

Internet Infrastructure

K. U. Leuven 2005-2006

VPN

Table of Contents

Table of Contents	2
Virtual Private Networking	2
Why VPN?	2
A very short cryptography sidestep.....	2
Digest	2
Symmetric key cryptography	3
Public Key Cryptography.....	3
IPsec	3
Security policy.....	4
Security Association (SA).....	5
Key management.....	5
Generic Routing Encapsulation.....	5
What is GRE?.....	5
GRE usage.....	7

Virtual Private Networking

Why VPN?

Why do we need Virtual Private Networking (VPN)? What is wrong with TCP/IP? For many uses of the network it is not secure enough. It is insufficient to protect commercial internet traffic. VPN provides additional security measures to safeguard integrity, authentication, and confidentiality

A VPN implementation using cryptographic measures to achieve its goals. Its operation is based on digest computation, symmetric key cryptography (private key), and public key cryptography (asymmetric cryptography).

A very short cryptography sidestep

Digest

A digest is also called a one-way (hash) function. It maps many bytes to one bit string of defined length. The function has the following properties:

- It is very sensitive to -even single bit- changes
- It is hard to reverse: it is very difficult to find any message with a given digest. This property is why it called one way: easy to compute, but hard to reverse to some input.
- A birth day attack is highly unlikely: just finding any two messages with same digest.
- Collisions (multiple messages mapping onto the same hash) is highly unlikely: massive amounts of digest still are all unique. This property is based on the large target space, and a uniform distribution of results over this space.

The best –known hash functions are MD5, SHA-1, RIPEM.

Symmetric key cryptography

The sender and the receiver share a secret, the one symmetric key. The sender and the receiver use an algorithm they both agreed to use. Encryption and decryption may be different computations. The whole strength of the encryption is in the key (space), not in the algorithm. The best-known symmetric key algorithms are RC4, DES and 3DES, and AES.

Apart from the cipher, the way the algorithm operates is also important. The first distinction is between block per block mode or stream mode. RC4 is a stream cipher, the others are block ciphers. Within block ciphers, one can encrypt each and every block independently, or the last result can be used to compute the result of the next block, chaining. Chaining starts typically with a random block of data, the initialization vector (IV). The algorithm, the block handling are all known and not secret.

A crucial problem with symmetric key algorithms is the problem of how to establish the secret? How is the key agreed upon? Sending the key unencrypted to start is blowing all security out of the water. There are three prime methods: out-of-band exchange (via telephone, mail (not e-mail)), using Diffie-Helman, or using public key cryptography.

Public Key Cryptography

Public key cryptography is based on key pairs, two linked keys. One key is kept private (secret), the other one may be published (in principle). A message encrypted with one key can only be decrypted with the other:

- $m = \text{decrypt}(\text{public}, \text{encrypt}(\text{private}, m))$
- $m = \text{decrypt}(\text{private}, \text{encrypt}(\text{public}, m))$

The way this is used is simple: to prove that you have the private key, you encrypt something with your private key. Anyone can check that you did it. They just decrypt it with your public key. This system supports authentication and digital signing.

Alternatively, anyone can encrypt something for you. They use your public key, and only the one who possesses the private key can decrypt the message. This mechanism is the basis for confidentiality protection.

