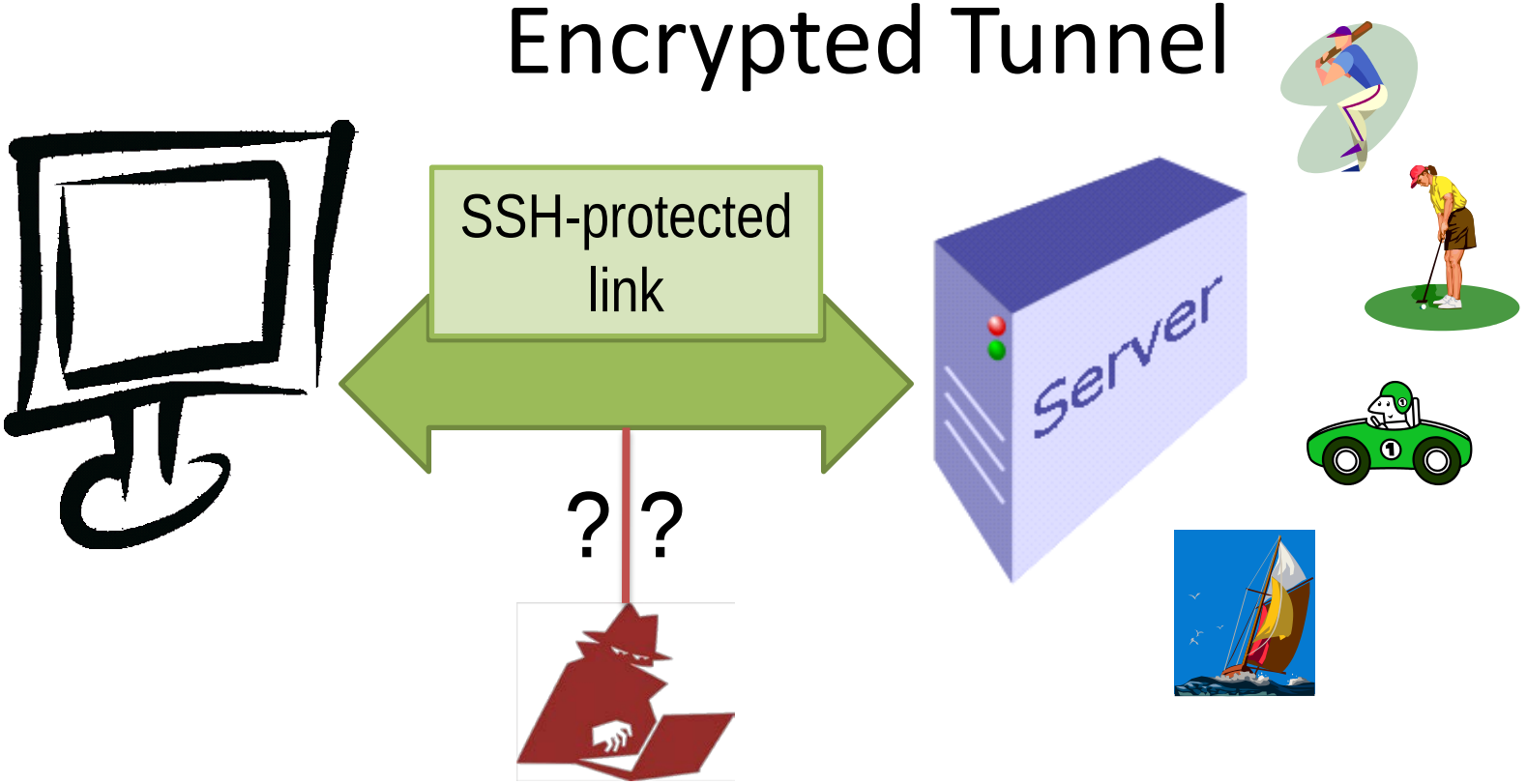
Computer Security
Covert Channels, Information Hiding

