаты могут быть использованы для разработки модели безопасности КС, включающей средства защиты от угроз, реализуемых АЗ.

Литература: 1. Девянин П. Н., Михальский О. О., Правиков Д. И., Щербаков А. Ю. и др. Теоретические основы компьютерной информации. – М.: Радио и связь, 2000. –189 с. 2. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.452., ил. 3. Горбачев В. А., Степаненко В. В. Сертификация периферийных устройств компьютерных систем.// Радиотехника: сб. научн. трудов. Выпуск 134.-Харьков: ХНУРЭ, 2003. С. 206 – 209.

УДК 681.3

СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК ДЛЯ ЗАЩИТЫ ИНТРАНЕТ

Вячеслав Шорошев

НИИ НАВД Украины

Аннотация: Система обнаружения атак – перспективная технология защиты информационных ресурсов сетей Intranet, которая получает все более широкое распространение в ведущих странах мира и в Украине. Даются рекомендации для Intranet – что, от чего, от кого, как и чем защищать. Также даются практические советы по критериям оценки и выбора систем обнаружения атак и их краткий обзор.

Summary: System of detection of attacks - perspective technology of protection of information resources of networks Intranet, which receives more and more wide circulation in the conducting countries of the world and on Ukraine. The recommendations for Intranet - that are given, from what, from whom, as well as than