Steganografia w sieciach TCP/IP

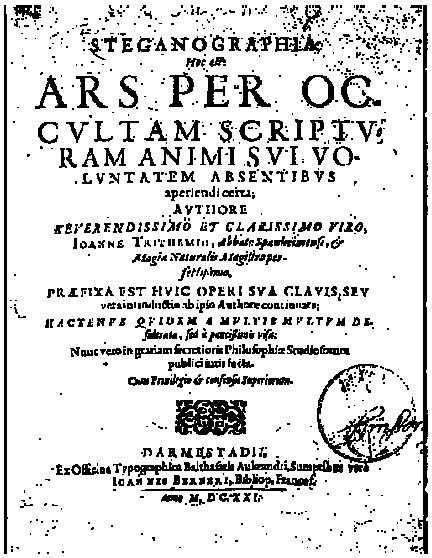
Krzysztof Szczypiorski
Instytut Telekomunikacji PW
`ksz@stegano.net`
`http://stegano.net`

VI Krajowa Konferencja Bezpieczeństwa Sieciowego
Warszawa, 15-16 października 2003

Problemy (czyli plan referatu)

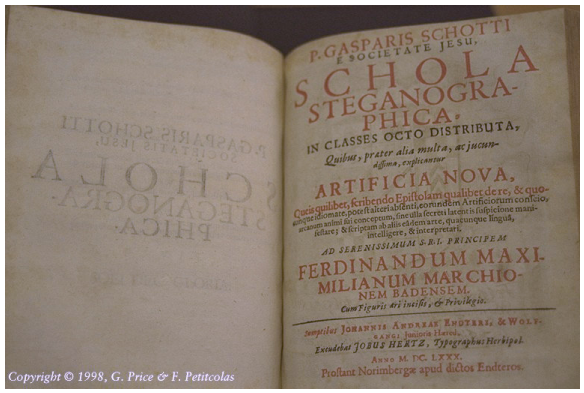
- Historia steganografii i jej wpływ na teraźniejszość
- Współczesna steganografia, a ukrywanie informacji „w zawartości" przesyłanej w sieciach
- Ryzyko związane z użyciem steganografii
- Stegano* kontra krypto*
- Nowa (?) gałąź w dziedzinie: steganografia sieciowa
- **Znane** przykłady steganografii sieciowej dla stosu protokołów TCP/IP

Historia steganografii i jej wpływ na teraźniejszość


STEGANOGRAPHIA,
Hoc eſt:
ARS PER OC-
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &
Magiæ Naturalis Magiſtrapo-
liſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
ratio intuitiua ab ipſo Authore conſcripta;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à paucissimis viſa:
Nunc verò in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
DARMSTADII,
Ex Officina Typographica Balthaſaris Aulenndi, Sumptibus vero
IOANNIS BERNERI, Bibliopolæ Francof.
Anno M. DC. XXI.

Johannes Trithemius, Steganographia, 1499

Gaspari Schotti, Schola steganographica, 1665

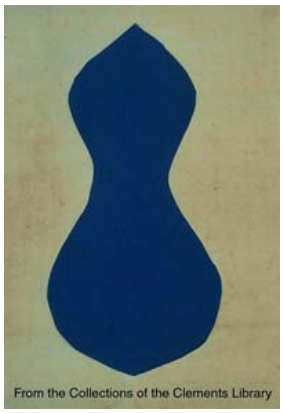

P. GASPARIS SCHOTTI
E SOCIETATE JESU,
SCHOLA
STEGANOGRA-
PHICA,
IN CLASSES OCTO DISTRIBUTA,
Quibus, præter alia multa, ac jucun-
diſſima, explicantur
ARTIFICIA NOVA,
Cuicuis quilibet, ſeribendo Epiſtolam qualibet de re, & quo-
cunque idiomate, poſſit abſenti, eamdem Artificiorum conſcio,
arcanum mittat ſui conceptum, ſine ulla ſecreti iacturâ ſubſidione mani-
feſtare, & ſcripturn ab alio eadem arte, quæcunque lingua,
intelligere, & interpretari.
AD SERENISSIMUM S.R.I. PRINCIPEM
FERDINANDUM MAXI-
MILIANUM MARCHIO-
NEM BADENSEM.
Cum Figuris æri inciſis, & Privilegio.
Sumptibus JOHANNIS ANDREAE ENDTERI, & WOLF-
GANGI, Junioris Hæredum.
Excudebat JOSUA HERTZ, Typographus Herbipol.
Anno M. DC. LXXV.
Proſtant Norimbergæ apud dictos Endteros.
Copyright © 1998, G. Price & F. Petitcolas

