



# **Steganography in TCP/IP Networks.**

**State of the Art  
and a Proposal of a New System - HICCUPS**

**Krzysztof Szczypiorski**

Warsaw University of Technology, Poland  
Institute of Telecommunications

Warsaw, November 4<sup>th</sup>, 2003

# Outline

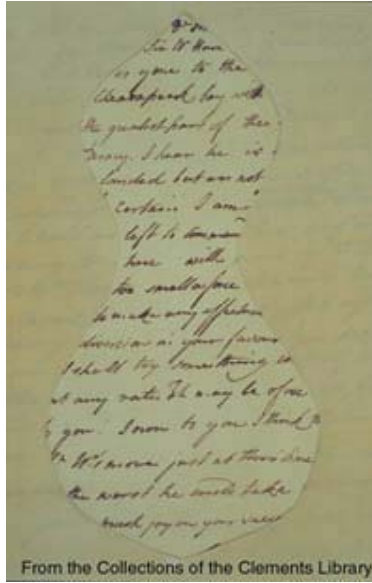
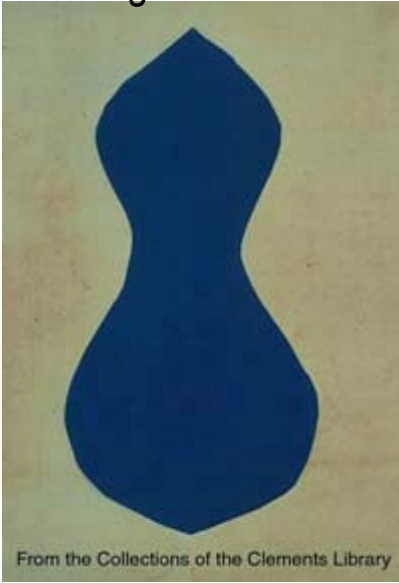
- ◆ Background: etymology, historical inheritance, stegano vs. crypto...
- ◆ State of the art – hidden channels in:
  - Ethernet (CSMA/CD), IP, ICMP, TCP, UDP, HTTP, HTML, XML...
- ◆ A proposal of a new system - HICCUPS
  - HICCUPS concept
  - Network environment for HICCUPS and hidden data channels
  - HICCUPS operation and functional parts
  - Example of implementation framework for wireless local area networks (WLAN) IEEE 802.11
  - Future work
- ◆ Conclusions
- ◆ References



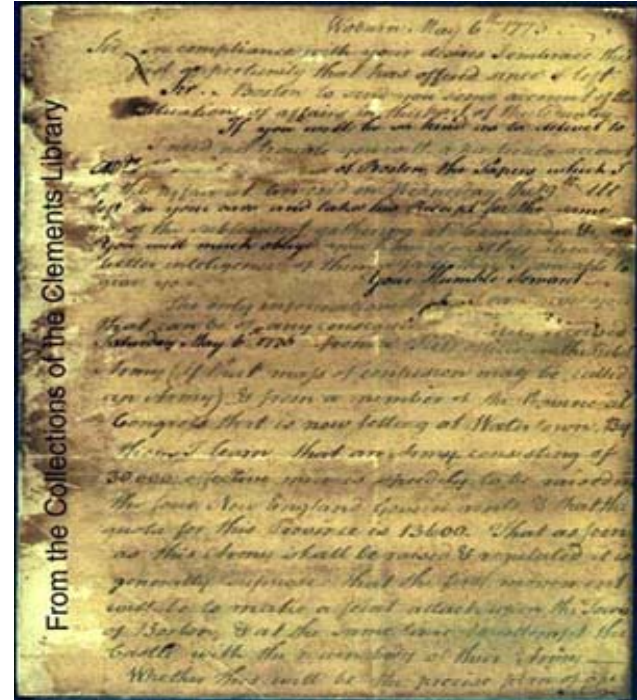
# Historical Background (2/2)

## Human vs. Human Problem

### Masking



### Invisible ink



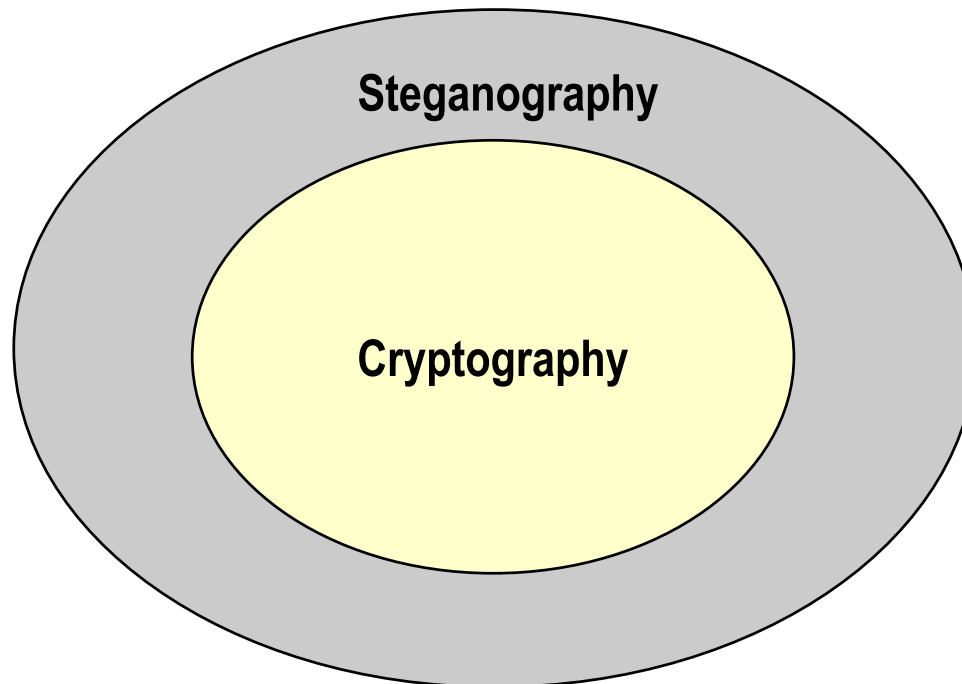
### Tattoo



- ↑ <http://www.si.umich.edu/spies/methods-ink.html>
- ↖ <http://www.si.umich.edu/spies/methods-mask.html>
- ← <http://www.miki.hg.pl/tatoo%20maly/Image72.jpg>

Steganography was dedicated to hide information **from human**

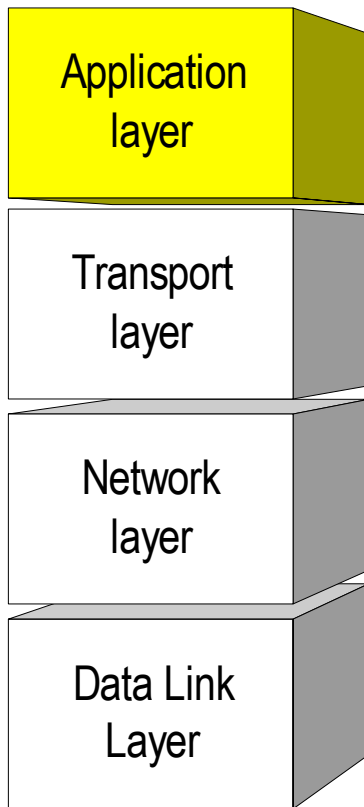
# Stegano\* vs. crypto\*



- Steganography vs. cryptography
- Steganalysis vs. cryptanalysis

# Related Work: Top Layer

TCP/IP protocol suite



- ◆ In the TCP/IP protocol suite **multimedia applications** are equivalent of old techniques – hidden data is distributed in sound files, images and movies (→) via WWW, Usenet, E-mail, etc.
- ◆ **Watermarking** to protect intellectual property rights
- ◆ Network (protocol) steganography – **machine vs. machine problem**
- ◆ Field of knowledge established in scientific literature in 1996
- ◆ Discovered again after 911 (September 11<sup>th</sup>, 2001)
- ◆ At **application layer**: not only applications, but also protocols exist (HTTP, NNTP, SMTP, etc.)

# Steganography „embedded in content”



An image distributed in Internet (April 2003):  
<http://www.michaelpang.com/upload/newupload/image001.jpg>

- ◆ multimedia
  - sound files
  - images
  - movies



TOOL	VENDOR - AUTHOR	OPERATING SYSTEM	STEG TYPE
1 Hidesite	John Collemassa 1 jcol@gc@eth.w.ch <a href="http://www.hidesite.co.uk/">http://www.hidesite.co.uk/</a>	WEB (WinDOS ) Unix/Linux (C)	IMAGES: (DMP)
2 DMP Server	Parallel Worlds Parallel Worlds is an offshore software development company based in Kiev, capital of Ukraine. Tel.: +380 (94) 442 6077 Tel.Fax: +380 (94) 442 6518 Fax: +380 (94) 451 6546 skf 180252 GSM SMS: dshk@pww.com.ua e-mail: dshk@pww.com - General Information: info_PW@hikiev.ua - Services: Services_PW@hikiev.ua - Customer and Product Support: Support_PW@hikiev.ua - Products Sales: Sales_PW@hikiev.ua - Web design: webmaster_PW@hikiev.ua - Other questions: admin_PW@hikiev.ua Visit Parallel Worlds page at <a href="http://www.pworld.com">http://www.pworld.com</a> Visit our steganography page at <a href="http://www.pworld.com/steganography.html">http://www.pworld.com/steganography.html</a> Visit DMP Server page at <a href="http://www.pworld.com/products/dmp-server.html">http://www.pworld.com</a>		IMAGES: (Data: JPEG, GIF, BMP, Other Output: BMP (24-bit))
3 DMPEmbed v1.38 (DMP) Data Embed	Brook Sandford and Ted Handal (LAJE.gov) Brook.Sandford@lajefed.gov Ted.Handal@lajefed.gov	DOS (DOS ) WEB (WinDOS )	IMAGES: (DMP)
4 DMPTable v2.16 (DMP) Data Embed	Brook Sandford and Ted Handal (LAJE.gov) Brook.Sandford@lajefed.gov Ted.Handal@lajefed.gov	DOS (DOS ) WEB (WinDOS )	IMAGES: (DMP)
5 Camouflage 3.0	Frederic Peter Frederic Peter rue Chauxville, 30 4420 Montegnée Belgique per telephone : +32(0)4263 30 61 per e-mail : rfr@133@planet.nl w.b. peter@home.alpha.net.ch peter@xyzpik.org	WEB (X)	IMAGES: (TGA (24-bit uncompressed, 640x480, maximum of 52118 bytes). Author recommends using PNG.)
6 Controlled Hall Embed (CHE)	Julia B. Thyssen & Hans Zienowien hans@thysen / JTHE Productions Lindendreef 52 B 1015 KE Amsterdam The Netherlands E-mail: dshk@pww.com 343945 Tlx.v. J.B. Thyssen". Tel@pww.net, julia@hidesite.com hans@pww.com	WEB (w)	IMAGES: (BMP (24-bit only))

