One Time Chat

Jake Barnwell, Andres Perez, Miles Steele

One Time Pad

Encrypt:

ciphertext = message $\oplus$ pad

Decrypt:

message = ciphertext $\oplus$ pad

One Time Pad - Perfect Security!

Information-theoretically secure, but...

- length(pad) == length(message)
- pad bits must not be re-used
- pad must be random

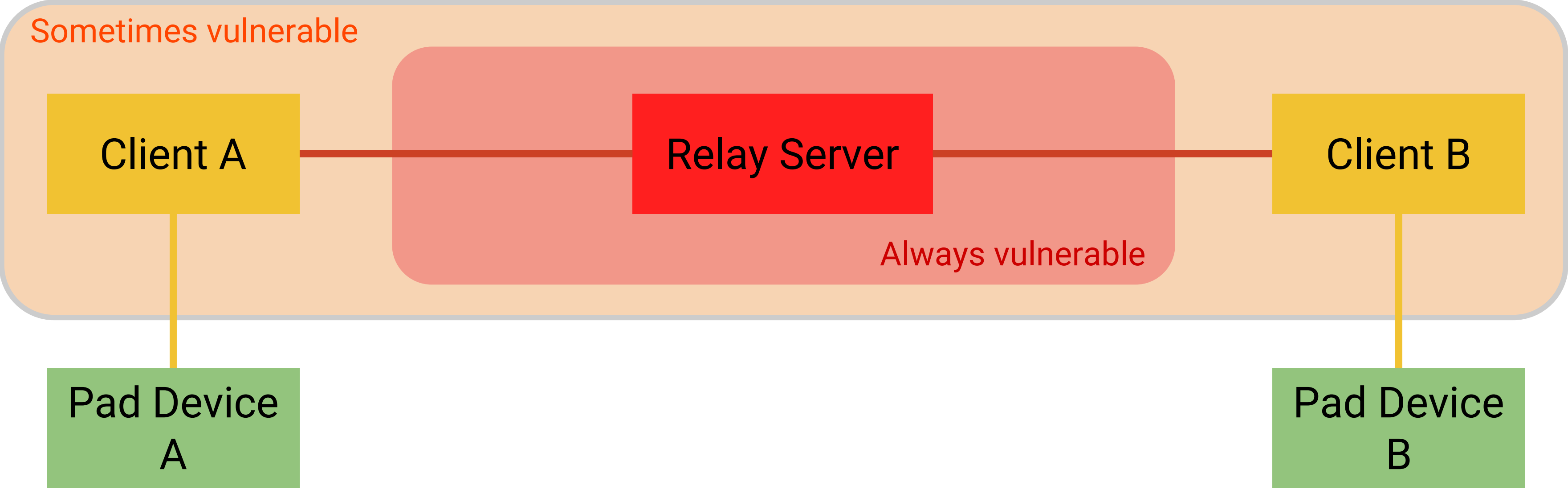
Design Goals

Confidentiality: Keep messages private

Integrity: Attacker can’t modify or inject messages

~~**Availability**~~: Not concerned with this for now

Threat Model - Architecture



Threat Model - Crypto Assumptions

Attacks:

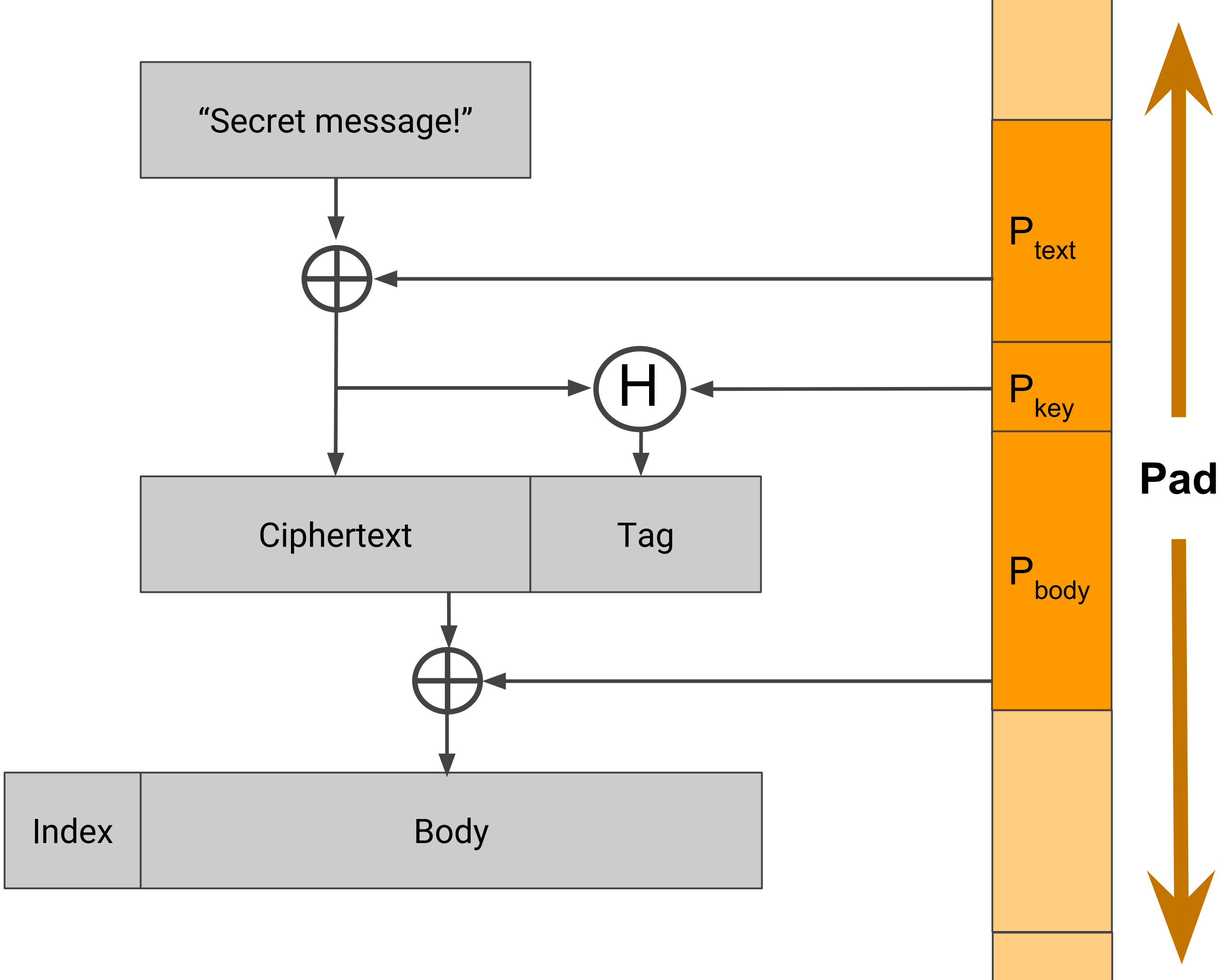
- Eve wants to read messages.
- Eve wants to forge messages.

Assurances:

- Pad generation is secure
- Users obtain pad securely.
- Sha256-based HMAC probably OK.

Home-Baked Crypto

$$\begin{aligned} package &:= index \mid\mid (p_{body} \oplus body) \\ body &:= ciphertext \mid\mid tag \\ ciphertext &:= p_{text} \oplus message \\ tag &:= HMAC(p_{key},\ ciphertext) \end{aligned}$$


"Secret message!"
H
Ciphertext
Tag
Index
Body
P_{text}
P_{key}
P_{body}
Pad

Demo...

One Time Chat

github.com/mlsteele/one-time-chat