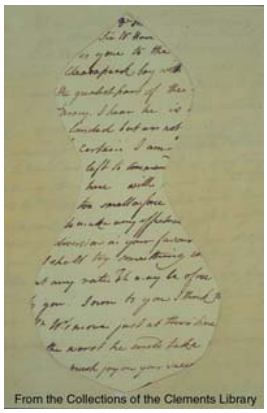
↑ http://www.petitcolas.net/fabien/steganography/steganographica/schola-steganographica-1.html
←http://www.esotericarchives.com/tritheim/stegano.htm

z greckiego steganos (ukryty)

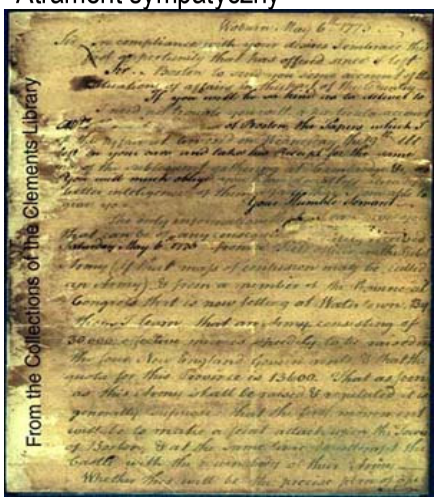
Historia steganografii... (cd)