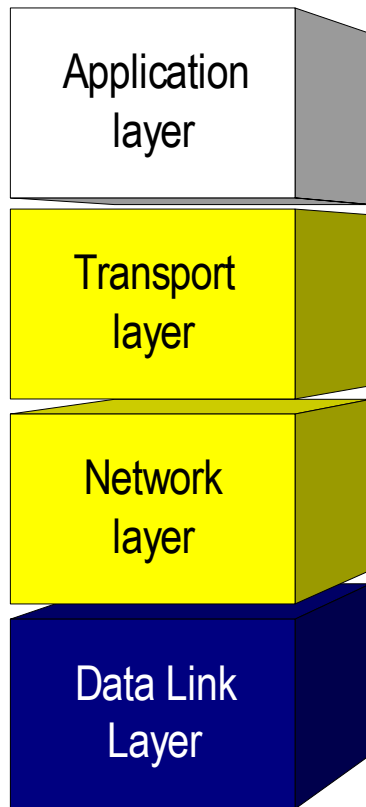
**Steganography's Web Page by Neil F. Johnson, PhD**  
<http://www.jjtc.com/Steganography/toolmatrix.htm>  
**A list\* of 146 tools (incl. only one tool for TCP/IP networks)**  
 \* October 2003

	<a href="http://www.profiles.net/robby/robby/">http://www.profiles.net/robby/robby/</a>		(DMP (24-bit only) cannot lower resolution to 24-bit)
8 Cover-TCP	Craig H. Rowland crowland@psnic.com <a href="http://www.psnic.com/cover/">http://www.psnic.com/cover/</a>		TEXT/HTML/ PRO TO COL: HTML/HTML



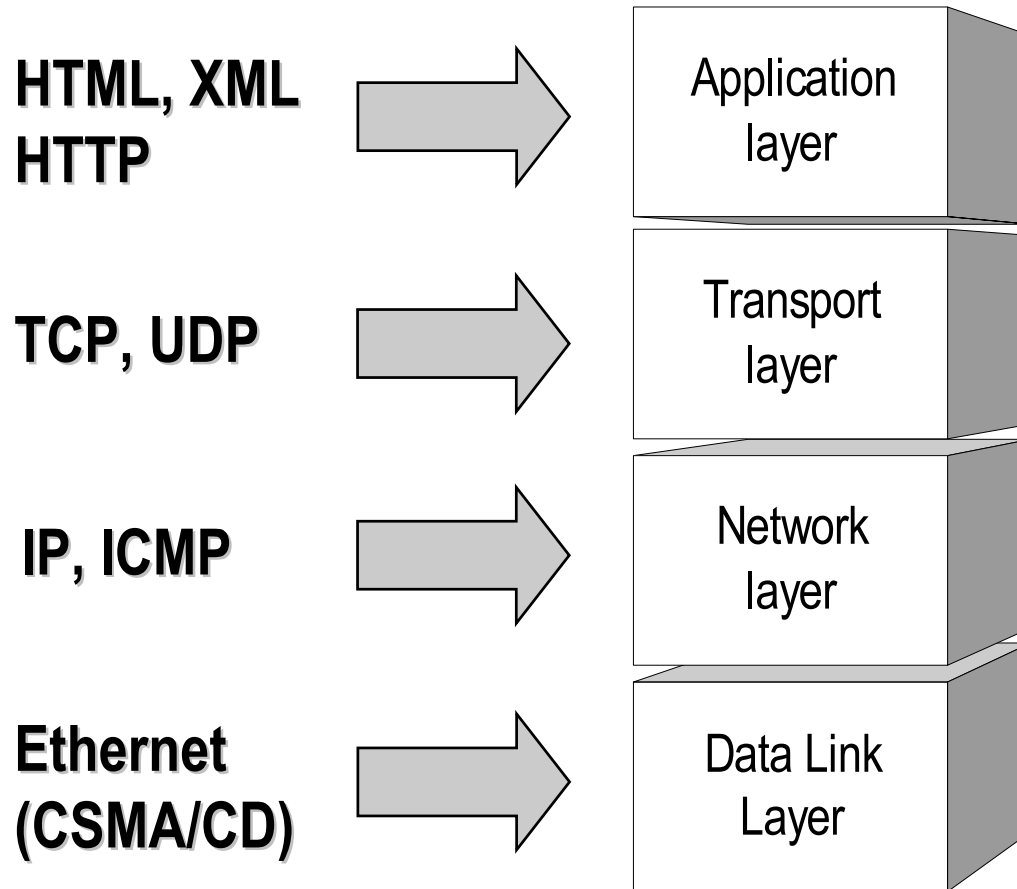
# Related Work: Beneath Top Layer

TCP/IP protocol suite



- ◆ A focus on transport and network layers hidden communication (because of WAN):
  - Usage of optional fields
  - Semantic changes
  - Improper, but acceptable construction of protocol data units (packets)
- ◆ In a data link layer
  - As above plus:
  - Usage of unused transmission code space
  - In LAN: CSMA/CD manipulation (→)

# Examples of TCP/IP Protocol Suite Hidden Channels



# CSMA/CD Manipulation

- ◆ Handel T. I Sandford M.: **Hiding Data in the OSI Network Model**. In: Anderson, R. (Ed.): Proceedings of: Information Hiding – First International Workshop, Cambridge, U.K., May 30 – June 1, **1996**, vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc, pp. 23–38
- ◆ Weapon Design Technology Group – Los Alamos National Laboratory
- ◆ A control over the retransmission time after packet collision (“back off”) allows to send “bit-per-packet” information
- ◆ To send “bit-per-packet” information station uses zero or maximum time instead of random amount of time

# Network Layer and Transport Layer Manipulation (1/2)

- ◆ Rowland C. H.: **Covert Channels in the TCP/IP Protocol Suite**. Psionics Technologies, November 14, 1996
  - Covert TCP
  - [http://www.firstmonday.dk/issues/issue2\\_5/rowland/](http://www.firstmonday.dk/issues/issue2_5/rowland/)
- ◆ Fisk G., Fisk M., Papadopoulos C., Neil J.: **Eliminating Steganography in Internet Traffic with Active Wardens**. In: Petitcolas, F. A. P. (Ed.): Proc. of: Information Hiding – 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7-9, 2002, vol. 2578 of Lecture Notes in Computer Science, Springer-Verlag Inc., pp. 29-46
  - Los Alamos National Laboratory
  - <http://public.lanl.gov/mfisk/papers/ih02.pdf>

# Network Layer and Transport Layer Manipulation (2/2)

## ◆ Ka0ticSH

- "Diggin Em Walls (part 3) - Advanced/Other Techniques for ByPassing Firewalls"
- <http://neworder.box.sk/user.php?name=Ka0ticSH>

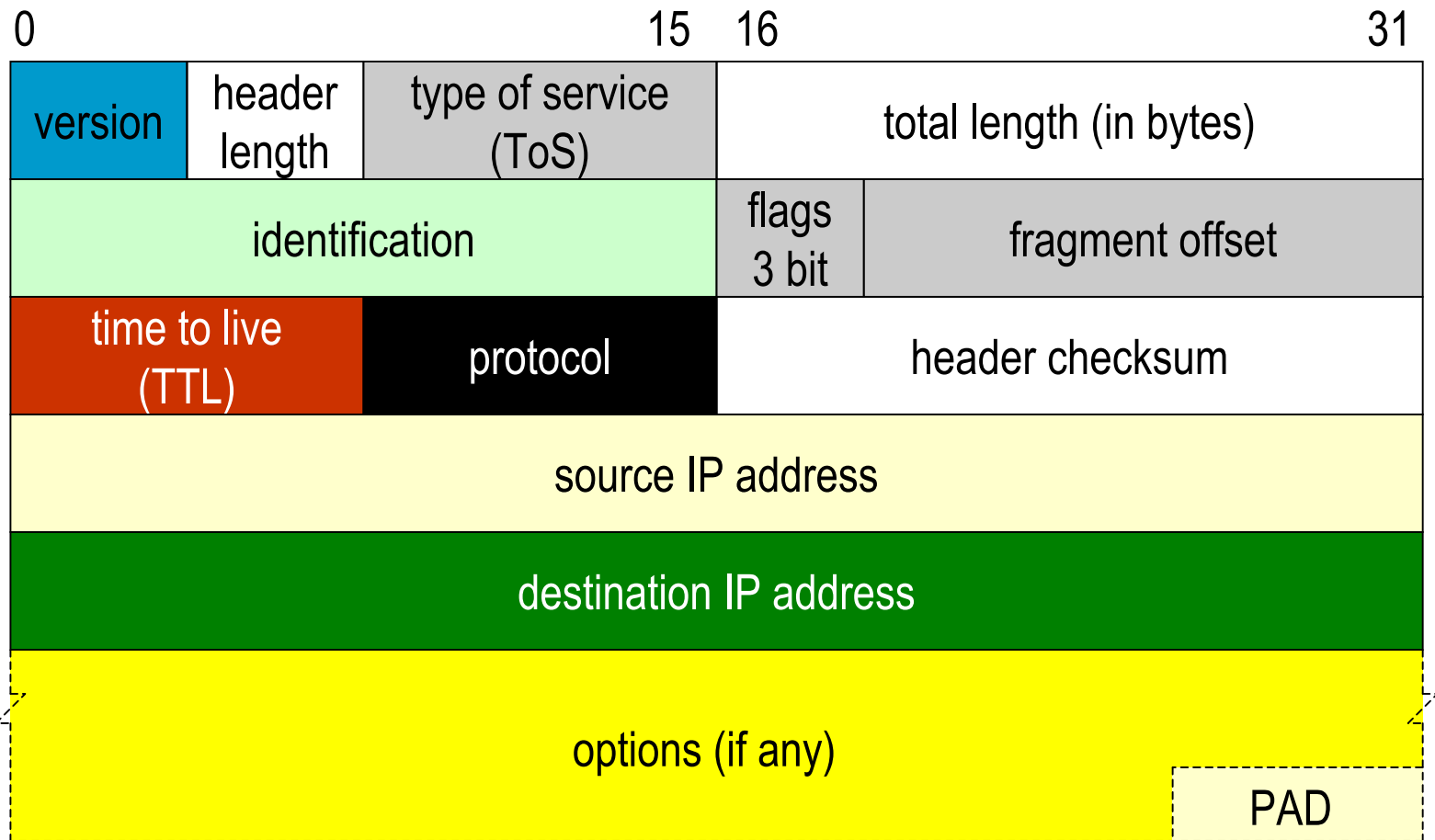
## ◆ Project Loki

- Phrack Magazine 49, 1996-11-08
- <http://www.phrack.org/show.php?p=49>

## ◆ Lee Boyer

- "Firewall bypass via protocol steganography"
- [http://www.networkpenetration.com/protocol\\_steg.html](http://www.networkpenetration.com/protocol_steg.html)

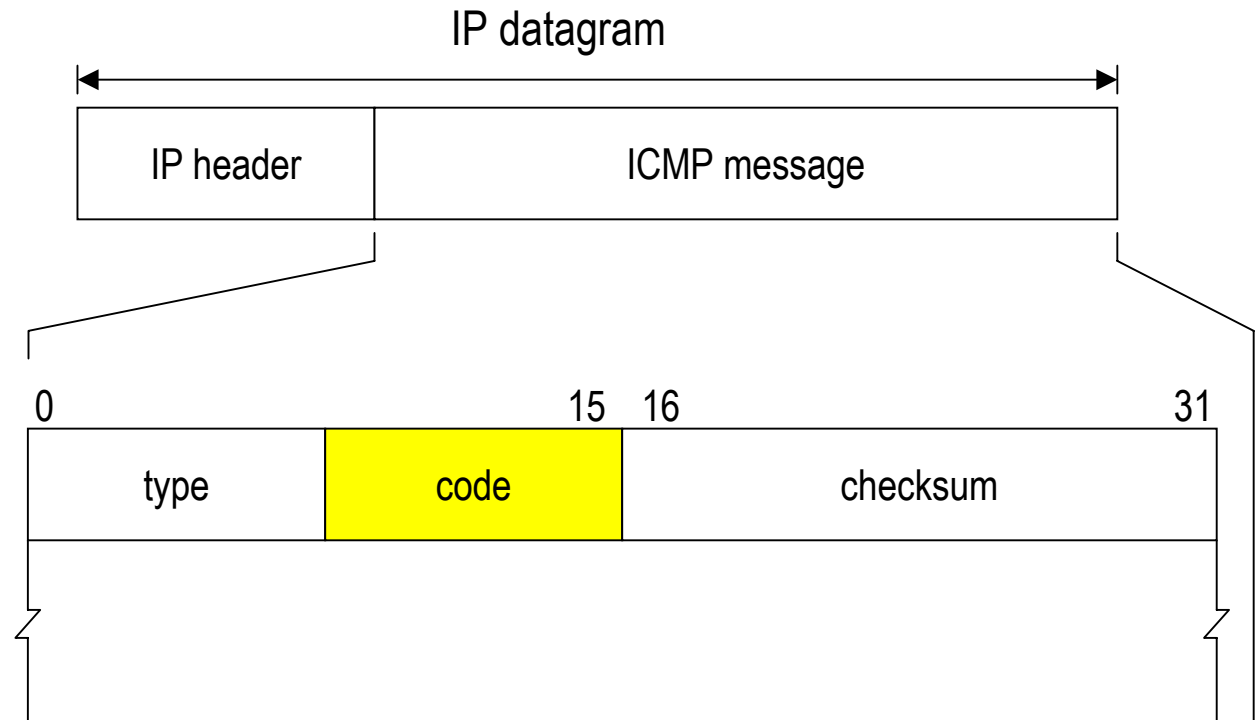
# IP header – Possible Hidden Channels (1/2)



# IP header – Possible Hidden Channels (2/2)

- ◆ PAD (padding bits) – bandwidth 31 bits/packet
- ◆ IP identification – 16 bits/packet
- ◆ Fake source IP address – 32 bits/packet
- ◆ Usage of IP destination address as a flag – 8 bits/packet
- ◆ Usage of the unnecessary fields (ToS, options, some flags for example Don't Fragment - DF for the fragmented packet) – various bandwidth

# ICMP msg – Possible Hidden Channels (1/3)

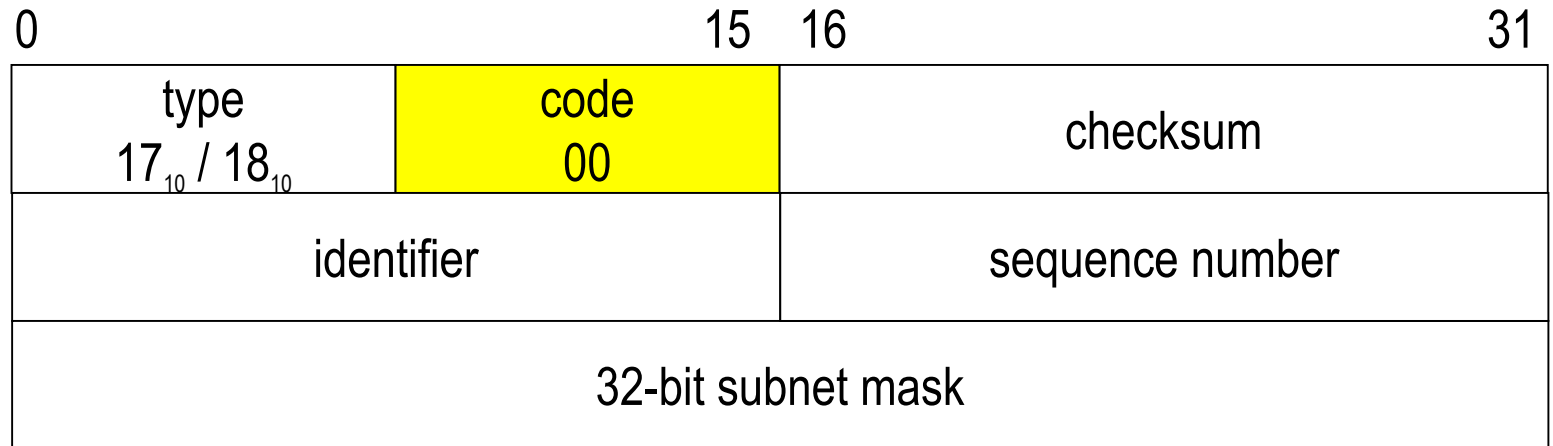


- ◆ Usage of the **Code** field, when only the **Type** field is sent (for example ICMP Address Mask Query →) – 8 bits/packet
- ◆ Usage of optional fields or field that should have strict value (for example ICMP Destination Unreachable →)



