Эссе.

«Модели политики безопасности»

Выполнила студентка 916 гр.
Кыдырова А. Е.

"По-настоящему безопасной можно считать лишь систему,которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, - но и в этом случае сомнения не оставляют меня".

Юджин Х. Спаффорд

Предисловие.

В этой работе рассказано о строении, развитии и использовании моделей политики безопасности для автоматизированных информационных систем (AIS), которые используются для защиты секретной информации от запретного разглашения, изменения, потери или разрушения.

Политика безопасности и модели политики безопасности обычно обсуждаются вместе, потому что часто трудно определить, где заканчивается политика безопасности и начинается модель.

История.

Национальный комитет компьютерной безопасности (NCSC) был основан в 1981 г. и получил свое нынешнее название в 1985 г. Главной его целью является содействовать широкому распространению защищенных AIS. С 1983 по 1988 год Министерство обороны США и Национальный комитет компьютерной безопасности разработали систему стандартов в области компьютерной безопасности, которая включает более десяти документов. Этот список возглавляют "Критерии оценки безопасности компьютерных систем" (TCSEC), которые по цвету обложки чаще называют "Оранжевой книгой". В 1995 году Национальный центр компьютерной безопасности США опубликовал "Пояснения к критериям безопасности компьютерных систем", объединившие все имеющиеся на тот момент дополнения и разъяснения к "Оранжевой книге".

Цель.

Потребность в безопасности информации обычно делят на четыре главных пункта:
конфиденциальность: контроль доступа к информации;
сохранность: контроль за изменением информации и использованием ресурсов;
отчетность: учет лиц, имевших доступ к информации;
доступность: обеспечение быстрого доступа к информации и ресурсам.

Каждый пользователь должен решить, что безопасность значит для него. Например, службы безопасности больше заботятся о конфиденциальности, коммерческие фирмы о сохранности и отчетности имущества, а телефонные компании о доступности. Конфиденциальность важна также и в коммерческих областях: финансовая и личная информация должна быть закрыта для посторонних лиц.

Угрозы конфиденциальности данных реализуется в том случае, если информация, представляющая коммерческую или какую-то другую тайну становится доступной лицам, не имеющих прав на обладание этой информации. Как правило, утечка информации происходит в результате несанкционированного доступа к данным путем подключения злоумышленника к системе на правах легального пользователя, хотя такая информация может быть получена путем технических средств шпионажа на этапе ввода данных, анализа электромагнитного излучения, или косвенным способом – путем наблюдения за трафиком при обмене сообщениями без доступа к их содержанию.

Угроза достоверности данных включает в себя несанкционированное удаление, добавление или модификацию информации в системе или не санкционированный запуск процессов приводящих к искажению данных в системе. Такие действия могут привести к серьезным последствиям, в результате которых предприятию будет нанесен материальный урон. Примером таких действий в банковском деле может, например, служить незаконный перевод средств с одного счета на другой.

Угроза отказа доступа к данным возникает всякий раз, когда в результате преднамеренных действий злоумышленников легальный пользователь не получает доступа к легально выделенным ему ресурсам. Примером реализации таких угроз может служить несанкционированный захват ресурсов файлового сервера, блокировкой линий связи путем передачи по ним своей информации и т.д. Результатом реализации этой угрозы является невозможность или задержка выполнения легальным пользователем процедур, предусмотренных технологией функционирования предприятия.

Построение эффективной системы защиты от перечисленных угроз является первоочередной задачей системы обеспечения безопасности. Однако выполнение этой задачи невозможно без проведения грамотной и сбалансированной политики безопасности, определяющей совокупность условий получения пользователями доступа к информационным ресурсам.

В основе формальных политик безопасности лежат модели безопасности. Под моделью безопасности будем понимать описание поведения целого класса систем без рассмотрения конкретных деталей их реализации.

Построение формальных политик безопасности должно базироваться на методологии построения моделей безопасности, отвечающей требованиям унификации элементов модели, удобства и однозначности синтаксиса описания, возможности декомпозиции и детализации модели, возможности оценки эффективности системы защиты, программной реализуемости.

В основе моделей безопасности должна лежать объект - субъектная схема взаимодействия компонентов моделируемой системы. Субъектами являются активные элементы, которые могут инициировать запросы ресурсов и использовать их для выполнения каких либо вычислительных заданий. К таким элементам относятся пользователи, процессы, устройства, и т.д., запрашивающие ресурсы системы. Объектами являются пассивные элементы, используемые для хранения или получения информации, например, записи, блоки, страницы, файлы, терминалы, узлы сети и т.д.

Надежная система.

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".
Надежность систем оценивается по двум основным критериям:

- *Политика безопасности* - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные

механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

- *Гарантированность* - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность можно определить тестированием системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться *аудитом*, то есть анализом регистрационной информации.

При оценке степени гарантированности, с которой систему можно считать надежной, центральной является концепция надежной вычислительной базы. *Вычислительная база* - это совокупность защитных механизмов компьютерной системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит административный персонал (например, это могут быть данные о степени благонадежности пользователей).

Основное назначение надежной вычислительной базы - выполнять функции *монитора обращений*, то есть контролировать допустимость выполнения субъектами определенных операций над объектами. Каждое обращение пользователя к программам или данным проверяется на предмет согласованности со списком действий, допустимых для пользователя.

От монитора обращений требуется выполнение трех свойств:

- *Изолированность*. Монитор должен быть защищен от отслеживания своей работы;
- *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов его обхода;
- *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Основные элементы политики безопасности

Согласно "Оранжевой книге", политика безопасности должна включать в себя по крайней мере следующие элементы:

- произвольное управление доступом (метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.);
- безопасность повторного использования объектов (важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора".);
- метки безопасности (метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации.);
- принудительное управление доступом (сопоставление меток безопасности субъекта и объекта.).

Общий алгоритм построения системы защиты.

Алгоритм построения системы защиты заключается в следующем:

1. Неформальное описание компонент (архитектуры) системы и неформальное задание правил политики безопасности.
2. Формализация описания архитектуры исследуемой системы и выработка формальных правил разграничения доступа, реализующих заданную в п.1. политику безопасности.
3. Формальное доказательство соответствия разработанной системе задаваемой политики безопасности.
4. Взаимно-однозначная интерпретация условий выполнения политики безопасности и распределение обязанностей выполнения этих правил между субъектами системы.
5. Выявление требований, которым должна удовлетворять система безопасности для адекватного выполнения возложенных на нее функций.
6. Составление списков существующих средств и механизмов обеспечения информационной защиты, выполняющие требующиеся функции.
7. Оптимальное проектирование: выбор компонент для реализации системы защиты.

Рассмотрим более подробно каждый из шагов алгоритма.

1. Неформальное описание компонент (архитектуры) системы и неформальное задание правил политики безопасности.

Осуществляется обзор, из каких компонент состоит система, как они функционируют. Каким образом осуществляется взаимодействие между компонентами системы: общедоступные или закрытые вычислительные сети, какие сетевые протоколы используются и т.п. Какие системные (в том числе операционные системы) и прикладные программы используются. Как осуществляется обработка информации (в том числе ценной), циркулирующей в системе.

Словесное описание политики безопасности заключается в задании простых правил, выполнение которых позволяет контролировать безопасность. Данные высказывания (словесные утверждения) определяют правильный режим обработки ценной информации в системе, с точки зрения ее владельца или заказчика.

Например: пользователь системы при использовании банкомата при удостоверении своих прав имеет возможность получения доступа к информации о своем счете; кассир за терминалом, установленном в магазине способен только писать некоторую информацию на определенный счет; банковский аналитик через внутренний терминал получает права только на чтение заданного списка документов и т.п.

2. Формализация описания архитектуры исследуемой системы и выработка формальных правил разграничения доступа, реализующих заданную политику безопасности.

Для данной предметной области, пользуясь составленным неформальным описанием системы и политикой управления безопасности, производится формализация этого описания и правил в терминах формальной модели безопасности.

Выявляются объекты и субъекты системы. Объекты группируются по принадлежности к субъектам. Формальная модель позволяют обосновать практическую пригодность системы, определяя ее базовую архитектуру и используемые технологические решения при ее построении. В терминах формальной модели задаются словесные утверждения политики безопасности. Таким образом, строится полная и непротиворечивая формальная модель системы.

3. Формальное доказательство соответствия разработанной системе задаваемой политики безопасности.

Выявляются достаточные и необходимые условия выполнения политики безопасности в терминах формальной модели. Выполняется формальное доказательство выполнимости утверждений модели безопасности. В результате выполнения доказательства выявляются условия обработки ценной информации, при которых требования политики безопасности оказываются выполнимыми.

4. Интерпретация условий выполнения политики безопасности и распределение обязанностей выполнения этих правил между субъектами системы.

Условия выполнения политики интерпретируются для реальной системы и реализуются в виде использования средств и механизмов информационной безопасности и их соответствующей настройки. Для того, чтобы система реально была безопасной, необходимо выполнение двух условий:

- модель безопасности, лежащая в основе разрабатываемой системы защиты была безопасна;
- интерпретация модели безопасности производится корректно (необходимо взаимно однозначное соответствие).

Основываясь на результатах предыдущего этапа, производится распределение функций обеспечения информационной безопасности между субъектами системы. Для каждого субъекта формализуются правила доступа к принадлежащим ему объектам, далее субъект, пользуясь данной информацией, будет осуществлять контроль выполнения правил разграничения доступа.

После этого осуществляется переход к следующему шагу алгоритма.

5. Выявление требований, которым должна удовлетворять система безопасности для адекватного выполнения возложенных на нее функций.

На основе анализа процессов взаимодействия между субъектами системы (исследование информационных потоков), выделяются требования, выполнение которых позволят субъектам системы организовать безопасное взаимодействие между собой и управление потоками, осуществляемыми в системе. Среди этих требований могут быть: авторизация и аутентификация взаимодействующих сторон, криптографическая защита передаваемых данных, использование специальных механизмов при подключении к сетям общего пользования и т.п.

Используя данные, полученные на этапе исследования процессов обработки информации в системе, формулируются требования, необходимые для обеспечения безопасной обработки данных. Среди них могут быть: безопасная инициализация системы,

защищенное резервирование объекта, композиция функций, выполняемых субъектом в атомарно-неделимые и т.п.

Задаются требования. Среди основных требований можно выделить: подсчет хэш-функции, невозможность изменения состояний защитных механизмов в процессе работы системы…

6. Составление списков существующих средств и механизмов обеспечения информационной защиты, выполняющие требующиеся функции.

В результате проделанной работы составляется полный перечень требований, которым должна удовлетворять проектируемая системы защиты для адекватной реализации политики безопасности. Пусть создана идеальная системы защиты, у которой уровень соответствия задаваемой политики безопасности равен 100% (или единице) и, таким образом, уровень обеспечиваемой защищенности также равен единице.

Но на практике, подобные системы строятся из имеющихся в наличии средств и механизмов безопасности. В реальной жизни показатель надежности, защищенности и т.п. никогда не смогут достигнуть 100%. Для выполнения заданных требований используются соответствующие технологии. Данные технологии безопасности (криптография, датчики случайных чисел и другие) могут быть реализованы некоторыми устройствами, аппаратно или программно. Реализация всегда возможна с какой-то степенью достоверности (близкой к единице). Каждое средство реализации обладает рядом важных для нас параметров. Это, прежде всего, стоимость и уровень обеспечиваемой защищенности реализуемой технологии. Создаются списки доступных средств, реализующих требуемую технологию.

Как правильно сформировать систему защиты путем выбора средств из каждого списка решается на следующем шаге алгоритма.

7. Оптимальное проектирование: выбор компонент для реализации системы защиты.

Производится оценка и ранжирование показателей критериев по каждому объекту из списка. В случае невозможности прямого или косвенного измерения величины исследуемого параметра, применяются неформальные методы оценивания, например, методы экспертной оценки. Все объекты ранжируются в соответствии с привлекательностью наиболее важных для проектировщиков параметров. Требования к системе защиты должны быть классифицированы в соответствии с их стратегическими значениями для всей системы. В результате классификации, требования ранжируются и получают определенные веса важности. Составляется целевая функция безопасности, учитывающая показатели по каждому требованию и все этого требования.

Далее необходимо решить задачу оптимального проектирования. Ее решение заключается в выборе такого набора средств защиты, который наиболее оптимально соответствует заданным ограничениям. Чаще всего на практике решаются два вида задач оптимального проектирования. Прямая задача: нахождение максимального достижимого уровня защищенности при заданном ресурсе стоимости и обратная задача: выбор системы с минимальной стоимостью, обеспечивающей необходимый уровень защищенности.

Прямая задача выбора варианта системы, обеспечивающая максимальный достижимый уровень защищенности:

$$\begin{cases} P(p_1, p_2, \ldots, p_l) \to \max \\ C_0 + \sum_{i=1}^{l} \Delta c_i \le C_{\text{доп}} \\ T_{\text{тр}} + \sum_{i=1}^{l} \Delta t_i \le T_{\text{тр}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases} \quad (1)$$

Задача выбора системы с минимальной стоимостью при достижении уровня защищенности заданного параметра:

$$\begin{cases} P(p_1, p_2, \ldots, p_l) \ge P_{\text{доп}} \\ C_0 + \sum_{i=1}^{l} \Delta c_i \to \min \\ T_{\text{тр}} + \sum_{i=1}^{l} \Delta t_i \le T_{\text{тр}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases} \quad (2)$$

Решение задачи оптимального проектирования, чаще всего, представляет собой некоторое подмножество приблизительно равных по качеству вариантов, называемое областью Парето (или областью компромиссов). Если применение численных методов невозможно, то используются неформальные методы поиска оптимальных решений.

Вывод.

Описанная методология позволяет на основе неформального описания системы и правил политики безопасности создать формальную модель процессов, протекающих в исследуемой системе. Формализовать правила политики безопасности и доказать соответствие разработанной модели задаваемым правилам политики безопасности. Доказательство соответствия и интерпретация условий выполнения правил политики безопасности позволяют получить набор требований к системе защиты информации. Безопасное функционирование системы, построенной на основе предложенной модели, гарантируется формальным доказательством основной теоремы безопасности.

Список используемой литературы.

http://www.research.microsoft.com

http://www.quorus.ru/technical/checkpoint/osm/index.htm

http://www.fssr.ru/icccs/1251/smirnov_2000.htm

http://www.melnikoff.com/yuriy/content1.htm

“Requirements and Technology for Computer Security”, W. Lampson, Digital Equipment Corporation, July 1990