Maskowanie

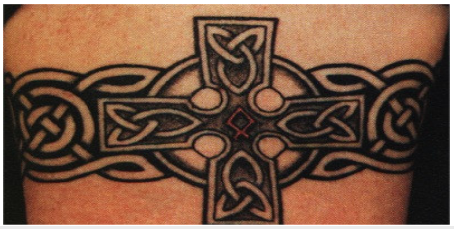

From the Collections of the Clements Library


From the Collections of the Clements Library

Atrament sympatyczny


From the Collections of the Clements Library

Tatuaż

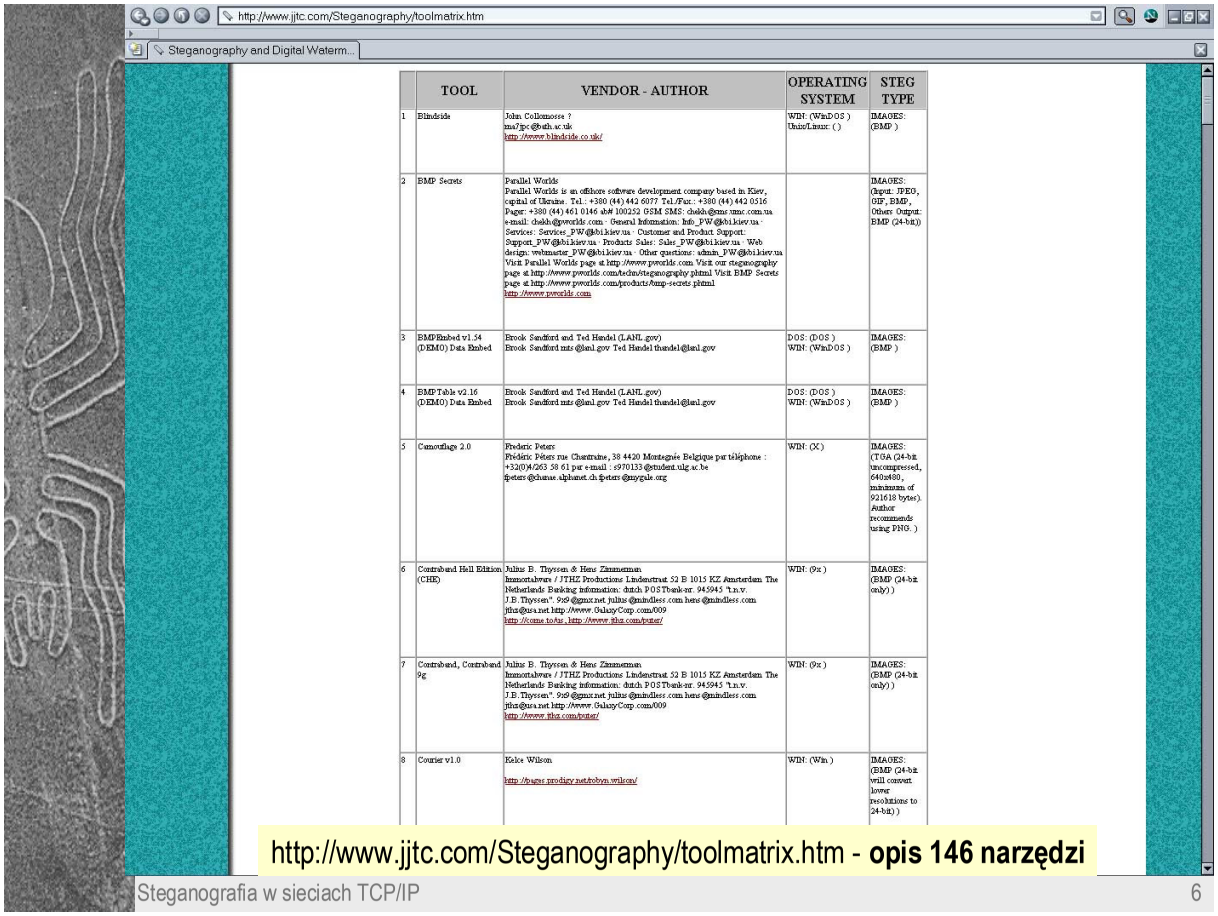


↑ http://www.si.umich.edu/spies/methods-ink.html
↖ http://www.si.umich.edu/spies/methods-mask.html
← http://www.miki.hg.pl/tatoo%20maly/Image72.jpg

Steganografia „zanurzona w zawartości”

- multimedia
  - obraz nieruchomy
  - film
  - dźwięk
- watermarking

Rysunek „krążacy” w Internecie w kwietniu 2003:
http://www.michaelpang.com/upload/newupload/image001.jpg



	TOOL	VENDOR - AUTHOR	OPERATING SYSTEM	STEG TYPE
1	Blindside	John Collomosse ? ms7jpc@ath.ac.uk http://www.blindside.co.uk/	WIN: (WinDOS) Unix/Linux: ( )	IMAGES: (BMP)
2	BMP Secrets	Parallel Worlds Parallel Worlds is an offshore software development company based in Kiev, capital of Ukraine. Tel.: +380 (44) 442 6077 Tel./Fax.: +380 (44) 442 0516 Pager: +380 (44) 461 0146 ab# 100252 GSM SMS: chekh@gmc.xmc.com.ua e-mail: chekh@pworlds.com · General Information: Info_PW@kbi.kiev.ua · Services: Service_PW@kbi.kiev.ua · Customer and Product Support: Support_PW@kbi.kiev.ua · Products Sales: Sales_PW@kbi.kiev.ua · Web design: webmaster_PW@kbi.kiev.ua · Other questions: admin_PW@kbi.kiev.ua Visit Parallel Worlds page at http://www.pworlds.com Visit our steganography page at http://www.pworlds.com/techn/steganography.phtml Visit BMP Secrets page at http://www.pworlds.com/products/bmp-secrets.phtml http://www.pworlds.com		IMAGES: (Input: JPEG, GIF, BMP, Others Output: BMP (24-bit))
3	BMPEmbed v1.54 (DEMO) Data Embed	Brock Sandford and Ted Handel (LANL.gov) Brock Sandford mts@lanl.gov Ted Handel thandel@lanl.gov	DOS: (DOS) WIN: (WinDOS)	IMAGES: (BMP)
4	BMPTable v2.16 (DEMO) Data Embed	Brock Sandford and Ted Handel (LANL.gov) Brock Sandford mts@lanl.gov Ted Handel thandel@lanl.gov	DOS: (DOS) WIN: (WinDOS)	IMAGES: (BMP)
5	Camouflage 2.0	Frederic Peters Frédéric Péters rue Chestraine, 38 4420 Montegnée Belgique par téléphone : +32(0)4/263 58 61 par e-mail : s970133@student.ulg.ac.be fpeters@chanas.alphanet.ch fpeters@mygale.org	WIN: (X)	IMAGES: (T16A (24-bit uncompressed, 640x480, minimum of 921618 bytes). Author recommends using PNG.)
6	Contraband Hell Edition (CHE)	Julius B. Thyssen & Henz Zimmerman Immortalwave / JTHZ Productions Lindenstraat 52 B 1015 KZ Amsterdam The Netherlands Banking information: dutch POSTbank-nr. 945945 "t.n.v. J.B. Thyssen". 9x9@gmx.net julius@mindless.com henz@mindless.com jthz@sa.net http://www.GalaxyCorp.com/009 http://crime.to/ha...http://www.jthz.com/hyster/	WIN: (9x)	IMAGES: (BMP (24-bit only))
7	Contraband, Contraband 9g	Julius B. Thyssen & Henz Zimmerman Immortalwave / JTHZ Productions Lindenstraat 52 B 1015 KZ Amsterdam The Netherlands Banking information: dutch POSTbank-nr. 945945 "t.n.v. J.B. Thyssen". 9x9@gmx.net julius@mindless.com henz@mindless.com jthz@sa.net http://www.GalaxyCorp.com/009 http://www.jthz.com/hyster/	WIN: (9x)	IMAGES: (BMP (24-bit only))
8	Courier v1.0	Kelce Wilson http://pages.prodigy.net/robyn.wilson/	WIN: (Win)	IMAGES: (BMP (24-bit will convert lower resolutions to 24-bit))