Magnus Almgren & Erland Jonsson

Department of Computer Science and Engineering

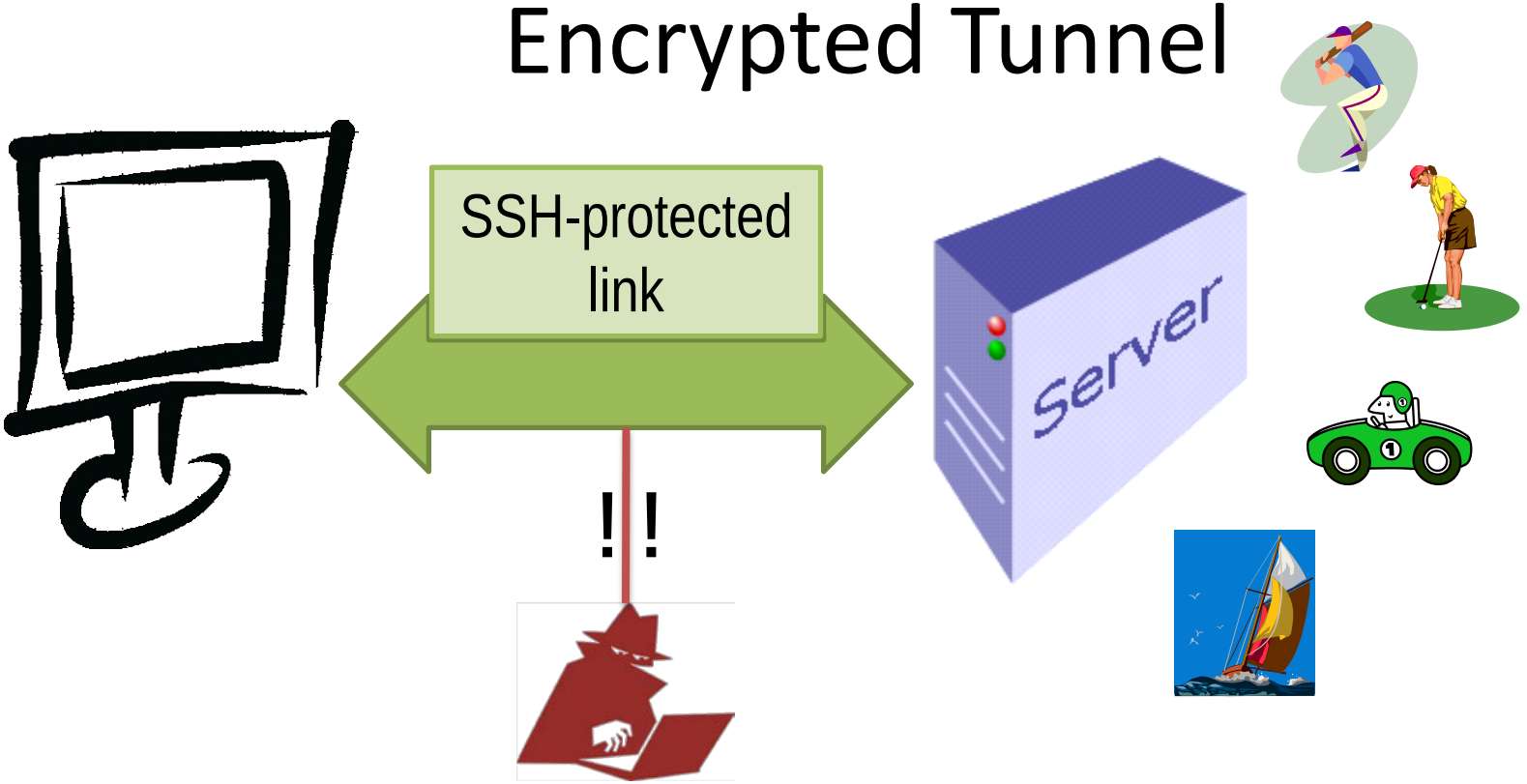
Chalmers University of Technology, Sweden

Protection Mechanism: Encrypted Tunnel



- Attacker's goal is to identify the webpage requested.
- Possible?

