“Nothing shocks me. I'm a scientist”
Indiana Jones

Warsaw University of Technology: M.Sc. ('97), Ph.D. ('07), D.Sc. ('12) – telecommunications (ICT and information security)

Budapest Tech, Hungary ('03): advanced networking

University of Social Sciences and Humanities, Poland ('13): psychology of motivation (post graduated)

University of California, Berkeley ('13): business in science
Research areas

- Theory of observing change
- Network security
  - network steganography
  - anomalies detection
  - and fraud management
- Digital forensics
- Open-source intelligence

ECE 646 @ GMU.edu
Over 160 press information worldwide
http://stegano.net/press.html

“I once told you that secrets have a cost. The truth does too”
Aunt May Parker
Scope of this lecture

- Introduction to steganography including history and examples
- Network steganography
- Steganalysis
- Examples of network steganography
  - WLAN steganography
  - VoIP steganography
  - Steganographic router
  - Retransmission steganography

Στεγανογραφία

- From Greek: covered writing
- Hiding one information (steganogram) inside another (carrier)
- Example: hidden communication between the terrorists
# Cryptography vs. steganography

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Cryptography</th>
<th>Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Obfuscate the content of communication</td>
<td>Hide the fact of communication</td>
</tr>
<tr>
<td>Secrecy</td>
<td>Cipher text is illegible</td>
<td>Embedded information is &quot;invisible&quot; to an unaware observer</td>
</tr>
<tr>
<td>Security of communication</td>
<td>Relies on the confidentiality of the key</td>
<td>Relies on the confidentiality of the method of embedding</td>
</tr>
<tr>
<td>Warranty of robustness</td>
<td>Complexity of the ciphering algorithm</td>
<td>Perceptual invisibility / statistical invisibility / compliance with protocol specification</td>
</tr>
<tr>
<td>Attacks</td>
<td>Detection is easy / extraction is complex</td>
<td>Detection is complex / extraction is complex</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>Technical</td>
<td>Reverse engineering</td>
</tr>
<tr>
<td></td>
<td>Legal</td>
<td>Cryptography export laws</td>
</tr>
</tbody>
</table>

## Classical steganography - examples

![Mask Letters](http://www.si.umich.edu/spies/methods-mask.html)

![Invisible Ink](http://www.si.umich.edu/spies/methods-ink.html)

![Tattoos](http://www.miki.hg.pl/tatoo%20maly/Image72.jpg)
Current steganography applications

Main carriers of hidden data: images, voice and text


Steganography vs. 911

- Terrorist attack on September 11 (probably) was planned with steganography
- After these attacks there has been a growing interest in modern methods of steganography and its detection

WASHINGTON — Osama bin Laden and other Muslim extremists are posting encrypted, or scrambled, photographs and messages on popular Web sites and using them to plan terrorist activities against the United States and its allies, U.S. officials say. The officials said bin Laden and his associates are using the Internet to conduct what some are calling “virtual” or遥控 war. Mr. bin Laden, a dissident Saudi businessman, has been indicted for the 1998 bombing of two U.S. embassies in East Africa and is believed to be responsible for last fall’s bombing of the USS Cole in Yemen. Four alleged bin Laden associates went on trial Monday in federal court in New York for the embassy bombings. “To a greater and greater degree, terrorist groups, including al-Qa’ida, Hamas, and bin Laden’s al Qaeda group, are using computerized files, e-mail, and encryption to support their operations,” CIA Director George Tenet wrote last March to the Senate Foreign Relations Committee. The testimony, at a closed-door hearing, was later made public.
Jihad magazine on technology

- Magazine printed since 2006
- Al Qaeda community
- Issue 2 (March 2007): article on modern steganography


Spies and steganography

June 2010

Indictment act:

III. MANNER AND MEANS OF THE CONSPIRACY

A. SECRET COMMUNICATIONS

21. To further the aims of the conspiracy, McVeigh and or other co-conspirators used a Russian-developed steganography program that was steganography software that was not commercially available. The software package permitted the DNR to surreptitiously insert encrypted data into images that are being transmitted electronically. The encrypted data can be removed from the image, and then decrypted, using DNR-provided software. Similarly, DNR-provided files can be used to conceal data, and then clandestinely be used to hide the data in images on publicly-available websites.

22. The indictment further alleges that

...
Who is who in the Russian spy ring?

In 2004, a report emerged, revealing that certain printer manufacturers enriched their products with the capability to hide tracking information in printouts. The yellow tracking dots coded machine identification numbers.

Printer steganography

- In 2004, a report emerged that certain printer manufacturers enriched their products with the capability to hide tracking information in printouts.
- The yellow tracking dots-coded machine identification numbers.
Secret communication for disidents

In 2010, scientists at Georgia Tech had created a method of communication by means of popular photo-sharing sites, like Picassa or Flickr. The Collage program enables hiding of short text messages in multiple pictures, from which data can be retrieved by means of combining.


Printed arrays of microbes

Researchers from Tufts University have showed in 2011 that information can be hidden with the aid of bacteria possessing fluorescent capabilities. Strains of genetically modified *Escherichia coli* can glow in growth.

http://www.yalescientific.org/2012/03/the-name-is-coli-escherichia-coli/
Malware

- Computer worms and other forms of malware are presently exploiting steganography for the purpose of obtaining functioning commands and transferring hijacked data.

  This was the case with Operation Shady RAT in 2011, where instructions were smuggled in crafted HTML and JPEG files.

- The Duqu worm (2011) transferred collected data to its command and control centers by means of tampered image files.

- It seems that steganography is starting to be popular with Android malware – recent reports (30 Jan 2012) suggest that images are used to hide control information on sending premium rate SMS.

  ![Malware Diagram](http://www.f-secure.com/weblog/archives/00002305.html)

Computer games

- It is suspected that multiplayer games may be a good cover for covert communication.

- Private chatrooms shared by players are out of scope of network monitoring and thus may serve as meeting place of would-be terrorists.

- Playstation and Xbox communication is free of legal invigilation (as of beginning 2012).

  ![Computer Games](http://www.dealspwn.com/sun-wouldbe-jihadists-call-duty-training-96910#57168)
Developments in steganographic carriers

- Ancient Greece
- Rome
- Medieval Ages
- Age of Enlightenment
- Romanticism

- Wooden tablet
- Parchment
- Astragal
- Eggshell
- Woodcut
- Music notes
- Newspapers

- Hare corpse
- Human skin

- Time

Developments in steganographic carriers

- Digital text and source codes
- OS filesystem
- Digital media files
- Free/redundant fields of network protocols
- Specific computer services and networking environments
- Network protocols and services' behavior
- Bacteria

- Present time

- Image files
- Printed matter
- Image collage
- Malware's commands hidden in HTML or images
- Computer game's chats
Modern steganography trends

- Steganographic techniques are aiming towards utilizing communication methods escaping typical monitoring activities.
- The variety of steganographic carriers is constantly increasing.
- Steganography shall remain an attractive means of communication due to the relatively small complexity of implementation.

Steganography as a tool of fighting with censorship

Somewhere in Middle East

Somewhere in China
Network steganography (definition)

- Information hiding techniques which utilise **modifications of the packets** to perform hidden communication
  - Modification to the **structure** of the packet: payload and protocol specific fields
  - Modification to packets’ **time relations**: e.g. changing the sequence of the packets or inter-packet delays

A simple example of network steganography

Idea:
- change of frequency interpreted by sender and receiver ("common secret") as transmission of 1 bit of steganographic message
- Hidden message is very hard to detect by an observer
Network steganography applications

Network steganography adjusts to:

- Services: type of information exchange (e.g. query-response, file transfer)
- Transport network: form of messages (e.g. fragmentation, segmentation)
- Communication channel: imperfection of the channels (e.g. errors, delays)

OSI RM

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

Examples by protocol type

Examples:

- HTTP header manipulation (Van Horenbeck, 2006)
- LSB of voice samples modification for VoIP (Bender et al., 1996)
- SIP header manipulation (Mazurczyk and Szczypiorski, 2006)
- Intentional TCP segments retransmissions (Mazurczyk et al., 2009)
- Packets sorting and IP header manipulation (Kundur and Ahsan, 2003)
- Ethernet frame's padding for different upper layers protocols (Jankowski et al., 2011)
- Intentionally corrupted frames (Szczypiorski [12], 2003)
- Padding of OFDM symbols for WLANs (Szczypiorski and Mazurczyk [13], 2011)
Clasification of steganographic methods

Intra-protocol steganography
- Modification of packets
- Modification of structure of packets stream
- Reordering of the packets
- Modification of inter-packet delay
- Intentional losses of packets

Payload
Mixed
Protocol specific fields
Hybrid

Inter-protocol steganography

Steganographic bandwidth vs. undetectability

Steganographic bandwidth
Undetectability
How to estimate the steganographic bandwidth?
- mathematical models (Markov chains)
- simulations
- implementations

