Arquitetura IP Security

Aluno Erick Dantas Rotole
Professor: Pedro Antonio Dourado de Rezende
Curso: Criptografia e Segurança na Informática

Arquitetura IP Security

No início do desenvolvimento do conjunto de protocolos TCP/IP, pouco ou quase nada se falava ou se desenvolvia em relação à segurança de redes. Com o surgimento de várias aplicações e o rápido crescimento da Internet, passou-se a perceber que as questões relativas à segurança de redes e sistemas tornaram-se demandas cada vez mais crescente. Enquanto a Internet se restringia aos meios científicos e acadêmicos, os problemas de segurança não eram tão críticos porque havia um certo controle baseado nos códigos de uso ético da rede. Mas, com a abertura da Internet para o setor privado, principalmente comercial, os problemas de segurança se intensificaram e ficaram críticos.
IP Security é uma das plataformas de segurança desenvolvida pelo grupo de trabalho IP Security Protocol (IPSec) da IETF (Internet Engineering Task Force) em resposta aos desafios de segurança de redes.

INTRODUÇÃO

O objetivo do grupo de trabalho *IP Security Protocol*, da IETF, é desenvolver mecanismos que forneçam proteção ao pacote IP e às aplicações que rodam sobre o protocolo IP, estabelecendo níveis de segurança para as comunicações *host-to-host, subnet-to-subnet* e *host-to-subnet*.
O *IP Security* é uma plataforma aberta formada por um conjunto de protocolos que provêm serviços de autenticação, integridade, controle de acesso e confidencialidade na camada de rede IP, tanto em ambientes IPv4 como em ambientes IPv6. Assim, a tecnologia IPSec é uma das opções de se implementar VPNs (*Virtual Private Networks*) e seus serviços podem ser utilizados por quaisquer protocolos das camadas superiores como TCP, UDP, ICMP, BGP, etc.
Será apresentado os aspectos principais da arquitetura IPSec. São apresentados os serviços fornecidos pelos protocolos, os conceitos e requisitos para associação de segurança, o esquema de funcionamento e inter-relacionamento entre os componentes IPSec e como os serviços podem ser implantados em redes IP.

ARQUITETURA BÁSICA IPSEC

OBJETIVOS E PLATAFORMA BÁSICA
A plataforma IPSec foi desenvolvida para prover serviços de segurança de alta qualidade, baseados em criptografia, para o nível IP e/ou para as camadas superiores. O conjunto de serviços oferecidos inclui controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e confidencialidade (criptografia).
Estes serviços são implementados através da utilização conjunta de protocolos de segurança de tráfego de dados, de autenticação de cabeçalho (AH - *Authentication Header*), de encapsulamento seguro do *payload* ou conteúdo dos dados (ESP - *Encapsulating Security Payload*) e de procedimentos e protocolos de gerência de chaves.
Além de ser um padrão aberto IETF que está sendo adotado por todos os fabricantes de equipamentos de redes de computadores e desenvolvedores de sistemas, por definição o IPSec possui uma arquitetura aberta no sentido de possibilitar a inclusão de outros algoritmos de autenticação e criptografia. A RFC 2411 - *IP Security Document Roadmap* - apresenta as diretrizes para produção, organização e inter-relacionamento entre os diversos documentos que descrevem o conjunto de protocolos IPSec, conforme mostrado na Figura 1 abaixo.

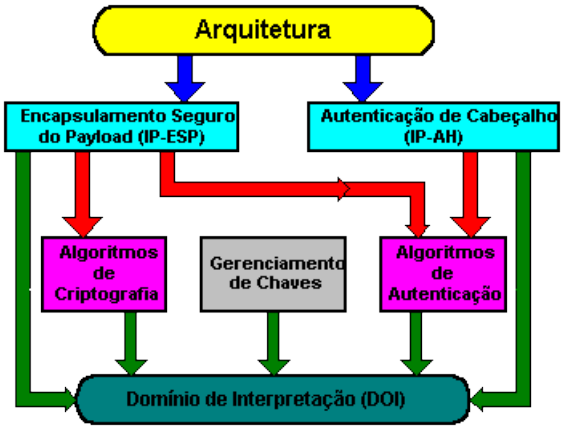

Figura 1 - Roadmap para Documentos IPSEc

O esquema apresentado acima apresenta o *roadmap* para especificações que descrevem o uso de novos algoritmos de autenticação e criptografia definidas pelo protocolo ESP (RFC 2406 - ***IP Encapsulating Security Payload***), e de autenticação definidas pelo protocolo AH (RFC 2402 - ***IP Authentication Header***).

PROTOCOLOS AH E ESP

A mesma Figura 1 pode ser utilizada para ilustrar a arquitetura IPSec de uma forma geral. Os protocolos AH e ESP fazem parte da arquitetura básica IPSec e, por questões de garantia de interoperabilidade, estes protocolos estabelecem que todas as implementações IPSec suportem alguns algoritmos pré-definidos. Para autenticação de cabeçalho, os algoritmos obrigatórios são os seguintes:

- HMAC-MD5, RFC 2403 - ***The Use of HMAC-MD5 within ESP and AH***;
- HMAC-SHA-1, RFC 2404 - ***The Use of HMAC-SHA-1 within ESP and AH***;

e para o encapsulamento seguro do *payload*, além destes dois já citados acima, os outros algoritmos são:

- DES-CBC, RFC 2405 - ***ESP DES-CBC Cipher Algorithm With Explicit IV***;
- ***Null Authentication Algorithm***;
- ***Null Encryption Algorithm***.

As especificações IPSec também suportam negociação de compressão IP definidas pela RFC 2393 - ***IP Payload Compression Protocol***.

GERENCIAMENTO DE CHAVES

Como os serviços de segurança IPSec compartilham chaves secretas que são utilizadas para autenticação, integridade e criptografia, as especificações IPSec definem um conjunto separado de mecanismos para o gerenciamento de chaves, com suporte para distribuição automática ou manual das chaves. Para distribuição manual e automática de chaves foram especificados procedimentos baseados em chaves públicas definidos pelas seguintes RFCs:

- RFC 2408 - ***Internet Security Association and Key Management Protocol (ISAKMP)***;
- RFC 2409 - ***The Internet Key Exchange (IKE)***;
- RFC 2412 - ***The OAKLEY Key Determination Protocol*** .

Mesmo com as definições dos padrões acima, as especificações IPSec permitem a inclusão de outros protocolos de gerência de chaves públicas como, por exemplo, SKIP.

FUNCIONAMENTO

O protocolo IPSec opera num *gateway* ou num *host*, com os requisitos de segurança

estabelecidos por um banco de dados de política de segurança (SPD - *Security Policy Database*) mantido pelo usuário, pelo administrador da rede ou por uma aplicação operando dentro de limites pré-definidos. Pode ser utilizado para proteger uma ou mais conexões entre um par de *hosts*, entre dois *gateways* de segurança ou entre um *host* e um *gateway*.

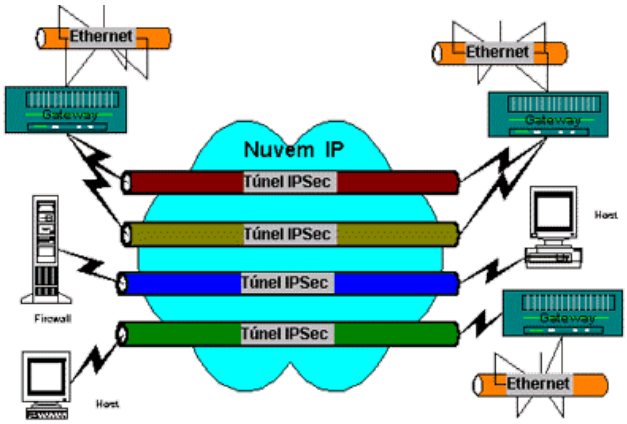

Figura 2 - Túneis IPSec entre sistemas

Os pacotes IP são selecionados através de três formas de processamento definidas por seletores. Os seletores utilizam o pacote IP e as informações do cabeçalho da camada de transporte, comparando-os com as entradas do banco de dados SPD. Com base nas políticas aplicadas e identificadas pelos seletores, cada pacote ou é submetido aos serviços IPSec, ou é permitido desprezar tais serviços ou então é descartado.
Como citado anteriormente, a arquitetura básica IPSec é formada pelos protocolos ESP e AH. O protocolo *IP Authentication Header* fornece integridade não orientada a conexão, autenticação da origem dos dados e serviço opcional *anti-replay*. Já o protocolo *IP Encapsulating Security Payload* provê confidencialidade (criptografia) e também pode prover as mesmas funções do protocolo AH já citadas. Ambos são meios para controle de acesso baseado na distribuição de chaves e no gerenciamento do fluxo de tráfego referentes aos protocolos de segurança. Podem ser empregados independentemente um do outro, ou em associação, para que um conjunto de serviços de segurança seja disponibilizado em redes IPv4 e IPv6.
Cada um destes protocolos suporta dois modos de utilização: modo transporte e modo túnel. No modo transporte, os protocolos provêm proteção primária aos protocolos das camadas superiores; e no modo túnel, os protocolos são aplicados para "tunelar" pacotes IP. Há a possibilidade do usuário ou administrador controlar a granularidade dos serviços IPSec oferecidos. Por exemplo, pode-se criar um único túnel de criptografia que transporta todos os dados entre dois *gateways* de segurança (como apresenta a Figura 2), ou podem ser criados túneis separados para cada conexão TCP entre os pares de *hosts* que se comunicam através desses *gateways*.
Os aspectos relacionados à associação de segurança serão discutidos no item reservado para este assunto, a seguir.

ONDE PODE SER IMPLEMENTADO

Em termos de desenvolvimento, o conjunto de protocolos IPSec pode ser implementado de três formas. A primeira refere-se à implementação IPSec na pilha nativa IP, aplicável tanto em *hosts* como em *gateways*. O pré-requisito para isso é o acesso ao código fonte do protocolo IP. A segunda forma de implementação, conhecida como *Bump-in-the-stack* (BITS) é usualmente utilizada em *hosts*, onde o IPSec é implementado sob o protocolo IP, entre este e o *driver* de rede local. Neste caso, o acesso ao código fonte IP não é necessário. *Bump-in-the-wire* (BITW) é a terceira forma de implementação IPSec, na qual

é utilizada uma placa processadora de criptografia tanto em *hosts* como em *gateways*.

ASSOCIAÇÃO DE SEGURANÇA

O conceito de **Associação de Segurança** - AS, (*Security Association - SA*) é um dos conceitos fundamentais do IPSec. Uma associação de segurança é uma "conexão" que viabiliza o tráfego de serviços seguros. A segurança dos serviços é garantida pela utilização dos protocolos de segurança (AH, ESP, ou ainda de ambos). Observa-se que, no caso de se usar AH e ESP em conjunto, mais de uma AS deve ser definida.

Uma associação de segurança é identificada unicamente por três parâmetros: o SPI (*Security Parameter Index*), o endereço IP de destino e o identificador do protocolo (AH ou ESP).

O **SPI** é um número que identifica uma AS, sendo definido durante a negociação que antecede o estabelecimento da mesma. Assim, todos os membros de uma AS devem conhecer o SPI correspondente e usá-lo durante a comunicação.

O **endereço IP de destino** pode ser *unicast*, *broadcast* ou ainda *multicast*. No entanto, para a definição dos mecanismos de gerenciamento de AS, o IPSec assume um endereço destino *unicast*, estendendo as definições para os casos de *broadcast* e *multicast*.

O **identificador do protocolo** é o número 51 para o AH e o número 50 para o ESP.

Ressalta-se que a negociação para o estabelecimento de uma AS envolve a definição da chave, os algoritmos de criptografia e autenticação e os parâmetros usados por estes algoritmos.

Uma AS pode ser estabelecida de dois modos diferentes: transporte ou túnel.

No **Modo Transporte**, uma Associação de Segurança é estabelecida entre dois *hosts*. No IPv4, o cabeçalho do protocolo de segurança é inserido entre o cabeçalho IP e os cabeçalhos dos protocolos de mais alto nível, como TCP ou UDP. Por outro lado, no IPv6, o cabeçalho do protocolo de segurança é inserido após o cabeçalho básico IPv6 e dos cabeçalhos de extensão *end-to-end*, e antes dos protocolos de mais alto nível.

No caso do ESP, uma AS em modo transporte provê serviços de segurança somente para os protocolos de mais alto nível, não incluindo o cabeçalho IP ou os cabeçalhos de extensão que precedem o ESP. No entanto, o AH estende a proteção a estes cabeçalhos. Isto se deve ao fato do ESP cifrar os dados que o sucedem no pacote, além de autenticar apenas a "porção ESP" do pacote, enquanto que o AH autentica o pacote todo.