http://www.jjtc.com/Steganography/toolmatrix.htm - **opis 146 narzędzi**

Ryzyko związane z użyciem steganografii

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

http://www.fbi.gov/mostwant/topten/fugitives/laden.htm

FBI Ten Most Wanted Fugitive - Us...

FBI TEN MOST WANTED FUGITIVE

MURDER OF U.S. NATIONALS OUTSIDE THE UNITED STATES; CONSPIRACY TO MURDER U.S. NATIONALS OUTSIDE THE UNITED STATES; ATTACK ON A FEDERAL FACILITY RESULTING IN DEATH

USAMA BIN LADEN

Date of Photograph Unknown

Aliases: Usama Bin Muhammad Bin Ladin, Shaykh Usama Bin Ladin, the Prince, the Emir, Abu Abdallah, Mujahid Shaykh, Hajj, the Director

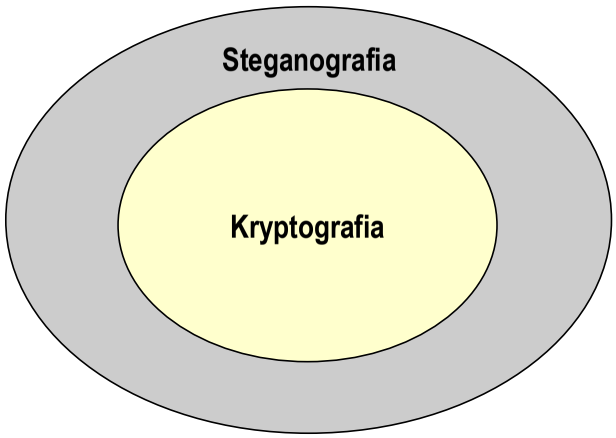
DESCRIPTION

Date of Birth:	1957	**Hair:**	Brown
Place of Birth:	Saudi Arabia	**Eyes:**	Brown
Height:	6' 4" to 6' 6"	**Complexion:**	Olive
Weight:	Approximately 160 pounds	**Sex:**	Male
Build:	Thin	**Nationality:**	Saudi Arabian
Occupation:	Unknown		
Remarks:	Bin Laden is the leader of a terrorist organization known as Al-Qaeda, "The Base". He is left-handed and walks with a cane.		
Scars and Marks:	None		

CAUTION

USAMA BIN LADEN IS WANTED IN CONNECTION WITH THE AUGUST 7, 1998, BOMBINGS OF THE UNITED STATES EMBASSIES IN DAR ES SALAAM, TANZANIA, AND NAIROBI, KENYA. THESE ATTACKS KILLED OVER 200 PEOPLE. IN ADDITION, BIN LADEN IS A SUSPECT IN OTHER TERRORIST ATTACKS THROUGHOUT THE WORLD.

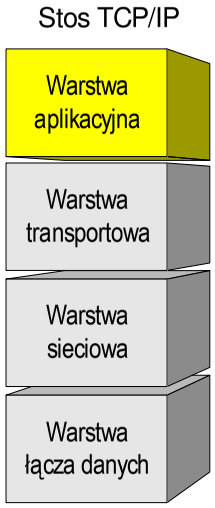
Stegano* kontra krypto*



- Steganografia a kryptografia
- Steganoanaliza a kryptoanaliza

Nowa (?) dziedzina:
Network (protocol) steganography=

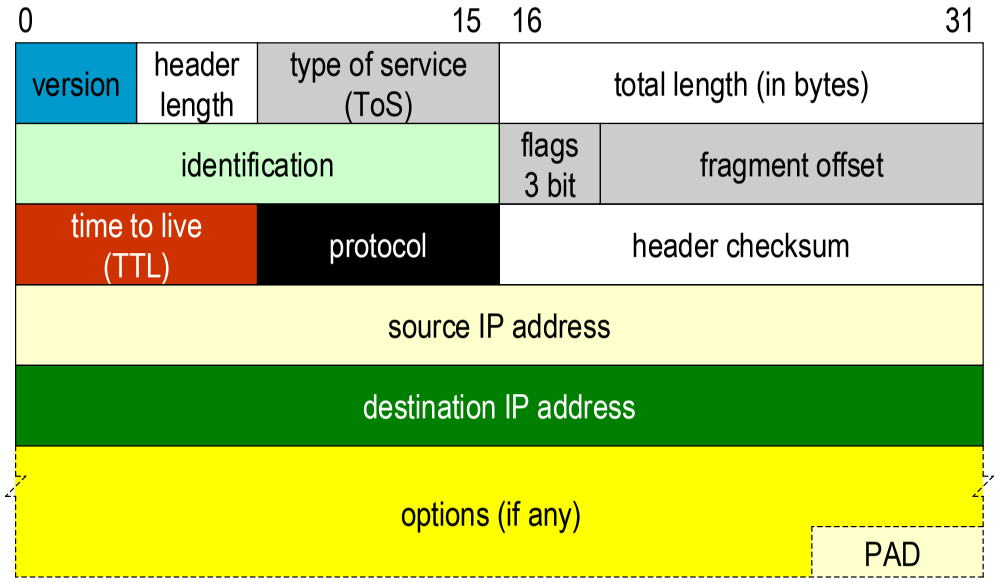
Steganografia sieciowa



„Zawartość”

Rozproszony „kontener”

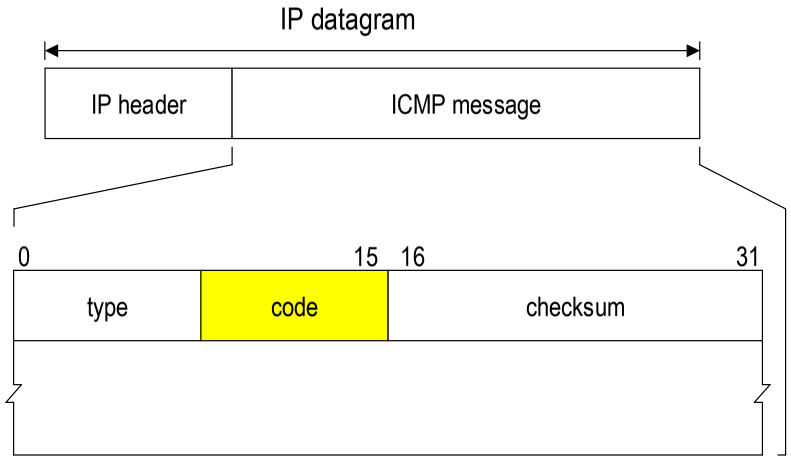
Nagłówek IP – możliwe ukryte kanały



Nagłówek IP – możliwe … (cd)

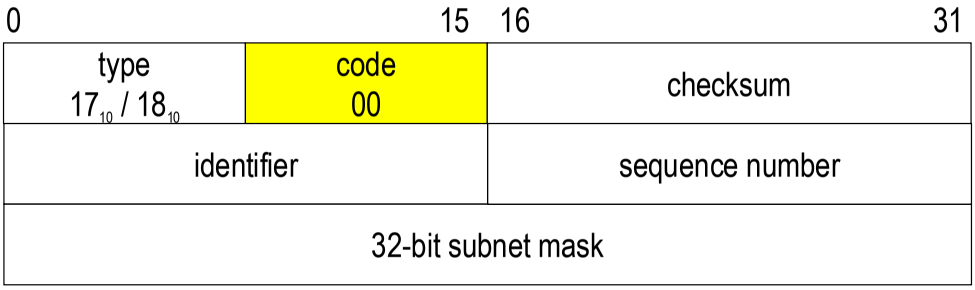
- PAD (padding bits) – pasmo 31 bitów/pakiet
- IP identification – 16 bitów/pakiet
- Fałszywy adres nadawcy – 32 bity/pakiet
- Użycie adresu przeznaczenia jako flagi – 8 bitów/pakiet
- Użycie niekoniecznych pól (ToS, options, flagi np. Don‘t Fragment - DF dla fragmentu pakietu) – różne pasmo

Wiadomość ICMP – możliwe ukryte kanały



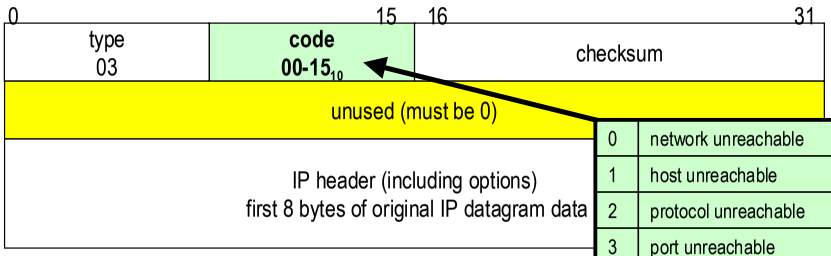
- Użycie pola code, gdy wysyłany jest jedynie type (np. ICMP Address Mask Query ⟶) – 8 bitów/pakiet
- Użycie opcjonalnych pól, lub pól które powinny mieć konkretną wartość (np. ICMP Destination Unreachable ⟶)

ICMP Address Mask Query



17 – Request; 18 - Reply

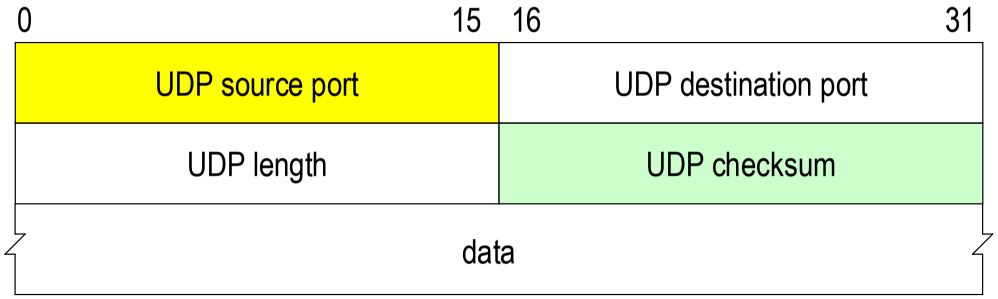
ICMP „Destination Unreachable”



0	network unreachable
1	host unreachable
2	protocol unreachable
3	port unreachable
4	fragmentation needed but don't fragment bit set
5	source route failed
6	destination network unknown
7	destination host unknown
9	destination network administratively prohibited
10	destination host administratively prohibited
11	network unreachable for ToS
12	host unreachable for ToS
13	communication administratively prohibited by filtering
14	host precedence violation
15	precedence cutoff in effect

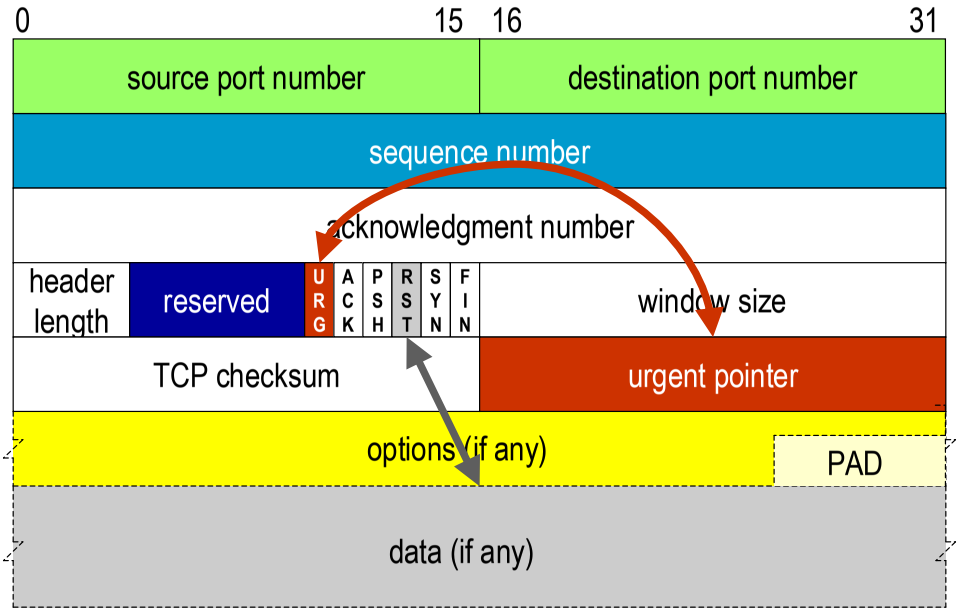
Podobnie:
ICMP Time exceeded,
ale pole code przyjmuje tylko dwie wartości
- 0 - Time-To-Live count exceeded
- 1 - Fragment reassembly time exceeded

Nagłówek UDP – możliwe ukryte kanały



- UDP source port i UDP checksum – opcjonalne

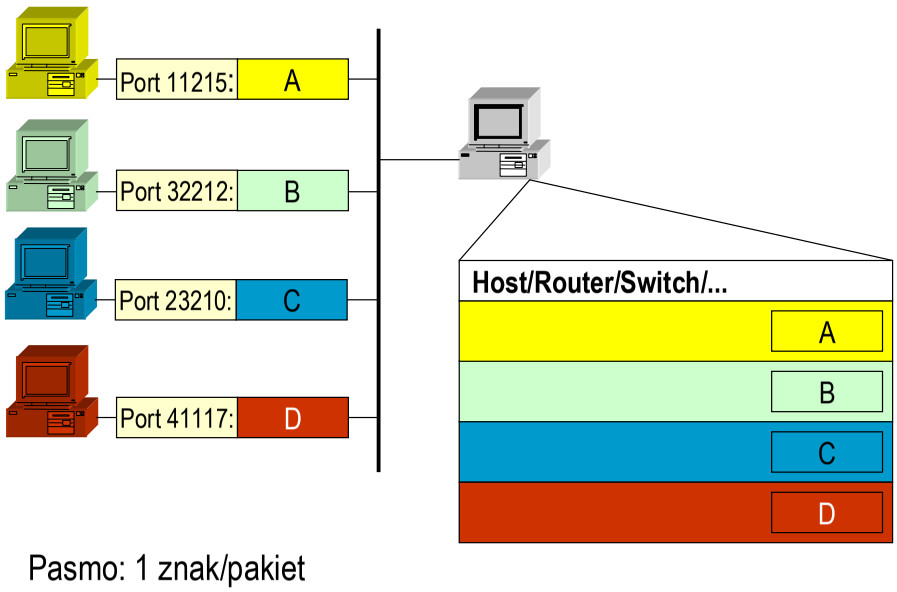
Nagłówek TCP – możliwe ukryte kanały



Nagłówek TCP – możliwe… (cd)

- PAD (padding bits) – pasmo 31 bitów/pakiet
- Użycie inicjującego numeru sekwencyjnego – 32 bity na połączenie
- Użycie pola urgent pointer, gdy URG=0 – 16 bitów/na pakiet
- Użycie bitów zarezerwowanych – 6 bitów/pakiet
- Użycie pola danych, gdy RST=1
- Użycie pola z numerami portów (→)

„Алфавит мы уже знаем, Уже пишем и читаем…”



Pasmo: 1 znak/pakiet

Manipulacja 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: Wed, 15 Oct 2003 10:12:59 GMT
Content-Type: text/html
Content-Length: 903
Expires: Wed, 15 Oct 2003 10:12:59 GMT
X-Squid-Error: ERR_INVALID_REQ 0
X-Cache: MISS from w3cache.pw.edu.pl
Proxy-Connection: close
...
```


Manipulacja HTML, XML...

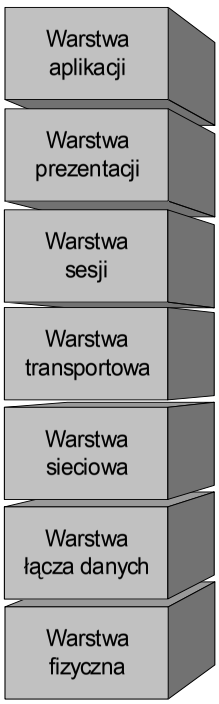
```
<html>
<head>
<title>:::: s t e g a n o . n e t ::::</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
</head>

<body bgcolor="#CCCCCC" text="#CCCCCC" link="#CCCCCC" vlink="#CCCCCC"
alink="#CCCCCC">
<div align="center"><br>
  <img src="stegano.jpg" width="662" height="442" usemap="#Map_1" border="0">
<br>
  <map name="Map_1">
    <area shape="rect" coords="15,413,254,437" href="mailto:info@stegano.net">
  </map>

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

- wielkość liter, opcje tagów, spacje, znaki nowej linii...

„Ukrywanie danych w modelu OSI”

- Handel T. I Sandford M.: **Hiding Data in the OSI Network Model.** w: 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, str. 23–38
- Weapon Design Technology Group – Los Alamos National Laboratory
- Najważniejsza (bo pierwsza) pozycja literatury w tej dziedzinie
- Opis 9 metod ukrywania danych dla każdej z 7 warstw modelu OSI (→)

„Ukrywanie danych…” (cd)



9. Manipulacja słownikami

8. Zanurzanie danych w multimediach

7. Wybór plików na dysku sieciowym jako ukryty kanał

6. Użycie pola Reserved w TCP

5. ToS w IP
4. ICMP

3. Dodawanie ukrytych danych do ramki, której rozmiar jest mniejszy od maksymalnego.

2. Manipulacja komunikacją szeregową (CTS/RTS)
1. Manipulacja mechanizmem kolizji w sieciach CSMA/CD (Ethernet)

„Ukryte kanały w stosie TCP/IP”

- Rowland C. H.: **Covert Channels in the TCP/IP Protocol Suite**. Psionics Technologies, November 14, **1996**
- http://www.firstmonday.dk/issues/issue2_5/rowland/
- narzędzie Covert-TCP
- Trzy metody
  - manipulacja polem IP Identification
  - pole Initial Sequence Number (ISN)
  - TCP Acknowledge Sequence Number "Bounce"

„Praktyczne ukrywanie danych w TCP/IP”

- Ahsan K., Kundur D.: **Practical Data Hiding in TCP/IP**. W: Proceedings of Workshop on Multimedia Security at ACM Multimedia '02, Juan-les-Pins (on the French Riviera), December **2002**
- http://ee.tamu.edu/~deepa/pdf/acm02.pdf
- Techniki bazujące na strategii fragmentyzacji pakietów i polu IP identyfikującym protokół

„HICCUPS - system ukrytej komunikacji dla zepsutych sieci”

- Szczypiorski K.: HICCUPS: **Hidden Communication System for Corrupted Networks.** The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, October 22-24, **2003**
- http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf
- System dla sieci o współdzielonym medium, w szczególności sieci bezprzewodowych WLAN 802.11, wykorzystujący „zepsute” ramki podwarstwy MAC

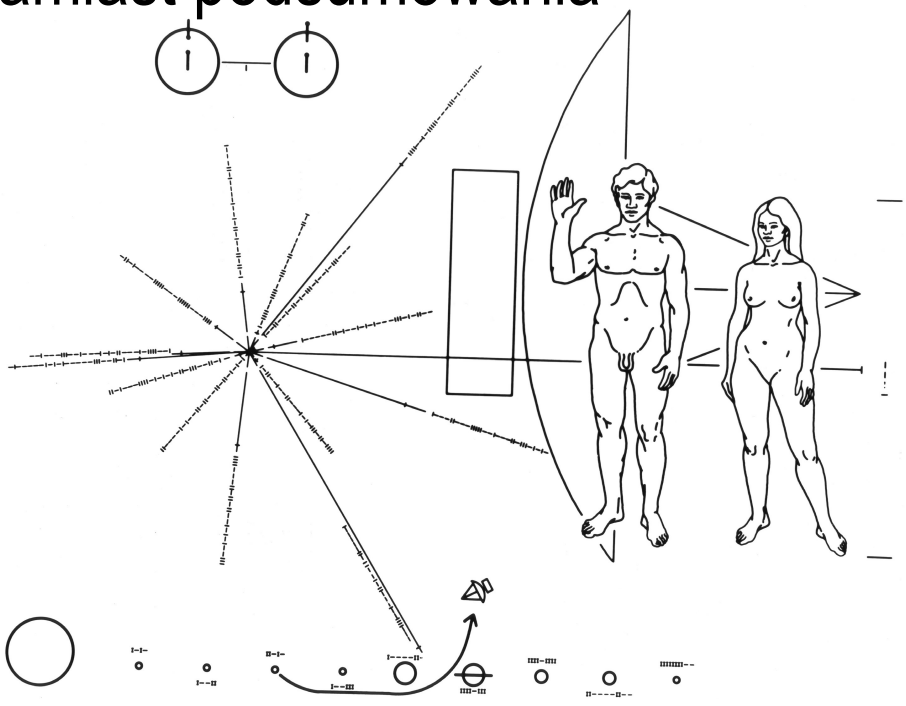
„Eliminowanie steganografii...”

- Fisk G., Fisk M., Papadopoulos C., Neil J.: **Eliminating Steganography in Internet Traffic with Active Wardens.** w: 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., str. 29-46
- http://public.lanl.gov/mfisk/papers/ih02.pdf
- Koncepcja silnej kontroli semantycznej nagłówków sieciowych

Wybrane „projekty hackerskie”

- **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

Zamiast podsumowania



http://grin.hq.nasa.gov/IMAGES/LARGE/GPN-2000-001623.jpg

Koniec

Krzysztof Szczypiorski
Instytut Telekomunikacji PW
`ksz@stegano.net`
`http://stegano.net`