Политика и модели безопасности в компьютерных системах

Политика и модели безопасности в компьютерных системах

1. Понятие политики и моделей безопасности информации в КС
2. Субъектно-объектная модель КС в механизмах и процессах коллективного доступа к информационным ресурсам
3. Монитор безопасности и основные типы политик безопасности
4. Гарантирование выполнения политики безопасности

Понятие политики и моделей безопасности информации в КС

Политика и модель безопасности

- Политика безопасности организации
  - совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности (ГОСТ Р ИСО/МЭК 15408)

- Политика безопасности КС
  - интегральная **совокупность норм и правил**, **регламентирующих процесс обработки информации**, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз.
- Модель безопасности -
  - **формальное выражение политики безопасности** (математическое, схемотехническое, алгоритмическое и т. д.)

Политика безопасности (интегральная совокупность норм и правил…)

- Многоуровневая схема:
  - **законодательный уровень** (меры ограничительной направленности + направляющие и координирующие меры,
  - **административный** (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
  - **процедурный** (меры безопасности, ориентированные на людей);
  - **программно-технический**.

Модели безопасности служит для

- **выбора и обоснования** базовых принципов архитектуры защищенных КС, определяющих механизмы реализации средств и методов защиты информации;
- **подтверждения свойств** (защищенности) разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев);
- составления **формальной спецификации политики безопасности** как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем.

Модель безопасности включает

- модель компьютерной системы
- критерии, принципы или целевые функции защищенности и угроз
- формализованные правила, алгоритмы, механизмы безопасного функционирования КС

Место моделей безопасности

На основе Модели безопасности	
Заказчик (Потребитель)	может формулировать требования к защищенным КС, которые соответствуют политике безопасности, технологическим процессам обработки информации, принятым в своих организациях и предприятиях
Разработчик (Производитель)	формируют технико-технологические требования и программно-технические решения по разрабатываемым системам
Эксперт (Аудитор)	строят методики и спецификации оценки защищенности конкретных систем, осуществляют сертификацию разработанных систем по требованиям защиты информации

Субъектно-объектная модель КС

в механизмах и процессах коллективного доступа к информационным ресурсам

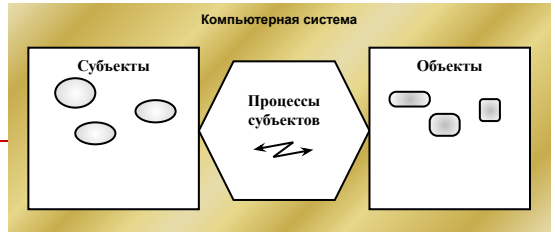
Модель безопасности включает

1. модель компьютерной системы
2. критерии, принципы или целевые функции защищенности и угроз
3. формализованные правила, алгоритмы, механизмы безопасного функционирования КС

Модели компьютерных систем

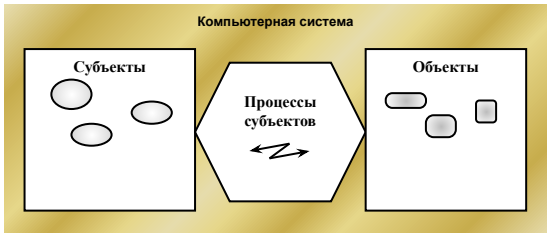
- Большинство моделей КС относится к классу моделей конечных состояний

Субъект, объект, пользователь



- Субъект доступа
  - **активная** сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов.
- Объект доступа
  - **пассивная** сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.
- Пользователь КС
  - **лицо, внешний фактор**, аутентифицируемый некоторой информацией, и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет.

Свойства субъектов



1. угрозы информации исходят от субъектов, изменяющих состояние объектов в КС
2. субъекты-инициаторы могут порождать через объекты-источники новые объекты
3. субъекты могут порождать потоки (передачу) информации от одних объектов к другим

Субъектно-объектная модель КС в аспекте КБ. Основные положения

1. В КС действует **дискретное время**.
2. В каждый момент времени t_k КС представляет собой конечное множество элементов, разделяемых на два подмножества:
   I. подмножество **субъектов** доступа ***S, S*** ***≠∅*** *(активных сущностей; как действия, процессы; могут порождать потоки информации)*;
   II. подмножество **объектов** доступа ***O*** *(пассивных сущностей)****;***
   (Пример ПС – файл с программой, АС – исполняемая программа)
3. **Пользователи** КС (лицо, внешний фактор) представлены одним или некоторой совокупностью **субъектов доступа (СД)**, действующих от его имени. (пользователи получают информацию о КС через свои СД, но не могут изменять СД)
4. **Субъекты** КС могут быть порождены из объектов только активной сущностью (другим СД). ***Create*** (***sj, oi***)→ ***sm*** – "из объекта ***oi*** порожден субъект ***sm*** при активизирующем воздействии субъекта ***sj*** ".
5. Все **процессы безопасности** в КС **описываются доступами** субъектов к объектам, вызывающими **потоки информации**.

