Information Security and Privacy (COM-402)

Part 7: Privacy enhancing technologies
Steganography

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Some slides/ideas adapted from: JP Hubaux, Bryan Ford, Vitaly Shmatikov

What about Unobservability? Steganography

Goal: concealing a file, message, image, or video within another file, message, image, or video.

WWI example -Sent by a German spy during WWI:

“Apparently neutral’s protest is thouroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.”

What about Unobservability? Steganography

Goal: concealing a file, message, image, or video within another file, message, image, or video.

WWI example -Sent by a German spy during WWI:

“A**p**parently n**e**utral’s p**r**otest is t**h**ouroughly d**i**scounted a**n**d i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects p**r**etext f**o**r e**m**bargo o**n** b**y**products, e**j**ecting s**u**ets a**n**d v**e**getable o**i**ls.”

Pershing sails from NY June 1!

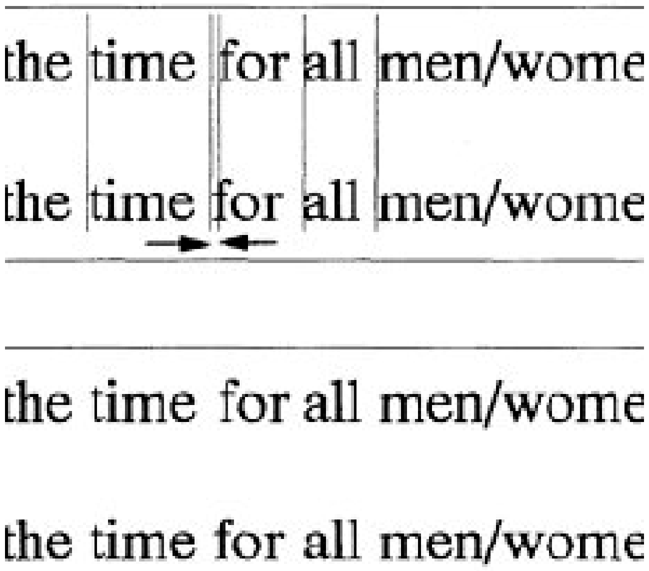
Steganography: example methods

Hide in LSB of an image

Alter the LSB of an image to encode words / other image

Hide in text

Modify spaces to encode words



the time for all men/wome

the time for all men/wome

the time for all men/wome

the time for all men/wome

Steganography: security

The goal is to hide the message

Unobservability - Pr[real action |observation]

Pr[observation | real action] = Pr [observation]

Analysis:

- Check whether there are anomalies in the text, image,…

- Requires to know how the original looks like!

  - Except for local correlations (e.g., color pixels in a photo)

    steganography must take them into account!

But do people use this…?

1) Yes, this is important from a message secrecy point of view, and it is used by both governments and criminals

2) This is key for censorship resistance! The key to not be censored is to not be seen!
   - Steganographic properties and lessons are very much used in privacy technologies.

Takeaways PETs

Cryptography → Confidentiality!

Traditional: computer security context

Privacy goes BEYOND than traditional confidentiality.

What makes Privacy Enhancing Technologies (PETs) different:

- Threat model: **weak** actors, **powerful** adversaries.

- Susceptibility to **compulsion**.

- Cannot assume the existence of **Trusted Third Parties (TTP)**

- You should also worry about **Cost, Collusion, Corruption, Carelessness**.