Лекция 15 Обеспечение безопасности распределенных систем

Введение в обеспечение безопасности

Распределенная система представляет набор программных компонент, использующих те или иные промежуточные среды для своего взаимодействия (рис. 1). Каждая промежуточная среда использует так называемый транспортный протокол, в роли которого может выступать:

- промежуточная среда (например, Remoting или COM+ поверх MSMQ);
- протокол верхнего уровня модели OSI (например, HTTP или HTTPS);
- протокол транспортного уровня модели OSI (например, TCP).

Транспортный протокол промежуточной среды, в свою очередь, использует протоколы нижних уровней.

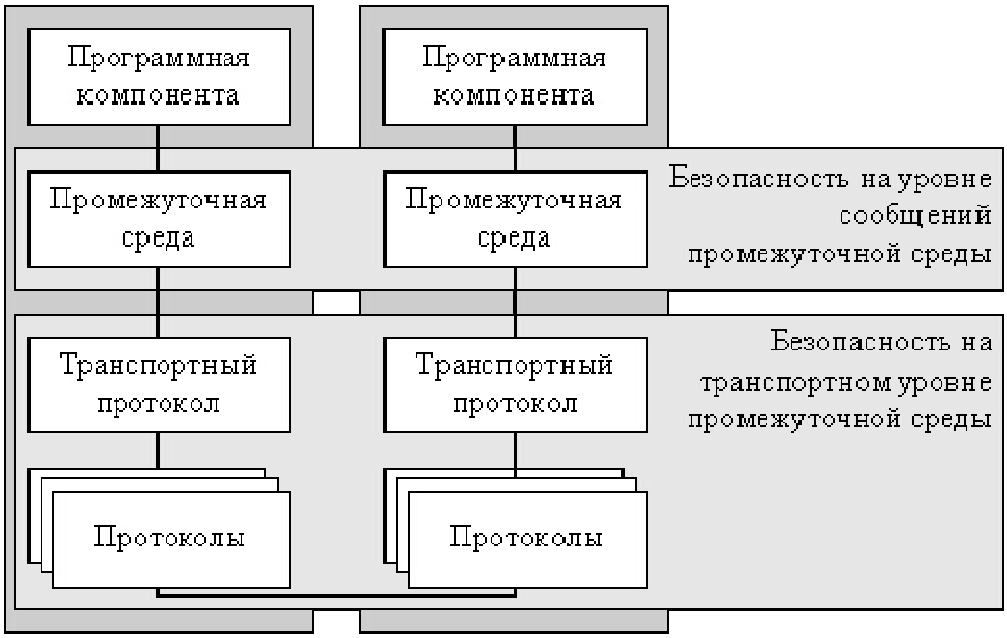

Рис. 1. Обеспечение безопасности взаимодействия компонент

Напомним, что обеспечение безопасного взаимодействия программных компонент включает в себя:

- идентификацию пользователя сервисов компоненты (аутентификацию);
- защиту передаваемой информации от просмотра и изменения (шифрование и цифровая подпись);
- ограничение доступа пользователей к сервисам компоненты в соответствии с результатом их идентификации (авторизацию).

Указанные функции могут выполняться промежуточной средой, ее транспортным протоколом или протоколами нижних уровней. Сами программные компонента не должна участвовать в выполнении функций безопасности каким-либо образом. В качестве примера рассмотрим веб службы ASP.NET. Безопасность в них может обеспечиваться:

- самой промежуточной средой (при использовании WSE);
- транспортным протоколом HTTPS;
- или даже безопасным IP соединением (IPSec), как при использовании веб служб поверх TCP, так и при использовании HTTP.

Другим примером является среда .NET Remoting. Ее безопасность может обеспечиваться только на транспортом уровне, например при использовании HTTP или HTTPS с IIS, MSMQ в качестве транспорта, а так протокола IPSec. При этом функция авторизации в среде Remoting отсутствует, невозможно разграничить доступ пользователей для методов удаленного класса.

Обеспечение функций безопасности на уровне промежуточной среды имеет определенные преимущества.

1. Большая гибкость. Например, возможно шифровать только отдельные части сообщения, а цифровая подпись применять к целому сообщению.
2. Переносимость. Промежуточная среда с собственной поддержкой безопасности может работать с различными транспортами и не выдвигает каких либо требований к безопасности транспортного уровня.
3. Возможность аудита. При использовании систем с маршрутизацией сообщений (например, веб служб) промежуточные маршрутизаторы сообщений могут добавлять в него дополнительную служебную информацию.
4. Большое время защиты сообщения. Сообщение остается зашифрованным максимально возможное время, в то время как при обеспечении безопасности транспортом оно поступает в промежуточную среду уже в расшифрованном виде.

Однако реализация безопасности транспортом также имеет ряд достоинств.

1. Меньшие затраты времени. При идентификации на уровня транспортного протокола решение об идентичности пользователя принимается без участия промежуточной среды. Шифрование на уровне транспорта обычно также работает быстрее.
2. Универсальность. Безопасность транспортного протокола позволяет защитить любые промежуточные среды, его использующие. Не возникает проблем с реализацией функций безопасности промежуточных сред разных производителей.
3. Можно сделать вывод, что обычно безопасность на уровне сообщений более предпочтительна. Если промежуточная среда не поддерживает необходимую функцию безопасности, и ее реализация на транспортом уровне невозможна, то не следует реализовывать данную функцию на уровне компоненты. Вместо этого следует сменить промежуточную среду или используемый ею транспорт на другие, удовлетворяющие требованиям к безопасности распределенной системы.

Механизмы обеспечения безопасности

Электронные сертификаты

В настоящее время наиболее распространенным базовым механизмом обеспечения безопасности являются цифровые сертификаты, используемые для организации инфраструктуры открытых ключей (public key infrastructure, PKI). Наиболее распространенным стандартом сертификата является стандарт X.509. Инфраструктура PKI основана на использовании доверенных систем. Целью организации инфраструктуры открытых ключей является привязка сторон обмена к сертификатам, содержащих их

открытые ключи. Это позволяет как идентифицировать пользователя по сертификату, так и использовать асимметричное шифрование с открытым и закрытым ключами при передаче информации (рис. 2).

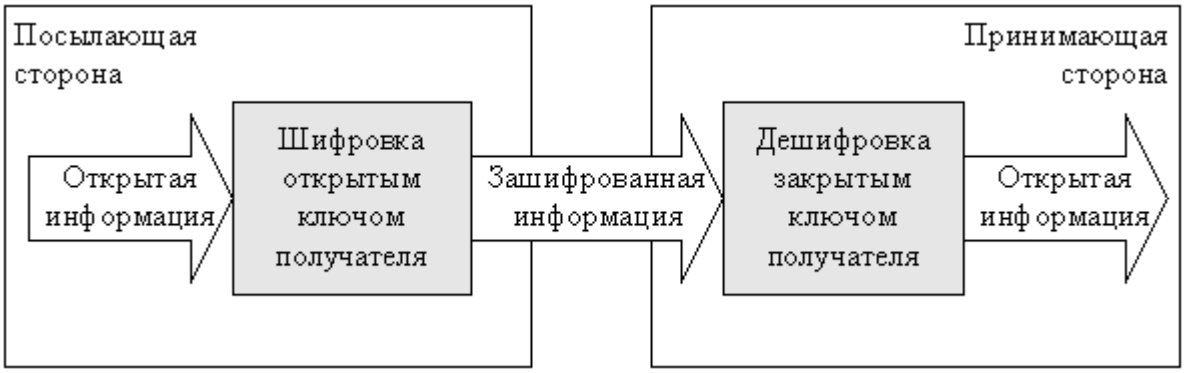

Рис. 2. Шифрование с открытым ключом

Открытые ключи содержаться в сертификатах X.509, которые представляют собой текстовый цифровой документы, связывающий набор реквизитов стороны (адрес, название) с ее открытым ключом. Сертификат подписывается закрытым ключом некоторой доверенной третьей стороной (certificate authority, CA). Цифровая подпись заключается в вычислении образа сертификата, вычисленного криптографической хеш функцией MD5, и последующего шифрования образа закрытым ключом CA. Результат шифрования образа сертификата называется цифровой подписью (рис. 3). Таким образом, сертификат содержит:

- реквизиты предъявляющей его организации или подразделения организации;
- реквизиты подписавшей его доверенной третьей стороны;
- сроки действия сертификата;
- открытый ключ;
- цифровую подпись.

После получения сертификата другая сторона обмена информацией проверяет его, используя открытый ключ подписавшей его организации. Если результат дешифровки подписи сертификата совпадает с образом остальной части сертификата, то сертификат верен. Сертификат доверенной стороны подписывается им самим.

Рис. 3. Подпись сертификата

В роли доверенной стороны могут выступать коммерческие фирмы, занимающиеся выдачей сертификатов или созданный внутри организации сервер PKI (например, Windows Certificate Services). В простейших случаях доверенная сторона может быть представлена самоподписанным сертификатом, который выдается заранее всем участникам обмена информацией после подписи их сертификатов соответствующим закрытым ключом. Иногда используется и вариант с предъявлением серверу клиенту самоподписанного сертификата. Такой сертификат не может быть проверен клиентом на подлинность и предполагает доверие серверу, но может быть использован для защиты передаваемой информации.

Сертификаты имеют двоякое применение:

- идентификация стороны, предъявивший сертификат;
- защита передаваемой информации парой из закрытого и открытого ключей.

При применении сертификатов основной объем информации может шифроваться и симметрично, с использованием временного сессионного ключа. Более медленное асимметричное шифрование в таком случае применяется для передачи временного ключа между сторонами обмена.

Сертификаты применяются во многих протоколах, из которых можно выделить следующие применяемые с распределенными системами, построенных с .NET Framework:

- безопасный транспортный протокол SSL;
- безопасный сетевой протокол IPsec;
- безопасная передача гипертекста HTTPS;
- расширение безопасности веб служб WS-Security;
- MSMQ.

Как видно из данного списка, электронные сертификаты могут обеспечивать безопасность распределенной системы как на транспортном уровне, так и на уровне сообщений промежуточной среды.

Протокол Kerberos

Протокол Kerberos позволяет осуществлять идентификацию клиента и симметричное шифрование трафика на основе временных сессионных ключей. В настоящее время его модификация применятся в сетях Microsoft Windows 2000 и более поздних.
Протокол Kerberos основан на использовании третьей доверенной стороны, называемой центром распространения ключей (key distribution center, KDC). При идентификации в домене Active Directory клиент программной компоненты получает так называемый билет на дарование билета (ticket-granting ticket, TGT), который затем используется для обращения к применяющим протокол Kerberos сетевым службам. При обращении к программной компоненте клиент посылает запрос к KDC, получает от него билет на доступ к сервису (service ticket), содержащий реквизиты клиента для авторизации сервисом и сессионный ключ, зашифрованные основным ключом сервиса, а так же сессионный ключ, предназначенный для клиента. Билет на доступ к сервису используется затем клиентом при доступе к сервису. Передаваемый сервису токен состоит из информации из билета доступа к сервису, к которой добавляется уникальная клиентская информация (authenticator), включающая в себя в частности время посылки запроса. Данная информация шифруется полученным клиентом сессионным ключом. Сервис дешифрует своим основным ключом полученный от клиента билет на доступ к сервису, извлекает из него сессионный ключ и дешифрует им реквизиты пользователя. В случае успеха дешифровки клиент проходит аутентификацию.
Протокол Kerberos используется в Microsoft Windows в:
интегрированной безопасности Windows (Windows integrated security, WIS);
безопасном сетевого протокола IPSec/IKE;
расширении безопасности веб служб WS-Security.
Протокол Kerberos в Microsoft Windows используется в пределах домена Active Directory. WIS в частности используется службами MSMQ, IIS и COM+.

Безопасность промежуточных сред .NET Framework

Для сравнительного описания безопасности рассмотренных промежуточных сред можно выделить следующие основные их конфигураций:
MSMQ в пределах LAN;
MSMQ / HTTP: запись сообщений в очереди MSMQ 3.0 через HTTP / IIS;
Enterprise Services / COM+;
WS: веб службы с использованием WSE 3.0;
Remoting без использования IIS, со стандартными каналами ;
Remoting с использованием IIS.
В таблице 1 перечислены решения обеспечения безопасности указанных конфигураций на транспортном уровне и уровне сообщений. Под VPN понимается развертывание виртуальной частной сети на основе протоколов SSL или IPSec. Из таблицы видно, что наибольшие трудности с точки зрения безопасности возникают с технологией Remoting, у которой в частности нет обеспечения безопасности на уровне промежуточной среды.

Таблица 1. Безопасность промежуточных сред .NET Framework

Промежуточная среда	**Безопасность**	
	на транспортном уровне	**на уровне промежуточной среды**
MSMQ	VPN, WIS	Сертификаты X.509
MSMQ / HTTP	HTTPS, VPN, WIS	Нет
ES / COM+	WIS, VPN	Авторизация доступа (WIS)
WS	HTTPS, VPN, WIS	WS-Security (X.509, Kerberos)
Remoting	VPN	Нет
Remoting / IIS	HTTPS, VPN, WIS	Нет

Рис. 4. Классификация промежуточных сред с точки зрения безопасности распределенной системы

На рис. 4 представлена классификация рассмотренных сред с точки зрения возможности применения в различных сетях различной степени доверенности. Классификация носит вложенный характер, поскольку боле безопасные среды, применимые в общественных сетях, могут применяться и в незащищенной локальной сети – но не наоборот. Следует отметить, что понятие "полностью доверенной сети" не может иметь места в случае каких либо приложений автоматизации бизнеса, а может иметь место только в научных, экспериментальных и подобных приложениях.

Выводы по безопасности промежуточных сред

Веб службы с использованием WSE являются промежуточной средой с наиболее широкими возможностями обеспечения безопасности, благодаря которым веб службы можно использовать в сетях общего доступа. Среды MSMQ и COM+ в основном предназначены для создания безопасных распределенных систем в локальной сети предприятия. Промежуточная среда Remoting может использоваться только либо вместе со службами IIS / MSMQ, либо для организации локального взаимодействия, либо для научных или подобных целей.