Protection Mechanism: Encrypted Tunnel



- Yes, with 68% accuracy. Packet length, packet direction, packet timing ➔ traffic analysis attacks

[SoK]: Peek-a-Boo, I Still See you: Why Efficient Traffic Analysis Countermeasures Fail
Kevin P. Dyer (Portland State University), Scott E. Coull (RedJack, LLC), Thomas Ristenpart (University of Wisconsin-Madison), and Thomas Shrimpton (Portland State University)

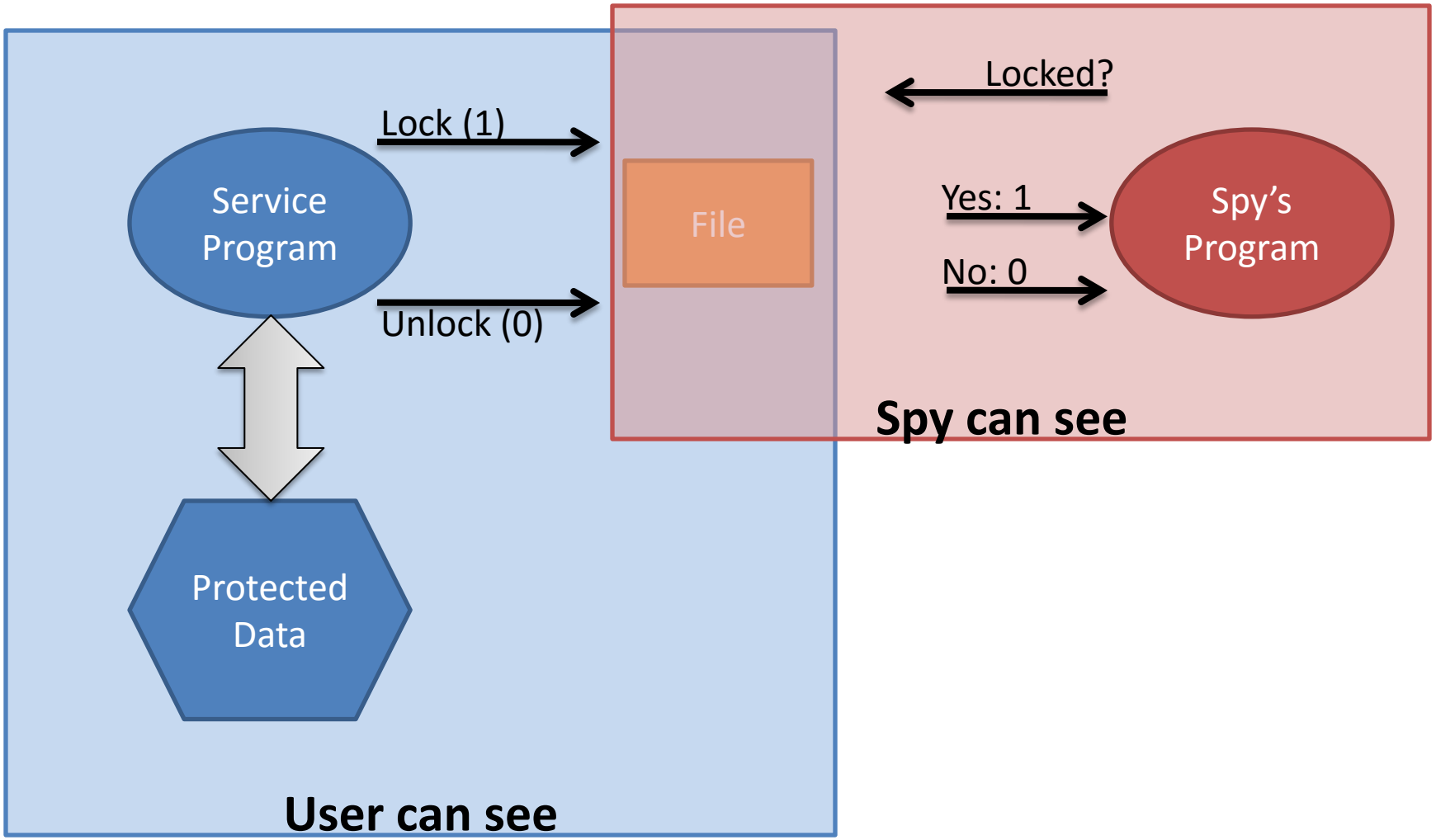
Covert Channel Basics

- a **covert channel** is a channel that leaks information from a protected area (module/program) to an unprotected area. Also called **leakage path** (swedish: hemlig kanal/dold kanal)
- its most important characterization is **bandwidth** (bits/s)
- covert channels can make use of almost any means for the information transfer
- a typical environment is a highly sensitive system
- Cmp steganography (“hidden writing”), watermarking and fingerprinting

Covert Channel Types
Storage Channels

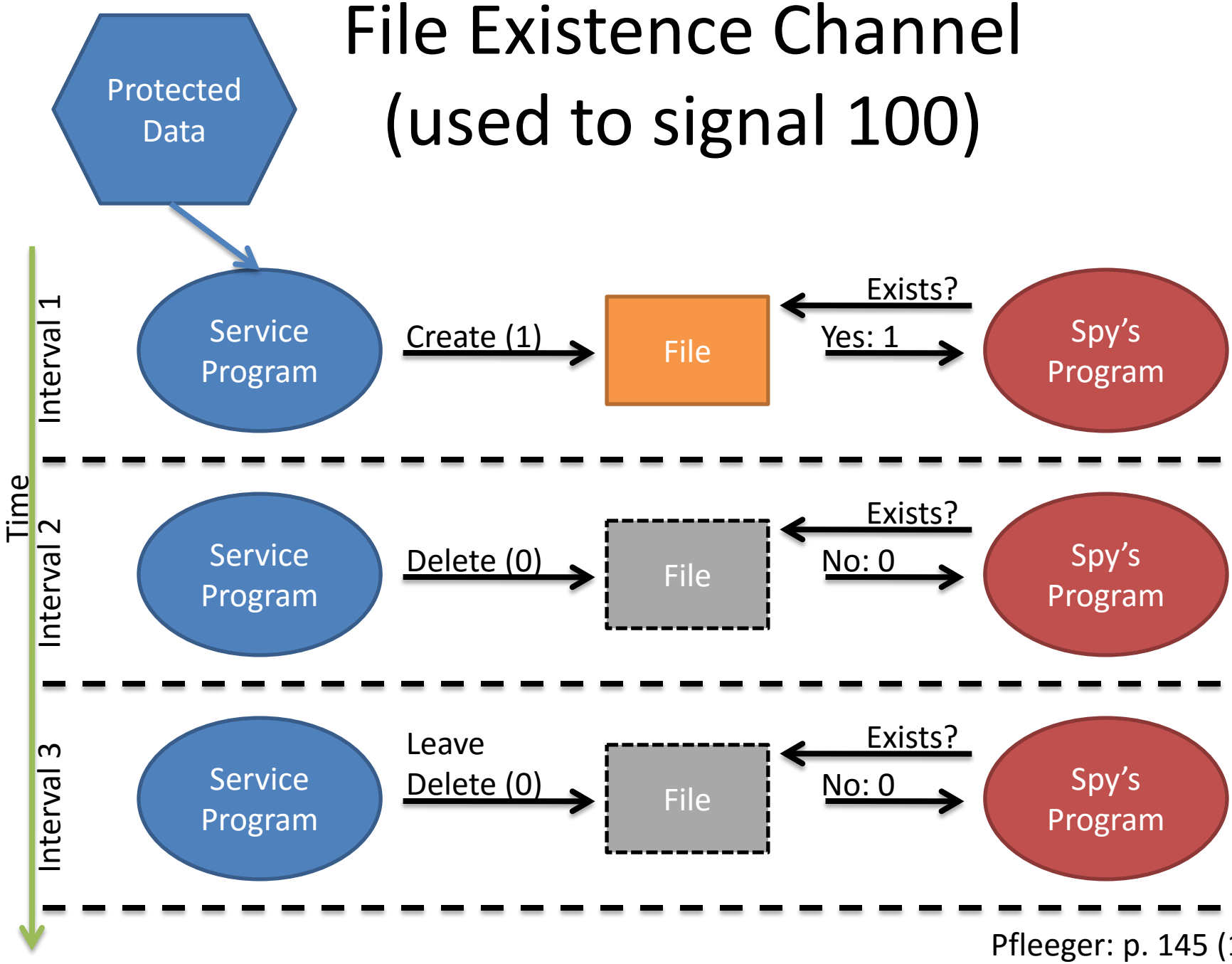
- Two main types: storage and timing channels
- **A. storage channels:**
  Eg. process 1 writes to an object and process 2 reads it
  - **A1: object attributes**:
    file attributes (length, format, date of change, ACL,…)
  - **A2: object existence**:
    check the existence of a certain file
  - **A3: shared resources**:
    use printing queue (full or empty)

File Lock Covert Channel



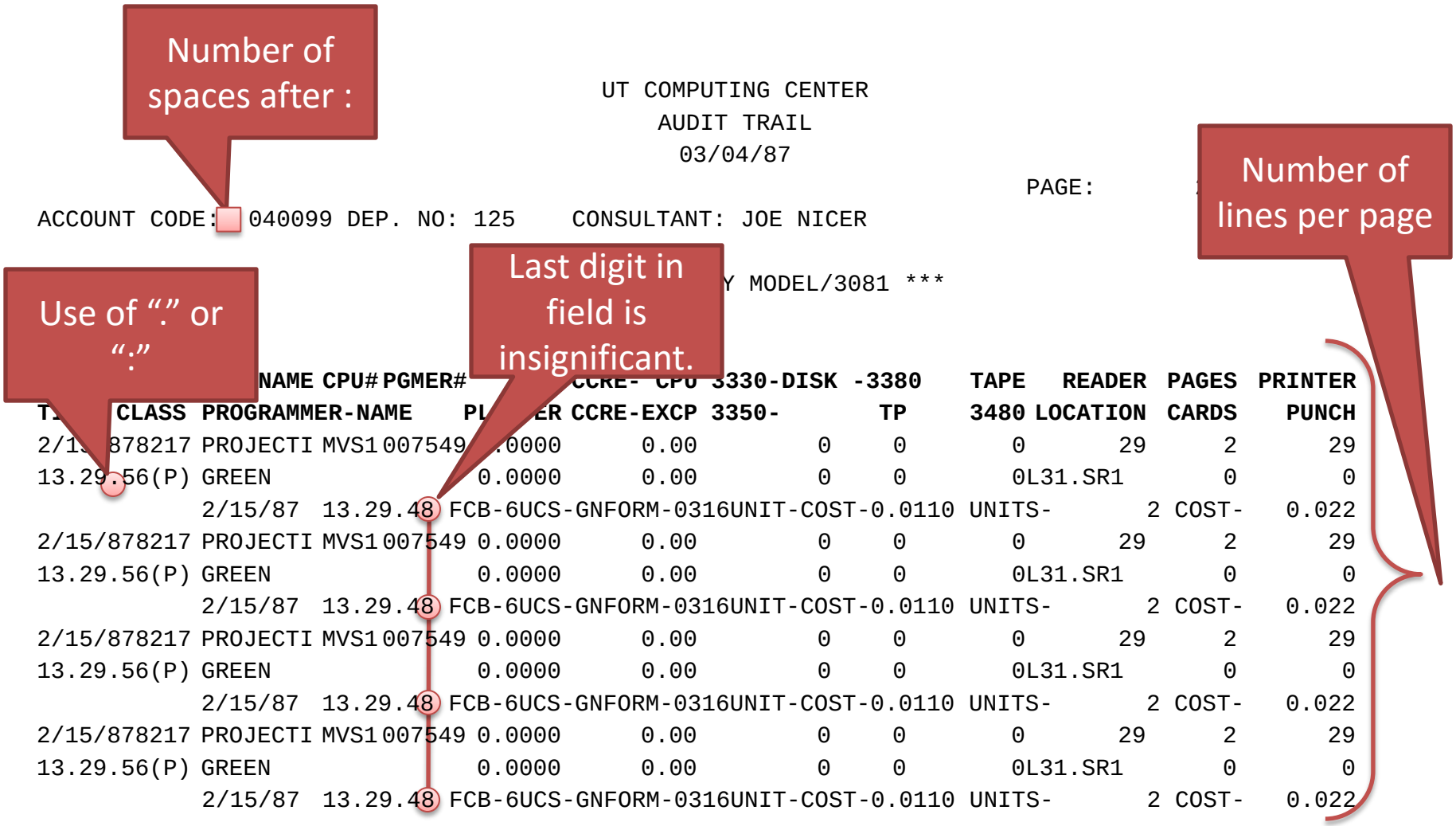
Pfleeger: p. 144 (154)

File Existence Channel (used to signal 100)



Pfleeger: p. 145 (155)

Example Covert Channel



Number of spaces after :

Number of lines per page

Use of “.” or “:”

Last digit in field is insignificant.

```
                         UT COMPUTING CENTER
                             AUDIT TRAIL
                              03/04/87
                                                      PAGE:
ACCOUNT CODE: 040099 DEP. NO: 125    CONSULTANT: JOE NICER

                                   Y MODEL/3081 ***

          NAME CPU# PGMER#       CCRE- CPU 3330-DISK -3380   TAPE   READER PAGES  PRINTER
TI    CLASS PROGRAMMER-NAME    PL    ER CCRE-EXCP 3350-        TP     3480 LOCATION CARDS  PUNCH
2/1  878217 PROJECTI MVS1 007549  .0000     0.00        0     0      0        29     2      29
13.29.56(P) GREEN               0.0000     0.00        0     0     0L31.SR1           0       0
            2/15/87  13.29.48 FCB-6UCS-GNFORM-0316UNIT-COST-0.0110 UNITS-       2 COST-   0.022
2/15/878217 PROJECTI MVS1 007549 0.0000     0.00        0     0      0        29     2      29
13.29.56(P) GREEN               0.0000     0.00        0     0     0L31.SR1           0       0
            2/15/87  13.29.48 FCB-6UCS-GNFORM-0316UNIT-COST-0.0110 UNITS-       2 COST-   0.022
2/15/878217 PROJECTI MVS1 007549 0.0000     0.00        0     0      0        29     2      29
13.29.56(P) GREEN               0.0000     0.00        0     0     0L31.SR1           0       0
            2/15/87  13.29.48 FCB-6UCS-GNFORM-0316UNIT-COST-0.0110 UNITS-       2 COST-   0.022
2/15/878217 PROJECTI MVS1 007549 0.0000     0.00        0     0      0        29     2      29
13.29.56(P) GREEN               0.0000     0.00        0     0     0L31.SR1           0       0
            2/15/87  13.29.48 FCB-6UCS-GNFORM-0316UNIT-COST-0.0110 UNITS-       2 COST-   0.022
```

Pfleeger: p. 143 (153)

Covert Channel Types
Timing Channels

- Two main types: storage and timing channels
- **B. timing channels**
  E.g. process 1 creates some "effect" and process 2 measures time.
  - Examples:
    - vary the CPU load in e.g. 1 ms intervals (works well if only 2 processes)
    - make program execution dependent on program data

- Timing channels tend to be noisy and hard to detect.
- Countermeasure:
  - deny access to system clock (but: it is possible to make your own clock)

Information Hiding Basics

- **information hiding** is a general concept that includes
  - steganography (covert communication) and
  - (digital) watermarking.
- steganography
  - means "*hidden writing*" (as does cryptography), but here it is the ***existence*** of the message that is secret.
  - steganography "embeds a secret message in some carrier, such as an open message".
- (digital) watermarking
  - means embedding a message into a cover message, normally to discourage theft of intellectual property rights (IPR).
  - Example: media watermarking:
- cover = digital image, secret = copyright notice

Practical Steganography (1)

- Steganography was used in WWII:
  - Germans used hem stitching patterns to hide Morse Code.
  - Invisible ink, indentation etc. were also used.

http://www.washingtonpost.com/wp-dyn/content/article/2006/09/03/AR2006090300811.html

Practical Steganography (2)

Randolph Femmer /life.nbii.gov

Practical Steganography (3)

http://utilitymill.com/utility/Steganography_Encode

Lenny Domnitser

Randolph Femmer /life.nbii.gov

First chapter of “Around the world in eighty days”, Jules Verne

Practical Steganography (4)

- It is also possible to hide an image within another image.

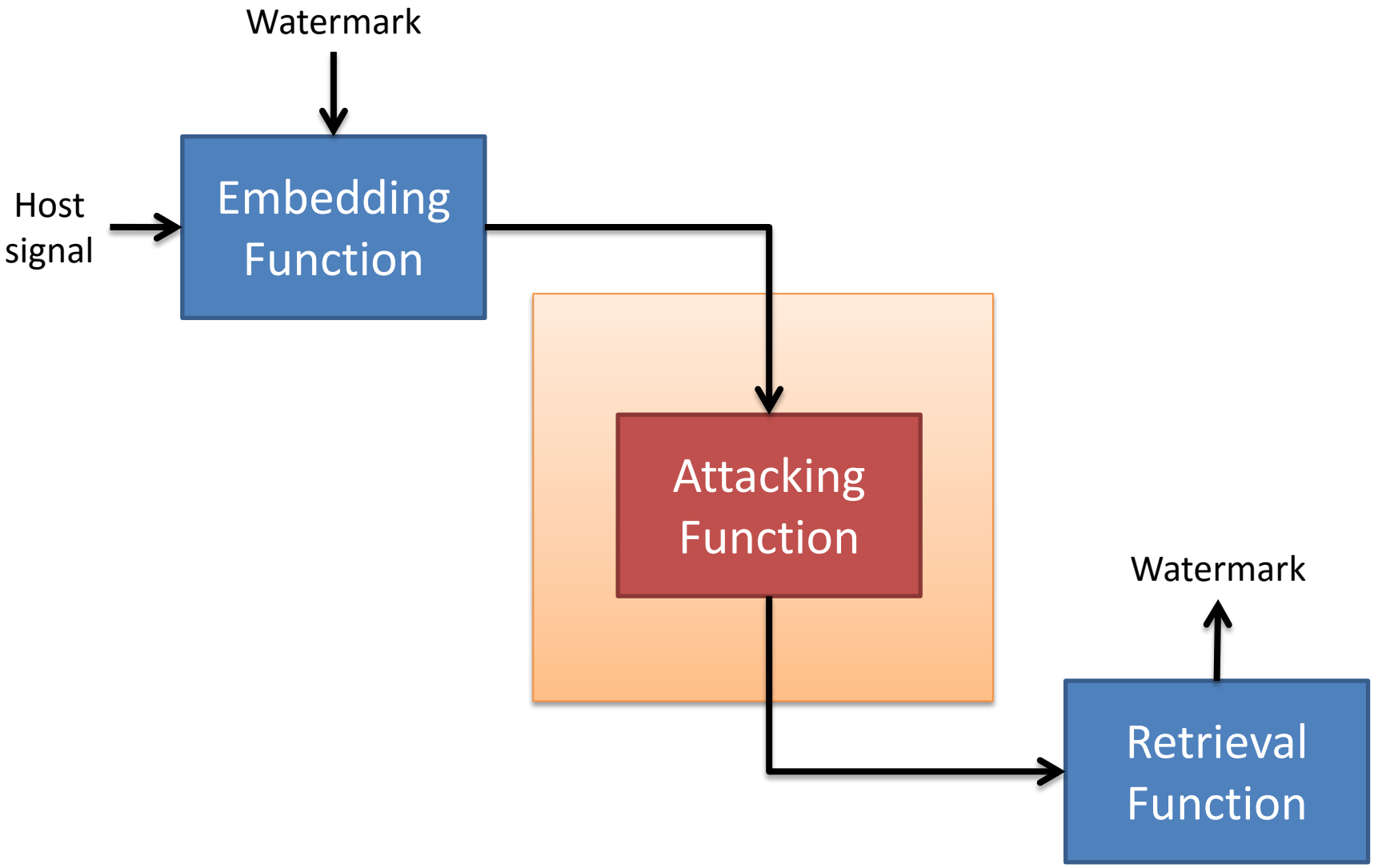
By removing all but the last 2 bits of each color component, an almost completely black image results. Making the resulting image 85 times brighter results in the following.

http://en.wikipedia.org/wiki/Steganography

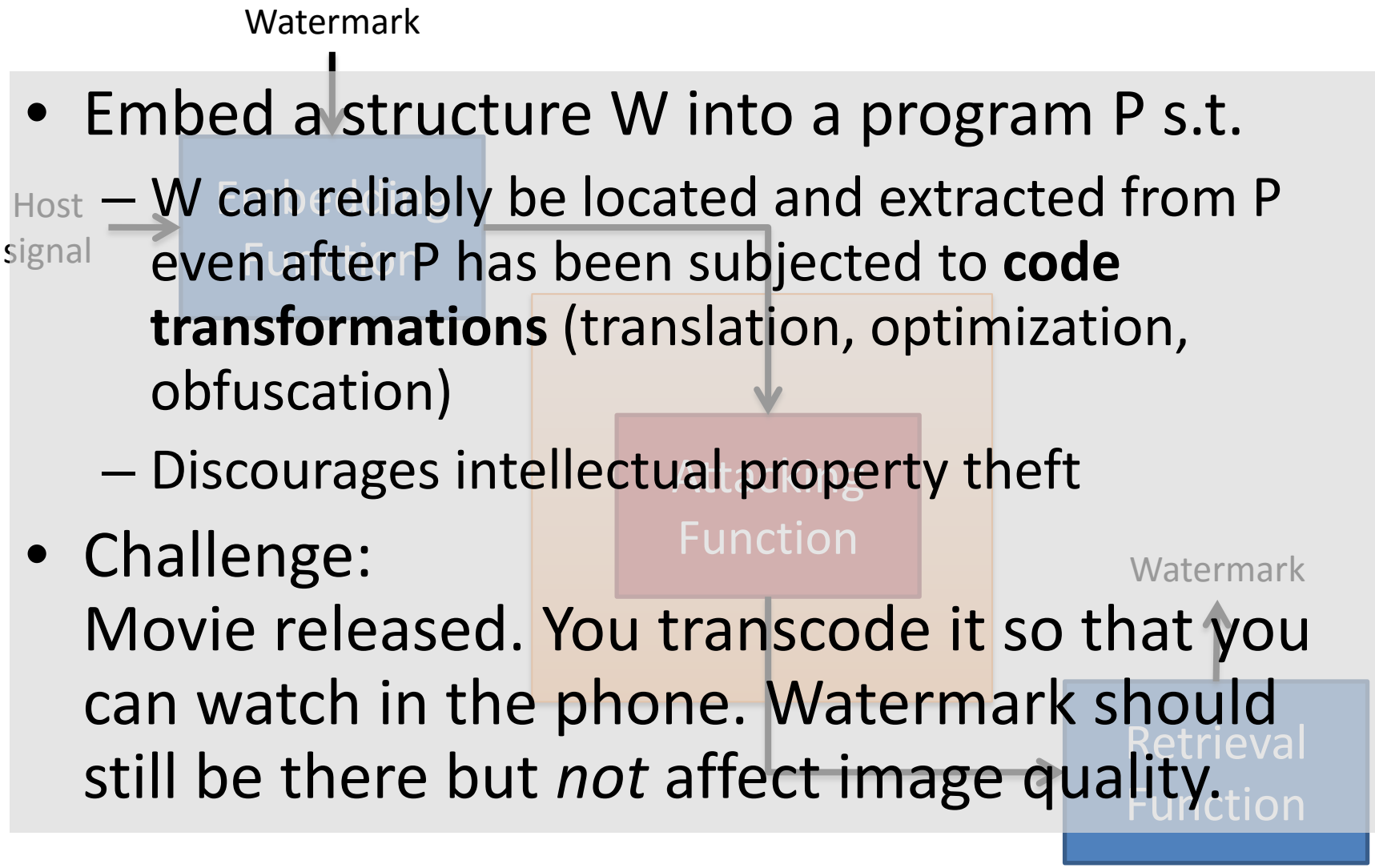
Digital Watermarking

- Technique to add a ”secret” message into a cover message:
  cover=movie, secret=copyright msg
- can be hidden or open
- **Objective**: should not be able to remove
- Usually: goal is to detect if there
- Use cases
  - Copyright protection
  - Fingerprinting: different marks for different users
  - Broadcast monitoring: watermarked video

Watermarking



Watermarking



- Embed a structure W into a program P s.t.
  - W can reliably be located and extracted from P even after P has been subjected to **code transformations** (translation, optimization, obfuscation)
  - Discourages intellectual property theft
- Challenge:
  Movie released. You transcode it so that you can watch in the phone. Watermark should still be there but *not* affect image quality.

Summary

- A *covert channel* allows an inside malicious process to send sensitive data to an outside receiver, using an existing baseline communication band.
- Contrary, *steganography* presents the communication in clear sight, but in a form that is not likely to be noticed (instead of hiding it).
- With *Cryptography* the content is concealed but the existence of the encrypted data is visible to all.

ieee spectrum INSIDE TECHNOLOGY

MAGAZINE MULTIM

AEROSPACE BIOMEDICAL COMPUTING CONSUMER ELECTRONICS ENERGY

TELECOM / INTERNET

FEATURE

Vice Over IP: The VoIP Steganography Threat

A growing cadre of criminals is hiding secret messages in voice data

By JÓZEF LUBACZ, WOJCIECH MAZURCZYK, KRZYSZTOF SZCZYPIORSKI / FEBRUARY 2010

Email Print Share

Page 1 2 3 4 5 // View All

Image: Mick Wiggins

http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat/