Authenticated Encryption

Hyoungshick Kim

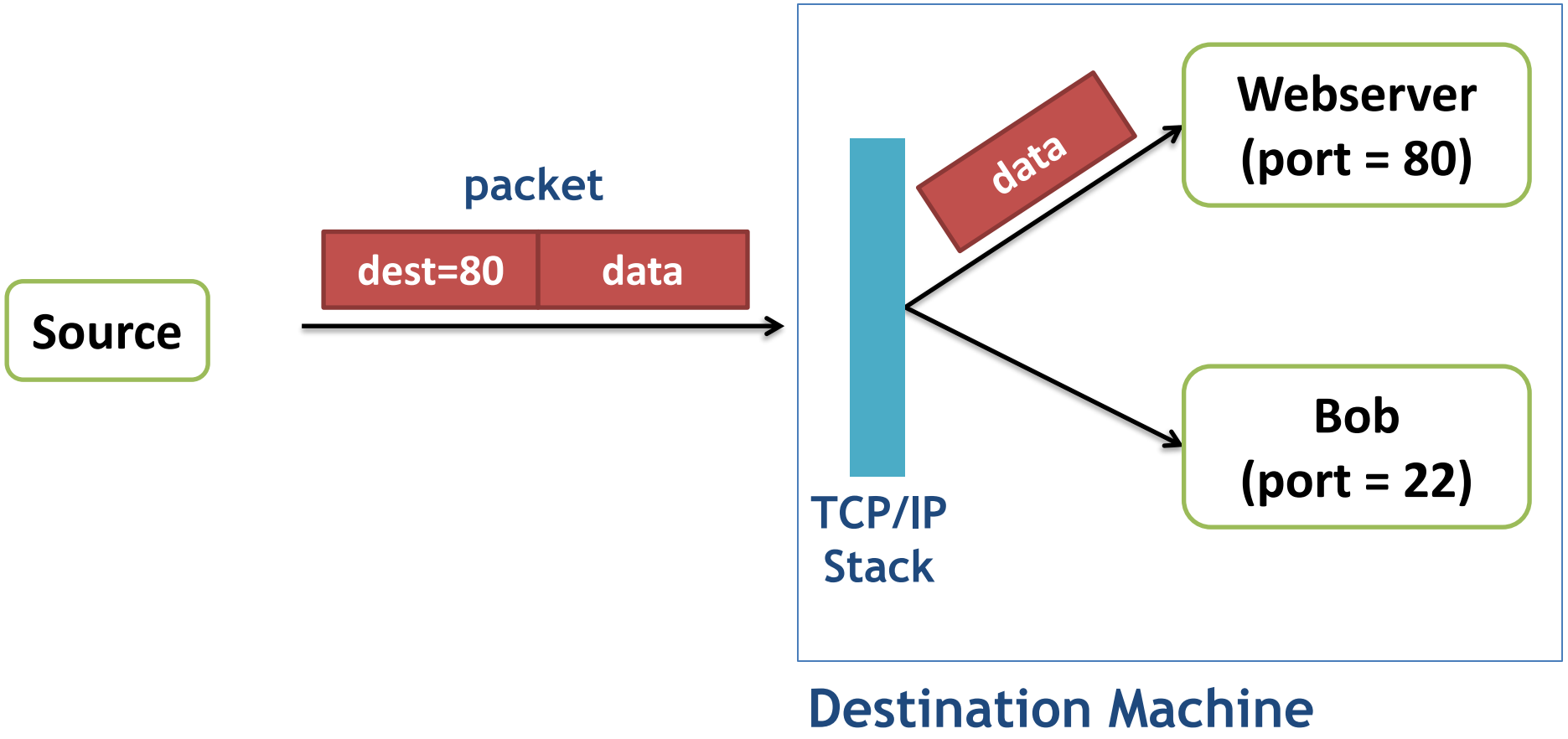
Department of Software

College of Software

Sungkyunkwan University

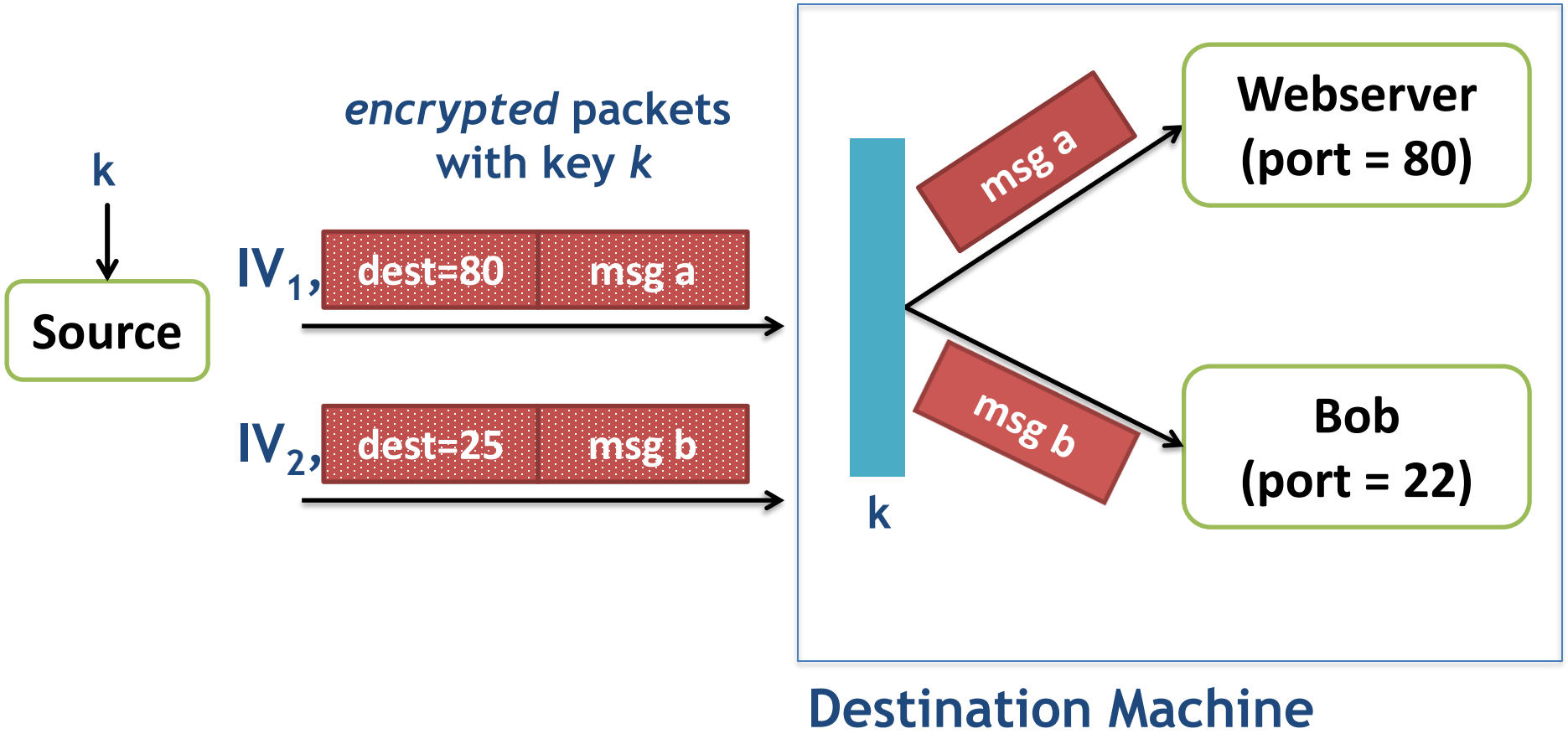
Example tampering attack

TCP/IP (highly abstracted)



