Modified ESP

Steven M. Bellovin

smb@research.att.com

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

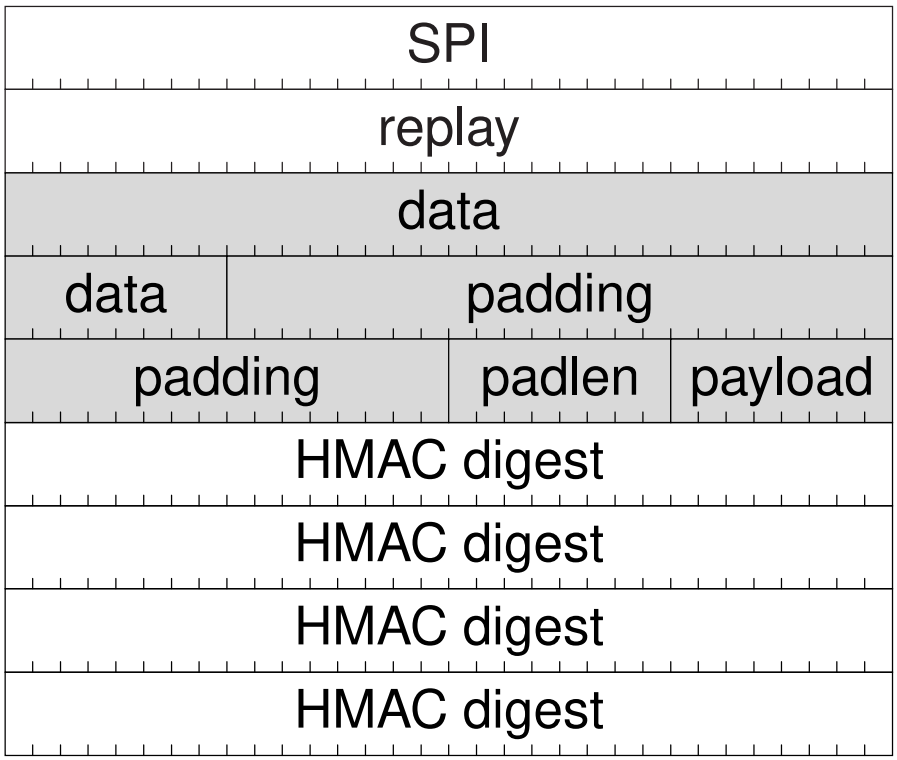
Intent

- Suggest *possible* new ESP variant.
- *Not* yet time for a standards-track RFC.
- Let's discuss if it's secure enough, and useful enough.
- Lynch me at some other meeting, not today.

Why Other Areas Hate ESP...

- Can't look at port numbers, sequence numbers, etc.
  $\Rightarrow$Problem for firewalls, too.
- Harder to do traffic engineering.
- Can't replay packets to help wireless nets.
- Can't diddle window size.
- NAT-unfriendly.
  $\Rightarrow$Some of us think of that as a feature...

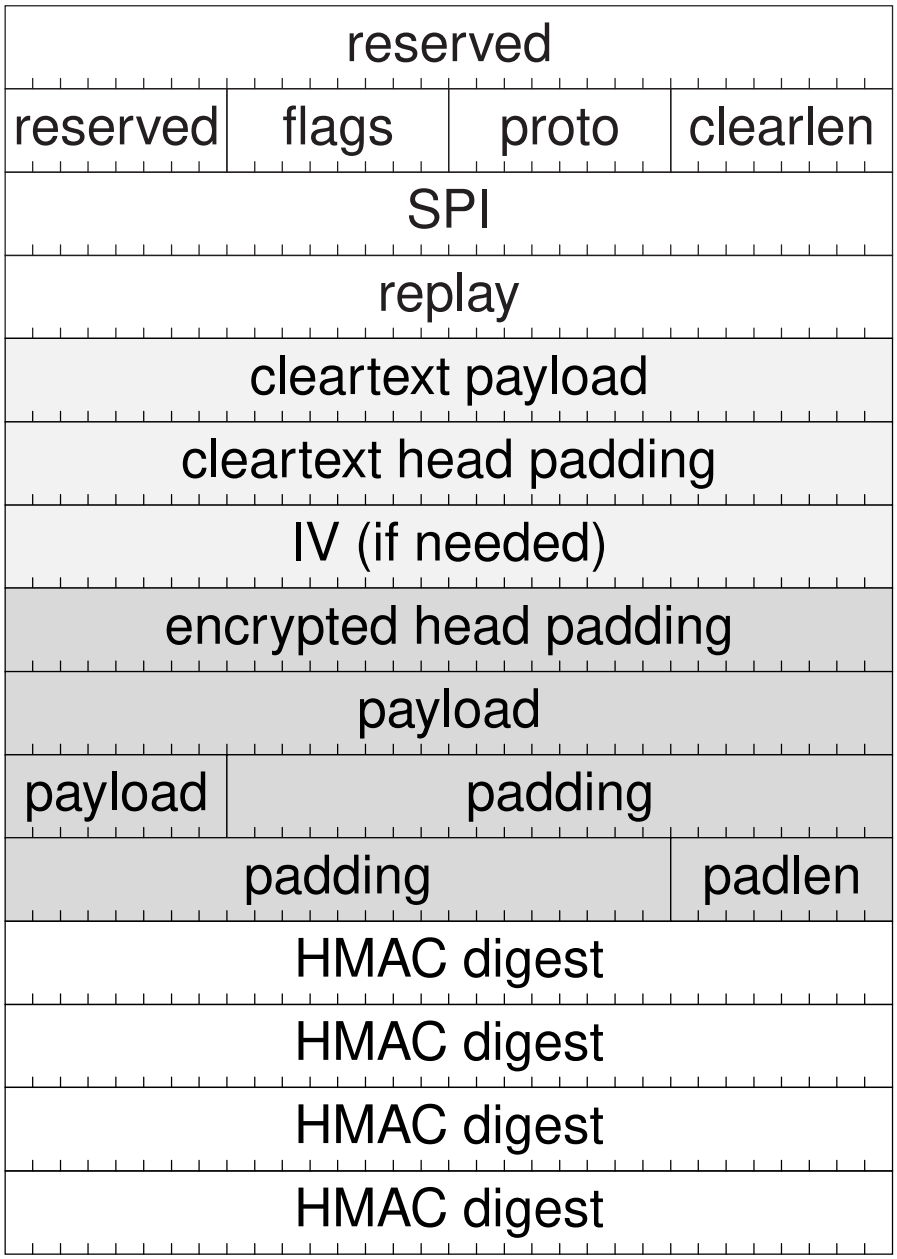
Current Format



New Ideas

- Specify that leading portion of payload (i.e., IP and TCP headers) *may* be in clear.
- Add cleartext header padding after cleartext, so that cleartext can be a multiple of cipher block size.
- Add encrypted header padding, for boundary alignment. (N.B. If cleartext header is multiple of cipher block size, no padding is used; otherwise, the total header padding is exactly one cipher block.)
- Move protocol number to start, in the clear.
- Except for protocol number, exposure completely under control of endpoints—negotiate cleartext size.

Proposed New Format



Flags, Reserved

- Flag bit—”replayable”.
- Other flags—diffserv use?
- Can we exclude first word from authentication check? If so, we can add modifiable fields.