ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Модель информационных потоков

Федоров Дмитрий Николаевич
dnf@dnf.su

IX

РАЗДЕЛЫ ТЕМЫ

- Направления защиты процессов обмена информацией
- Защита сетевых процессов обмена данными
- Защита экспорта файлов
- Вопросы построения полной и функциональной схемы информационных потоков
- Средства создания схем информационных потоков
- Контроль построения модели информационных потоков

ОТ БЕЗОПАСНОСТИ СИСТЕМЫ К БЕЗОПАСНОСТИ ВСЕХ СИСТЕМ

- Ранее мы производили анализ информационных систем — обследование и классификация – для информационного пространства, в котором функционирует одна информационная система.
- Теперь необходимо сконцентрироваться на рассмотрении вопроса безопасности для всех систем пространства (предприятия) в целом.
- Среда передачи данных между отдельными системами должна рассматриваться как полноценная информационная система со своими свойствами и уязвимостями.

Раздел 1

НАПРАВЛЕНИЯ ЗАЩИТЫ ПРОЦЕССОВ ОБМЕНА ИНФОРМАЦИЕЙ

ПРОБЛЕМЫ КОМПЛЕКСА СИСТЕМ

- При внедрении информационных систем возможны ситуации, когда система с тщательно продуманной моделью безопасности допускает экспорт практически всех значимых данных (например, для некоторого круга пользователей, у которых есть право на подобный экспорт) в виде абсолютно незащищенного набора данных (обычного текстового файла).
- С точки зрения бизнес-логики в этом нет ничего противоестественного, система должна обмениваться данными с другими системами, которые могут ничего не знать о форматах данных исходной системы, о ее криптографических алгоритмах и тем более о способах обмена ключами шифрования и т.д.
- С точки зрения самой системы также все в порядке — она надежно защищала данные внутри себя, предоставила право на экспорт только уполномоченному лицу.
- Однако с точки зрения комплексной безопасности всего информационного пространства возникает проблема — система освободила себя от забот по обеспечению безопасности! Кто должен взять на себя эти обязанности?

ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ ЭКСПОРТА ДАННЫХ

- Проективный
  - Соответствующие специалисты задумались о проблеме безопасности обмена данных до того, как была приобретена или разработана информационная система.
  - В этом случае есть возможность определить и выставить требование поддержки защищенного обмена данными для каждой устанавливаемой в информационном пространстве системы
- Реактивный:
  - Определенное число информационных систем уже внедрено.
  - Необходимо обеспечить безопасность обмена данными между ними.
  - Решение: дополнительная доработка — прикладные программные интерфейсы (англ. Application Programming Interface — API) или интерфейсы, ориентированные специально на обеспечение безопасности (англ. Security Services Provider Interface, в некоторых источниках — Security Support Provider Interface, — SSPI).

Раздел 2

ЗАЩИТА СЕТЕВЫХ ПРОЦЕССОВ ОБМЕНА ДАННЫМИ

КЛАССЫ FTP И FCS

- В «Классификация средств обработки информации: стандарт CCITSE« представлены классы FTP и FCS, которые составляют для системы основу безопасного обмена данными с другими системами.
- Данные механизмы обеспечения защиты обмена данными обеспечивают реализацию ситуаций, когда информация не остается незащищенной ни на каком из этапов перемещения между системами.
- Как правило работа таких механизмов основана на работе криптографических средств.

ЛОКАЛЬНЫЕ СЕТИ И ДОСТУП ЧЕРЕЗ ИНТЕРНЕТ

- Если информационное пространство предприятия ориентировано на стек TCP/IP и есть возможность в случае необходимости дорабатывать системы, то в настоящее время с появлением новых механизмов и протоколов защиты обеспечивать безопасность такого пространства становится проще.
- Существует средства (IPSec, ISAKMP, IKE, SSL и пр.), которые делают обмен данными защищенным и работают одинаково вне зависимости от того, располагаются ли информационные системы в одной локальной сети или используют в качестве канала связи Интернет.

СЕМИУРОВНЕВАЯ МОДЕЛЬ OSI

- Эталонная модель взаимодействия открытых систем (модель OSI) предназначена для описания процесса пересылки информации через сетевую среду от одного программного приложения другому программному приложению, работающему на другом компьютере. Эталонная модель OSI является семиуровневой концептуальной моделью. Каждый уровень выполняет определенные сетевые функции.
- В начале 80-х годов ряд международных организаций по стандартизации – ISO, ITU-T и некоторые другие – разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется моделью взаимодействия открытых систем (Open System Interconnection, OSI) или моделью OSI. Модель OSI определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

Каждый уровень является настолько самодостаточным, что задачи любого уровня могут выполняться независимо. Это позволяет вносить изменения в работу одного уровня, не влияя на работу других уровней.

Модель OSI

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединие точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

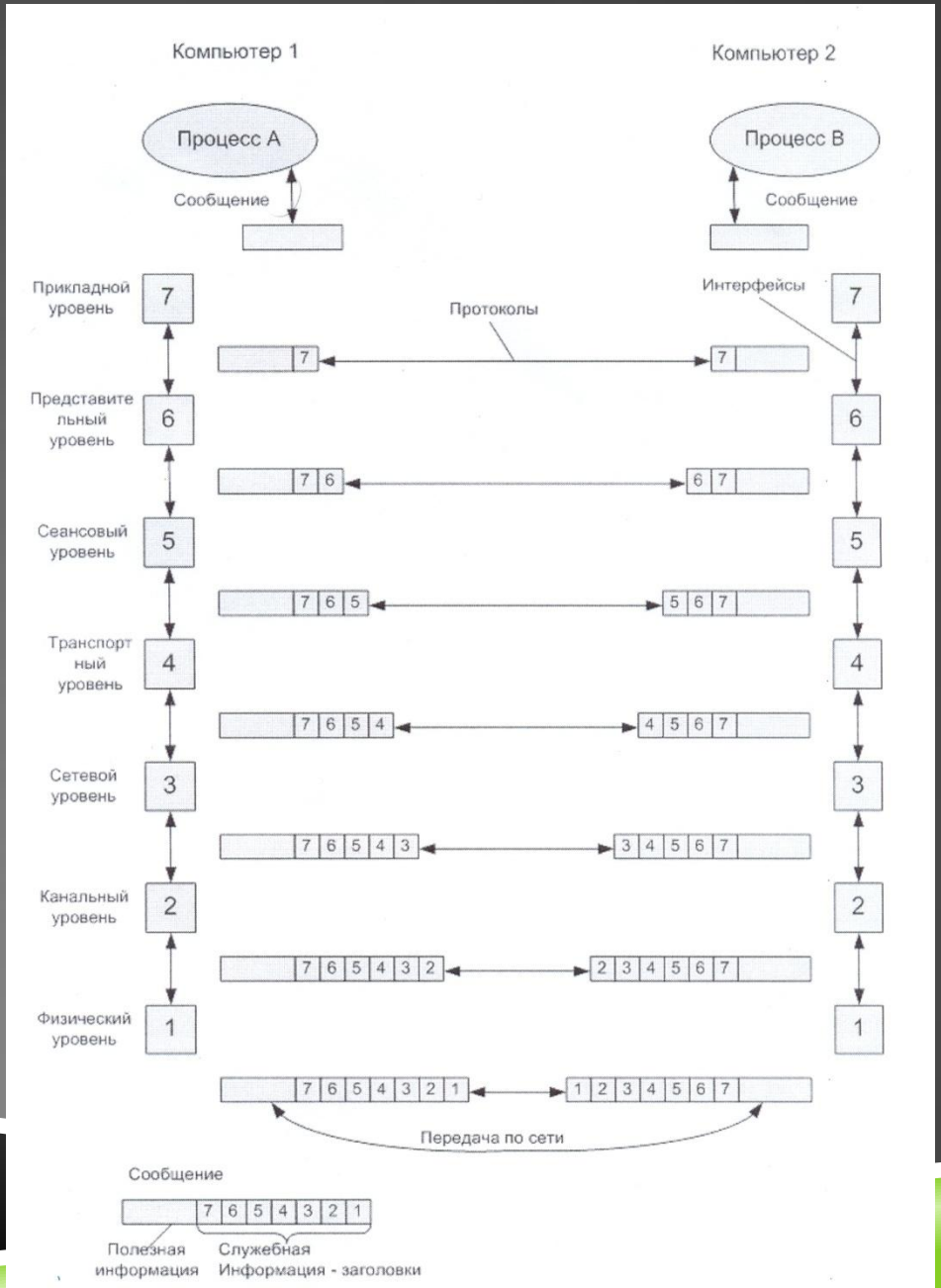


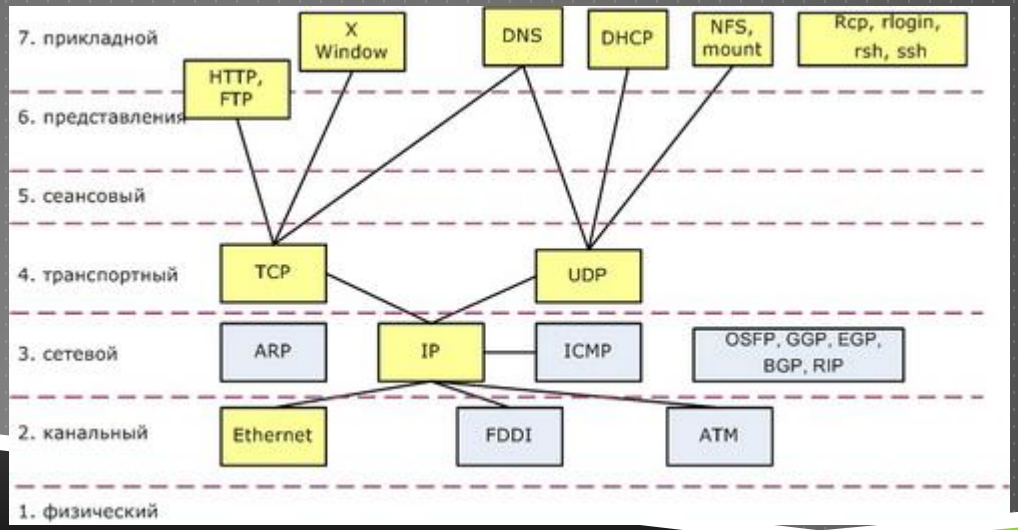
Рисунок 1. Модель взаимодействия открытой системы OSI

ПЕРЕДАЧА ИНФОРМАЦИИ ПО УРОВНЯМ

- После формирования сообщения прикладной уровень направляет его вниз по стеку представительному уровню.
- Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию — заголовок представительного уровня.
- Сообщение достигает нижнего, физического уровня, который собственно и передает его по линиям связи машине-адресату. К этому моменту сообщение «обрастает» заголовками всех уровней.
- Когда сообщение по сети поступает на машину-адресат, оно принимается ее физическим уровнем и последовательно перемещается вверх с уровня на уровень.

МОДЕЛЬ OSI

Прикладной	
Презентационный	
Уровень сессий	
Транспортный	
Сетевой	Q.931 (I.451), Q.932 (I.452), Q.933 (I.453) (Пакетный)
Канальный	Q.921 (I.441), Q.922
Физический	X.21 (I.430, I.431, I.432)



МНОГОУРОВНЕВЫЙ ХАРАКТЕР ЗАЩИТЫ

- Независимо от того, используется ли в качестве сетевого протокола TCP/IP или другой стек протоколов, следует помнить о классической семиуровневой сетевой модели (OSI — Open System Interconnection).
- Это означает, что построение механизмов защиты должно также носить многоуровневый характер.
- Примеры.
  - Если нас интересует только защита конфиденциальности и целостности данных в приложениях, то, обычно, этот вопрос можно решить на верхних уровнях (приложения или представления данных).
  - Если встает вопрос об обеспечении надежной доставки — акценты смещаются к транспортному уровню.
  - Если обмен информацией между системами должен скрывать внутреннюю сетевую структуру систем, то речь идет о сетевом уровне.
  - Если необходимо учесть опасность широковещательных сообщений (например, угрозы использования пассивного прослушивания сегмента), следует говорить о канальном уровне.