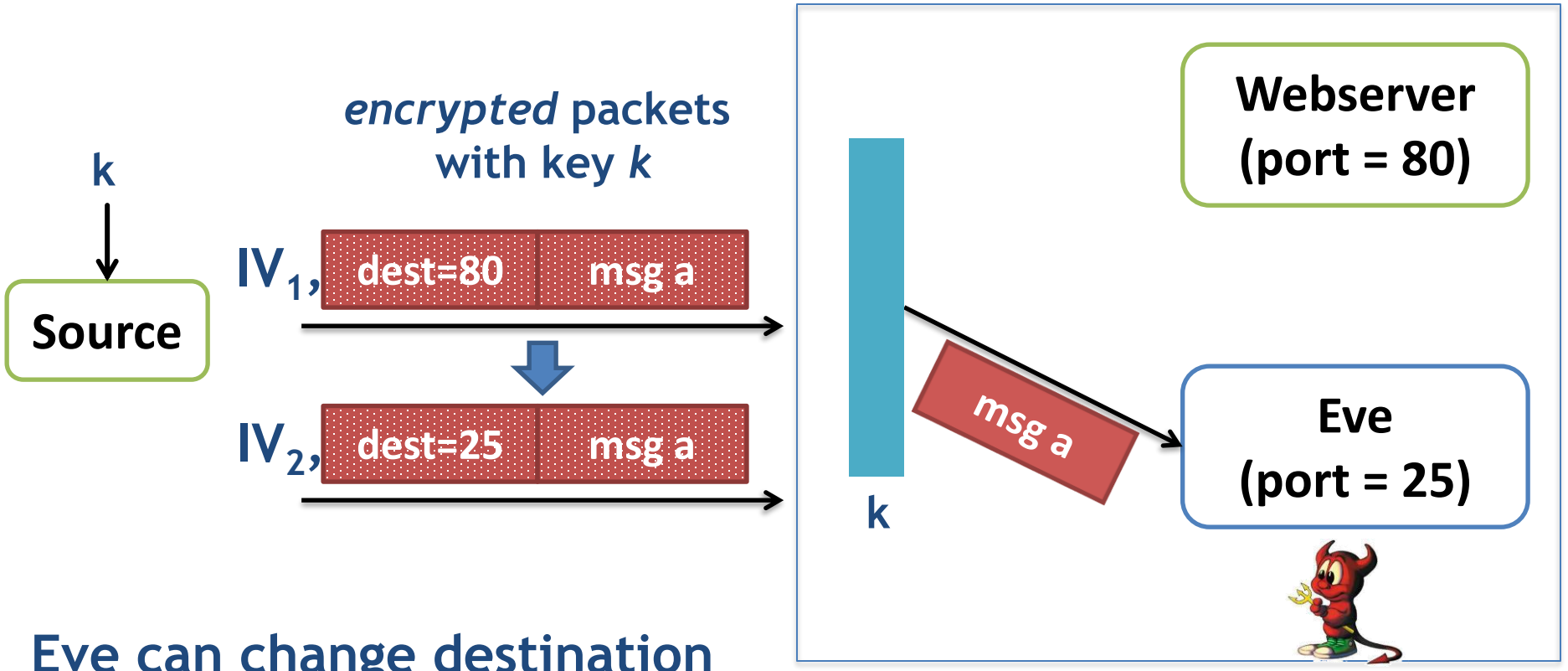
Example tampering attack

Encrypted with CBC and random IV



Example tampering attack

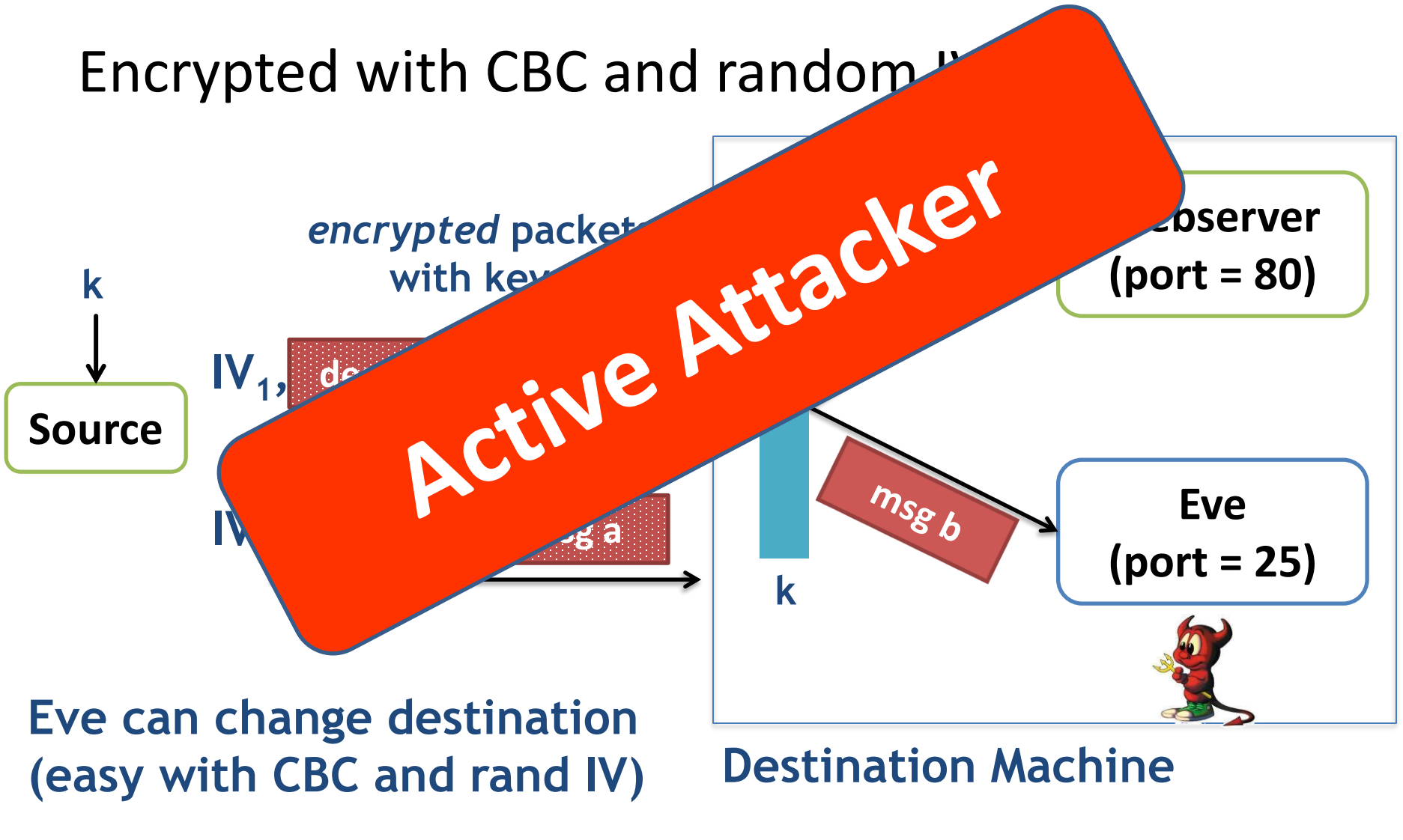
Encrypted with CBC and random IV



Eve can change destination
(easy with CBC and rand IV)

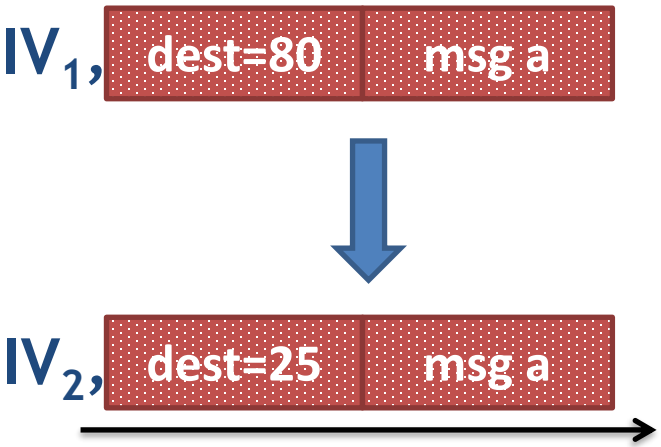
Example tampering attack

Encrypted with CBC and random IV



Eve can change destination
(easy with CBC and rand IV)

How?



Eve

CBC encryption:

$D(k, c[0]) \oplus IV_1 = 000\ldots80$

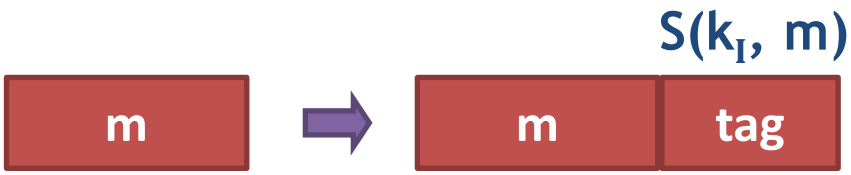
Attack:

$IV_2 = IV_1 \oplus 000\ldots80 \oplus 000\ldots0025$

xor out “80” and xor in “25”

How can we solve this …

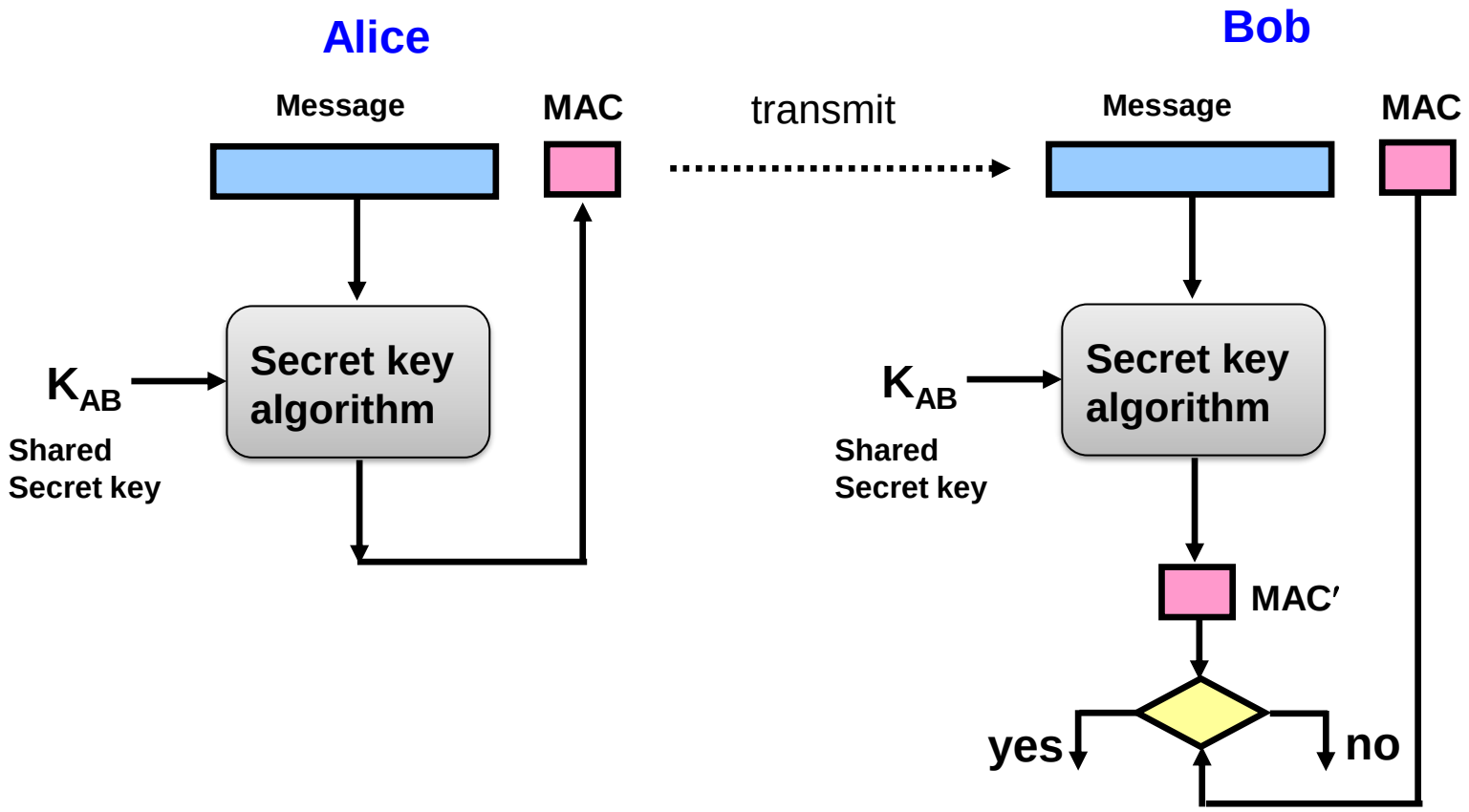
Message authentication is needed.



How can we integrate this with encryption?

Message Authentication Code (MAC)

- A message authentication code (MAC) is a key-dependent message digest function
  - MAC(M,k) = h

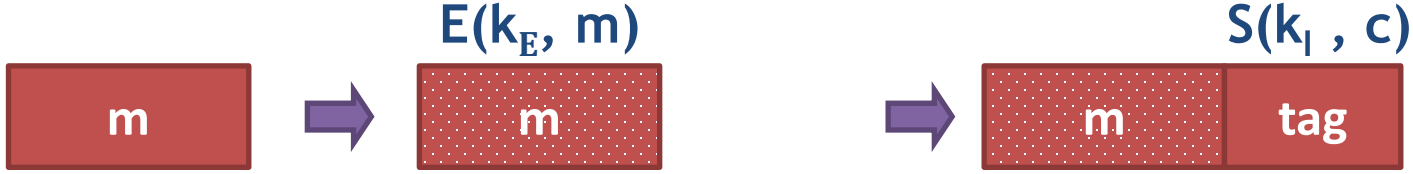


Motivating Question: Which is best?

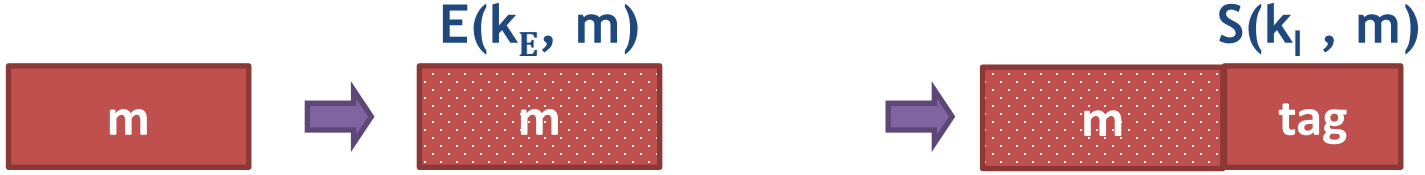
Encryption Key = k_E; MAC key = k_I

Option 1: SSL (MAC-then-encrypt)

Option 2: IPsec (Encrypt-then-MAC)



Option 3: SSH (Encrypt-and-MAC)



Theorems

Let (E,D) by a CPA secure cipher and (S,V) a MAC secure against existential forgery. Then:

1. Encrypt-then-MAC *always* provides authenticated encryption
2. MAC-then-encrypt *may* be insecure against CCA attacks
   - However, when (E,D) is rand-CTR or rand-CBC mode, MAC-then-encrypt also provides authenticated encryption

Authenticated encryption modes

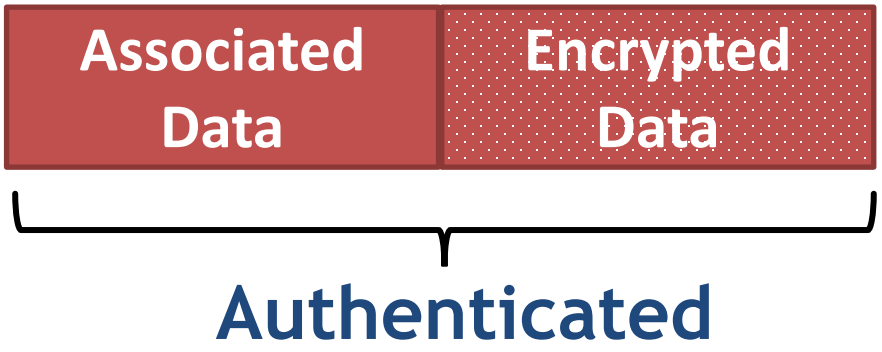
GCM: CTR mode encryption with Carter-Wegman (CW) MAC

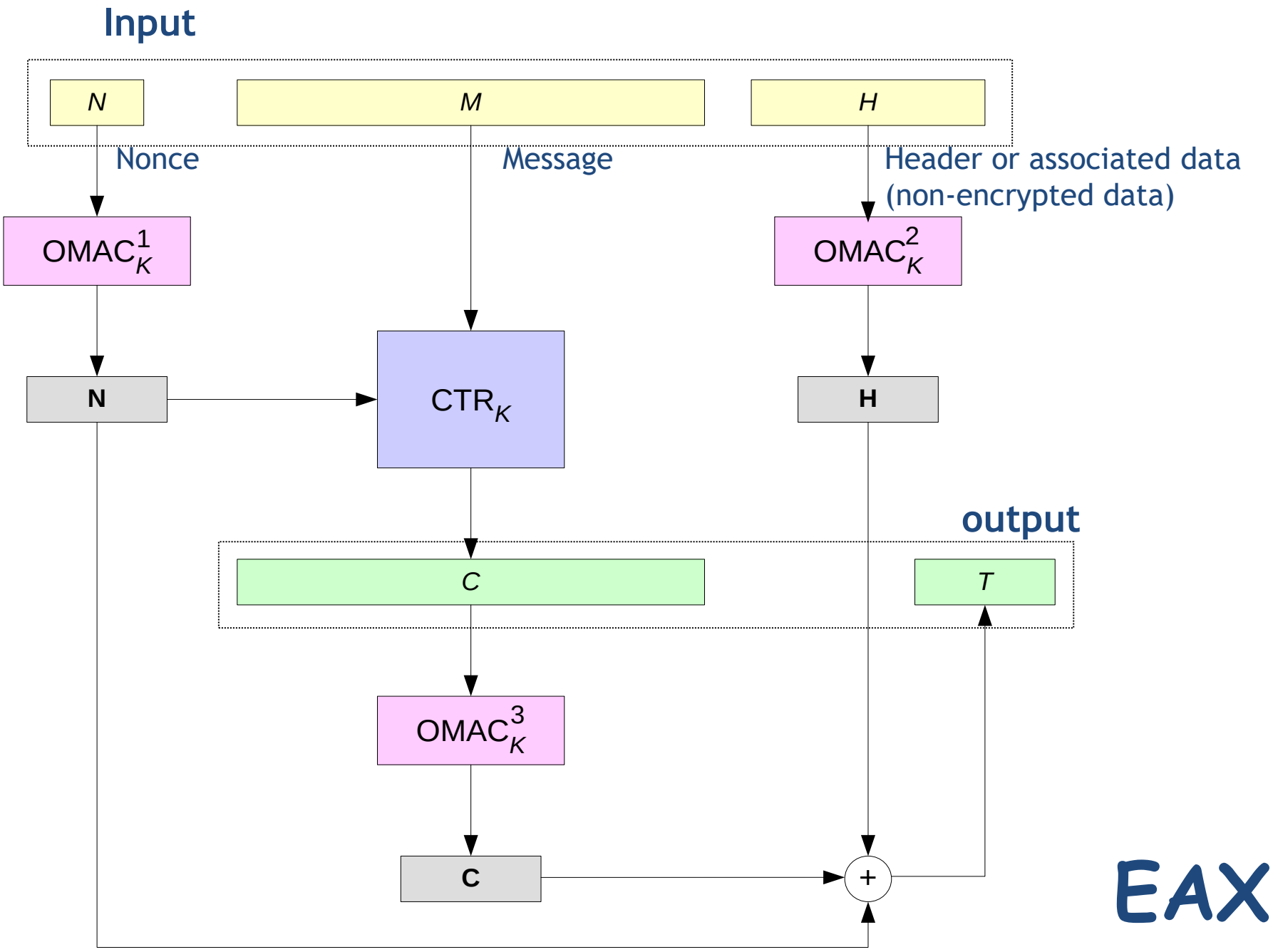
CCM: CTR mode encryption with CBC-MAC

EAX: CTR mode encryption with OMAC

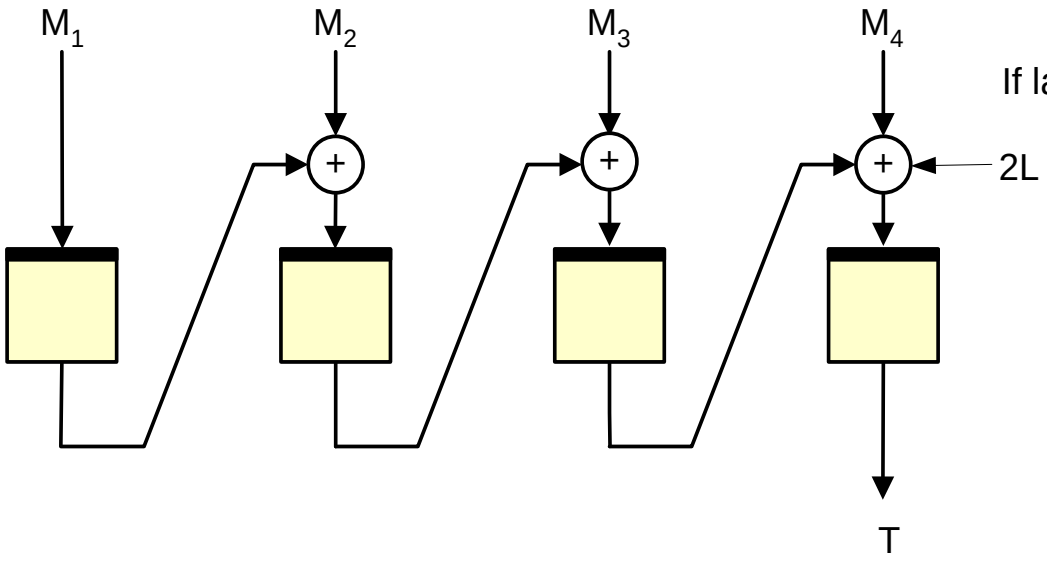
All are nonce-based.

All support *Authenticated Encryption with Associated Data (AEAD)*.




Input
N
M
H
Nonce
Message
Header or associated data
(non-encrypted data)
OMAC^1_K
OMAC^2_K
N
CTR$_K$
H
output
C
T
OMAC^3_K
C
+
EAX

[Iwata, Kurosawa]

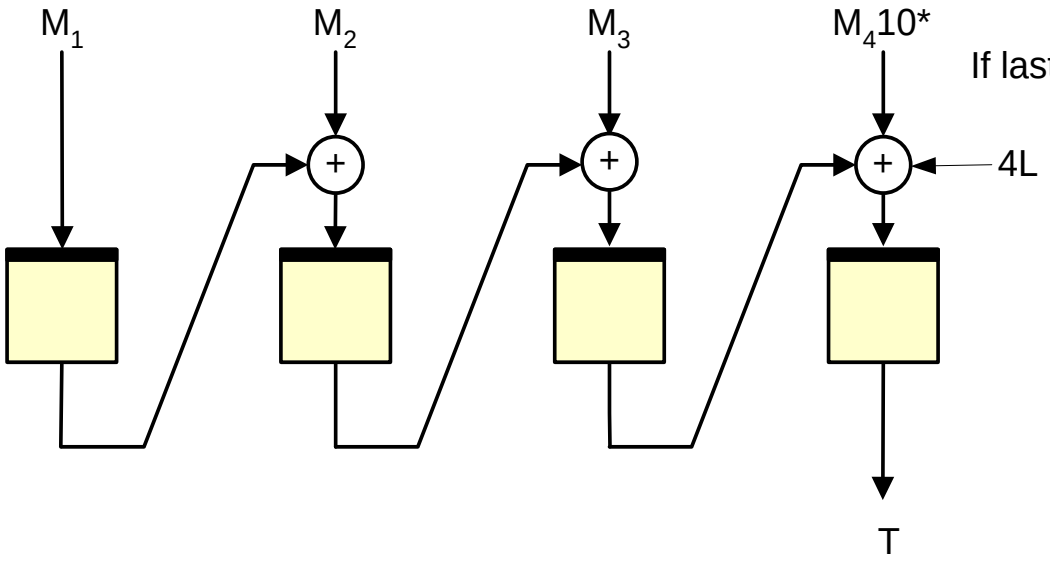


OMAC

$L = E(0^n)$

$2L = msb(L)? \; L<<1 : L<<1 \oplus 0x87$

$4L = 2(2L)$



"Tweaked" OMAC:

$OMAC_k^T(x) = OMAC_k(T \,||\, x)$

An example API (OpenSSL)

int **AES_GCM_Init**(AES_GCM_CTX *ain,
unsigned char ***nonce**, unsigned long noncelen,
unsigned char ***key**, unsigned int klen)

int **AES_GCM_EncryptUpdate**(AES_GCM_CTX *a,
unsigned char ***aad**, unsigned long aadlen,
unsigned char ***data**, unsigned long datalen,
unsigned char ***out**, unsigned long *outlen)

Performance

From Crypto++ 5.6.0 [by Wei Dai, the creator of "b-money"]

AE Cipher	Code Size	Speed (MB/sec)	Raw Cipher	Raw Speed
AES/GCM	large	108	AES/CTR	139
AES/CCM	smaller	61	AES/CBC	109
AES/EAX	smaller	61	AES/CMAC	109
AES/OCB*	small	129	AES/CTR	147

* OCB mode may have patent issues.

Recommendations for authenticated encryption

- Use "Encrypt-then-MAC".
  - Use two different keys, one for encryption and one for the MAC.
    - If you use the same key for multiple schemes, you need to consider interactions between the different schemes.
    - If one scheme might get broken, the key for both schemes can be recovered.
- Use proper "authenticated encryption" modes with random initialization vector.
  - GCM
  - EAX
  - CCM

Questions?


Sungkyunkwan
Campus
Social
Graduate
campus
Sciences
University
Seoul
Natural
Suwon
School
Korean
university
established
constructed
English
Professors
Global
edit
Humanities
lecturers