# iaPCBC for IPsec

*Steven M. Bellovin*

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

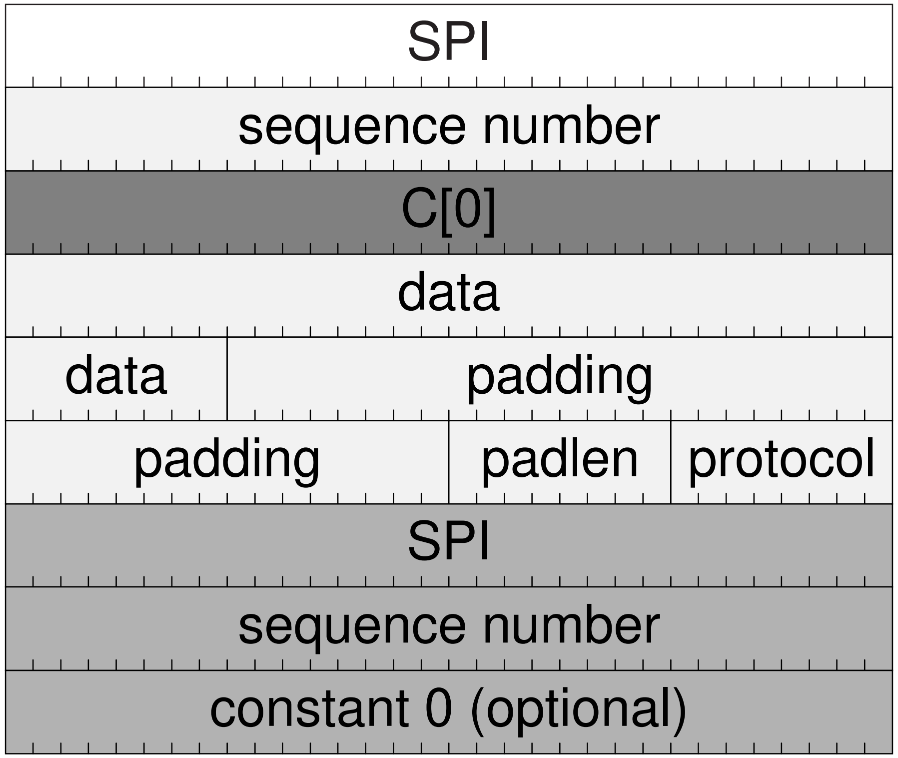
# Why iaPCBC?

- "Integrity-aware Plaintext-Ciphertext Block Chaining", devised by Gligor and Donescu.
- Very efficient — provides confidentiality and integrity in one pass.
- Short key-length ciphers such as DES are secure if used that way.
- Operates by having chaining value depend on all prior blocks of ciphertext.

# Operation

- IV-like initial block produced.
- Payload encrypted with new mode of operation.
- Any 0-cost integrity-check value can be appended (and encrypted); we use the SPI and the sequence number, since those must be protected as well.
- Decryptor verifies that decrypted version of SPI, seq match plaintext versions.

# Packet Layout



# Keying

- Two keys needed – one for confidentiality, one to produce C[0].
- Per-key, per-packet unique, secret number needed to produce C[0]. PRNG (or even a counter) can be used; seed MUST be unguessable.

# Structural Issues

- APIs, IKE not designed for combined transform.
- With some implementations, can used shared buffer between integrity module and encryption module.
- Use two iaPCBC DOI values, one for confidentiality and one for integrity; specify that these can only be used as a pair.
- Other possibilities discussed in draft.

# References

- Gligor will discuss iaPCBC design in the SAAG session on Thursday.
- My draft is at http://www.research.att.com/˜smb/papers/draft-bellovin-iapcbc-00.txt.