# ICMP msg – Possible Hidden Channels (2/3)

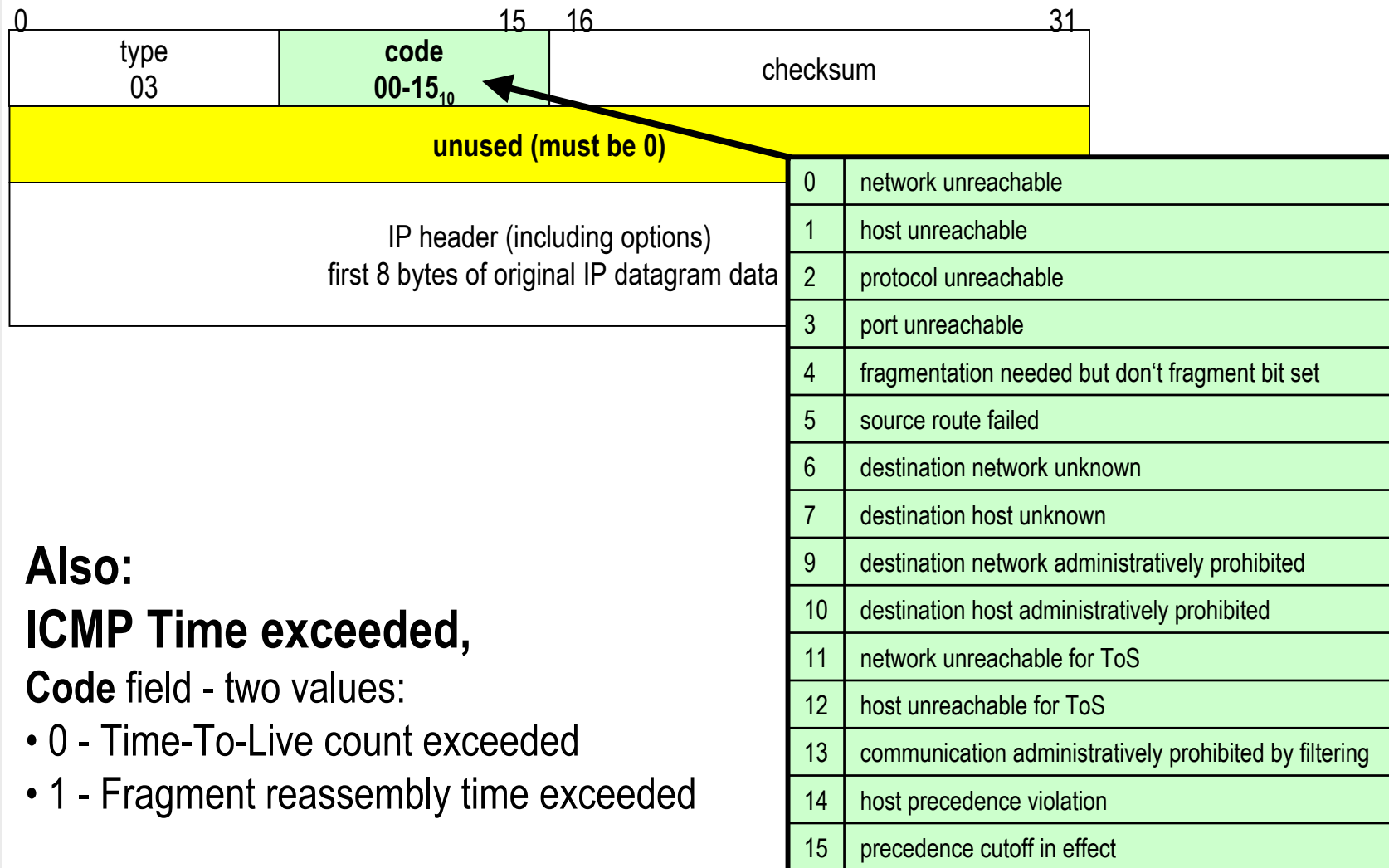
## ICMP Address Mask Query



17 – Request; 18 - Reply

# ICMP msg – Possible Hidden Channels (3/3)

## ICMP „Destination Unreachable”



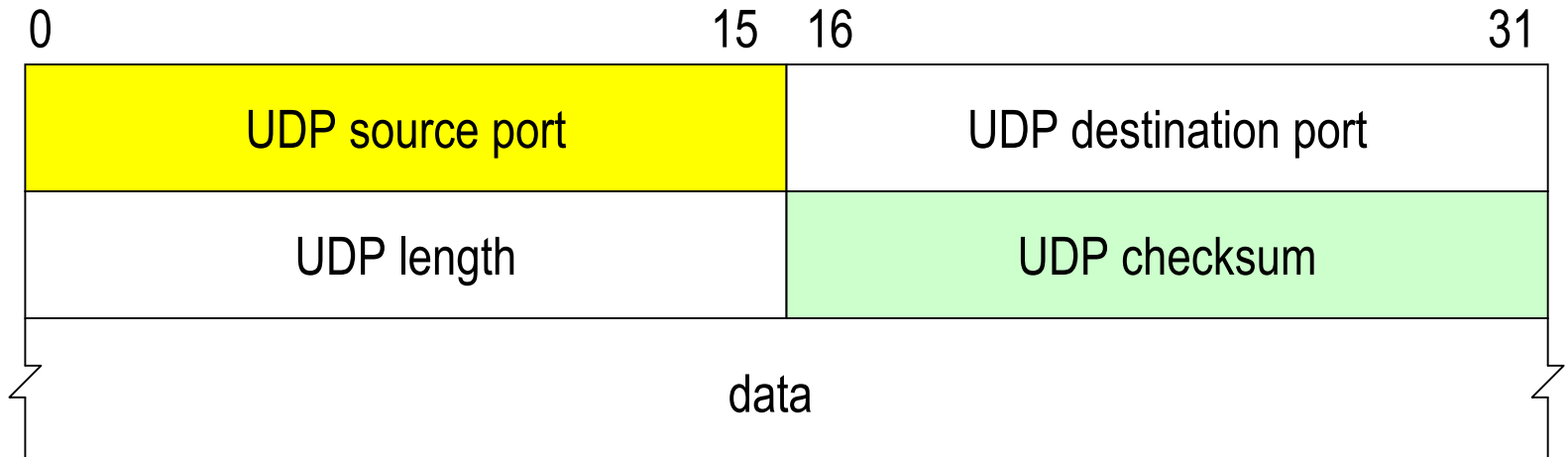
**Also:**

**ICMP Time exceeded,**

**Code** field - two values:

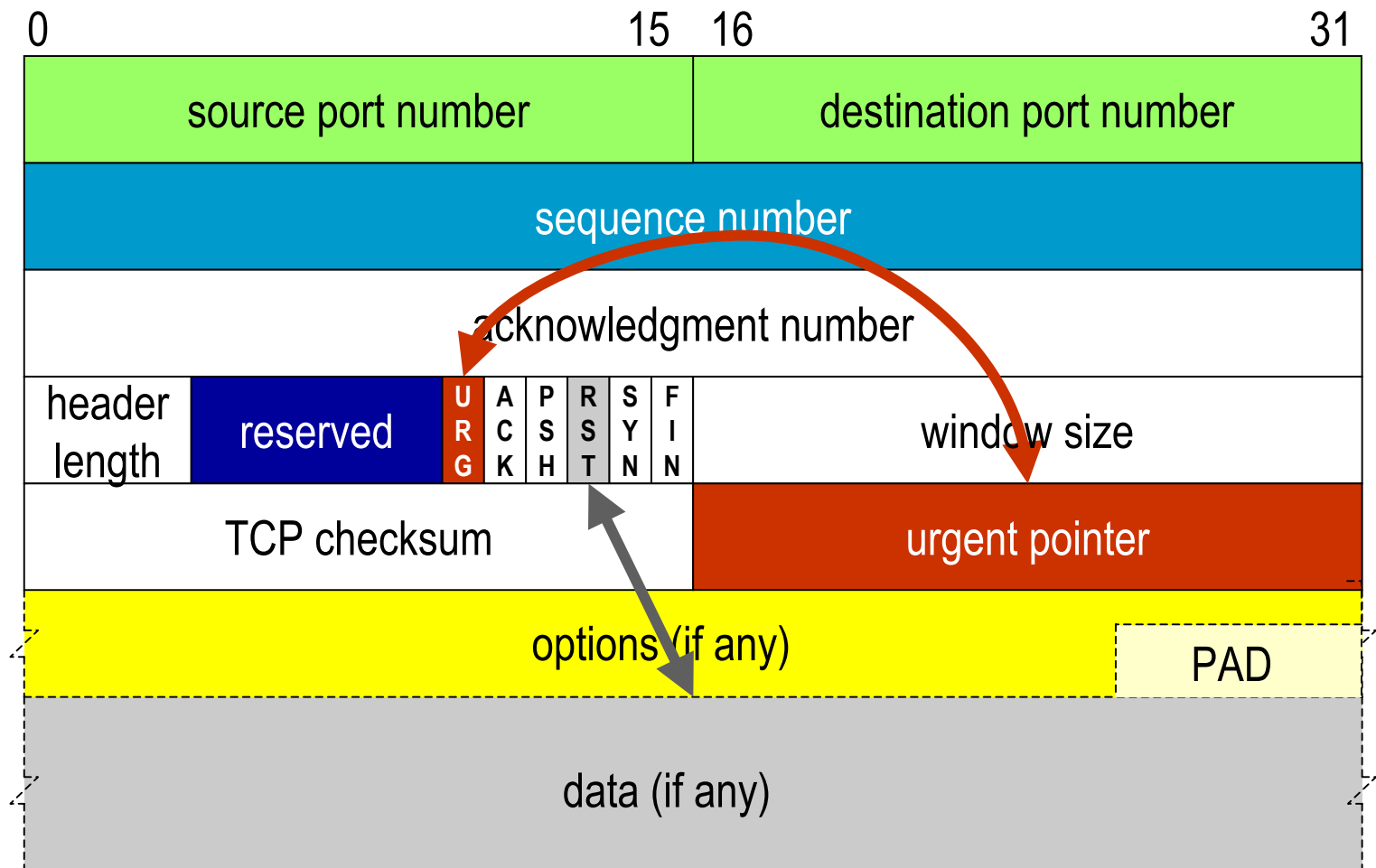
- 0 - Time-To-Live count exceeded
- 1 - Fragment reassembly time exceeded

# UDP Header – Possible Hidden Channels



- ◆ UDP source port and UDP checksum are optional

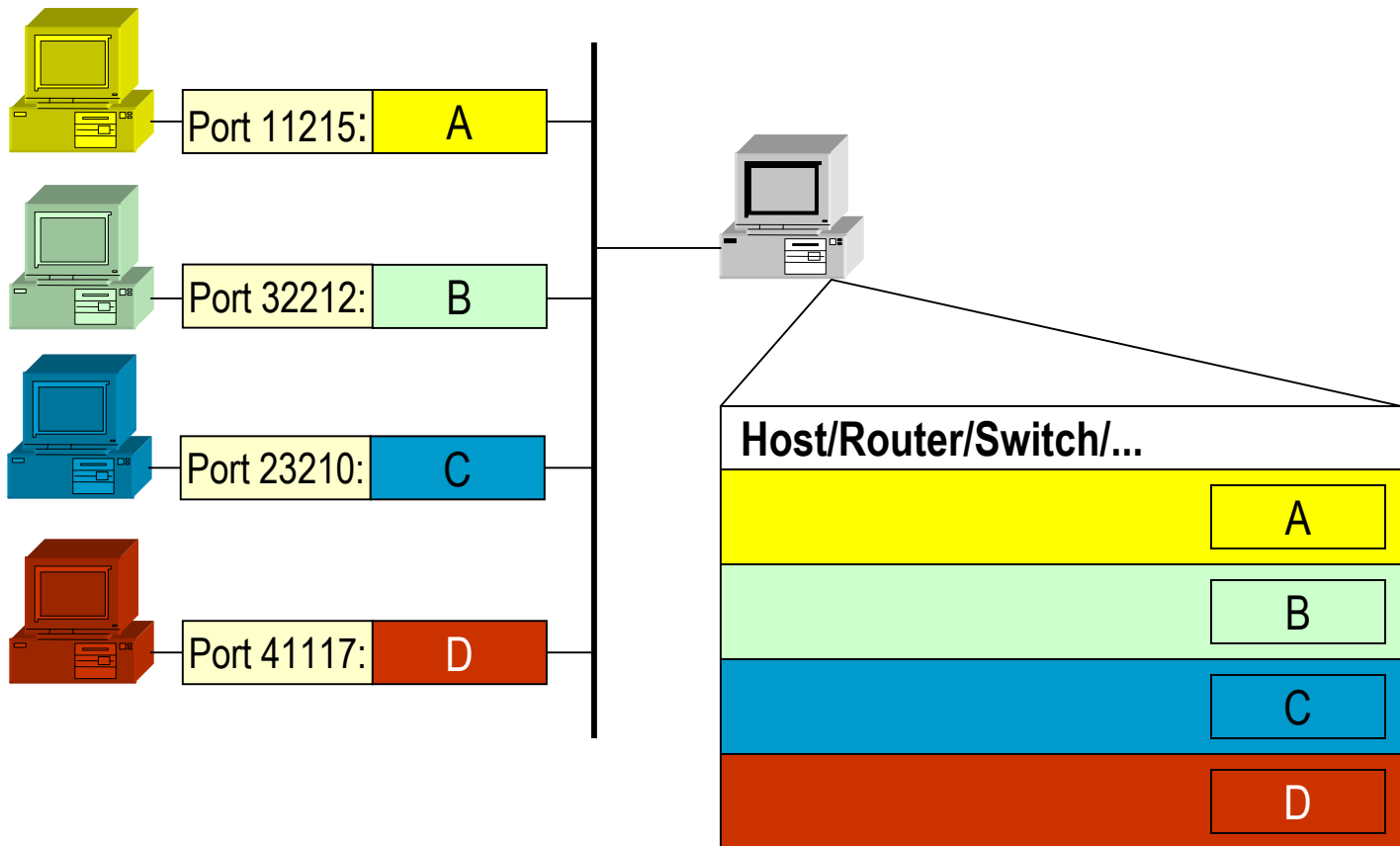
# TCP Header – Possible Hidden Channels (1/2)



# TCP Header – Possible Hidden Channels (2/2)

- ◆ PAD (padding bits) – bandwidth 31 bits/packet
- ◆ Usage of chosen ISN (initial SN) – 32 bits per connection
- ◆ Usage of urgent pointer, when URG=0 – 16 bits/packet
- ◆ Usage of reserved bits – 6 bits/packet
- ◆ Existence of data, when RST=1
- ◆ Port numbers as an alphabet (→)

# „Алфавит мы уже знаем, Уже пишем и читаем...”



Bandwidth: 1 letter/packet

# Manipulation of HTTP

```
titan<krzysiek>(3)> telnet stegano.net 80
```

```
Trying 66.150.161.136...
```

```
Connected to stegano.net.
```

```
Escape character is '^]'.  
Hi, Stupid
```

```
HTTP/1.0 400 Bad Request
```

```
Server: Squid/2.4.STABLE7
```

```
Mime-Version: 1.0
```

```
Date: Tue, 4 Nov 2003 10:12:59 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 903
```

```
Expires: Tue, 4 Nov 2003 10:12:59 GMT
```

```
X-Squid-Error: ERR_INVALID_REQ 0
```

```
X-Cache: MISS from w3cache.pw.edu.pl
```

```
Proxy-Connection: close
```

```
...
```

# Manipulation of HTML, XML...

```
<html>
<head>
<title>:::: s t e g a n o . n e t ::::</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
</head>

<body bgcolor="#CCCCCC" text="#CCCCCC" link="#CCCCCC" vlink="#CCCCCC"
alink="#CCCCCC">
<div align="center"><br>
  
<br>
  <map name="Map_1">
    <area shape="rect" coords="15,413,254,437" href="mailto:info@stegano.net">
  </map>

</div>
</body>
</html>
```

◆ Size of characters, tag options, spaces, NL...



# How to Be Affected with HICCUPS?

- ◆ **HICCUPS** =  
**H**idden **C**ommuni**C**ation system for corr**U**pted network**S**
- ◆ Original network steganographic system for shared medium networks developed at Warsaw University of Technology, Poland (since May **2002**)
- ◆ Polish patent pending P.359660 (April **2003**)
- ◆ **hiccup** (Merriam-Webster dictionary)

Variant: *also* **hiccough**

– *noun*

**1** : a spasmodic inhalation with closure of the glottis accompanied by a peculiar sound

**2** : an attack of hiccuping - usually used in plural but singular or plural in constr.

– *intransitive verb*; inflected forms: **hiccuped** *also* **hiccopped**; **hiccuping** *also* **hiccopping**

: to make a hiccup; *also* : to be affected with hiccups

# HICCUPS: Publications (1/2)

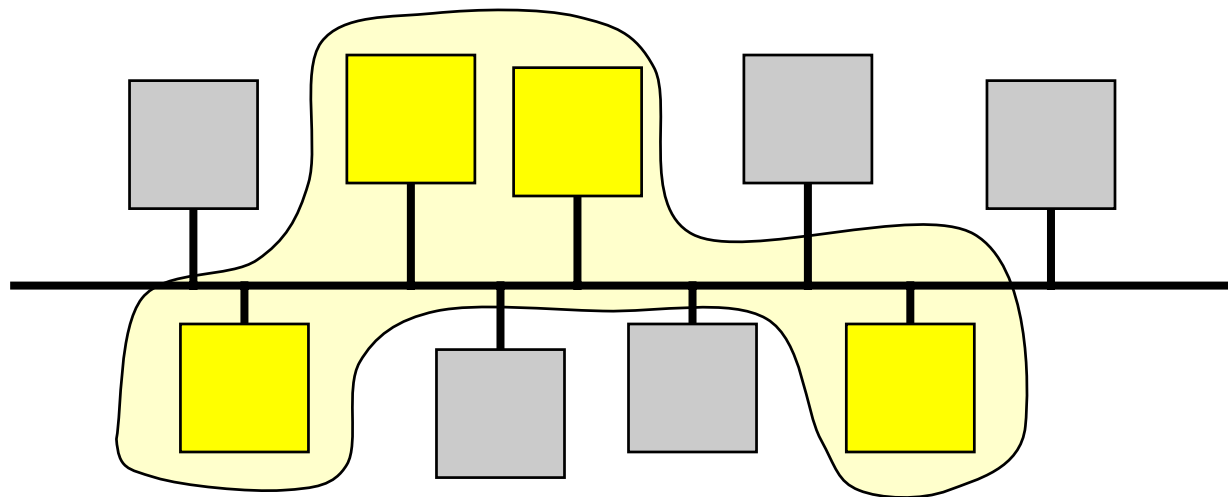
- ◆ **Polish patent application:** *Sposób steganograficznego ukrywania i przesyłania danych dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym oraz układ formowania ramek warstwy sterowania dostępem do medium* (in Polish) – P.359660. Warsaw University of Technology, **April 11, 2003**
- ◆ **Project's Website:** `stegano.net` – since **April 12, 2003**
- ◆ **Paper and presentation:** *HICCUPS – system ukrytej komunikacji dla "zepsutych" sieci* (in Polish) – Proc. of: VII Krajowa Konferencja Zastosowań Kryptografii Enigma'2003, **May 12-14 2003**, Warsaw, Poland, pp. 247-253, ISBN 83-918247-0-5
- ◆ **Paper and presentation:** *System steganograficzny dla sieci o współdzielonym medium* (in Polish) – Proc. of: Krajowe Sympozjum Telekomunikacji KST 2003, **September 10-12 2003**, Bydgoszcz, Poland, Vol. B, pp. 199-205, ISSN 1234-4699

# HICCUPS: Publications (2/2)

- ◆ **Invited talk:** *Steganografia w sieciach TCP/IP* (in Polish) – Proc. of: VI Krajowa Konferencja Bezpieczeństwa Sieciowego, **October 15-16 2003**, Warsaw, Poland
- ◆ **Paper and presentation:** *HICCUPS: Hidden Communication System for Corrupted Networks* – Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, **October 22-24, 2003** Międzyzdroje, Poland

