Информационная (компьютерная) безопасность с точки зрения технологии программирования

В.Б. Бетелин, В.А. Галатенко (Россия)

1. Введение

Информационная (компьютерная) безопасность (ИБ) является относительно замкнутой дисциплиной, развитие которой не всегда синхронизировано с изменениями в других областях информационных технологий. В частности, в ИБ пока не нашли отражения основные положения объектно-ориентированного подхода, ставшего основой при построении современных информационных систем (ИС). Не учитываются в ИБ и достижения в технологии программирования, основанные на накоплении и многократном использовании программистских знаний [1]. На наш взгляд, это очень серьезная проблема, затрудняющая прогресс в области ИБ.

В данном докладе рассматривается программно-технический аспект информационной (компьютерной) безопасности (комплексный подход к ИБ описан нами, например, в [2]). Можно утверждать, что в этом аспекте проблемы ИБ являются в первую очередь программистскими и, следовательно, решаться они должны на основе передовых достижений технологии программирования.

Попытки создания больших систем еще в 60-х годах вскрыли многочисленные проблемы программирования, главной из которых является сложность создаваемых и сопровождаемых систем. Результатами исследований в области технологии программирования стали сначала структурированное программирование, затем объектно-ориентированный подход.

Объектно-ориентированный подход является основой современной технологии программирования, наиболее апробированным методом борьбы со сложностью. Представляется естественным и, более того, необходимым, распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Сложность эта имеет двоякую природу. Во-первых, сложны аппаратно-программные системы, которые необходимо защищать, и сами средства безопасности. Во-вторых, быстро нарастает сложность семейства нормативных документов (таких, например, как Профили защиты на основе "Общих критериев", см. далее раздел 4). Эта сложность менее очевидна, но ей также нельзя пренебрегать; необходимо изначально строить семейства документов по объектному принципу.

2. Недостатки традиционного подхода к ИБ с точки зрения объектной ориентированности

Исходя из основных положений объектно-ориентированного подхода, следует в первую очередь признать устаревшим традиционное деление на активные и пассивные сущности (субъекты и объекты в привычной для ИБ терминологии). Пользователям объектов доступны только методы (активные сущности), реализация которых (и, в частности, доступ к пассивным сущностям, таким как переменные и их значения) является скрытой, инкапсулированной.

По-видимому, следует признать устаревшим и положение о том, что разграничение доступа направлено на защиту от злоумышленных пользователей. Как уже отмечалось, современные ИС характеризуются чрезвычайной сложностью, и их внутренние ошибки представляют не меньшую опасность.

Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости самой употребительной - дискреционной модели управления доступом. При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя определить троянские программы, противостоять которым дискреционное управление доступом, как известно, не в состоянии.

Одним из самых прочных стереотипов среди специалистов по ИБ является трактовка операционной системы как доминирующего средства безопасности. На разработку защищенных ОС выделяются крупные силы и средства, зачастую в ущерб остальным направлениям защиты и, следовательно, в ущерб реальной безопасности. В современных ИС, выстроенных в многоуровневой архитектуре клиент/сервер (см. также следующий раздел), ОС не контролирует

объекты, с которыми работают пользователи, равно как и самих пользователей, которые регистрируются и учитываются прикладными средствами. Основной функцией безопасности ОС становится защита возможностей, предоставляемых привилегированным пользователям, от атак пользователей обычных. Это важно, но это далеко не вся безопасность.

3. Трактовка информационной системы как совокупности сервисов, в число которых входят сервисы безопасности

Современные ИС представляют собой распределенный набор взаимодействующих объектов. Каждый объект предоставляет другим определенные услуги (сервисы), в число которых входят сервисы безопасности.

В многоуровневой архитектуре ИС одним из важнейших элементов является Web-сервис, играющий роль информационного концентратора и, одновременно, разграничивающий доступ пользователей. Если выдержан архитектурный принцип невозможности обхода защитных средств, то пользователи не имеют прямого доступа к другим уровням ИС; следовательно, соответствующие ОС "видят" только процессы, осуществляющие связь с сервисами соседних уровней. Эти процессы не выступают от имени пользователей. В свою очередь, пользователи осуществляют доступ не к ресурсам, контролируемым ОС нижних уровней, а к локаторам ресурсов, видимым на Web-сервере. Последний решает, что каждый из пользователей видит и какими правами доступа обладает.

На наш взгляд, следующая совокупность сервисов безопасности достаточна для построения защиты, соответствующей современным требованиям.

- Идентификация/аутентификация
- Разграничение доступа
- Протоколирование/аудит
- Экранирование
- Туннелирование
- Шифрование
- Контроль целостности
- Контроль защищенности
- Обнаружение и нейтрализация отказов
- Оперативное восстановление
- Управление

Как объединить сервисы безопасности для создания эшелонированной обороны, каково их место в общей архитектуре информационных систем?

На внешнем рубеже располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей (обычно объединяемых с межсетевыми экранами), образуют периметр безопасности, отделяющий корпоративную систему от внешнего мира.

Сервис активного аудита должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже если по каким-либо причинам она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу должна предшествовать идентификация и аутентификация субъектов.

Криптографические средства целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование. Масштабы пользовательской криптографии следует минимизировать.

Наконец, последний рубеж образуют средства пассивного аудита, помогающие оценить последствия нарушения безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

Управление должно быть "всепроникающим", позволяющим контролировать все компоненты ИС.

4. О концептуальном базисе стандартов в области ИБ

Международный стандарт ISO 15408 [3-6], известный также как "Общие критерии оценки безопасности информационных технологий" или просто "Общие критерии" (ОК), задал направление пересмотра нормативной базы информационной безопасности во многих странах, в том числе в России.

В данном докладе нас будут интересовать функциональные требования, присутствующие в ОК. По своему богатству, гибкости, детальности проработки они существенно превосходят более ранние стандарты. Тем досаднее, что авторы ОК не учли опыт технологии программирования, снизив тем самым ценность собственной разработки.

С точки зрения технологии программирования, авторы "Общих критериев" в плане функциональных требований придерживаются подхода "снизу вверх". Его ограниченность (в первую очередь из-за архитектурных проблем) стала очевидной лет тридцать назад. Остается только надеяться, что следующие "критерии" будут уже не "общими", а "объектными".

К сожалению, в "Общих критериях" отсутствуют архитектурные требования. На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям на протоколы и программные интерфейсы, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, безопасность интерфейсов - важная проблема, которую желательно решать единообразно.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

С точки зрения технологии программирования, положительным моментом ОК является выделение такого понятия, как функциональный пакет. Функциональный пакет (ФП) - это неоднократно используемая совокупность функциональных компонентов, объединенных для достижения определенных целей безопасности [7].

Функциональные пакеты представляют собой промежуточную (по отношению к профилю защиты (ПЗ)) комбинацию функциональных компонентов. "Общие критерии" не регламентируют их структуру, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода), при разработке иерархии руководящих документов целесообразно выделить базовый (минимальный) ПЗ, а дополнительные требования скомпоновать в функциональные пакеты.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) функциональным возможностям. Производные профили получаются из базового добавлением необходимых пакетов расширения, то есть в том же стиле, что и производные классы в объектно-ориентированных языках программирования.

5. Применение понятий объектно-ориентированного подхода к решению задачи разграничения доступа

Формальная постановка задачи разграничения доступа в рамках объектно-ориентированного подхода может выглядеть следующим образом.

Рассматривается множество. Часть объектов может являться контейнерами, группирующими объекты-компоненты, задающими для них общий контекст, выполняющими общие функции и реализующими итераторы. Контейнеры либо вложены друг в друга, либо не имеют общих компонентов.

С каждым объектом ассоциирован набор уникальных идентификаторов (УИ). К объекту можно обратиться только по УИ. Разные УИ могут предоставлять разные методы и быть доступными для разных объектов.

Каждый контейнер позволяет опросить набор УИ объектов-компонентов, удовлетворяющих некоторому условию. Возвращаемый результат в общем случае зависит от вызывающего объекта.

Объекты изолированы друг от друга. Единственным видом межобъектного взаимодействия является вызов метода.

Предполагается, что используются надежные средства аутентификации и защиты коммуникаций. В плане разграничения доступа локальные и удаленные вызовы не различаются.

Разграничивается доступ к уникальным идентификаторам объектов, а также к методам объектов (с учетом значений фактических параметров вызова). Правила разграничения доступа (ПРД) задаются в виде предикатов над объектами.

Рассматривается задача разграничения доступа для выделенного контейнера CC, компонентами которого должны являться вызывающий и/или вызываемый объекты. УИ этого контейнера предполагается общеизвестным. Считается также, что между внешними по отношению к выделенному контейнеру объектами возможны любые вызовы.

Выполнение ПРД контролируется монитором обращений.

При вызове метода будем разделять действия, производимые вызывающим объектом (инициация вызова) и вызываемым методом (прием вызова и завершение вызова).

При инициации вызова может производиться преобразование УИ фактических параметров к виду, доступному вызываемому методу ("трансляция УИ"). Трансляция может иметь место, если вызываемый объект не входит в тот же контейнер, что и вызывающий.

Структурируем множество всех ПРД, выделив четыре группы правил:

- политика безопасности контейнера;
- ограничения на вызываемый метод;
- ограничения на вызывающий метод;
- добровольно налагаемые ограничения.

Правила, общие для всех объектов, входящих в контейнер C, назовем политикой безопасности данного контейнера.

Пусть метод M1 объекта O1 в точке P1 своего выполнения должен вызвать метод M объекта O. Правила, которым должен удовлетворять M, можно подразделить на три подгруппы:

- правила, описывающие требования к формальным параметрам вызова;
- правила, описывающие требования к семантике M;
- реализационные правила, накладывающие ограничения на возможные реализации M;
- правила, накладывающие ограничения на вызываемый объект O.

Метод M объекта O, потенциально доступный для вызова, может предъявлять к вызывающему объекту следующие группы требований:

- правила, описывающие требования к фактическим параметрам вызова;
- правила, накладывающие ограничения на вызывающий объект.

Можно выделить три разновидности предикатов, соответствующих семантике и/или особенностям реализации методов:

- утверждения о фактических параметрах вызова метода M в точке P1;
- предикат, описывающий семантику метода M;
- предикат, описывающий особенности реализации метода M.

Перечисленные ограничения можно назвать добровольными, поскольку они соответствуют реальному поведению объектов и не связаны с какими-либо внешними требованиями.

Предложенная постановка задачи разграничения доступа соответствует современному этапу развития программирования, она позволяет выразить сколь угодно сложную политику безопасности, найти баланс между богатством выразительных возможностей и эффективностью работы монитора обращений.

6. Заключение

Применение методов технологии программирования является новым для информационной безопасности. Оно позволяет учесть семантику программ, привести в соответствие понятия информационной безопасности и объектно-ориентированного подхода - основного средства создания современных информационных систем.

7. Литература

1. Бетелин В.Б., Галатенко В.А. ЭСКОРТ - инструментальная среда программирования. - Юбилейный сборник трудов институтов Отделения информатики РАН. Том. II. Москва, 1993, 21 с.

2. Бетелин В.Б., Галатенко В.А. Информационная безопасность в России: опыт составления карты. - Jet info, 1998, 1.

3. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. - ISO/IEC 15408-1.1999.

4. Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. - ISO/IEC 15408-2.1999.

5. Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements. - ISO/IEC 15408-3.1999.

6. "Общие критерии" на сервере Национального института стандартов США. - http://csrc.nist.gov/cc/.

7. Guide for Production of Protection Profiles and Security Targets. - ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000.