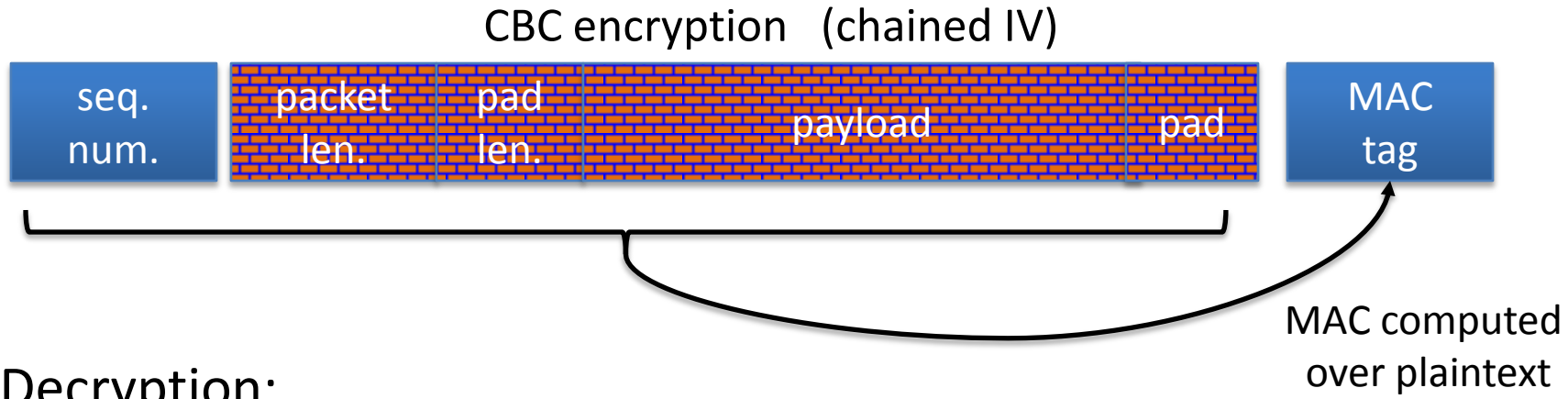
Authenticated Encryption

Attacking non-atomic decryption

SSH Binary Packet Protocol

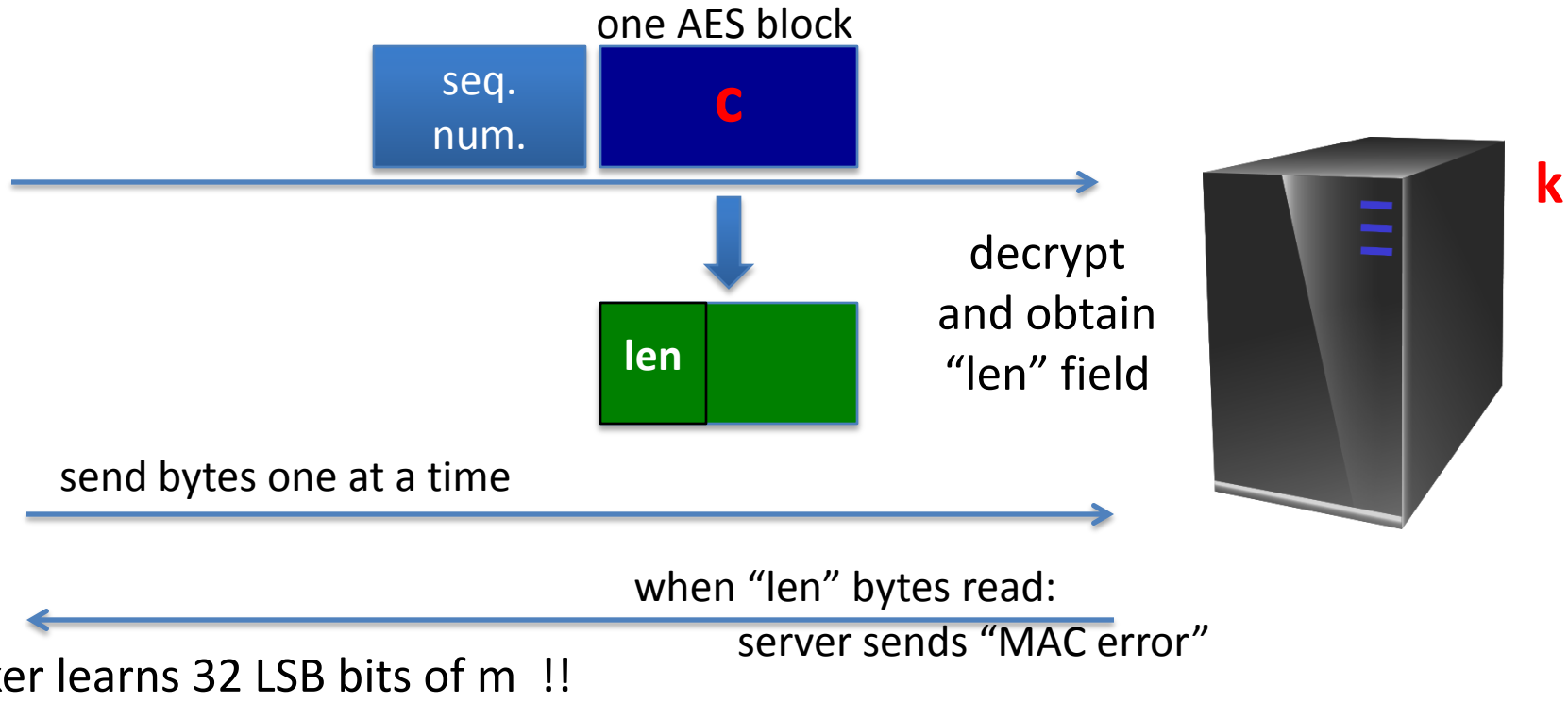


Decryption:

- step 1: decrypt packet length field only (!)
- step 2: read as many packets as length specifies
- step 3: decrypt remaining ciphertext blocks
- step 4: check MAC tag and send error response if invalid

An attack on the enc. length field (simplified)

Attacker has <u>one</u> ciphertext block **c = AES(k, m)** and it wants **m**



Lesson

The problem: (1) non-atomic decrypt

(2) len field decrypted and used it before it is authenticated

How would you redesign SSH to resist this attack?

- Send the length field unencrypted (but MAC-ed)
- Replace encrypt-and-MAC by encrypt-then-MAC

- Add a MAC of (seq-num, length) right after the len field
- Remove the length field and identify packet boundary by verifying the MAC after every received byte

Further reading

- The Order of Encryption and Authentication for Protecting Communications, H. Krawczyk, Crypto 2001.
- Authenticated-Encryption with Associated-Data, P. Rogaway, Proc. of CCS 2002.
- Password Interception in a SSL/TLS Channel, B. Canvel, A. Hiltgen, S. Vaudenay, M. Vuagnoux, Crypto 2003.
- Plaintext Recovery Attacks Against SSH, M. Albrecht, K. Paterson and G. Watson, IEEE S&P 2009
- Problem areas for the IP security protocols, S. Bellovin, Usenix Security 1996.

End of Segment