Тема "Защита IP-уровня. Области применения протокола IPSec. Архитектура защиты на уровне IP. "

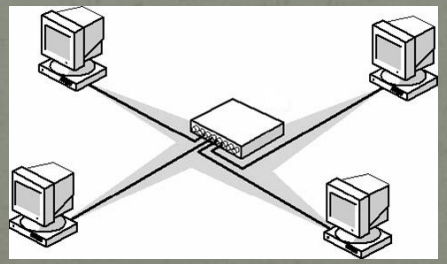
Выполнил:
Студенты группы 453 Карпов Евгений, Стрекнев Максим

Необходимость защиты данных

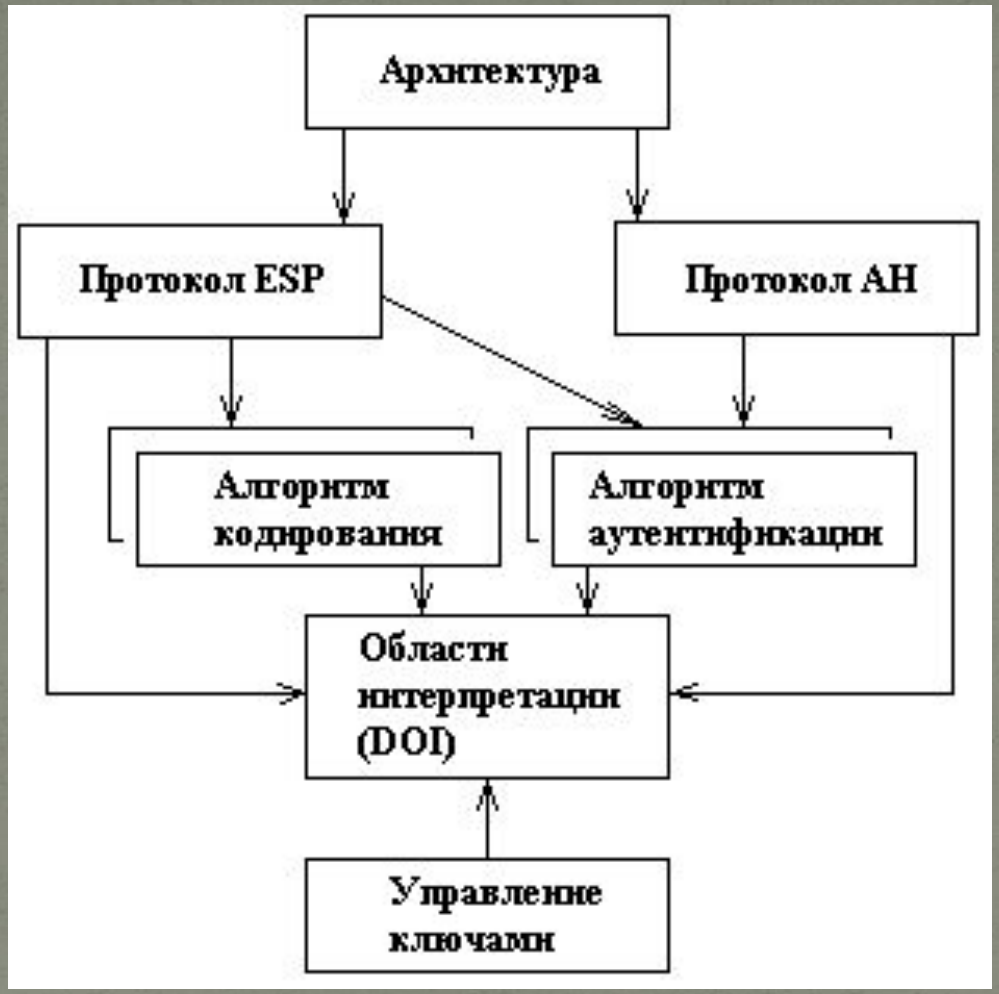
В конце шестидесятых годов американское агентство перспективных исследований в обороне DARPA приняло решение о создании экспериментальной сети под названием ARPANet. В семидесятых годах ARPANet стала считаться действующей сетью США, и через эту сеть можно было получить доступ к ведущим университетским и научным центрам США. В начале восьмидесятых годов началась стандартизация языков программирования, а затем и протоколов взаимодействия сетей. Результатом этой работы стала разработка семиуровневой модели сетевого взаимодействия ISO/OSI и семейства протоколов TCP/IP, которое стало основой для построения как локальных, так и глобальных сетей.

Краткая историческая справка появления протокола

- В 1994 году Совет по архитектуре Интернет (IAB) выпустил отчет "Безопасность архитектуры Интернет". В этом документе описывались основные области применения дополнительных средств безопасности в сети Интернет, а именно защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных. В числе первоочередных и наиболее важных защитных мер указывалась необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых телекоммуникационных сетях на базе существующих протоколов. Таким образом, начала создаваться спецификация Secure IP, дополнительная по отношению к протоколам IPv4 и IPv6.



Архитектура IPSec



Заголовок AH

- Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Транспортный режим

- Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Туннельный режим

- Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Security Associations

- Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

Политика безопасности

- Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трёх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

Оценка протокола

- Протокол IPSec получил неоднозначную оценку со стороны специалистов. С одной стороны, отмечается, что протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее (включая разработанный Microsoft PPTP). По мнению другой стороны, присутствует чрезмерная сложность и избыточность протокола. Так, Niels Ferguson и Bruce Schneier в своей работе "A Cryptographic Evaluation of IPsec" отмечают, что они обнаружили серьёзные проблемы безопасности практически во всех главных компонентах IPsec. Эти авторы также отмечают, что набор протоколов требует серьёзной доработки для того, чтобы он обеспечивал хороший уровень безопасности. В работе приведено описание ряда атак, использующих как слабости общей схемы обработки данных, так и слабости криптографических алгоритмов.

Заключение

- В этой презентации мы рассмотрели некоторые основные моменты, касающиеся протокола сетевой безопасности IPsec. Не лишним будет отметить, что протокол IPsec доминирует в большинстве реализаций виртуальных частных сетей. В настоящее время на рынке представлены как программные реализации (например, протокол реализован в операционной системе Windows2000 компании Microsoft), так и программно-аппаратные реализации IPsec - это решения Cisco, Nokia. Несмотря на большое число различных решений, все они довольно хорошо совместимы друг с другом.

Спасибо за внимание!