



# Length Extension Attack

**Vulnerable** : All Merkle–Damgård-based hash functions

so MD5, SHA-1 and SHA-2 (but not SHA-3)



# **Flickr's API Signature Forgery Vulnerability**

**Thai Duong and Julian Rizzo**

Date Published: Sep. 28, 2009

Advisory ID: MOCB-01

Advisory URL: [http://netifera.com/research/flickr\\_api\\_signature\\_forgery.pdf](http://netifera.com/research/flickr_api_signature_forgery.pdf)

Title: Flickr's API Signature Forgery Vulnerability

Remotely Exploitable: Yes

# Length Extension Attack



**Vulnerable** : All Merkle–Damgård-based hash functions  
so MD5, SHA-1 and SHA-2 (but not SHA-3)

## **Flickr's API Signature Forgery Vulnerability**

**Thai Duong and Juliano Rizzo**

Date Published: Sep. 28, 2009

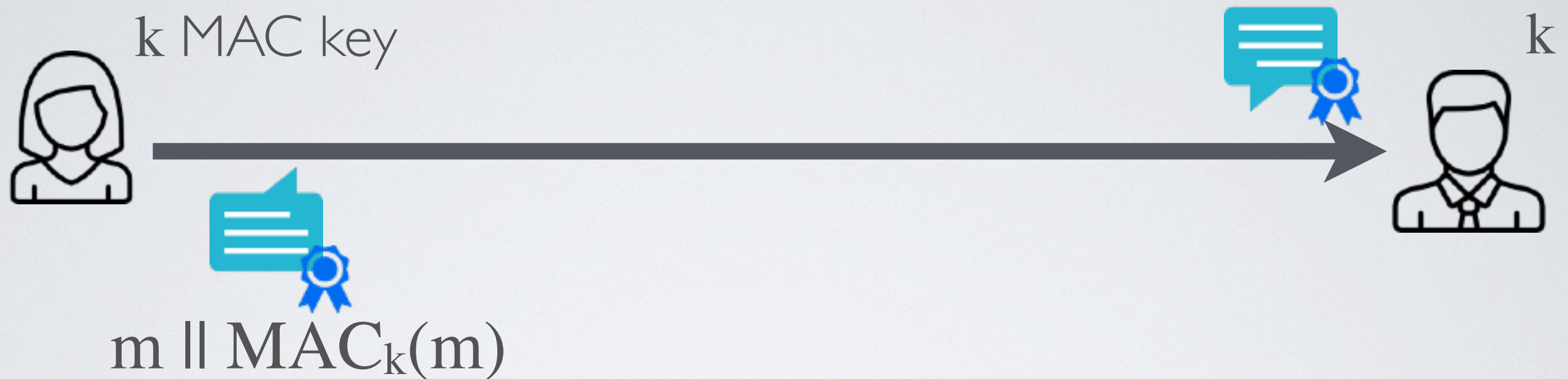
Advisory ID: MOCB-01

Advisory URL: [http://netifera.com/research/flickr\\_api\\_signature\\_forgery.pdf](http://netifera.com/research/flickr_api_signature_forgery.pdf)

Title: Flickr's API Signature Forgery Vulnerability

Remotely Exploitable: Yes

# Good HMAC



Alice and Bob share a key  $k$

➡ Option 1 : envelope method

$$\text{MAC}_k(m) = H(k \parallel m \parallel k)$$

➡ Option 2 : padding method (i.e. HMAC standard)

$$\text{HMAC}_k(m) = H((k \oplus \text{opad}) \parallel H((k \oplus \text{ipad}) \parallel m))$$