Authenticated Encryption

Active attacks on CPA-secure encryption

Recap: the story so far

Confidentiality: semantic security against a CPA attack

- Encryption secure against **eavesdropping only**

Integrity:

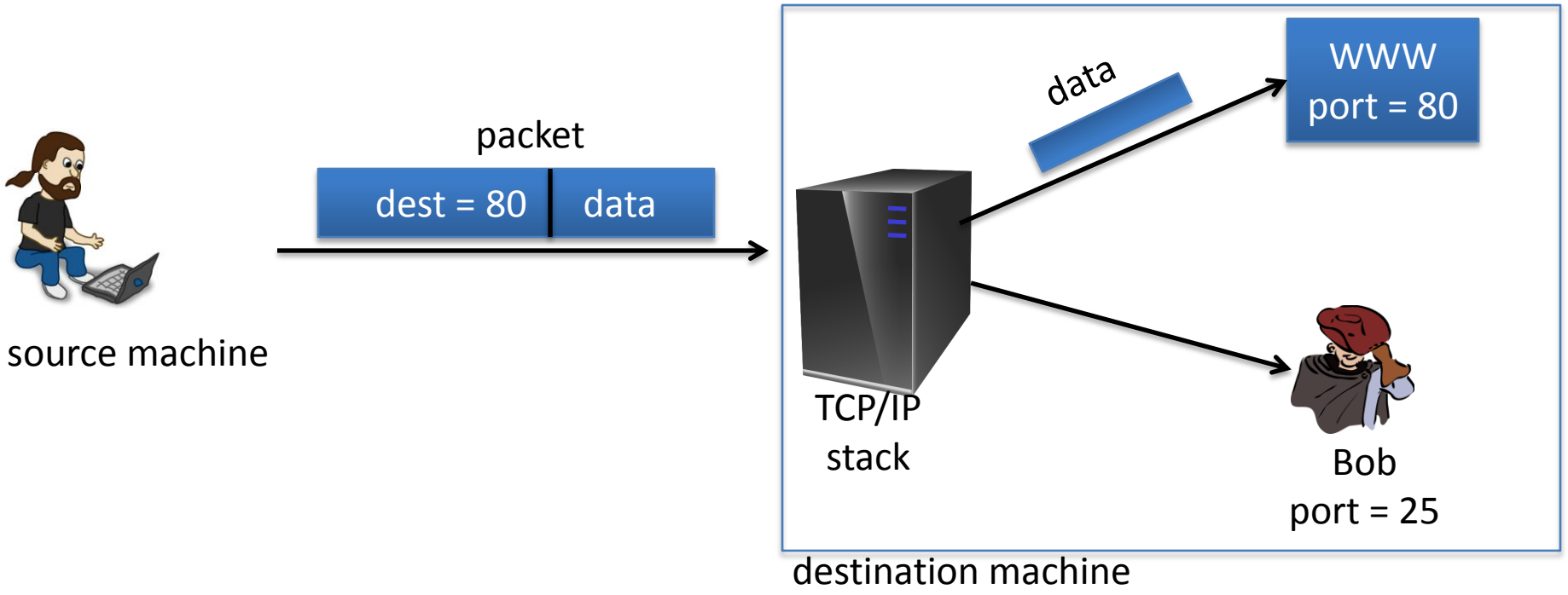
- Existential unforgeability under a chosen message attack
- CBC-MAC, HMAC, PMAC, CW-MAC

This module: encryption secure against **tampering** (active adversary)

- Ensuring both confidentiality and integrity

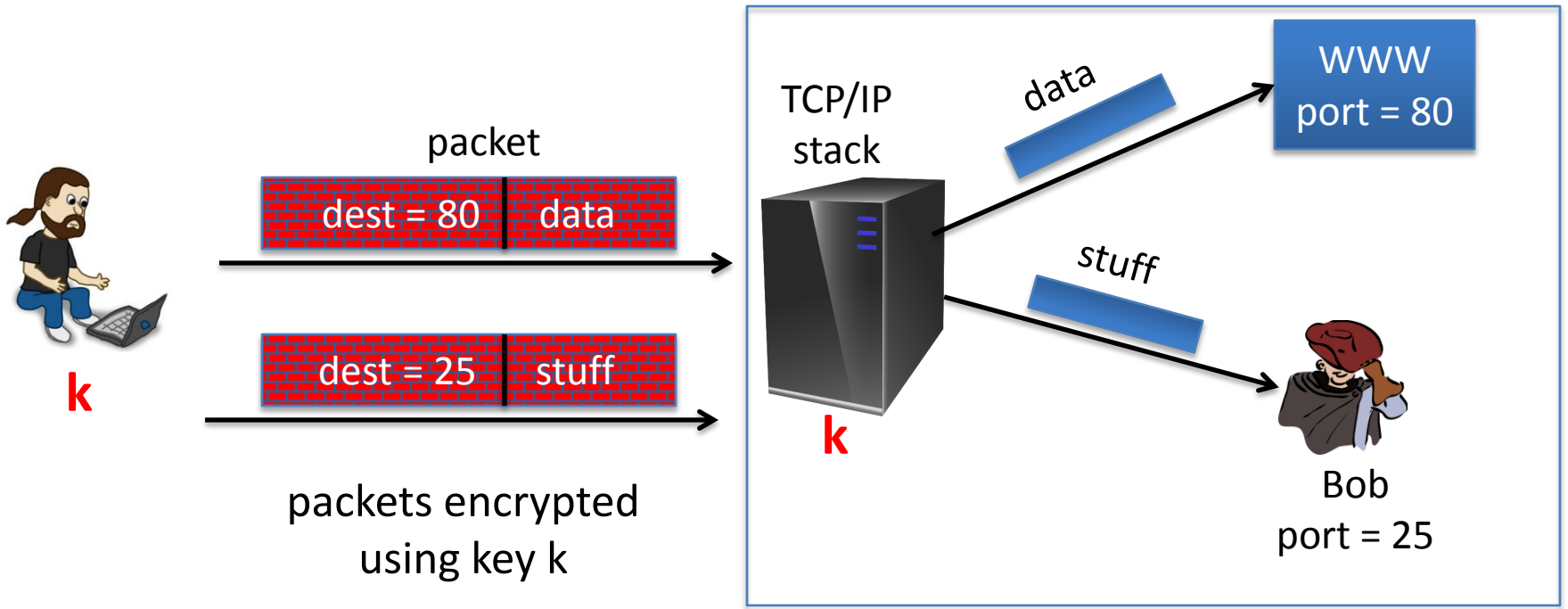
Sample tampering attacks

TCP/IP: (highly abstracted)



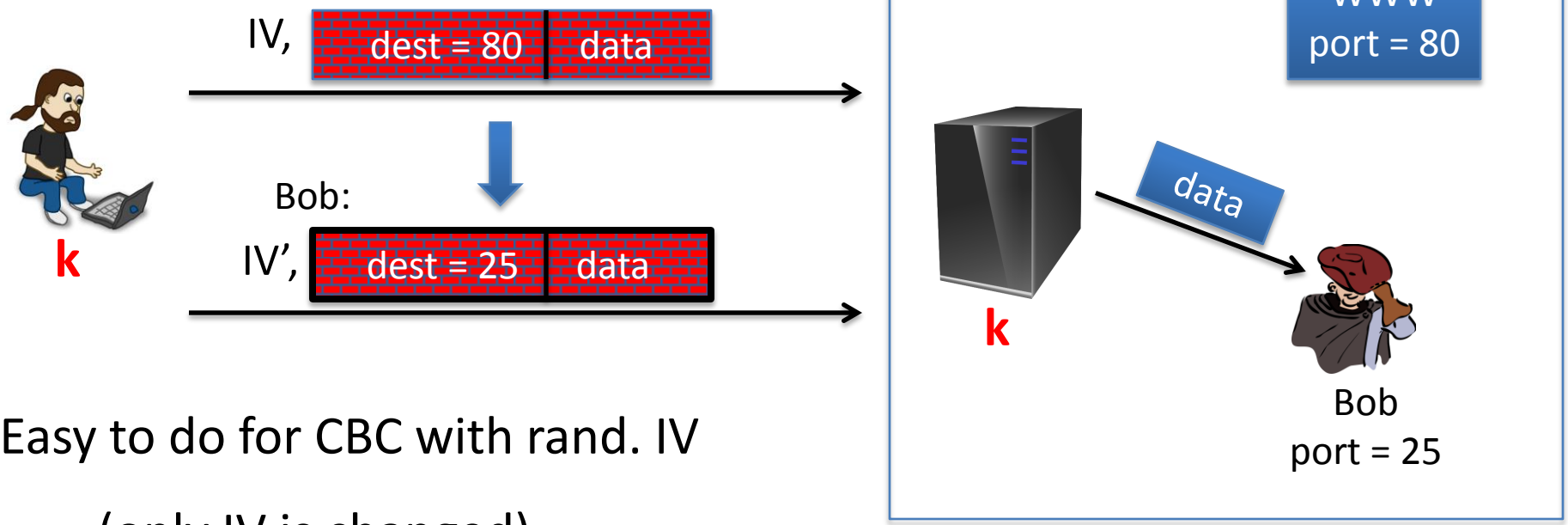
Sample tampering attacks

IPsec: (highly abstracted)



Reading someone else's data

Note: attacker obtains decryption of any ciphertext beginning with "dest=25"



Easy to do for CBC with rand. IV

(only IV is changed)

Encryption is done with CBC with a random IV.

What should IV' be?

$m[0] = D(k, c[0]) \oplus IV$ = "dest=80…"

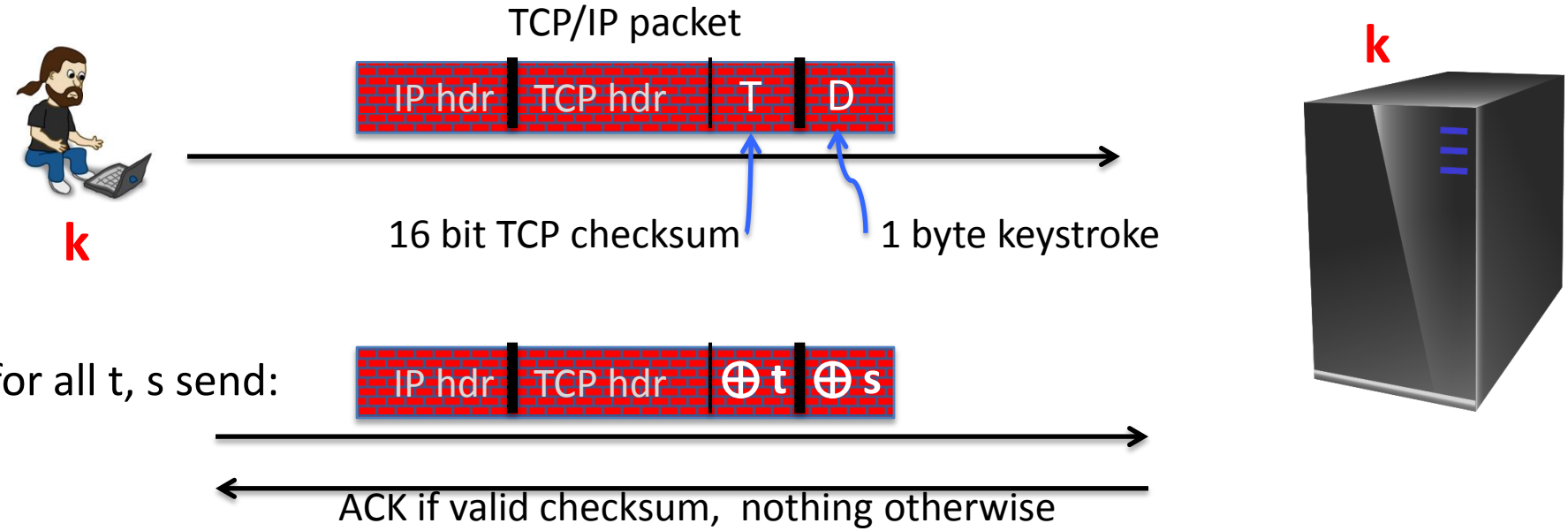
- ○ $IV' = IV \oplus (\ldots 25 \ldots)$
- ○ $IV' = IV \oplus (\ldots 80 \ldots)$
- ○ $IV' = IV \oplus (\ldots 80 \ldots) \oplus (\ldots 25 \ldots)$
- ○ It can't be done

$D(k, c[0]) \oplus IV' = D(k, c[0]) \oplus IV \oplus 80 \oplus 25$

$= \ldots 25 \ldots$

An attack using only network access

Remote terminal app.: each keystroke encrypted with CTR mode



{ checksum(hdr, D) = t ⊕ checksum(hdr, D⊕s) } ⇒ can find D

The lesson

CPA security cannot guarantee secrecy under active attacks.

Only use one of two modes:

- If message needs integrity but no confidentiality:

  use a **MAC**

- If message needs both integrity and confidentiality:

  use **authenticated encryption** modes (this module)

End of Segment