  - Физический уровень обычно затрагивается, когда речь идет о защите от побочных электромагнитных излучениях или возможности физического внедрения злоумышленника в канал связи.

ПРОТОКОЛЫ БЕЗОПАСНОСТИ ДВУХ СИСТЕМ

- Если обе системы, между которыми происходит обмен данными, поддерживают одни и те же протоколы безопасности, то при соответствующей настройке они смогут обеспечить требуемый уровень безопасности.
- Если одна из систем представляет собой "черный ящик" без возможности модификаций и не может импортировать/экспортировать никакие другие данные, кроме как в обычном текстовом или другом незащищенном формате, необходимо проведение работ по оценке категорий безопасности:
  - к какой категории относится данная информация,
  - какая составляющая для нее наиболее критична: конфиденциальность, целостность, доступность и т. д.
  - какие альтернативные средства защиты, предоставляемые системой, можно использовать. Возможно, система может рассчитывать некую контрольную сумму экспортируемых/импортируемых данных (аналог электронно-цифровой подписи), либо она ведет расширенный регистрационный журнал загруженных/выгруженных данных и т. п.
  - как имеющиеся средства могут быть использованы второй системой.

Раздел 3

ЗАЩИТА ЭКСПОРТА ФАЙЛОВ

ДОПОЛНИТЕЛЬНЫЕ ВАРИАНТЫ ЗАЩИТЫ

Если обмен данными ведется по самому примитивному варианту (одна система записывает текстовый файл в каталог на сервере, другая считывает его оттуда), возможно использовать дополнительные варианты защиты:

- средствами операционной системы (при условии, что сама операционная система поддерживает необходимые механизмы безопасности). Установить доступ на каталог импорта/экспорта только для специальных пользователей, от имени которых работают системы. Снизить до минимума или исключить возможность вмешательства администратора приложения или файлового сервера в работу систем.

