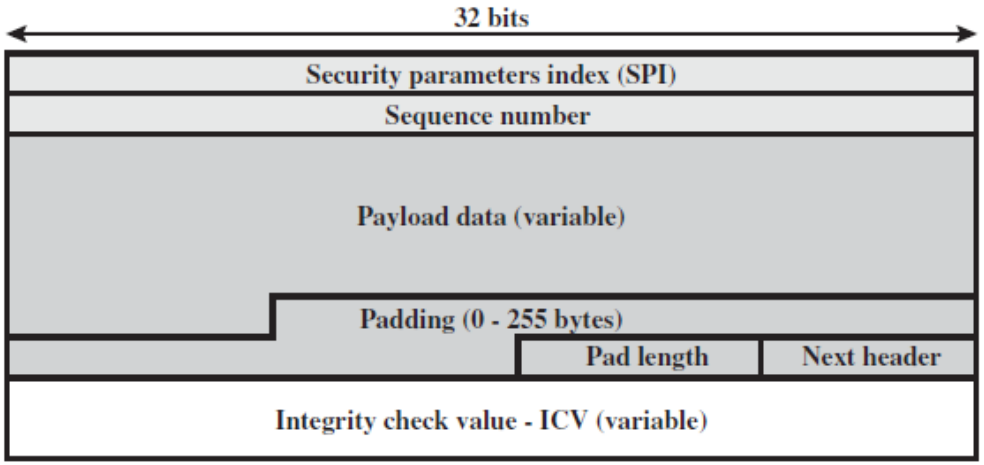
Tutorial 5

IPSec ESP Packet



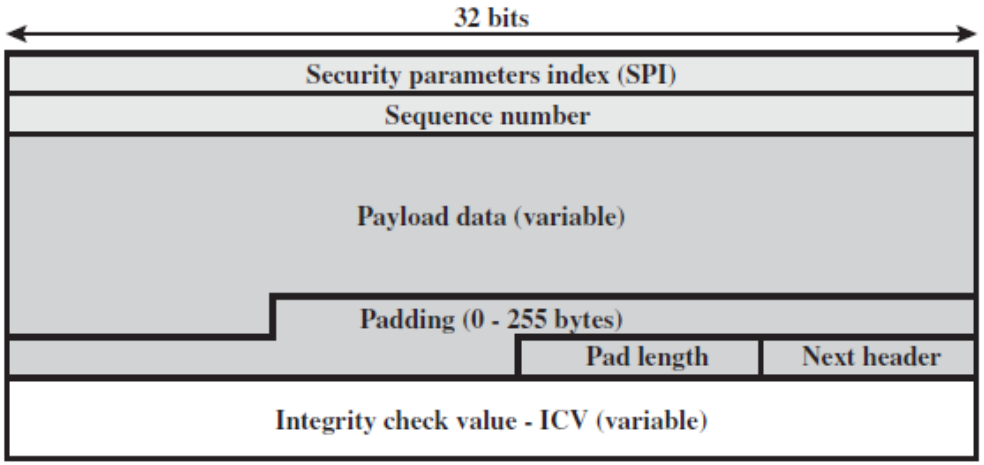
(a) Top-level format of an ESP Packet

Explain each component in the above picture.

1.1 Which components are encrypted?

- dark grey fields

IPSec ESP Packet



(a) Top-level format of an ESP Packet

Explain each component in the above picture.

1.2 Which components are authenticated?

- all the grey fields

Anti-replay in IPSec

1.3 How does IPSec prevent replayed packet?

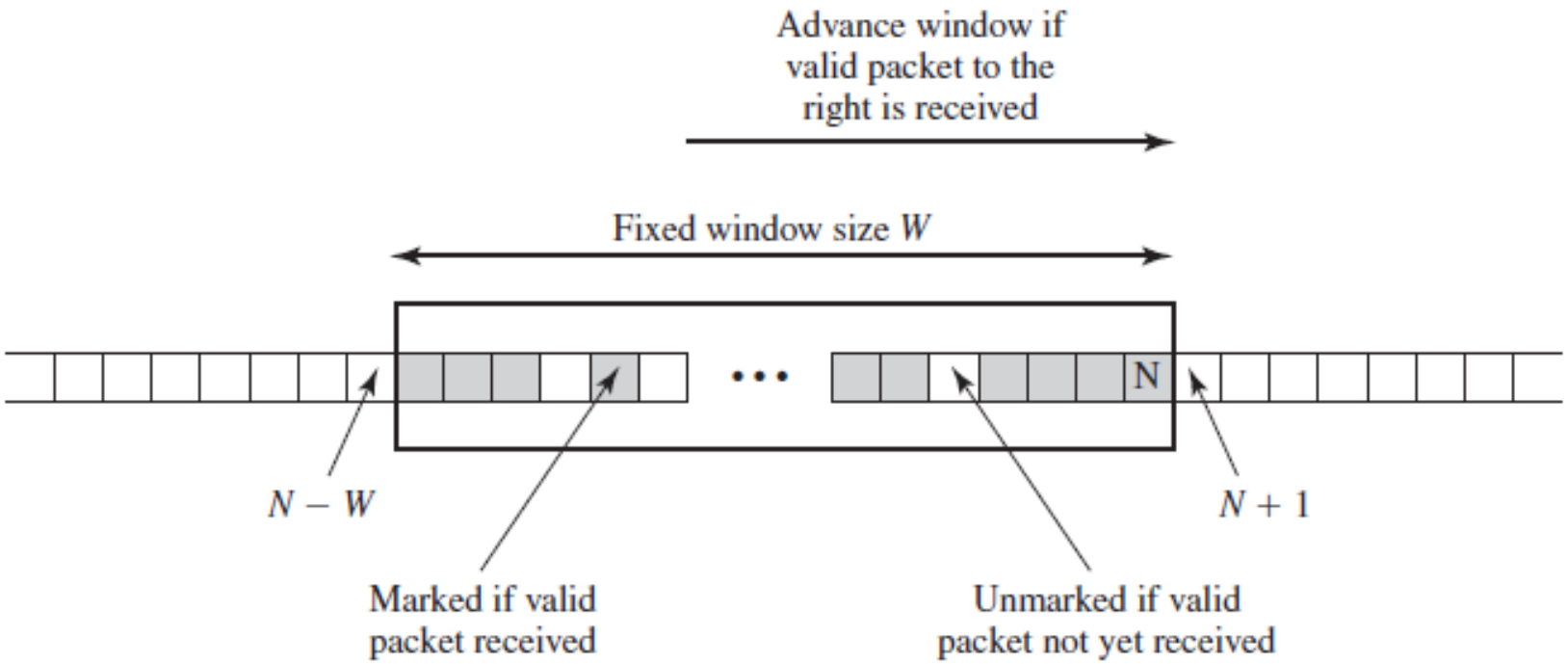
- A Non-repeating sequence number (refer to the figure in the previous slide) is used to prevent replay.

Anti-replay in IPSec

1.4 Internet protocol is connectionless, will this feature of IP affect IPSec operation?

- Yes, the sequence numbers in individual packets may not arrive in order, which could affect the validation of some late packets with smaller sequence numbers.
- Solution: use a sliding window (next slide).

Anti-replay in IPSec



1.5 What does “mutable but predictable” mean in the context of IPSec messages? Why can fields with this property be included in Authentication Header integrity checks?

- Mutable fields change during transmission. Sometimes though the final values of the fields are predictable, these fields are then referred to as mutable but predictable.

- They can be included in AH integrity since the sending system can determine the information the receiving system is going to have.

1.6 If IPSec provides security at the network/IP layer, why are security mechanisms still needed above that level (in applications for example)?

- The philosophy behind IPSec is that implementing security within the operating system causes all applications to be protected without the applications needing to be modified but...
- Not everyone has IPSec. The "not modifying the applications" clause is a problem.
- Many applications rely on user identification which isn't currently obtainable from IPSec.

1.7 What is a reflection attack?

The adversary replays an authentication tag from the original sender.
Such attacks are usually against symmetric key based authentication schemes.
Consider firstly the "optimized" mutual authentication based on a K_{AB}, a shared key between Alice and Bob.

A → B : I'm Alice, R_2
B → A : R_1, $f(K_{AB},R_2)$
A → B: $f(K_{AB},R_1)$

f is "some cryptographic function"…

Reflection phase One
E → B : I'm Alice, R_2
B → E : R_1, $f(K_{AB},R_2)$

Eve cannot go any further directly but …

Reflection phase Two
E → B : I'm Alice, R_1
B → E : R_3, **$f(K_{AB},R_1)$**

in this phase she uses R_1 as the authentication challenge to get the response she needs to fill in the third step in the reflection phase one.

1.8 Describe the following attacks:

a) *SYN flooding.*

b) *IP spoofing.*

c) *IP Hijacking.*

SYN flooding is a type of denial-of-service attack with some extra ramifications. It involves sending lots of (TCP) SYN packets to a server, from random IP addresses.

SYN packets are used in TCP to synchronise sequence numbers on between connecting computers. The packets are sent to lots of ports, often to all of them (repeatedly to perform DOS).

Acknowledgements or reset messages indicate which ports are open to communicate. Resets mean they are closed and not vulnerable. Open ones cannot respond to the fake IP addresses, but stay open and vulnerable until time-out, the idea being another SYN packet arrives before then.

Attempting to find the open ports is **SYN scanning**, **SYN flooding** is related.

IP spoofing is where an attacker uses the IP address of a trusted host. If they are going to be successful they have to modify packet headers to be consistent with the identity they are spoofing.

IP hijacking is similar. Sometimes a bit like man-in-the-middle in the context of client-server communications.

Three basic methods:

Hijack an unused address: Avoids conflict. DoS can be used to shut down the device normally at the address.

Redirect hijacking: Redirect a network connection to alternate hosts, using ICMP redirect messages.

Promiscuous hijacking: The attacker needs to be on the path between the source and destination and basically acts as a man-in-the-middle.

1.9 Consider the following protocol:

A → B : I want to talk, g^a mod p

B → A : OK, g^b mod p

A → B: g^{ab} mod p{"Alice", $[g^a \text{ mod } p]_{Alice}$}

B → A: g^{ab} mod p{"Bob", $[g^b \text{ mod } p]_{Bob}$}

These are messages encrypted with g^{ab} and containing signed identities.

a) *What is the general purpose of the protocol?*

b) *What is the advantage for Bob of this form?*

c) *Can you think of a mechanism to give this advantage to Alice instead of to Bob?*

d) *Can you describe a mechanism to provide this property for both Alice and Bob?*

You may need to give the parties additional key information to give protocols of the types requested.

1.9 Consider the following protocol:

A → B : I want to talk, g^a mod p

B → A : OK, g^b mod p

Let us have a key for secure communication

A → B: g^{ab} mod p{"Alice", $[g^a \text{ mod } p]_{Alice}$}

I am Alice. Who are you?

B → A: g^{ab} mod p{"Bob", $[g^b \text{ mod } p]_{Bob}$}

I am Bob.

a) The purpose is key establishment and mutual authentication.

b) Bob's identity is protected if the other party (who should be Alice) fails to provide a suitable signature in the third step.

c) Here goes one way:

$A \rightarrow B$: *I want to talk,* $g^a \bmod p$

$B \rightarrow A$: *OK,* $g^b \bmod p$, $g^{ab} \bmod p\{\text{“Bob”}, [g^b \bmod p]_{Bob}\}$

$A \rightarrow B$: $g^{ab} \bmod p\{\text{“Alice”}, [g^a \bmod p]_{Alice}\}$

d) Let Alice have Bob's public encryption key:

$A \rightarrow B$: *I want to talk,* $g^a \bmod p$

$B \rightarrow A$: *OK,* $g^b \bmod p$

$A \rightarrow B$: $g^{ab} \bmod p\{E_{Bob}[\text{“Alice”}, [g^a \bmod p]_{Alice}]\}$

$B \rightarrow A$: $g^{ab} \bmod p\{\text{“Bob”}, [g^b \bmod p]_{Bob}\}$

2.0 Two computers A and B are running IPSec protocols. Then, all applications (email, website, and other apps) communicating between A and B will be protected?

- YES. IPSec protocol provides security protections on all communications between two IP addresses.

2.2 Two computers A and B are running IPSec protocols. Then, a hacker cannot see the communications by all applications (email, website, and other apps) between A and B will be protected?

- No. IPSec provide both AH protocols (for integrity) and ESP protocols (for confidentiality).

2.3 Two computers A and B are running IPSec protocols. Then, an application such as gmail in computers A and B must communicate something. True?

- No. IPSec also provides tunel mode. That is, A might be communicating with C while asking B to forward the request from A and receive response from C.