Uma AS em **Modo Túnel**, é uma AS aplicada a um túnel IP. Quando, pelo menos um dos membros de uma AS for um *gateway* de segurança, ou seja, for um *gateway* que implementa IPSec, então a AS deverá ser estabelecida em modo túnel.

Em uma AS no modo túnel, o chamado cabeçalho IP externo especifica o destino no contexto do IPSec, e o cabeçalho IP interno especifica o destino real do pacote IP. Neste caso, os cabeçalhos dos protocolos de segurança são inseridos depois do cabeçalho IP externo e antes do cabeçalho IP interno. Assim, de modo análogo às considerações feitas para o modo transporte, em modo túnel, o AH provê segurança para o cabeçalho IP externo, e conseqüentemente para os protocolos de mais alto nível, assim como para o pacote IP "tunelado". Por outro lado, quando o ESP é usado em modo túnel, apenas a segurança do pacote IP "tunelado" é assegurada.

<u>AH</u>

O protocolo AH, *Authentication Header*, adiciona **autenticação** e **integridade**, ou seja, garante a autenticidade do pacote e também que este não foi alterado durante a transmissão. O AH pode ser usado no modo transporte ou no modo túnel, como descrito anteriormente.

O uso do AH previne ataques do tipo:

- *Replay*, ou seja, quando o atacante intercepta um pacote válido e autenticado pertencente a uma conexão, replica-o e o reenvia, "entrando na conversa". A

utilização do campo *Sequence Number* ajuda na prevenção a este tipo de ataque, pois permite numerar os pacotes que trafegam dentro de uma determinada AS.

- *Spoofing,* ou seja, quando o atacante assume o papel de uma máquina confiável para o destino e, dessa forma, ganha privilégios na comunicação. A utilização de mecanismos de autenticação previne este tipo de ataque.
- "Roubo de conexões" (*connection hijacking*), ou seja, quando o atacante intercepta um pacote no contexto de uma conexão e passa a participar da comunicação. A utilização de mecanismos de autenticação previnem este tipo de ataque.

A figura abaixo ilustra o cabeçalho do protocolo AH:
A figura abaixo ilustra o cabeçalho do protocolo AH:

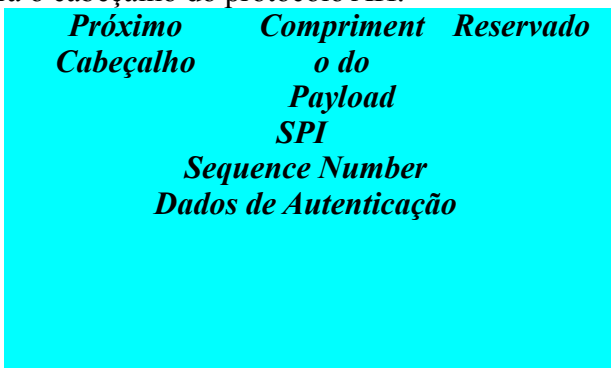

Figura 3 - Cabeçalho do Protocolo AH

A seguir são descritos os campos que compõe o cabeçalho do protocolo de segurança AH:
Próximo Cabeçalho: contém o identificador do protocolo do próximo cabeçalho.
Comprimento do Payload: comprimento do *payload* (conteúdo).
Reservado: 16 bits reservados para extensão do protocolo.
SPI (*Security Parameter Index*): este índice, em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma SA para um determinado pacote.
Sequence Number: contador que identifica os pacotes pertencentes a uma determinada AS (usado como mecanismo anti-replay).
Dados de Autenticação: campo de comprimento variável que contém o ICV (*Integrity Check Value*) para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela AS.
Observa-se que o AH adiciona autenticação, porém os dados continuam trafegando na rede intactos, e podem ser capturados através de *sniffers*, por exemplo. Assim, a confidencialidade é tratada por outro protocolo, o ESP, descrito a seguir.

ESP

O protocolo ESP, *Encapsulating Security Payload*, adiciona **autenticação** e **confidencialidade,** garantindo que somente os destinatários autorizados terão acesso ao conteúdo do pacote. O ESP pode ser usado no modo transporte ou no modo túnel, como descrito anteriormente.
O uso do ESP previne ataques do tipo:

- *Replay*, através da utilização do campo *Sequence Number,* de maneira análoga ao AH;
- "Particionamento de pacotes cifrados," que é o que acontece quando o atacante obtém partes de pacotes cifrados e consegue montar um pacote que pode ser aceito por um dos membros da conexão. O uso de autenticação previne este tipo de ataque;
- *Sniffer,* ou seja, quando o atacante obtém os pacotes que trafegam na rede. A utilização da criptografia previne este tipo de ataque.

A figura abaixo ilustra o cabeçalho do protocolo ESP:

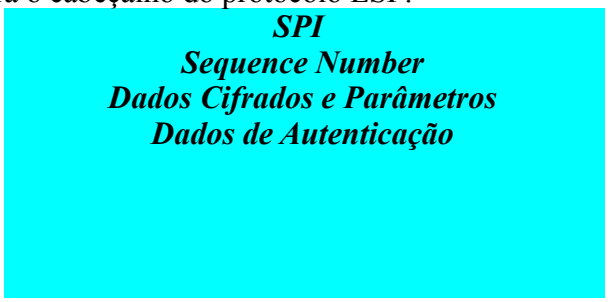

Figura 4 - Cabeçalho do Protocolo ESP

A seguir são descritos os campos que compõem o cabeçalho ESP:

SPI (*Security Parameter Index*): este índice, em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma SA para um determinado pacote.

Sequence Number: contador que identifica os pacotes pertencentes a uma determinada SA (usado como mecanismo anti-relay)

Dados Cifrados e Parâmetros: contém os dados cifrados e os parâmetros utilizados pelo algoritmo de criptografia usado, definido pela AS.

Dados de Autenticação: campo de comprimento variável que contém o ICV (*Integrity Check Value*) para este pacote, calculado seguindo o algoritmo de autenticação usado, definido pela AS.

CONCLUSÃO

O IPSec surgiu para suprir a demanda de segurança a nível de IP, tanto no IPv4 quanto no IPv6.Vários pontos devem ser analisados para uma implementação correta visando o melhor custo benefício possível à ser alcançado.

Para os casos em que se exige apenas a autenticação, ou ainda, onde a confidencialidade não deve ser usada, é recomendada a utilização do AH. No entanto, a situação ideal é a utilização de autenticação e confidencialidade, ou seja, a utilização do AH e ESP em conjunto. Mais especificamente, é recomendado o uso do ESP "**dentro**" do AH, permitindo que o destino verifique a autenticidade do pacote antes de decifrá-lo, ou ainda, verifique autenticidade e decifre o pacote em paralelo.

REFERÊNCIAS BIBLIOGRÁFICAS

http://www.rnp.br/newsgen
IPv6: The New Internet Protocol
by Christian Huitema, Second Edition, 1998, Prentice Hall
RFC 2401 - Security Architecture for Internet Protocol
ftp://ftp.ietf.rnp.br/rfc/rfc2401.txt
RFC 2402 - IP Authentication Header
ftp://ftp.ietf.rnp.br/rfc/rfc2402.txt
RFC 2403 The Use of HMAC-MD5 within ESP and AH
ftp://ftp.ietf.rnp.br/rfc/rfc2403.txt
RFC 2404 The Use of HMAC-SHA-1 within ESP and AH
ftp://ftp.ietf.rnp.br/rfc/rfc2404.txt
RFC 2405 - ESP DES-CBC Cipher Algorithm With Explicit IV
ftp://ftp.ietf.rnp.br/rfc/rfc2405.txt
RFC 2406 - IP Encapsulating Security Payload
ftp://ftp.ietf.rnp.br/rfc/rfc2406.txt

RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
ftp://ftp.ietf.rnp.br/rfc/rfc2408.txt
RFC 2409 - The Intenet Key Exchange (IKE)
ftp://ftp.ietf.rnp.br/rfc/rfc2409.txt
RFC 2411 - IP Security Document Roadmap
ftp://ftp.ietf.rnp.br/rfc/rfc2411.txt
RFC 2412 - The OAKLEY Key Determination Protocol.
ftp://ftp.ietf.rnp.br/rfc/rfc2412.txt
RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
ftp://ftp.ietf.rnp.br/rfc/rfc2460.txt