Создание и ассоциации

- *Все объекты делятся на 2 непересекающихся множества:*
  - *объекты источники и*
  - *объекты данные*
- ***Create*** (***s****j*, ***o****i*)→ ***s****m*
  - *Объект **o**i называется источником для субъекта **s**m,*
    - *если существует субъект **s**j , в результате воздействия которого на объект **o**i возникает субъект **s**m .*
    - *возможно **s**m пуст, если не может быть создан. Ex. пытаемся в CMD выполнить текстовый файл*
- *Объект **o**i в момент времени tk ассоциирован с субъектом **s**m ,*
  - *если состояние объекта повлияло на состояние субъекта в следующий момент времени tk+1 (т. е. субъект **s**m **использует информацию**, содержащуюся в объекте **o**i*).
  - Ассоциации в дальнейшем могут теряться. Например, запуск программы.

Ассоциированные объекты

- **Ассоциированные объекты** могут быть разделены на **два вида**:
  - функционально-ассоциированные объекты; влияют (определяют) на сами процессы субъекта (например, состояние сегмента кода определяет свойства субъекта в следующий момент времени).
  - ассоциированные объекты-данные; выступают в роли аргументов в операциях, порождающих потоки информации (например, буферы оперативной памяти, в которых помещается для отображения на экране информация при чтении файла).
- Таким образом,
  - если на первый взгляд в потоке участвует только один (одни) субъект(ы),
  - то, как правило, при более пристальном взгляде можно увидеть, что в данной операции участвуют еще и ассоциированные с субъектом доступа объекты.

Потоки информации

- ***Stream***(***s****m* , ***o****i*)→ ***o****j* – "поток информации от объекта ***o****i*(***o****j*) к объекту ***o****j*(***o****i*) в субъекте ***s****m* (через субъект ***s****m)*

- *Потоком информации*
  - *между объектом **o**i и объектом **o**j называется **произвольная операция** над объектом **o**j , реализуемая в субъекте **s**m и зависящая от объекта **o**i .*
  - Поток может осуществляться в виде различных операций над объектами – чтение, изменение, удаление, создание и т. д.

- Объекты ***o****i* и ***o****j*, участвующие в потоке
  - могут быть **как источниками, так и приемниками информации**,
  - могут быть как ассоциированными с субъектом, так и неассоциированными,
  - а также могут быть пустыми (∅) объектами (например, при создании или удалении файлов)

Потоки информации

- Потоки информации могут быть только между объектами, а не между субъектом и объектом,
  - в виду того, что субъект это
    - активная сущность, т. е. действия, процессы и т. д.,
  - а информация – пассивная сущность,
    - которая может размещаться, извлекаться, порождаться, изменяться и т. д. только в объектах.

- Активная роль субъекта заключается в
  - самой реализации потока,
  - в его локализации в субъекте (через субъект),
  - в том числе, через задействование в потоке ассоциированных с субъектом объектов (например, буферов оперативной памяти).

Доступы. Правила разграничения доступа

- Поток всегда порождается субъектом доступа
- *Доступом субъекта **s**m к объекту **o**j*
  - *называется порождение субъектом **s**m потока информации между объектом **o**j и некоторым(и) объектом **o**i (в т. ч., но не обязательно, объект **o**i ассоциирован с субъектом **s**m).*
- Пусть множество ***P*** является объединением потоков по всем моментам времени функционирования КС. ***P*** = ***PL*** ∪ ***PN***, ***PL*** ∩ ***PN*** =∅,
  - где ***PL*** – множество потоков, вызываемых **легальными** (безопасными, санкционированными) доступами;
  - ***PN*** – множество потоков, нарушающих состояние защищенности (конфиденциальность, целостность и доступность информации) в КС, **несанкционированные доступы.**

Резюме

- Основа формализации политики разграничения доступа в моделях безопасности:
  - *правила разграничения доступа субъектов к объектам или*
  - *формально описанные потоки, принадлежащие множеству* ***PL***
- Субъектно-объектная модель КС это
  - методологический фундамент большинства моделей разграничения доступа, выражающих
    - подходы, принципы и механизмы правил разграничения доступа (политику разграничения доступа),
    - а также формальные их спецификации (сами модели разграничения доступа).

Аксиомы защищенности компьютерных систем

A1. В любой момент времени любой субъект, объект (процесс, файл, устройство) д.б. **идентифицированы** и **аутентифицированы**

A2. В защищенной системе должна присутствовать **активная компонента** (субъект, процесс и объект-источник), осуществляющая **контроль процессов субъектов над объектами**

A3. Для осуществления процессов субъектов над объектами необходима (должна существовать) ***дополнительная информация*** (и наличие содержащего ее объекта), помимо информации идентифицирующей субъекты и объекты

Аксиомы защищенности компьютерных систем

A4. Все вопросы безопасности информации в КС описываются **доступами субъектов к объектам**

A5. Субъекты в КС могут быть порождены только **активной компонентой** (субъектами же) из объектов

A6. Система безопасна, если субъекты **не имеют возможности нарушать** (обходить) правила и ограничения Политики Безопасности

A6 – основной критерий безопасности

Политики безопасности компьютерных систем

- Политика ***избирательного* (дискреционного)** доступа
  - множество P_L задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек «субъект-поток(операция)-объект»
- Политика ***полномочного* (*мандатного*)** доступа
  - множество P_L задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности)
- Политика ***ролевого* (*типизованного*)** доступа
  - множество P_L задается через введение в системе дополнительных абстрактных сущностей – ролей, с которыми ассоциируются конкретные пользователи, и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы

- Продолжение следует

Монитор безопасности и основные типы политик безопасности