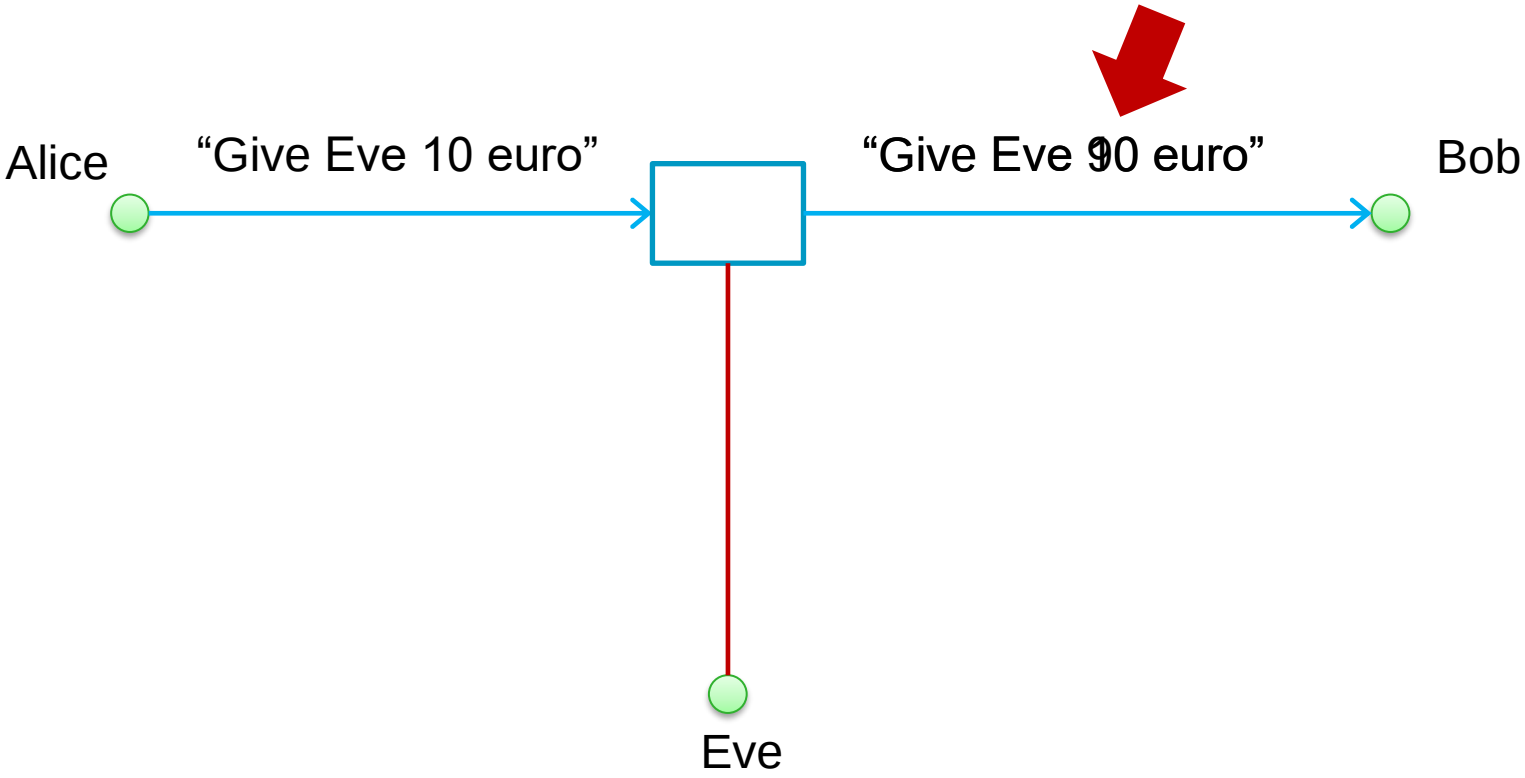
UNIVERSITY OF TWENTE.

Message authentication codes

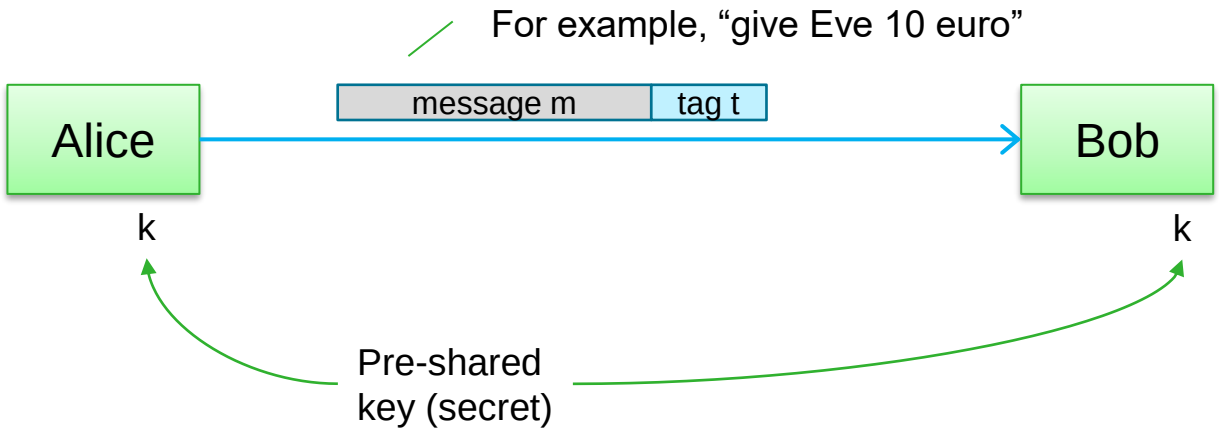
Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

INTEGRITY EXAMPLE (RECAP)



MESSAGE AUTHENTICATION CODES (MACS)



$t \leftarrow S(k, m)$ $\qquad$ $V(k, m, t) \stackrel{?}{=}$ ‘yes’

- Attacker cannot produce a valid tag for a *new* message
- Given (m,t), attacker cannot produce (m, t’) for t’ ≠ t

} Ensuring integrity

[Based on slides by Dan Boneh]

MAC FROM HASH FUNCTION (NAIVE FIRST ATTEMPT)

Hash function

Concatenation symbol

$$S(k, m) = H(k \mid\mid m)$$

Without k, it should not be possible to produce a valid tag for another message, right? Or is it?

Why is this not secure?

Given H(k || m), an attacker can compute H(k || m || PB || w) for any w.

Padding bytes

"give Eve 10 euro" || t → "give Eve 10 euro!@. and Eve 90 euro" || t'

HMAC: STANDARDIZED MAC FROM HASH

$$S(k, m) = H(k \oplus opad \,||\, H(\, k \oplus ipad \,||\, m)\,)$$

Padding

HMAC IN JAVA

```
String HMAC_ALGORITHM = "HmacSHA1";
Mac mac = Mac.getInstance(HMAC_ALGORITHM);
byte[] keyBytes = "HelloWorld".getBytes();
SecretKeySpec signingKey = new SecretKeySpec(keyBytes, HMAC_ALGORITHM);
mac.init(signingKey);
byte[] messageMac = mac.doFinal("Hello World, a signed message.".getBytes());
```

UNIVERSITY OF TWENTE.

Message authentication codes

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts