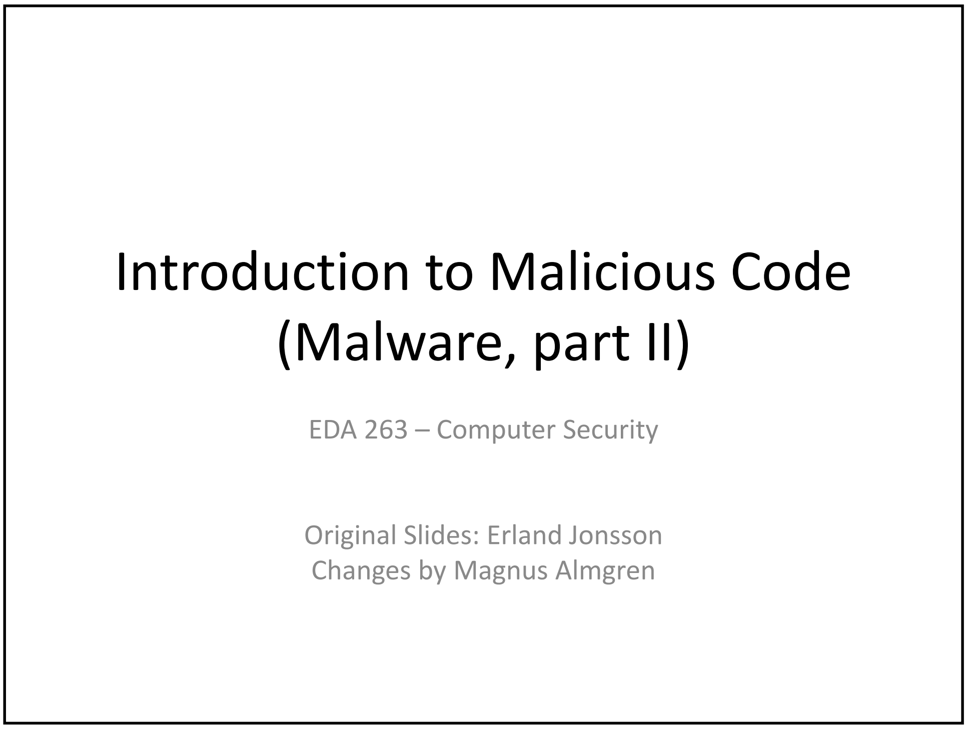
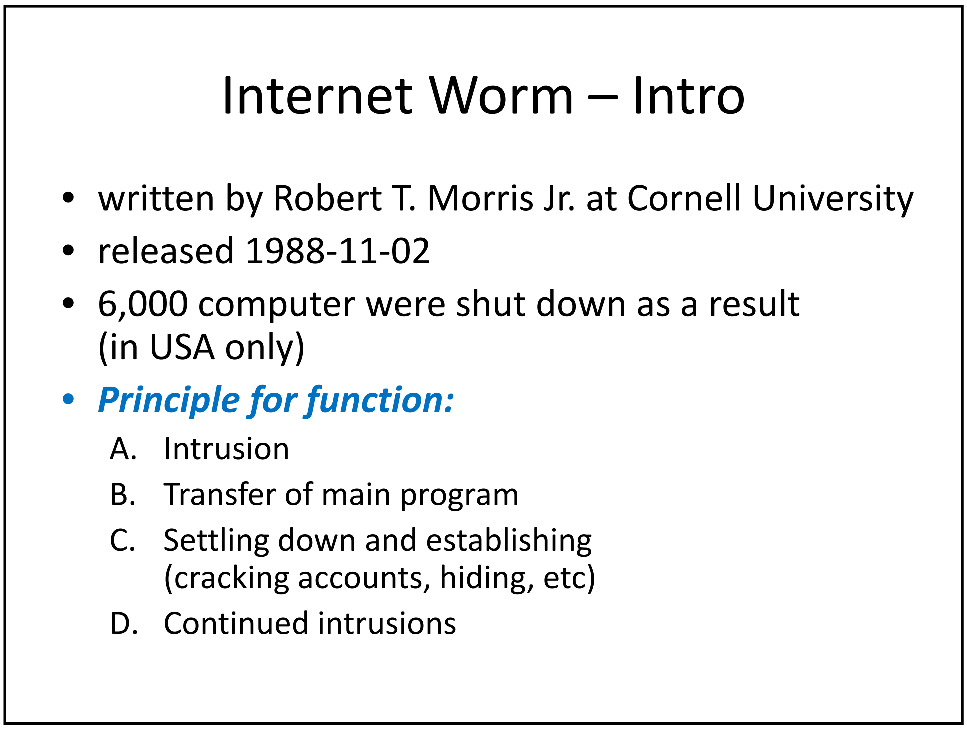


Introduction to Malicious Code (Malware, part II)

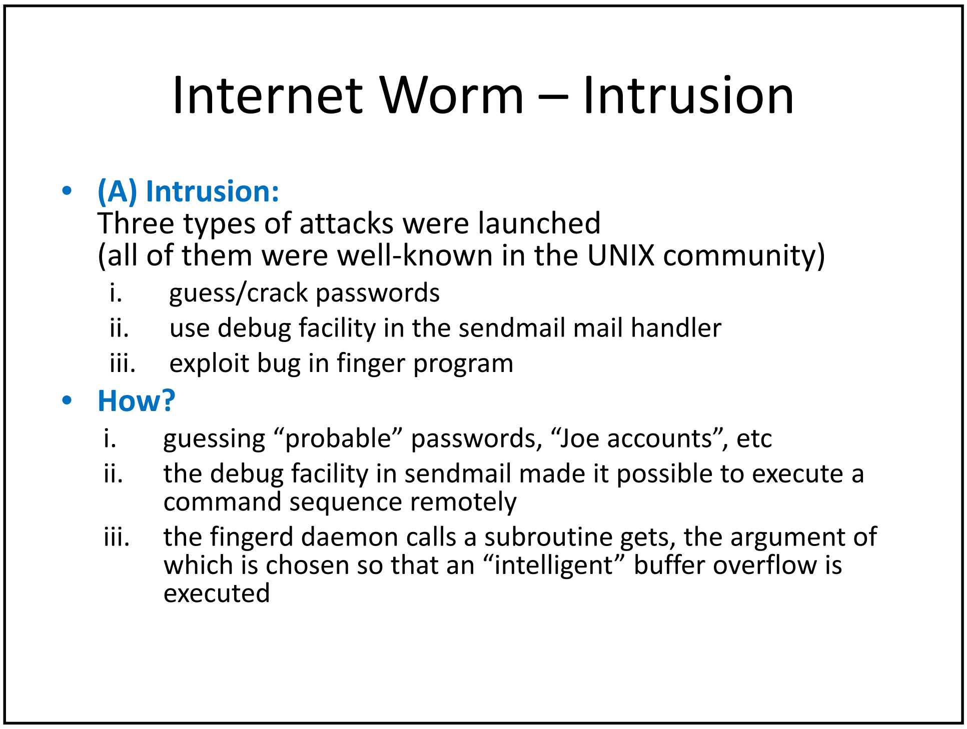
EDA 263 – Computer Security

Original Slides: Erland Jonsson
Changes by Magnus Almgren



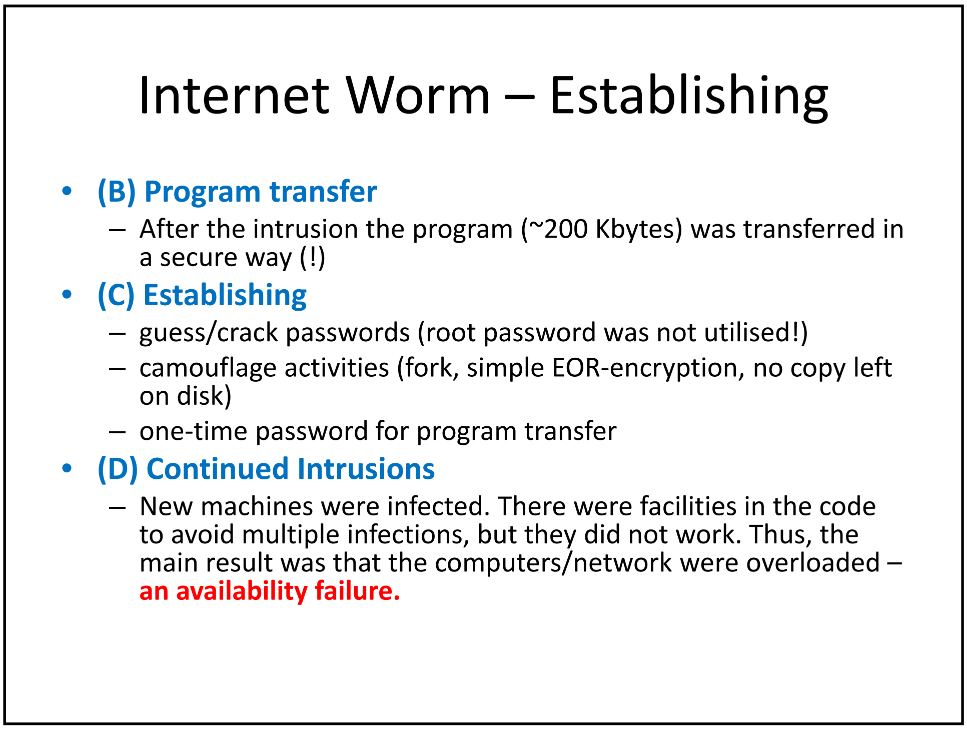
Internet Worm – Intro

- written by Robert T. Morris Jr. at Cornell University
- released 1988-11-02
- 6,000 computer were shut down as a result (in USA only)
- ***Principle for function:***
  A. Intrusion
  B. Transfer of main program
  C. Settling down and establishing (cracking accounts, hiding, etc)
  D. Continued intrusions



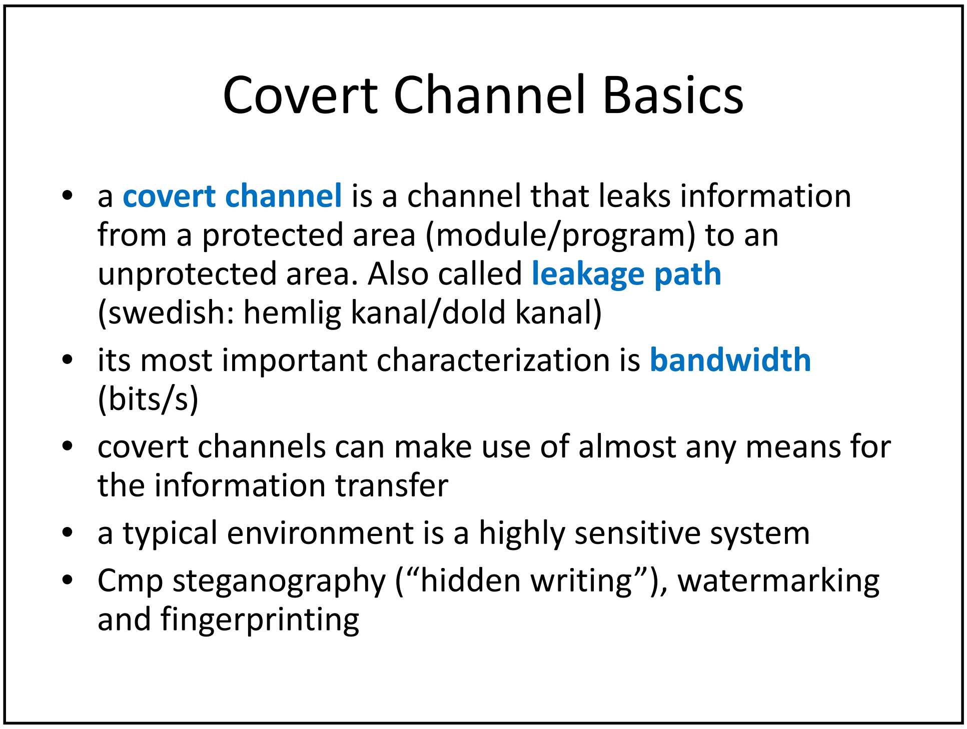
Internet Worm – Intrusion

- **(A) Intrusion:**
  Three types of attacks were launched
  (all of them were well-known in the UNIX community)
  i. guess/crack passwords
  ii. use debug facility in the sendmail mail handler
  iii. exploit bug in finger program
- **How?**
  i. guessing “probable” passwords, “Joe accounts”, etc
  ii. the debug facility in sendmail made it possible to execute a command sequence remotely
  iii. the fingerd daemon calls a subroutine gets, the argument of which is chosen so that an “intelligent” buffer overflow is executed



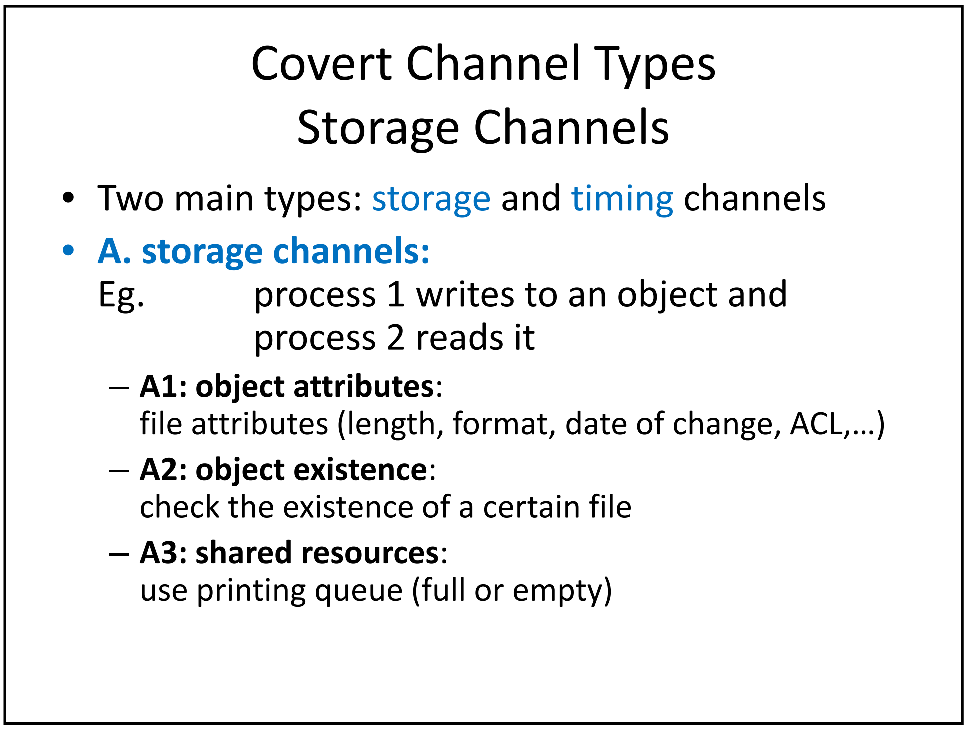
Internet Worm – Establishing

- **(B) Program transfer**
  - After the intrusion the program (~200 Kbytes) was transferred in a secure way (!)
- **(C) Establishing**
  - guess/crack passwords (root password was not utilised!)
  - camouflage activities (fork, simple EOR-encryption, no copy left on disk)
  - one-time password for program transfer
- **(D) Continued Intrusions**
  - New machines were infected. There were facilities in the code to avoid multiple infections, but they did not work. Thus, the main result was that the computers/network were overloaded – **an availability failure.**



Covert Channel Basics

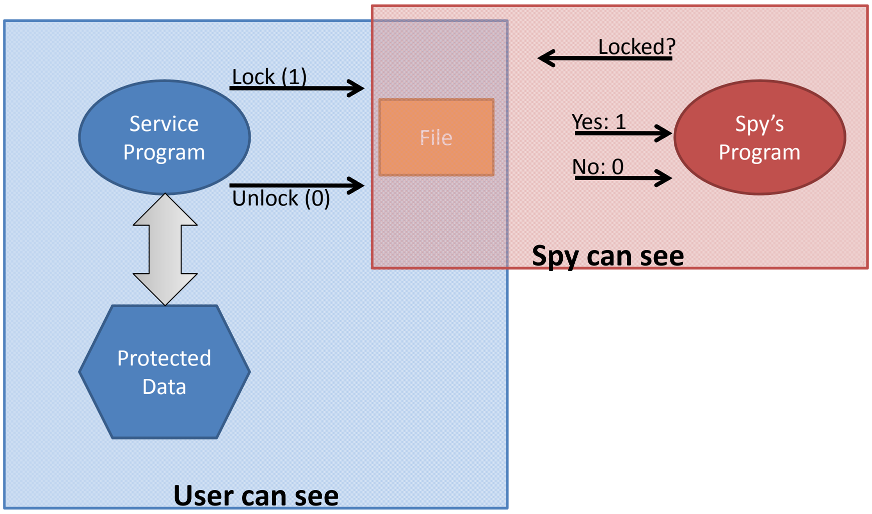
- a **covert channel** is a channel that leaks information from a protected area (module/program) to an unprotected area. Also called **leakage path** (swedish: hemlig kanal/dold kanal)
- its most important characterization is **bandwidth** (bits/s)
- covert channels can make use of almost any means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



Covert Channel Types
Storage Channels

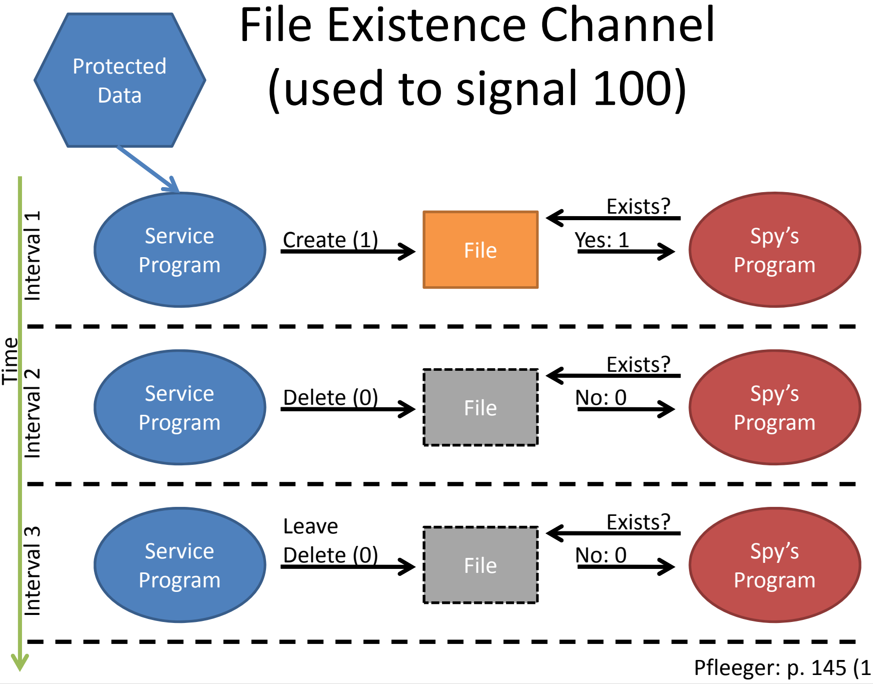
- Two main types: storage and timing channels
- **A. storage channels:**
  Eg. process 1 writes to an object and
  process 2 reads it
  - **A1: object attributes**:
    file attributes (length, format, date of change, ACL,…)
  - **A2: object existence**:
    check the existence of a certain file
  -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

File Lock Covert Channel



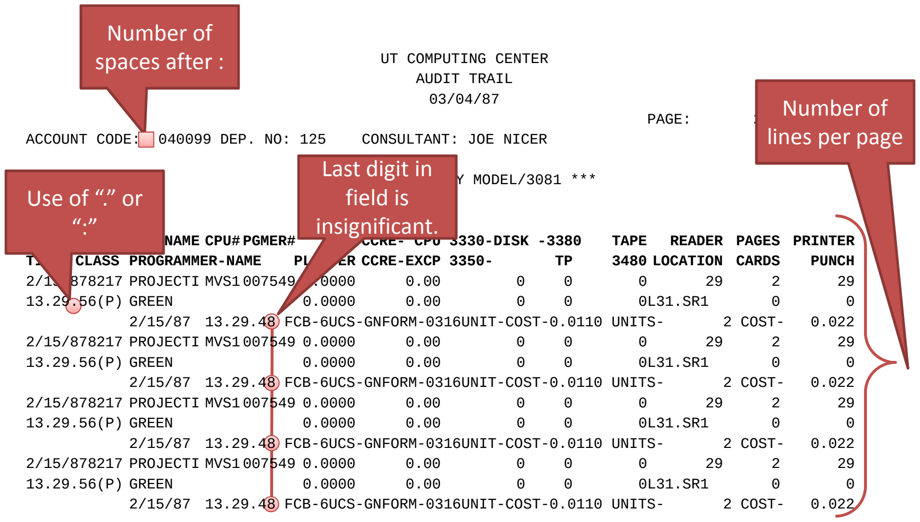
Pfleeger: p. 144 (154)

File Existence Channel (used to signal 100)



Pfleeger: p. 145 (155)

Example Covert Channel



```
                              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
T    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)

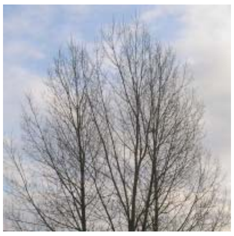
http://utilitymill.com/utility/Steganography_Encode

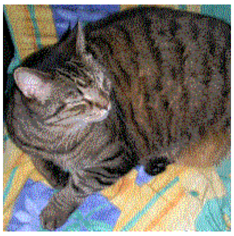
Lenny Domnitser

Randolph Femmer /life.nbii.gov
First chapter of "Around the world in eighty days", Jules Verne

Practical Steganography (4)

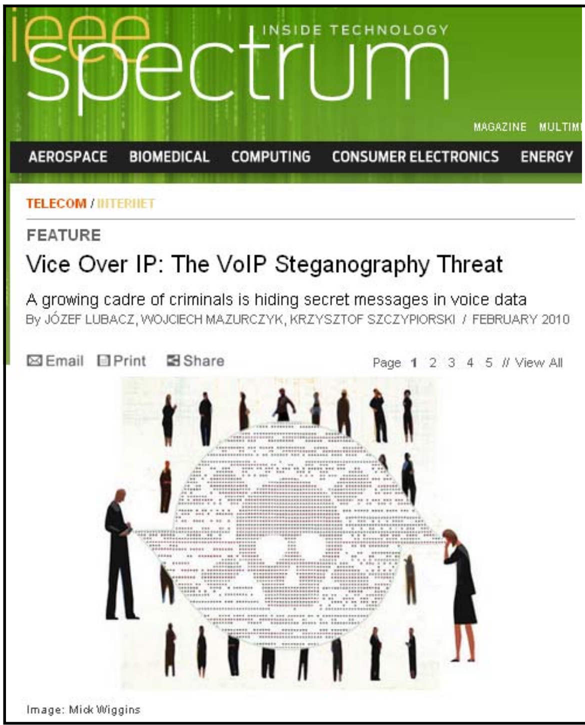
- It is also possible to hide an image within another image.





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



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

Image: Mick Wiggins

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