Transport-Friendly ESP

Steven M. Bellovin
AT&T Labs Research
smb@research.att.com
http://www.research.att.com/~smb

Layer Violations for Fun and Profit

Steven M. Bellovin
AT&T Labs Research
smb@research.att.com
http://www.research.att.com/~smb

Assumptions

- It is reasonable for some authorized parties to look at some packet header fields.
  - It is relatively harmless if unauthorized parties see the same fields.
- These authorized parties should not participate in the key management dialog, nor should they be given keying material.
- Packet examination should be context-free.
- Packet modification is not necessary (or desirable).

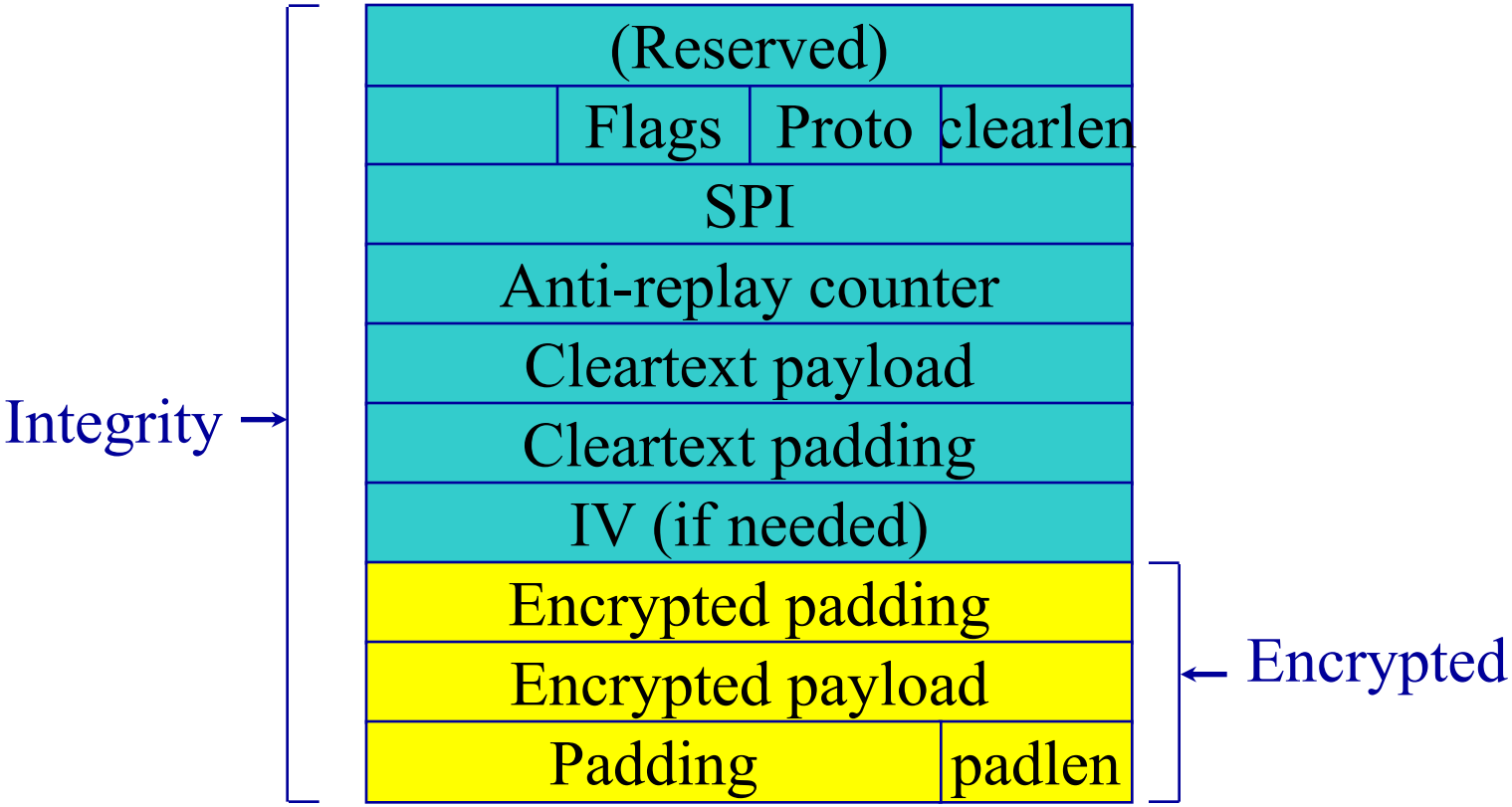
Is this Necessary? Safe?

- Many reasons already given for packet header inspection.
- (Unauthorized) eavesdropper primarily learns IP addresses and port numbers.
  - The former are very hard to conceal; the latter are probably discernable by traffic analysis.
- Don’t share keys, so monitoring station subversion not a serious problem.

Principles for Proposed Scheme

- Packets specify amount of leading portion that is in the clear.
  - Exposure amount optional and negotiated.
  - Don’t change integrity check boundary at all.
- Add padding, for boundary alignment and cipher blocksize match.
- Move protocol number to the start, in the clear.

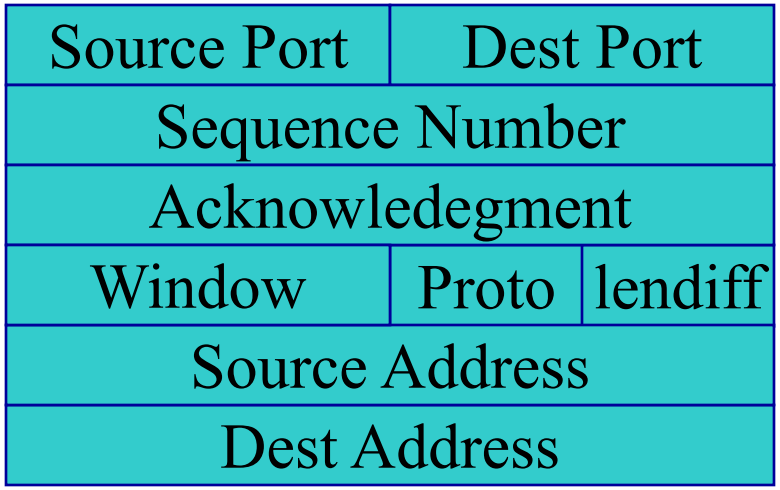
Proposed TF-ESP Format



Features

- Flag bit -- “replayable”.
- Possibly move integrity check boundary, to permit modifiable fields.
  - Are there any safe ones?
- Header fields at fixed offsets from start (unless, of course, there are IP options).
- Cleartext boundary is dangerous -- better not expose TCP checksum on short packets!

“Disclosure” Header



A Cleaner Solution?

- Contains copies of interesting encrypted fields.
  - Must be truthful or zero.
- Leaks almost as much information.
  - But easier to avoid mistakes.
- Possibly larger than TF-ESP scheme.
- Provides high-quality plaintext/ciphertext pairs.
  - Could we just use a stronger cipher?

Suggested Alternatives

- SSL
  - Must change every application.
  - Vulnerable to active denial-of-service attack.
  - Doesn’t handle UDP.
- SSL plus AH
  - Must still change every application.
  - Still doesn’t handle UDP.