- использованием дополнительного сервиса, который бы брал на себя контроль за состоянием файла после его создания первой системой и уничтожение его после импорта второй системой. Создание средствами операционной системы или коммуникационными устройствами шифрованного или VLAN-канала между серверами приложения взаимодействующих систем и файловым сервером импорта/экспорта;
- разработкой организационных мероприятий. Принудительное отключение пользователей от работы в сети на момент экспорта/импорта, запрет на использование анализаторов сетевого трафика даже для администраторов (в установленное время) и пр.

Раздел 4

ВОПРОСЫ ПОСТРОЕНИЯ ПОЛНОЙ И ФУНКЦИОНАЛЬНОЙ СХЕМЫ ИНФОРМАЦИОННЫХ ПОТОКОВ

МИГРАЦИЯ ИНФОРМАЦИИ ПО КАТЕГОРИЯМ КЛАССИФИКАЦИИ

При построении схемы информационных потоков следует задуматься о возможности миграции информации по категориям классификации в зависимости от того, на какой стадии информационного потока она находится.

- Наиболее простой пример таков. Ряд пользователей или систем, каждый сам по себе, обладает частью информации, не представляющей особой важности и находящейся в низкой категории классификации. Та же информация, собранная в одной системе вместе, составляет критически важные данные, подлежащие особой защите, требующие размещения в верхней части таблицы классификации.
- Обратный пример — часть критически важной по конфиденциальности информации, может быть разглашена на определенном этапе, без ущерба для общего набора информации.

НЕОБХОДИМО:

- Проводить оценку **безопасности информации** с точки зрения ее жизненных циклов и других условий.
- При построении информационного потока следует учитывать возможные ответвления от него, не являющиеся очевидными на первый взгляд.

ПРИМЕРЫ

- Информация следует от системы А через Б к В, на первый взгляд вся цепочка надежно защищена. Однако выясняется, что в системе Б пользователь распечатывает часть данных и передает другому пользователю для анализа. Поскольку данное ответвление находится вне электронного взаимодействия, оно может быть упущено, между тем если информация критична по конфиденциальности, необходимо применение соответствующих дополнительных мер.
- Информация также следует от системы А через Б к В. На этапе Б, перед тем как перейти к В, информация может быть изменена пользователем на основе других данных (например, на основе информации, поступившей от системы Б2). Как информационный поток защищен от ошибок в системе Б2, если система Б2 — это производственное совещание?

Раздел 5

СРЕДСТВА СОЗДАНИЯ СХЕМ ИНФОРМАЦИОННЫХ ПОТОКОВ

СОЗДАНИЕ СХЕМ ИНФОРМАЦИОННЫХ ПОТОКОВ

- Сложно предложить общую методику по причине специфики информационных систем и в значительной степени бизнес-процессов (и бизнес-потоков) в конкретном предприятии.
- Вполне возможно использование уже имеющегося механизма составления таких схем — универсального языка моделирования UML (Unified Modeling Language).
  - Это достаточно сложный инструмент, для серьезной работы с ним может потребоваться квалифицированный специалист. Однако для профессионалов, знакомых с объектно-ориентированной концепцией, не составит труда использовать элементы UML при составлении схем.

- При использовании UML или любого другого инструмента построения моделей следует помнить, что результирующая, рабочая схема должна описывать не абстрактную "**безопасность**", а конкретные ее категории.
- Оперируя параметрами и функциями объектов схемы, необходимо разделять их на отвечающие за конфиденциальность, целостность и т. д.
- С учетом необходимости многоуровневого анализа построения защиты задача построение качественной схемы является достаточно сложной.

Раздел 6

КОНТРОЛЬ ПОСТРОЕНИЯ МОДЕЛИ ИНФОРМАЦИОННЫХ ПОТОКОВ

ПОСТРОЕНИЕ МОДЕЛИ

- Убедиться, что всё информационные потоки определены правильно и информация во время всего следования защищена надежно — задача, сравнимая по сложности с самим построением схемы информационных потоков.
- Необходимо проанализировать техническую документацию к системам и конфигурацию работающих систем.

АНАЛИЗ СИТУАЦИИ

Для анализа следует получить ответы на следующие вопросы.

- Как защищен этот файл от постороннего прочтения?
- Как производится проверка того, что данные не были изменены непосредственно перед загрузкой в систему?
- Что происходит, если выгруженный файл был испорчен или удален?

В зависимости от ответов на них, можно представить картину мероприятий по организации защиты данных при перемещении от одной системы к другой.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru