Козин Филипп Александрович 015 гр.

Модели Политики Безопасности.

Введение:

С самого начала компьютерной эры одной из основных задач для разработчиков информационных технологий стала задача обеспечения безопасности. Ни одна существующая коммерческая или государственная электронная система не может обходится без защиты собственной информации от несанкционированного доступа. Начиная с 70-х годов прошлого века в мире стали разрабатываться различные концепции и методы защиты информации, что вскоре привело к созданию единообразного подхода к этой проблеме: были разработаны первые политики безопасности.

Политика безопасности – свод формальных правил, определяющих обработку,
распространение и защиту информации.

Модель политики безопасности – формальное представление политики безопасности для определенной системы или класса систем, определяющее методы обработки, распространения и защиты информации.

Общие принципы:

Формальные правила в большинстве моделей определяют следующие требования в порядке важности:

1) Доступность
2)Целостность
3)Конфиденциальность
4)Подотчетность

Каждое из требований отвечает за свою область в модели политики безопасности:

Доступность – требование, отвечающее за доступ к информации, а именно:

- Предоставление доступа легальным пользователям в разрешенных масштабах.
- Предотвращение отсутствия такового.
- Предотвращение от нелегального доступа.

Целостность отвечает за две области:

- Целостность информации – обеспечение защиты информации от нелегальных действий в процессе хранения, обработки и передачи.
- Целостность системы – отсутствие двойственности в работе системы.

Конфиденциальность – требование к защищенности личной и секретной информации, применяется к данным в процессе хранения, обработки и передачи. Является наиболее важным требованием для некоторых типов данных или систем, таких, как секретный ключ или сервер аутентификации.

Подотчетность – требование, по которому любое действие можно было бы проследить от начала и до конца. Позволяет обнаружить нелегальное использование системы, обеспечивает защиту систем от ошибок и восстановление системы в случае их возникновения.

Все эти требования, в конечном счете, и формируют защищенность, которую в каждом отдельном случае следует понимать лишь как определенный набор требований к вышеизложенным целям.

Помимо набора требований одним из важнейших атрибутов модели, непосредственно влияющих на её реализацию, являются предусмотренные в модели

методы контроля за доступом к системе. Большинство защищенных методов контроля за доступом к системе делятся на два класса:

- *Свободный (самостоятельный) контроль за доступом* в систему (Discretionary Access Control) является свободным в том смысле, что владелец или распорядитель информации может самостоятельно менять возможности доступа к своей информации. Характерен для моделей, предназначенных для реализации в коммерческих и научных целях.
- *Мандатный контроль за доступом* (Mandatory Access Control) в систему означает независимость доступности информации от её владельца. Как правило в подобных случаях контроль за доступом реализуется исходя из свойств самой информации и свойств желающего получить к ней доступ согласно независимым от них обоих правилам. Характерен для моделей, предназначенных для реализации в военных и государственных системах защиты.

Строго говоря критерии определения того, к какому классу относится тот или иной метод контроля за доступом, далеко не всегда дают определенный результат, но являются весьма точными для большинства классических моделей политики безопасности.

В 80-х годах под руководством Министерство обороны США (Department of Defense) разработало первый документ, определяющий систему стандартов в области компьютерной безопасности – “Критерии оценки безопасности компьютерных систем”
(The Trusted Computer System Evaluation Criteria), который чаще называют *“Оранжевой книгой”*. В частности этот документ содержит классификацию систем безопасности согласно строгости требований к безопасности, заложенных в их модели политики безопасности. В настоящий момент стандарты компьютерной безопасности определяются более чем десятком документов.

Модель Белла - Ла-Падулы.

Первой моделью системы безопасности стала модель Белла - Ла-Падулы (*Bell-LaPadula model*), созданная в 1973-74 годах в MITRE в городе Белфорде в штате Массачусетс по заказу Военно-Воздушных сил США. В 76 году была дополнена до использования в пределах концепции MULTICS (информационно-вычислительная система с мультиплексированием каналов передачи данных), в 86 году адаптирована для использования в сетевых системах. На протяжении 70-х годов оставалась главной моделью политики безопастности и оказала значительное влияние на формирование TCSEC. В изначальном варианте модель Белла – Ла-Падулы предусматривала возможность только мандатный контроль за доступом.

Модель полностью описывается следующими составляющими:

1)*Элементы* - составные части системы:

- Субъекты - активные объекты (пользователи, программы)
- Объекты – пассивные объекты (пароли, иные данные)
- Атрибуты доступа – всевозможные действия субъектов над объектами: чтение, изменение, дополнение (без чтения!), поиск, исполнение. Возможны различные вариации и дополнения к имеющемуся списку.
- Уровни безопасности – определенное дополнение к субъектам и объектам, определяющее возможность их взаимодействия. У объекта только один уровень безопасности. Уровень безопасности субъекта делится на 2 части:
  - Уровень доступа определяет возможность доступа субъекта к определенному классу информации: Совершенно секретно > секретно >

конфеденциально > для общего пользования. Субъект с высоким уровнем доступа имеет доступ ко всем последующим уровням доступа.

- Категории доступа – возможные области доступа, в отличие от уровней доступа субъект может обладать несколькими категориями доступа из имеющихся и не имеет доступа к иным категориям.

2)*Компоненты* - структуры, полностью описывающие состояние системы:

- Текущие состояние доступа составляют тройки субъект-объект + атрибуты доступа.
- Иерархия объектов определяет отношения главный-последующий в структуре объектов, состоит из корневых деревьев и изолированных точек. Главный объект имеет уровень допуска >= уровню допуска последующего объекта.
- Матрица допустимого доступа:
  Субъекты по строкам, объекты по столбцам, текущие состояния доступа на соответствующих пересечениях.
- Функция уровня определяет уровень доступа для субъектов и объектов.

3) *Свойства*

Система работает по принципу текущее состояние -> запрос -> решение -> последующее состояние. Работа системы регулируется набором свойств и правил.

Свойство Простой Безопастности (Simple Security Property): если в текущем состоянии доступа присутствует тройка субъект-объект-атрибуты доступа и атрибуты доступа разрешают просмотр, то уровень доступа субъекта доминирует над уровнем доступа объекта, т. е. нельзя просматривать объекты более высокого уровня.

Свойство ‘*’: нельзя записывать в объекты более низкого уровня.

Свойство самостоятельной защиты (Discretionary Security Property): все действия субъекта над объектом ограниченны матрицей допустимого доступа. В то время, как первые два свойства определяют по существу все возможные направления передачи информации, DS свойство определяет то, как контролируется доступ в систему в целом - мандатный контроль за доступом.

4) Правила

Правила определяют переходы системы из текущего состояния в последующее (т.е. задают всевозможные пары запрос-решение с положительным решением), в базовом наборе было 8 правил, далее список правил расширялся. Правила, добавленные в MULTICS модели позволили изменять уровень безопасности объекта и добавить возможность свободного контроля за доступам в систему.

5)Теоремы и доказательства подтверждающие защищенность системы. Основная теорема беозпастности: если начальное состояние системы является безопасным и все последующие переходы системы из одного состояния в другое являются безопастными, то система полностью безопастна.

В целом модель Белла - Ла-Падулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Еще из недостатков модели стоит отметить невозможность передачи информации от более высокого уровня к нижним, поскольку это значительно снижает возможности управления субъектами. В рамках модели возможно создание незащищенных систем.

Модель Биба.

Последующим расширением модели Белла - Ла-Палуды стала модель Биба (Biba Model), разработанная в 1977 году. Целью создания модели стало добавление

в модель Белла - Ла-Палуды целостности. Задача была реализована путем добавления к субъектам и объектам уровня целостности и запрета общения субъектов и объектов разных уровней.

Для дополнительного управления целостностью введены понижающие водяные знаки (нарушающие запрет на общение):

- Если субъект читает объект более низкого уровня, то его уровень целостности снижается до уровня целостности объекта.
- Если субъект дополняет объект более высокого уровня, то уровень целостности объекта снижается до уровня целостности субъекта.

Модель не только несет в себе достоинства и недостатки модели Белла – Ла-Палуды, но и добавляет собственные: основной недостаток модели состоит в том, что введение уровней целостности только ограничивает возможности доступа субъектов к объектам, создавая либо значительную изоляцию между уровнями целостности, либо после определения уровней целостности этот уровень может только понижаться, что само по себе лишает его управляемости, и как следствие функциональности. Область применения модели Биба так же не выходит за пределы военных организаций.

Модель Кларка-Вилсона.

Десять лет спустя была разработана модель Кларка-Вилсона (Clark-Wilson model), обеспечивающая требование целостности более практичным методом. В 1993 году модель была расширена и включила в себя разделение обязанностей. Основной областью применения данной модели является коммерция, в частности банковское дело.

В основе концепции модели стоят 2 принципа:

- Внутренняя целостность – свойства внутреннего состояния системы, достигаемые посредством “Правильных соглашений”.
- Внешняя целостность – взаимодействие внутреннего состояния системы с внешнем миром, реализуемая посредством разделение обязанностей.

Модель реализована посредством набора правил, и, в отличие от предыдущих моделей, не является математически формализованной моделью. Также субъекты теперь не имеют прямого доступа к объектам, между субъектом и объектом находится “слой” программ, которые обладает доступом к объектам. Контроль за доступом к системе является свободным.

Контроль за доступом к данным разделен на 2 группы:

- Определяются операции доступа, которые можно производить над каждым типом данных (только определенный набор программ имеет доступ к определенным объектам).
- Определяются операции доступа, которые могут быть произведены определенным субъектом (субъект имеет доступ только к определенному набору программ).

Все данные в модели Кларка-Вилсона разделены на 2 класса:

- *Необходимый элемент данных (CDI)*
- *Спонтанный элемент данных (UDI)*

Далее устанавливается набор правил, регулирующих взаимодействие с обоими типами данных (Certification Rules):

- Все начальные процедуры проверки (IVP) должны убедиться в том, что все CDI находятся в достоверном состоянии во время работы IVP.
- Все процедуры изменения (TP)должны быть сертифицированы, чтобы быть достоверными, т.е. все достоверные CDI должны переходить в достоверные CDI, причем каждая процедура изменения имеют право на доступ только к определенному набору CDI.

- Правила доступа должны удовлетворять всем требованиям разделения обязанностей.
- Все процедуры изменения должны быть записаны в доступный только-на-добавление журнал.
- Любая процедура изменения, получившая на вход UDI должна либо преобразовать его в CDI, либо отменить операцию.

Этот набор правил позволяет обеспечить работу с данными в таком режиме, когда полностью обеспечена безопасность и подотчетность переходов в системе. Главное достижение этих правил по сравнению с моделью Биба – разделение процедур по проверке целостности и процедур изменения. Позволяет предотвратить или исправить большинство нелегальных действий, совершаемых изнутри коммерческой организации.

Для усиления защиты в модель Кларка-Вилсона был введен еще один набор правил (Enforcements Rules):

- Система должна поддерживать и защищать список (Tpi:CDIa,CDIb,...), сопоставляющий TP и CDI и сертифицирующий доступ к ним.
- Система должна поддерживать и защищать список (UserID,Tpi:CDIa,CDIb,...), определяющий, какие TP пользователь может выполнять.
- Система должна аутентифицировать каждого пользователя, запрашивающего исполнение процедуры изменения.
- Только допущенный к сертификации правил доступа для TP субъект может изменять соответствующие записи в списке. Этот субъект не долен иметь прав на исполнение данного TP.

Этот свод правил обеспечивает дополнительную защиту для процедур изменения.

Несмотря на видимое отсутствие недостатков модель Кларка-Вилсона зачастую не может быть реализована в жизни в полном объеме по причине отсутствия единой математической модели. Основная сложность состоит в невозможности точного сопоставлении реальной системы правил работы банка значительного размера с моделью, поскольку в модели не заложены методы реализации наборов правил.

Модель “Китайская стена”

В 1989 году Бювером и Нэшем была разработана модель “Китайская стена”, поначалу задумывавшаяся как противоположность БЛП подобным моделям, но в последствии это утверждение было опровергнуто. Основная область применения модели – финансовые аналитические организации, для которых важно избежать конфликта интересов.

Модель состоит из следующих компонентов:

- Субъекты – аналитики.
- Объекты – данные на одного клиента.
- Набор данных компании – ставит в соответствие каждому объекту его набор данных компании.
- Классы конфликта интересов – компании – соперники. (присоединяются к каждому объекту конфликтующих компаний)
- Метки – набор данных компании и классы конфликта интересов.
- Оздоровляющая информация – не имеет ограничений к доступу.

Свойства:

- Свойство простой безопасности: доступ разрешается, если только объект свободен, т. е. только если все пытающиеся получить доступ объекты

принадлежат к одному набору данных компании или если не принадлежат к одному классу конфликта интересов.

- ‘*’ –свойство: субъекту будет запрещен доступ на запись к объекту только если у него нет доступа на чтение любого иного объекта, который находится в другом наборе данных компании и нездоров.

Эти свойства позволяют избежать прямого участия аналитической организации в конфликтах компаний их клиентов, но допускают непрямое участие: сведения об определенном объекте могут последовательно обновлять (за счет своей информации) компании – соперники, но в этом уже не будет вины аналитической компании (Indirect Information Flow). Контроль за доступом к системе является промежуточным между классическими DAC и MAC.

В целом модель ориентирована на реализацию в очень частном случае (обеспечение защиты от одновременного доступа к данным) и не претендует на значительную общность, но в достаточно полной мере реализует заложенные в неё требования в жизнь.

Выводы:

Общая теория моделей политики безопасности подразумевает выполнение всех требований, но существующие реализации теории ориентированны на выполнение только их части в полном объеме, что подразумевает значительное ограничение на возможные области каждой модели. С течением времени это тенденция усиливается, и в настоящее время модели фактически разрабатываются специально под определенные реализации, что в целом не уменьшает их ценности в практическом плане. Стоит заметить, что, как и большинство технологий безопасности, модели политики безопасности все больше переходят из области военных разработок в область коммерческого и общего использования, что в значительной мере связано с развитием сетевых технологий.

Источники:

http://www.zisc.ethz.ch/events/FS2003PDFs/L2.pdf
http://www.cccure.org/modules.php?name=Downloads&d_op=getit&lid=90
http://www.cse.ogi.edu/~crispin/527/cse527 Policy and BLP2.ppt

http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

http://www-users.cs.york.ac.uk/~fiona/PUBS/CAiSE04.pdf