Steganographic bandwidth – values

Maximal values (!)
Depend on undetectability

<table>
<thead>
<tr>
<th>Method</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiPad (802.11g 54 Mbit/s)</td>
<td>1.5 Mbit/s</td>
</tr>
<tr>
<td>HICCUPS (802.11g 54 Mbit/s)</td>
<td>216 kbit/s</td>
</tr>
<tr>
<td>TranSteg (G.711 (64 kbit/s) + G.726 (32 kbit/s))</td>
<td>32 kbit/s</td>
</tr>
<tr>
<td>Typical VoIP call</td>
<td>2.5 kbit/s</td>
</tr>
<tr>
<td>PadSteg</td>
<td>27 bit/s</td>
</tr>
<tr>
<td>StegSuggest</td>
<td>10 bit/s</td>
</tr>
</tbody>
</table>
Philosophy of steganalysis

For each steganographic method
the method of its detection (steganalysis) must be specified

(ethical issue)

Steganalysis method is an inherent component of
any effective steganographic method

(pragmatic issue)

Steganalysis requires anomaly detection
in communication protocols in real network conditions -
distinguish anomalies introduced by the steganographic method
from anomalies arising from non-ideal communication network

Quantitative estimation of effectiveness of steganalysis is a difficult issue
(distinct from the question of estimating the resistance
of cryptographic methods
usually expressed in terms of computational effort)

Steganalysis: practical methods

1) Detection of known steganographic applications
2) Detection of network anomalies by observing behavior of protocols
or exchanged content (jpegs, voice samples)
At the end...

About our project: stegano.net

- stegano.net is a project focused on steganography and anomaly detection
- since 2002 our efforts provide innovations in data hiding for existing networks including wireless LANs, Voice over IP (VoIP) and other sides of the Internet
- we believe that our solutions may exist in networks like chameleons in Nature
- Web: http://stegano.net
- FB: http://facebook.com/stegano.net
Conclusions

- Network steganography: a new discipline in network security
- Important because:
  - Information leakage
  - Fighting with censorship
  - “Military communications”
  - Anomalies in networks
  - Other ???
- Key issue for next years: steganalysis

Further reading

J. Lubacz, W. Mazurczyk, K. Szczypiorski: Vice over IP,
In: IEEE Spectrum, ISSN: 0018-9235, February 2010, pp. 40-45

W. Mazurczyk, K. Szczypiorski, J. Lubacz: The Spy Who Skyped Me - Four New Ways to Smuggle Messages Across the Internet

E. Zielińska, W. Mazurczyk, K. Szczypiorski: Trends in steganography
In: Communications of the ACM, Volume 57, Issue 3, March 2014, pp. 86-95 [also available in Chinese]

J. Lubacz, W. Mazurczyk, K. Szczypiorski: Principles and Overview of Network Steganography
Case Studies

Case studies
- 3 stories
- 3\*x groups
- One group per story
- Prepare framework of steganographic system(s) and system to detect it/them
Story #1

7:00 p.m.: Shanghai, China

An employee of an electronic equipment factory uploads a music file to an online file-sharing site. Hidden in the MP3 file (Michael Jackson's album *Thriller*) are schematics of a new mobile phone that will carry the brand of a large American company. Once the employee's Taiwanese collaborators download the file, they start manufacturing counterfeit mobile phones essentially identical to the original—even before the American company can get its version into stores.

Story #2

3:30 p.m.: somewhere in Afghanistan

A terrorist hunted by the U.S. Federal Bureau of Investigation posts an excerpt from the motion picture *High School Musical Three: Senior Year* on Facebook. Inside are hidden instructions for a bomb attack on a commuter rail line in southern Europe. Later that day, terrorists based in Athens follow the instructions to plan a rush hour attack that kills hundreds of people.
Story #3

- **4:00 a.m.: Malibu, CA**

A very famous actor (VFA) has a brief conversation with a well-known director (WKD) over Skype, an application that lets them make free voice calls over the Internet. They discuss the medical problems of VFA's cat in great detail. When the conversation is over, WKD's computer has a sleazy new addition—in a folder on his desktop, there is a picture of a nude teenager, along with her mobile number and the date and time at which WKD will meet her at VFA's pool party for a photo session.

---

**Спасибо! (Thanks!)**

Anna Vasylivna Kushenko
(Chapman)