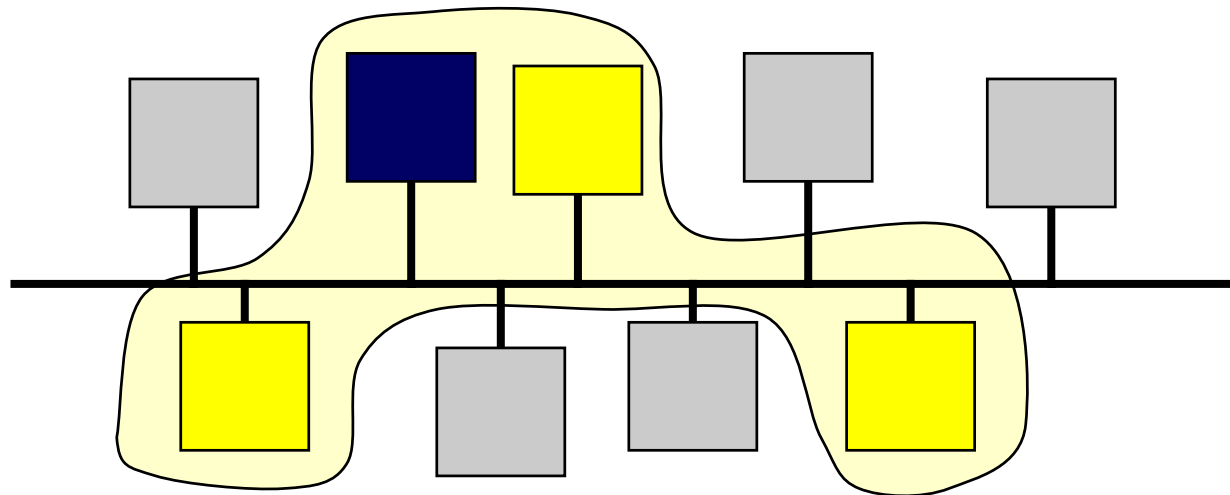
# HICCUPS Concept (1/2)

- ◆ Shared medium networks use broadcast medium (for example air) - it creates possibility of “hearing” all frames with data transmitted in medium
- ◆ **Hidden group** with common knowledge
- ◆ Basic mode for steganographic system – usage of low bandwidth hidden data channels (1% of frame size)



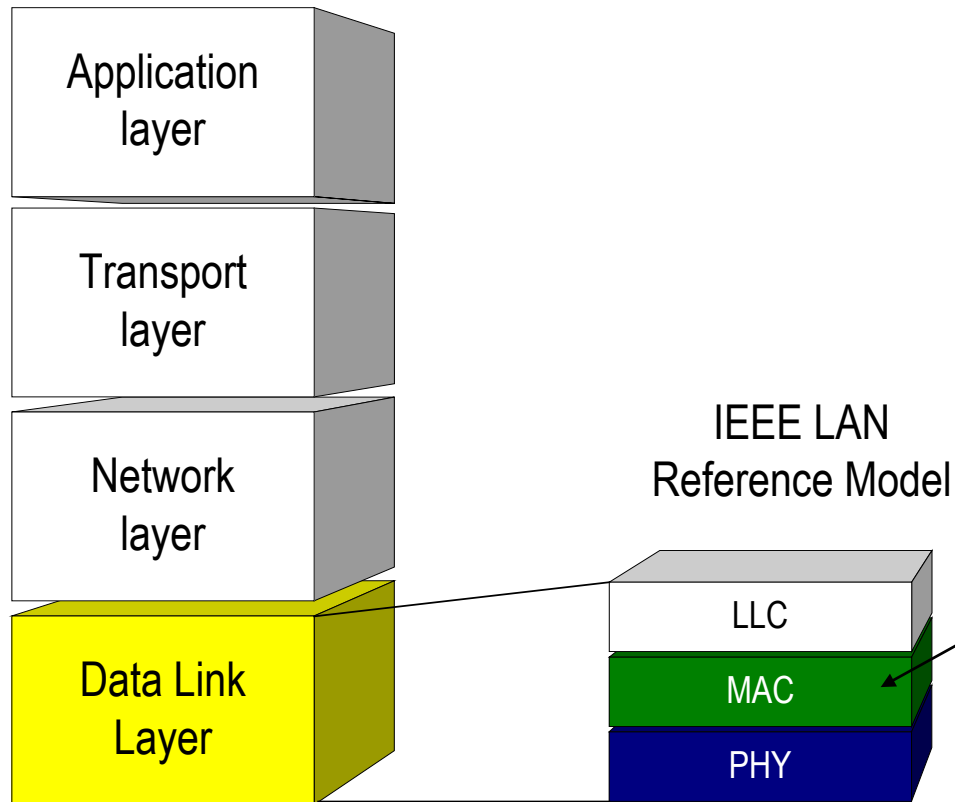
# HICCUPS Concept (2/2)

- ◆ **A station** sends corrupted (= with bad checksum) frame
- ◆ Remaining hidden stations are changing their mode of operation to the „corrupted frame mode” (high bandwidth - almost 100% of frame size) – for observers it looks like **hiccups**
- ◆ Additionally: usage of network protected by cryptographic mechanisms to have an exquisite noise



# IEEE LAN RM vs. TCP/IP Protocol Suite

TCP/IP protocol suite



MAC sublayer:  
placement of  
**HICCUPS**

Legend:

LLC - Link Layer Control

MAC - Medium Access Control

PHY - Physical Signalling

Shared medium networks

# Properties of Network Environment for HICCUPS

**P1:** shared medium network with possibility of frame's interception:

- CSMA (Carrier Sense Multiple Access) - **Aloha**
- CSMA/CD (CSMA with Collision Detection) - **Ethernet**
- CSMA/CA (CSMA with Collision Avoidance) – **WLAN IEEE 802.11**
- **Token Bus**

**P2:** publicly known method of cipher initiation for instance by initialization vectors

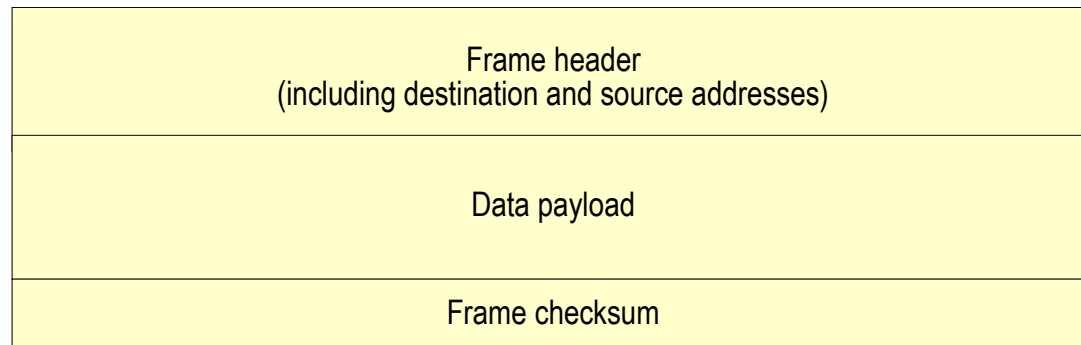
**P3:** integrity mechanisms for encrypted frames for instance one-way hash function, Cyclic Redundancy Code – CRC

(CRC is rarely strong enough for protecting integrity, but it is used in WLAN IEEE 802.11 for such purpose)

**P1** – essential, **P2** and **P3** - optional

# Hidden Data Channels

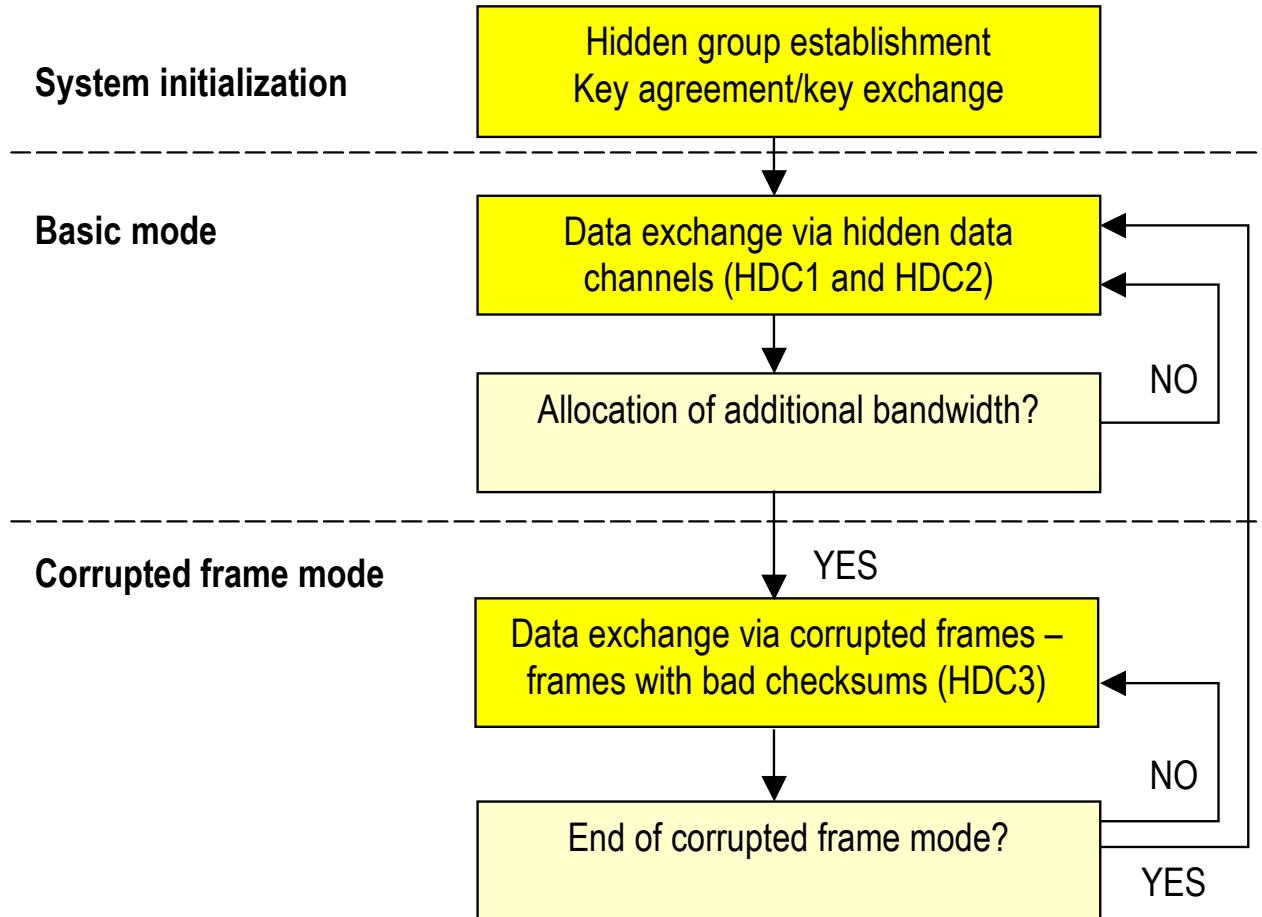
- ◆ **HDC1**: channel based on cipher's initialization vectors
- ◆ **HDC2**: channel based on MAC network addresses (for example destination and source)
- ◆ **HDC3**: channel based on integrity mechanism values (for example frame checksums)
- ◆ For network with **P1 only**: **HDC2** and **HDC3** are used



Generic MAC frame



# General HICCUPS Operation Scheme



# Functional Parts of HICCUPS

- ◆ **FP1:** network cards dedicated, for example, to IEEE 802.11b/g; network cards should have possibility to control HDC1-HDC3 and data payload in MAC frame
  - After investigations in network card market we found no interface that allows to produce frame with given CRC
  - Our work is focused on developing self-made network card or reprogramming existing software in available network cards
  - The patent application P.359660 includes a proposal of the generic network card for HICCUPS
- ◆ **FP2:** management system to control HDC1-HDC3 and data payload in MAC frame

# The Management System

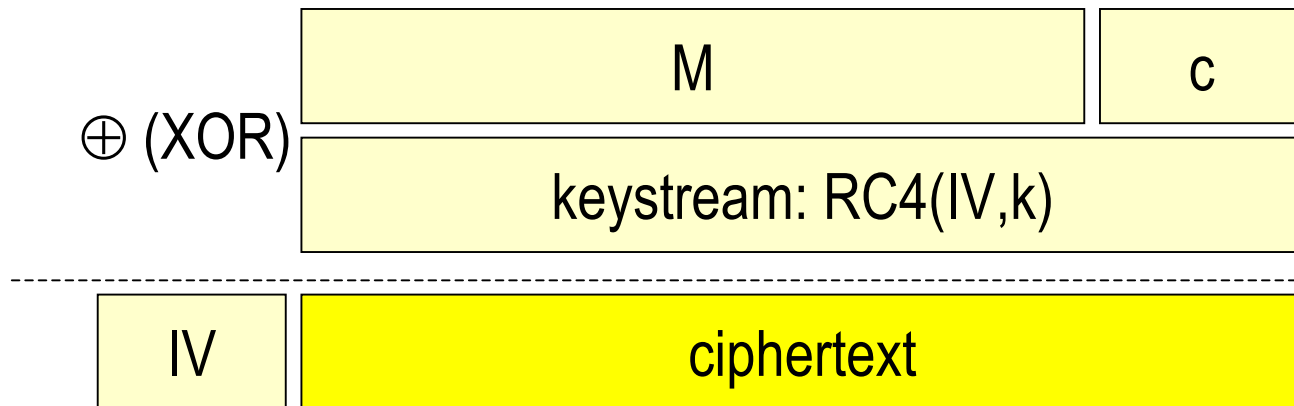
- ◆ The management system (FP2) may be produced as software or hardware and should perform such functions:
  - joining hidden group
  - leaving hidden group
  - providing interface to upper network layer to control HDC1-HDC3 and data payload in MAC frame
- ◆ with cryptographic extension:
  - key agreement/key exchange
  - key refresh
  - encryption/decryption

# Properties of WLAN Network Environment

- ◆ Mean bit error rate can range from  $10^{-3}$  to  $10^{-7}$ . Typical frame error rate (FER) for WLAN and TCP/IP protocol suite is 2-3% but mobility of station increases FER by about 30%
- ◆ **P1.WLAN:** wireless local area network with bus topology and medium access mechanism CSMA/CA
- ◆ **P2.WLAN:** publicly known method of RC4 cipher initiation by initialization vectors
- ◆ **P3.WLAN:** integrity mechanisms for encrypted frames  
– CRC-32

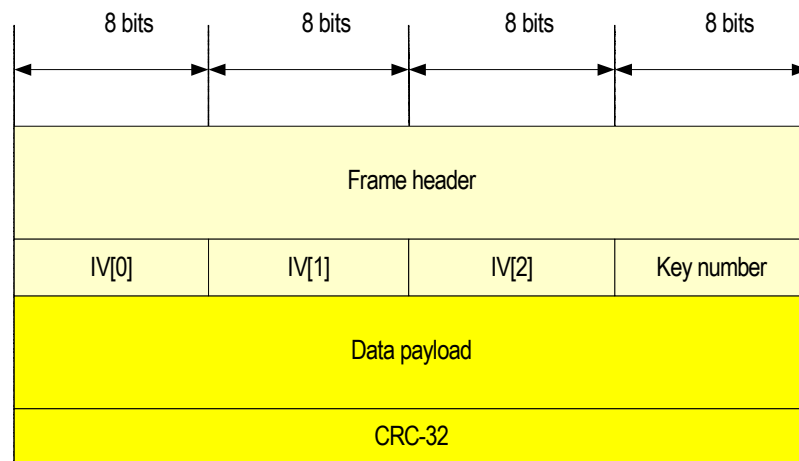
# IEEE 802.11 Wired Equivalent Privacy

- **64-bit RC4** (effective 40-bit)
- **128-bit RC4** (effective 104-bit) – vendor standard
- A sender and a receiver share secret key – **k**
- initialization vector – **IV**
- message – **M**
- **RC4(IV,k)** generates keystream
- checksum **c** performed by **CRC-32**
- manual key distribution




# Hidden Data Channels in WLAN

- ◆ **HDC1.WLAN:** channel based on RC4 initialization vectors: 24-bit
- ◆ **HDC2.WLAN:** channel based on MAC network addresses:
  - Destination Address: 48-bit
  - Source Address: 48-bit
  - Receiver Address: 48-bit
  - Transmitter Address: 48-bit
- ◆ **HDC3.WLAN:** channel based on integrity mechanism values – armed with WEP: 32-bit



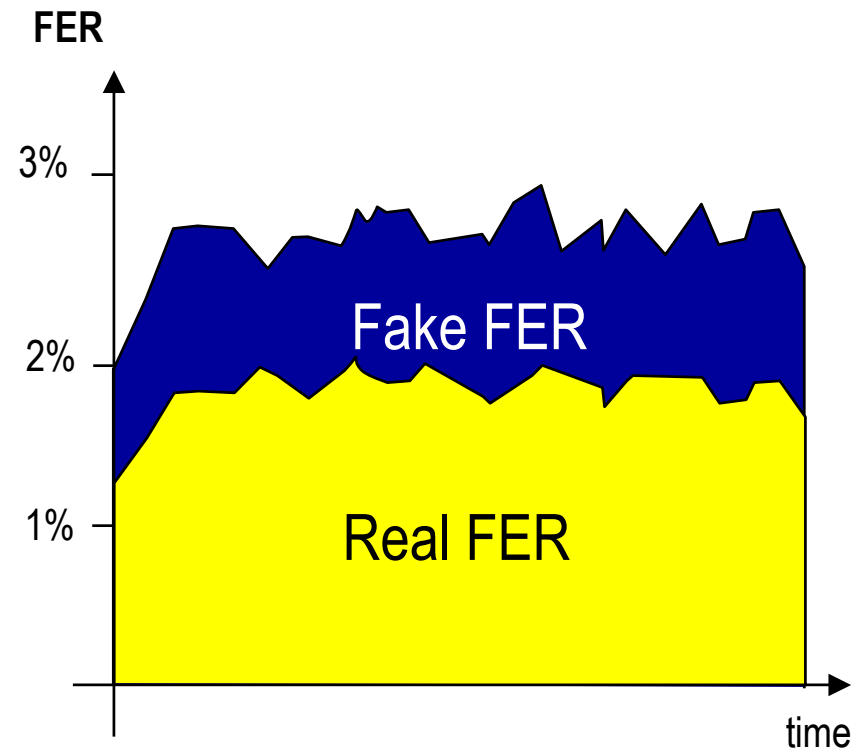
Legend:

 part of frame protected by WEP

IEEE 802.11 MAC frame armed with WEP

# „Right to Talk” System for WLAN

- ◆ All stations involved in hidden communications will be keeping frame error rate (FER) worse than it really exists
- ◆ In reality there is no way to predict FER at specific point of wireless network environment – only physical existence of station or sensor gives opportunity to measure frame error rate
- ◆ Keeping FER bad enough consists of generating corrupted packets with data useless for steganographic system



Assuming:

Real FER = 1.5% and

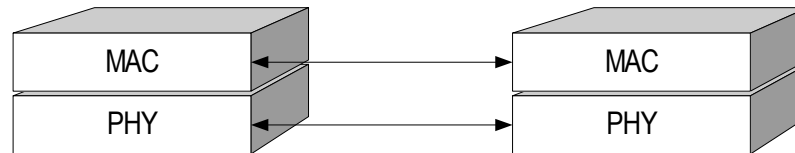
Fake FER = 2.5%

For 11 Mbit/s IEEE 802.11b network with 40% usage of bandwidth:  $11 \text{ Mbit/s} \cdot 40\% \cdot (2.5\% - 1.5\%) = 44 \text{ kbit/s}$  for steganographic system.

For 54 Mbit/s IEEE 802.11g network: 216 kbit/s.

# Future Work

- ◆ To finish the experiments with comparison of an error detection at PHY layer and MAC sublayer in WLAN



- ◆ To prepare a simulation of the system in a network simulator
- ◆ To create:
  - A prototype of a sensor to discover HICCUPS-like systems (as a support for steganalysis)
  - A prototype of the system for IEEE 802.3 networks (wired Ethernet)
  - A prototype of the system for WLAN (and Linux)
- ◆ To develop Stegano Detection System as a part of IDS



# General Conclusions

- ◆ Network steganography is a steganography in a **telecommunication container** (including protocols, codes)
- ◆ **Before 911**: how to construct?
- ◆ **After 911**: as above + how to fight? how to discover? But if there is no way to discover: how to eliminate?
- ◆ **Impossible mission**
- ◆ **Intrusion Detection Systems** will be developed to reveal network steganography
- ◆ **Warning** for business: a new (?) way of information leakage



<http://remember.worldatwar.org/main.mhtml/images/photography>

# HICCUPS: Conclusions

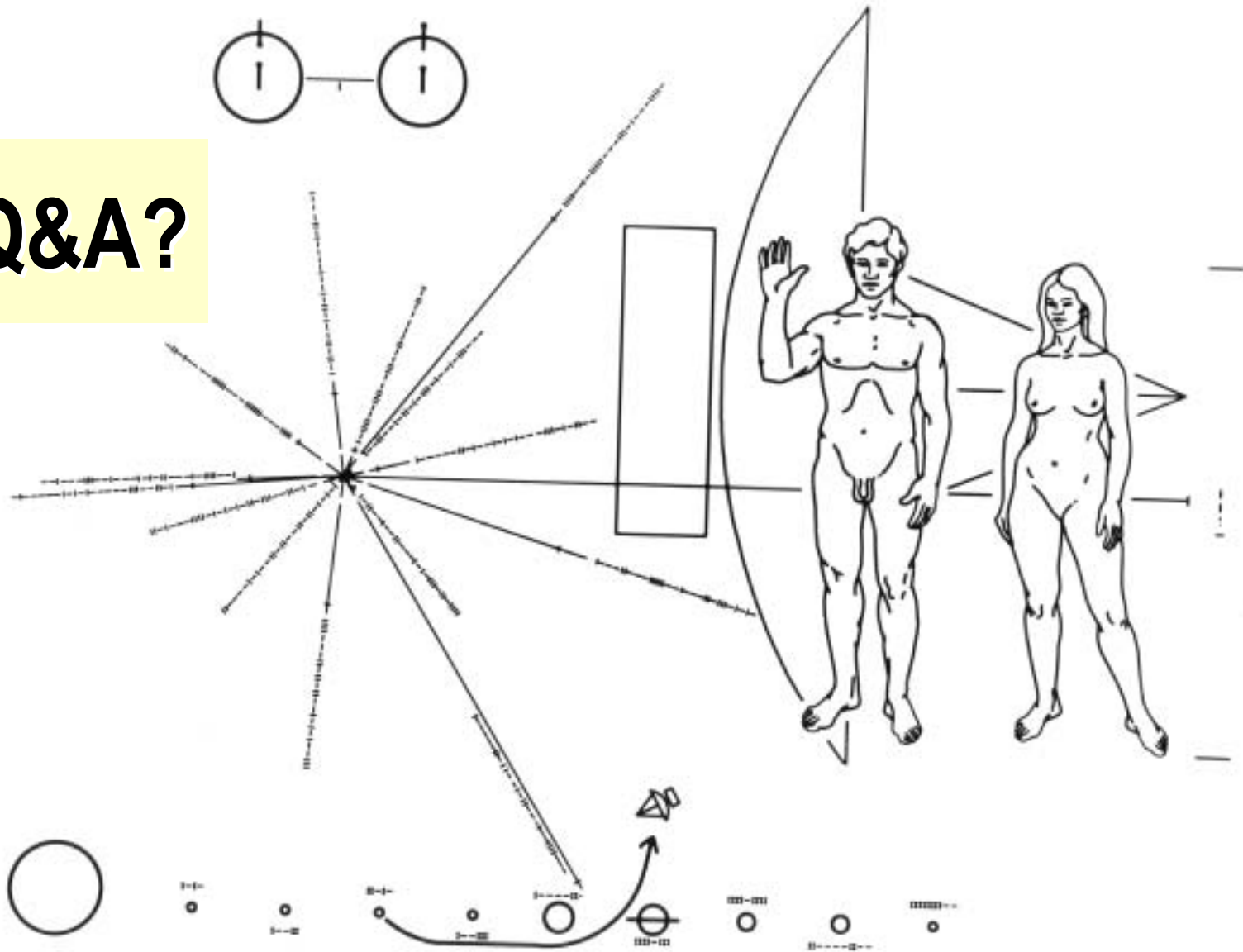
- ◆ HICCUPS is a **new network steganographic system** dedicated to shared medium networks especially to WLAN
- ◆ Main novelty of the system is **usage of frames with bad checksums** as a method of creating additional on-demand bandwidth for steganographic purposes
- ◆ **Elastic on-demand bandwidth**: kilobits-per-second (not several bits-per-second)
- ◆ System can be applied to many of the existing **wireless public networks** (including sensor networks)

# Credits

- ◆ Prof. Józef Lubacz
- ◆ Krzysztof Brzeziński, PhD
- ◆ Ryszard Kossowski, PhD
- ◆ Sławomir Kukliński, PhD
- ◆ Roman Dygnarowicz, MSc (Polish DoD)
- ◆ Piotr Szafran, MSc student
- ◆ Igor Margasiński, PhD student
- ◆ Aneta Zwierko, PhD student
- ◆ 9 anonymous reviewers



**Q&A?**



**Krzysztof Szczypiorski**  
e-mail: [ksz@stegano.net](mailto:ksz@stegano.net)  
<http://stegano.net>

# References 1/2

1. Ahsan K., Kundur D.: Practical Data Hiding in TCP/IP. In: Proceedings of Workshop on Multimedia Security at ACM Multimedia '02, Juan-les-Pins (on the French Riviera), December 2002
2. Anderson, R. (Ed.): Proceedings of: Information Hiding – First International Workshop, Cambridge, U.K., May 30 – June 1, 1996, vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc.
3. Aucsmith, D. (Ed.): Proceedings of: Information Hiding – Second International Workshop, IH'98, Portland, Oregon, USA, April 14-17, 1998, vol. 1525 of Lecture Notes in Computer Science, Springer-Verlag Inc.
4. Boyer L.: Firewall Bypass via Protocol Steganography – [http://www.networkpenetration.com/protocol\\_steg.html](http://www.networkpenetration.com/protocol_steg.html)
5. Chmielewski A.: Utilization of Transmission Code Redundancy for Additional Data Stream. Ph.D. dissertation (in Polish), Warsaw University of Technology, 1988
6. Fisk G., Fisk M., Papadopoulos C., Neil J.: Eliminating Steganography in Internet Traffic with Active Wardens. In: [13], pp. 29-46.
7. Fluhrer S., Mantin I., Shamir A.: Weaknesses in the Key Scheduling Algorithm of RC4. In Proceedings of SAC 2001, Eighth Annual Workshop on Selected Areas in Cryptography (Toronto, Ontario, Canada, August 2001), pp. 1-24

# References 2/2

8. Handel T. and Sandford M.: Hiding Data in the OSI Network Model. In: [2], pp. 23–38
9. Mironov I.: (Not So) Random Shuffles of RC4. In: Proceedings of: CRYPTO 2002, 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002, pp. 304-319, vol. 2442 of Lecture Notes in Computer Science, Springer-Verlag Inc.
10. Moskowitz, I. S. (Ed.): Proceedings of: Information Hiding – 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001, vol. 2137 of Lecture Notes in Computer Science, Springer-Verlag Inc.
11. Petitcolas, F. A. P. (Ed.): Proceedings of: Information Hiding – 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7-9, 2002, vol. 2578 of Lecture Notes in Computer Science, Springer-Verlag Inc.
12. Pfitzmann, A. (Ed.): Proceedings of: Information Hiding – Third International Workshop, IH'99, Dresden, Germany, September 29 – October 1, 1999, vol. 1768 of Lecture Notes in Computer Science, Springer-Verlag Inc.
13. Rowland C. H.: Covert Channels in the TCP/IP Protocol Suite. Psionics Technologies, November 14, 1996
14. Xylomenos G., Polyzos G.C., Mahonen P. and Saaranen M.: TCP Performance Issues over Wireless Links. IEEE Communications Magazine, April 2001