Length extension attack

Vulnerable : 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

Title: Flickr's API Signature Forgery Vulnerability

Remotely Exploitable: Yes

Length extension attack

Vulnerable : 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

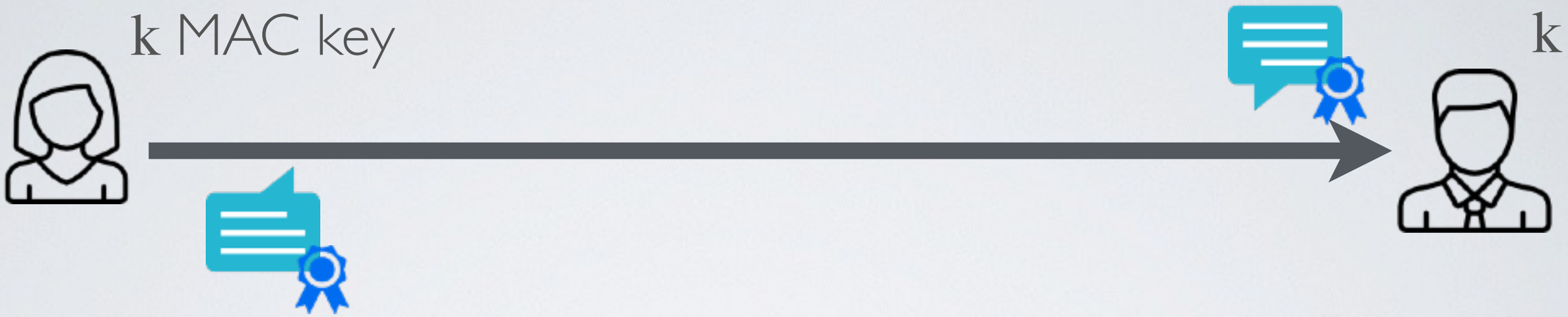
Advisory ID: MOCB-01

Advisory URL: http://netifera.com/research/flickr_api_signature_forgery.pdf

Title: Flickr's API Signature Forgery Vulnerability

Remotely Exploitable: Yes

Good HMAC



Alice an Bob share a key $\mathbf{k}$

➡ Option 1 : envelope method

$$\mathbf{MAC}_k(\mathrm{m}) = \mathrm{H}(\mathrm{k} \,||\, \mathrm{m} \,||\, \mathrm{k})$$

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

$$\mathbf{HMAC}_k(\mathrm{m}) = \mathrm{H}((\mathrm{k} \oplus \mathrm{opad}) || \mathrm{H}((\mathrm{k} \oplus \mathrm{ipad}) \,||\, \mathrm{m}))$$