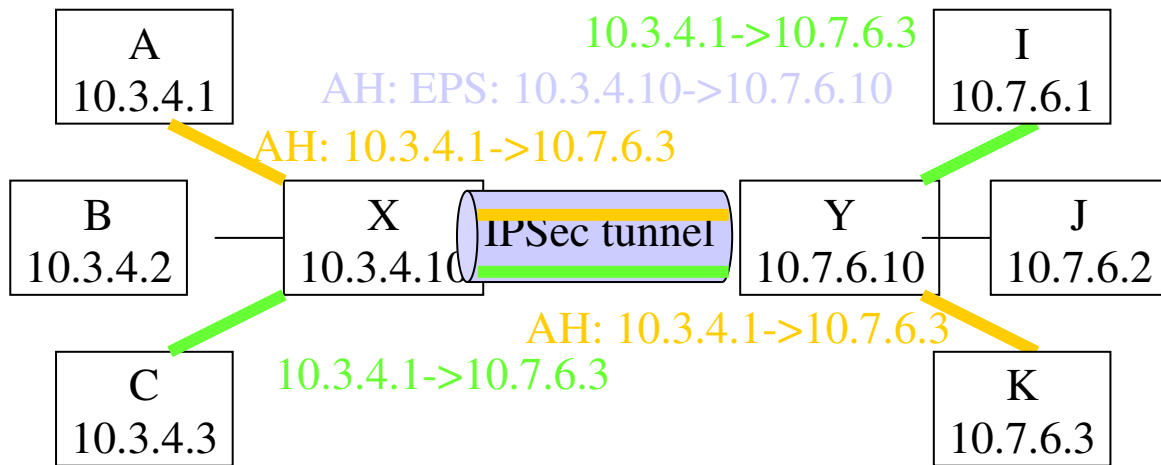
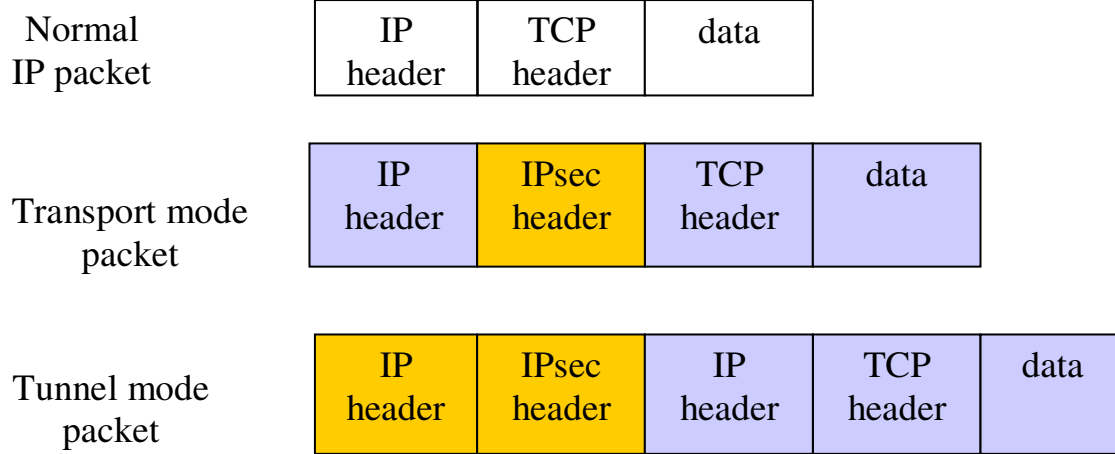
Note that the link between the public key and the entity is critical in both systems. If one cannot be sure about this link, the system does not work. Certificates use signing by a trusted party to vouch for this link. The public key of the trusted third party is now the weak spot.

The prime public key technology examples are RSA, DSA, and ECC.

IPsec

The IPsec architecture is published in RFC 2401. IPsec defines two protocols: AH and ESP. Authentication Header(AH) is defined in RFC 2402. It provides integrity and authentication. Encapsulating Security Payload (ESP) is defined in RFC 2406. It provides integrity and confidentiality.

There are two modes of operation: transport mode, which is point-to-point, and tunnel mode.



- A authenticates towards K (IPSec A & K)
- X authenticates towards Y (IPSec X & Y)
- X protects communication from 10.3.4.* to 10.7.6.* (IPSec X & Y)

Security policy

The IPSec security policy defines the required security services for connections.

The security policy is defined by:

- ✓ The source & destination IP
- ✓ The DNS name
- ✓ The protocol
- ✓ The source & destination port (if applicable)

The security policies are kept in the Security Policy Database (SPD).

The security policy is the starting point to negotiate the Security Associations (SA).

Security Association (SA)

A Security Association (SA) is the actual result of the negotiation between the two parties. It is an agreement on the communication parameters. There is an SA per direction: one from A to B, and one from B to A. Obviously:

✓ $SA_{out}(A) = SA_{in}(B)$

✓ $SA_{in}(A) = SA_{out}(B)$

Each SA has an identifier (ID). That identifier is called the Security Parameter Index (SPI). The SAs are kept in a database, the SA Database (SAD).

Key management

In all distributed systems that need to encrypt the communication there is a need to establish the encryption keys. The key exchange cannot be in the clear, otherwise all the security is gone.

There are a number of options to exchange the shared secret.

Option one is to exchange the keys out-of-band, that is, using an alternative channel. In practice, this often means that the key is manually configured on both sides. If there are too many systems manual configuration becomes unmanageable.

A second system is the use of a key exchange mechanism that establishes a shared secret in such a way that a passive attacker cannot derive the key from the communication exchange. The Diffie-Hellman key exchange accomplishes this. To prevent an active man-in-the-middle attack, the parties have to authenticate mutually.

A last system is the bootstrap on public key cryptography. The key seeds can be encrypted with the counterparty public key, which only the counter party can decrypt. Note that the public key must belong to that party for sure, otherwise there is a problem. One way to be sure is the use of a certificate. Now you need only to be sure of the CA public key.

IPSec has defined a key exchange mechanism: the Internet Key Exchange: IKE. It is described in RFC 2409. It uses Diffie-Hellman key exchange, with authentication based on either a shared secret, using HMAC-SHA, or DSA / RSA signatures.

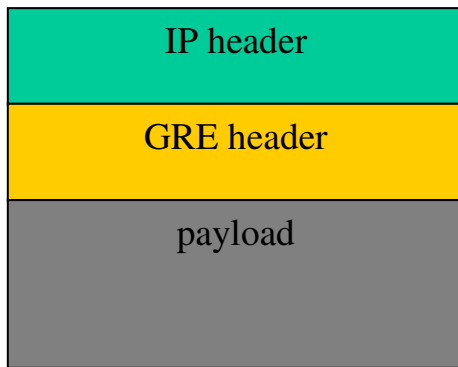
Generic Routing Encapsulation

What is GRE?

Generic Routing Encapsulation (GRE) is a generic encapsulation method to let any protocol run over TCP/IP, also TCP/IP. There is sometimes the need to encapsulate protocols in other protocols? For example, IPX over TCP/IP: some systems still use IPX, and are linked with IP networks. As another example, one may want to run broadcast-based systems over the extranet, whereby some links across the public internet must be bridged.

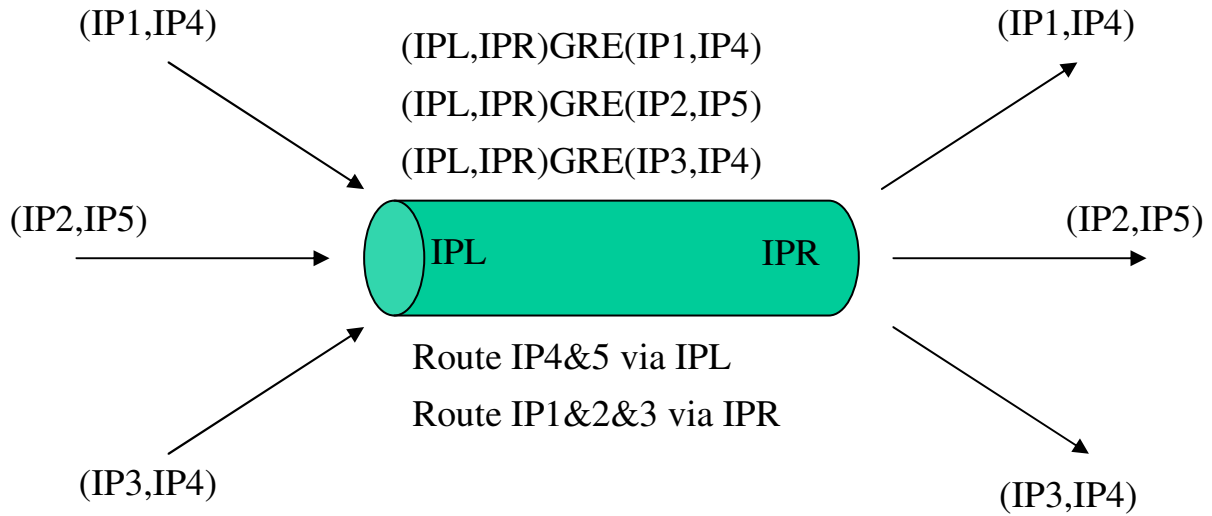
GRE encapsulation is defined in the RFC 2784. The original packet is called the payload packet. The payload packet is wrapped with a GRE header. Another protocol, called the carrier protocol, is used to deliver the packet. In this course we focus on IPv4 as carrier protocol.

GRE is defined as a specific IP protocol, number 47. The GRE protocol version for IPv4 is 0x800. An optional checksum provides packet integrity, when needed.



GRE usage

The main reason to discuss GRE here is for its nice cooperation with IPSec.



Combined with IPSec:

