Nowe metody steganografii w sieciach

Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski
Instytut Telekomunikacji PW

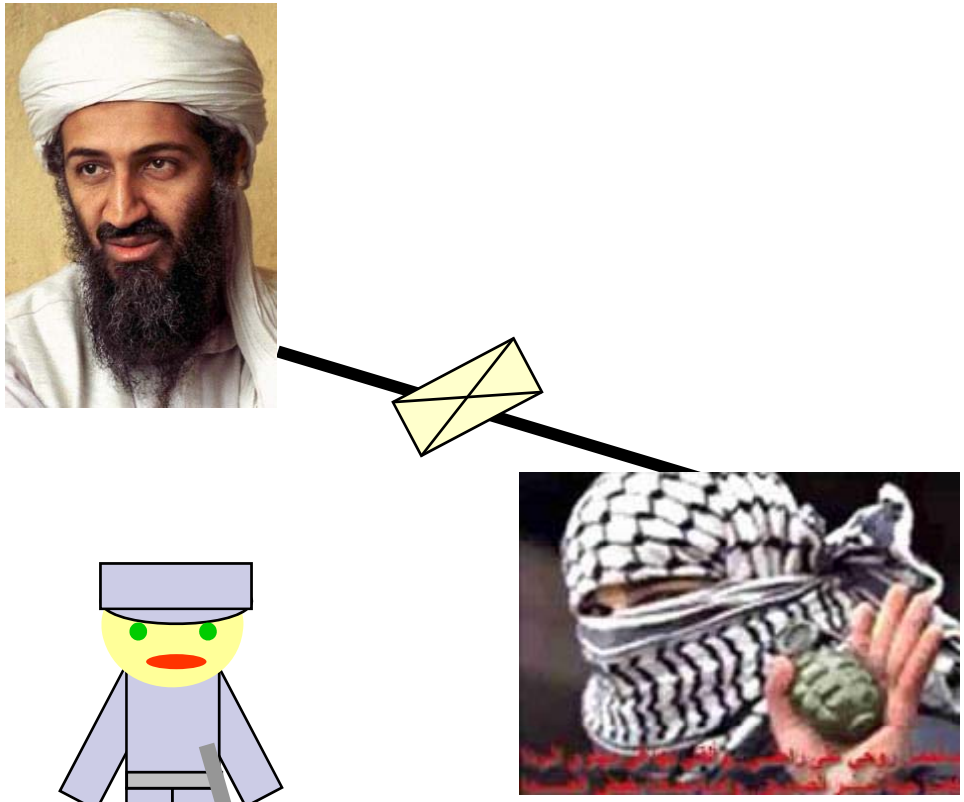
Sekcja Telekomunikacji KEiT PAN
Bydgoszcz, 11 września 2008

Plan prezentacji

- Idea i historia steganografii
- Steganografia współczesna w tym steganografia sieciowa
- Protokoły VoIP
- Klasyfikacja metod steganograficznych w VoIP oraz przykłady rozwiązań
- Zasada działania i cechy nowej metody LACK

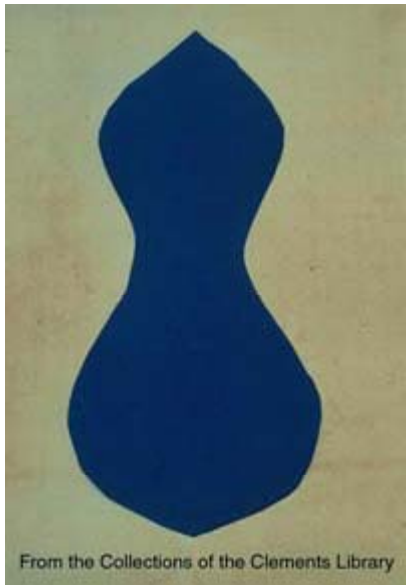
Idea steganografii

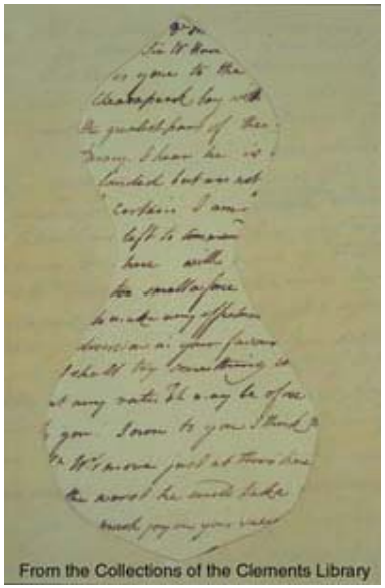
- *Στεγανογραφία* – dosłownie: osłonięte, zakryte pisanie
- Techniki **ukrywania** jednych informacji w drugich
- Przykład: ukryta komunikacja pomiędzy terrorystami



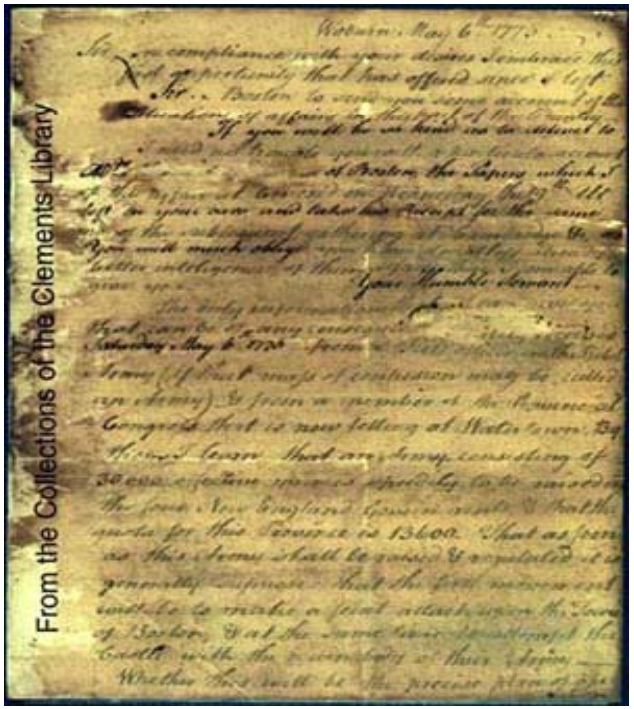
Steganogramy – historia

Maskowanie (przykładanie szablonów)





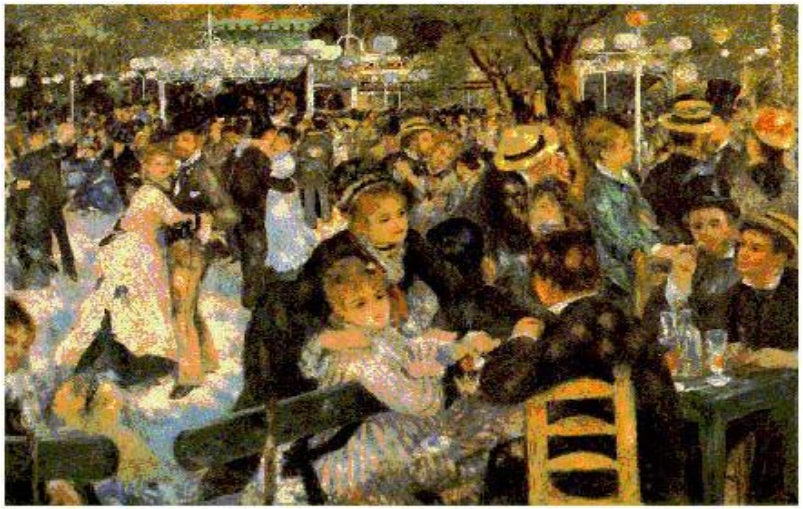
Atrament sympatyczny



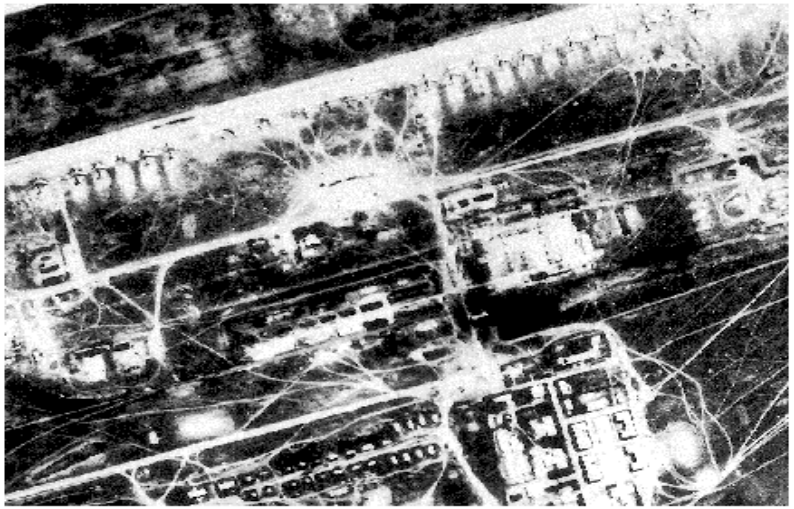
Tatuaże

↑ 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

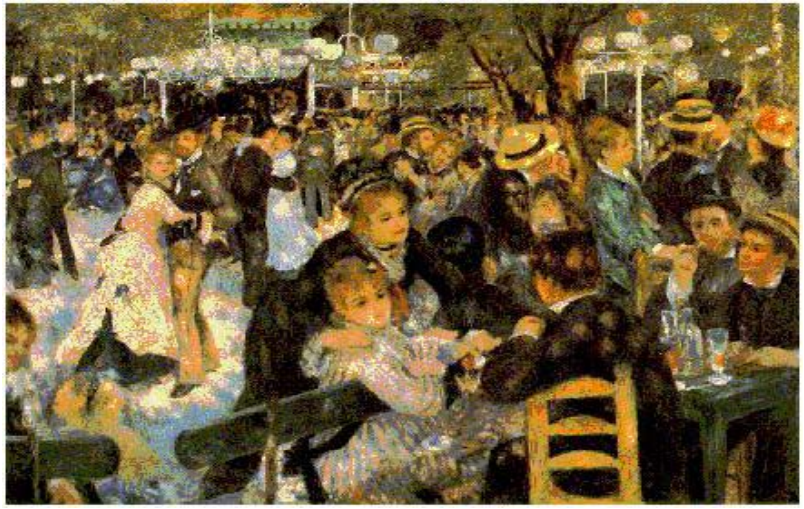
Steganografia współczesna



+



=



Główne nośniki ukrytych informacji: obrazy, dźwięk i tekst

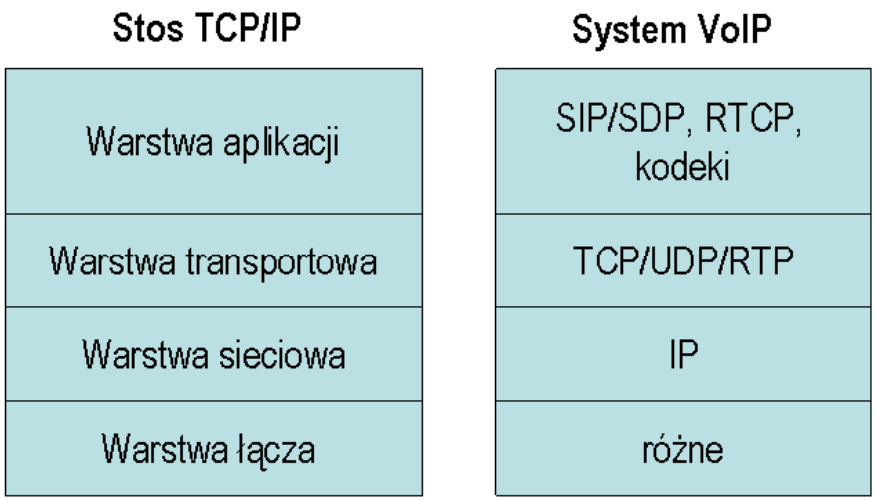
Neil F. Johnson, Sushil Jajodia: *Exploring Steganography: Seeing the Unseen* - http://www.jjtc.com/pub/r2026.pdf

Steganografia **sieciowa**

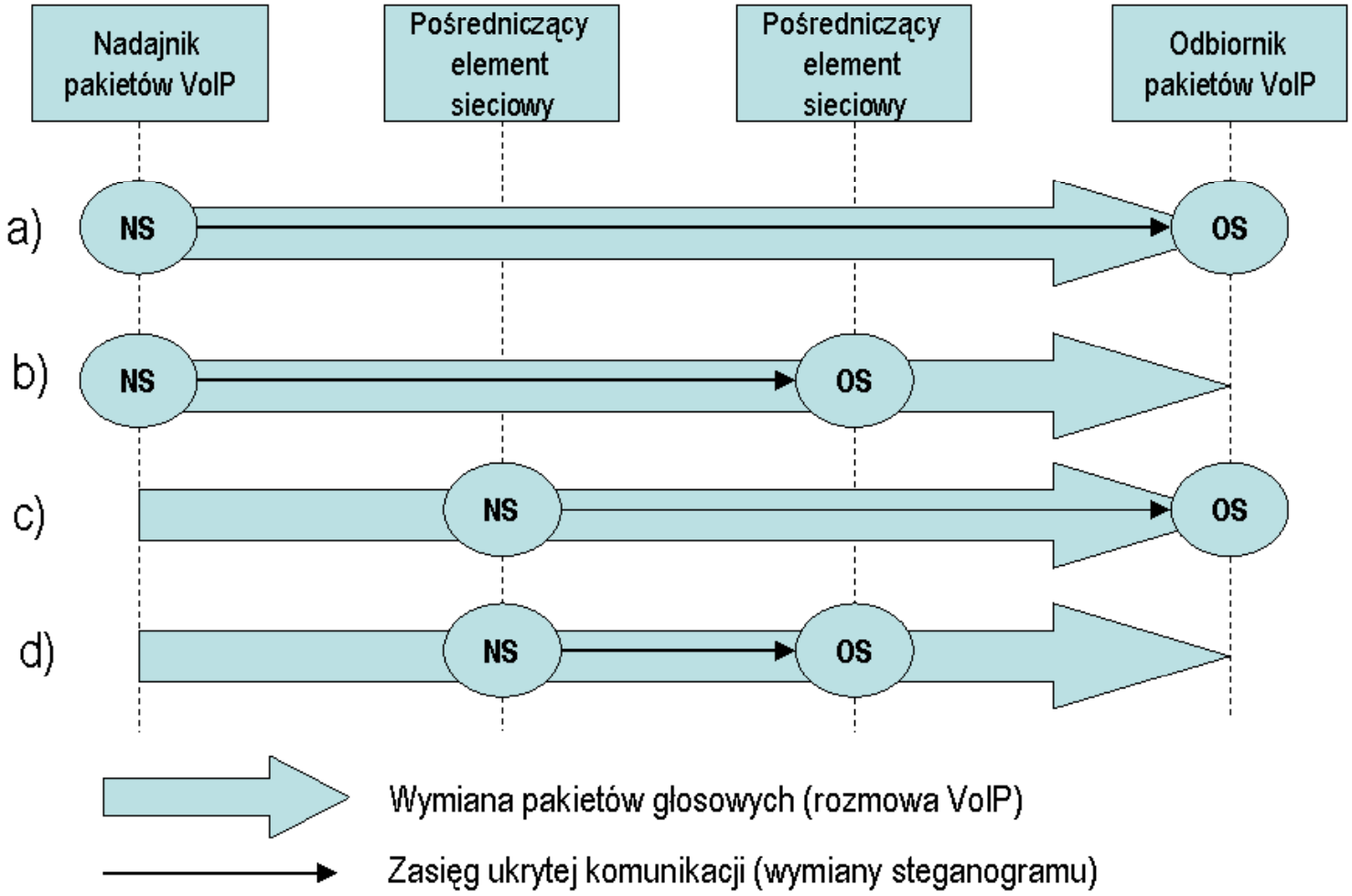
- Grupa technik ukrywania informacji wykorzystujących **strukturę** protokołów komunikacyjnych lub **oddziaływanie** na zachowanie tych protokołów
  - elementami **struktury** protokołów są m.in. opcjonalne pola nagłówków, kody nadmiarowe, wartości inicjujące numery wiadomości
  - **oddziaływanie** na zachowanie protokołów polega na realizacji konkretnego scenariusza bazującego np. na kolejności wymiany informacji, bądź uzyskaniu pożądanych opóźnień w reakcji na ustalone zdarzenie

Protokoły VoIP

- Cztery grupy protokołów tworzących VoIP:
  - **Protokoły sygnalizacyjne** (SIP, H.323, H.248/Megaco)
  - **Protokoły transportowe** (UDP, TCP, RTP)
  - **Kodeki** (np. G. 711, G.729, G.723.1)
  - **Protokoły uzupełniające** (np. SDP, RTCP)



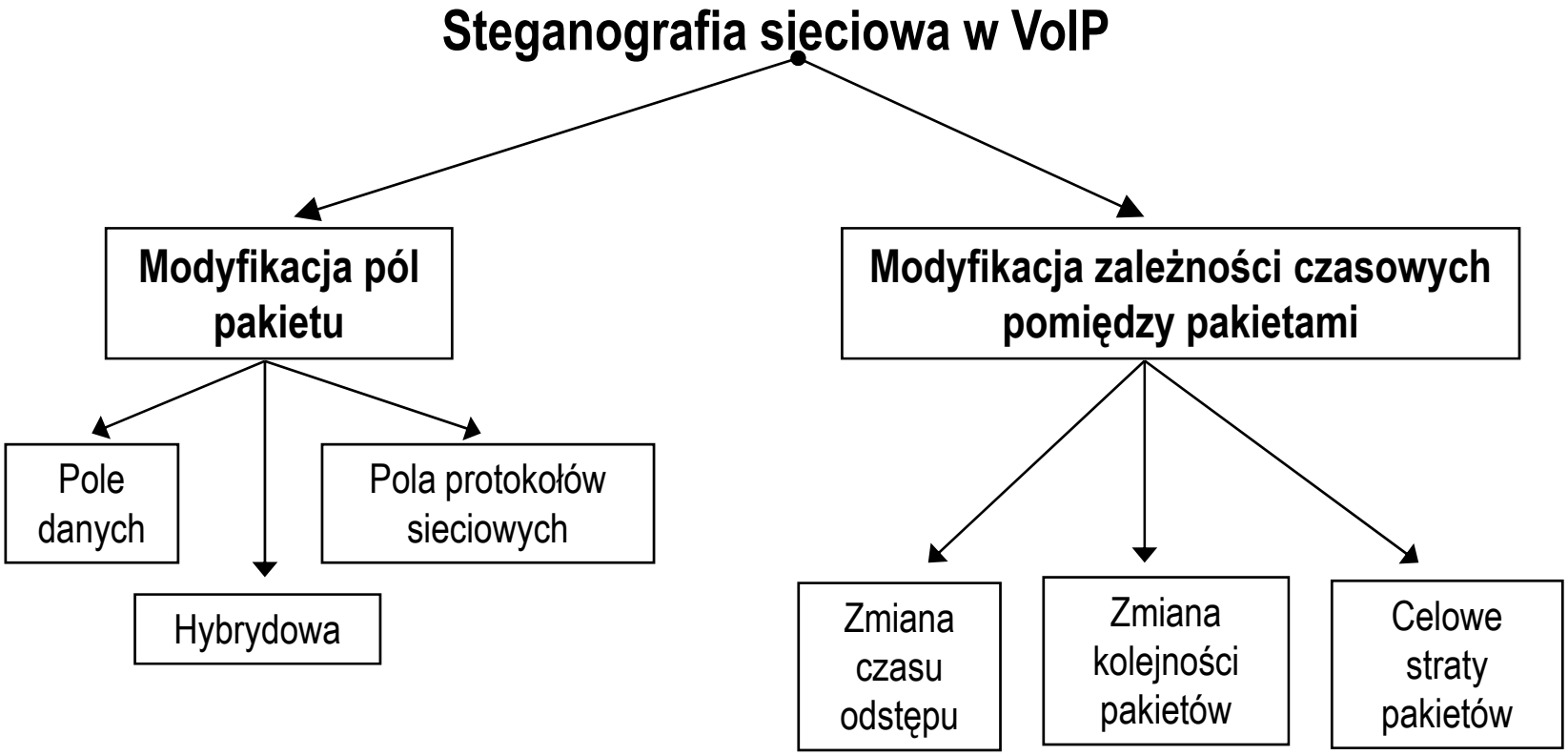
Steganografia w VoIP – scenariusze



NS – Nadawca steganogramu

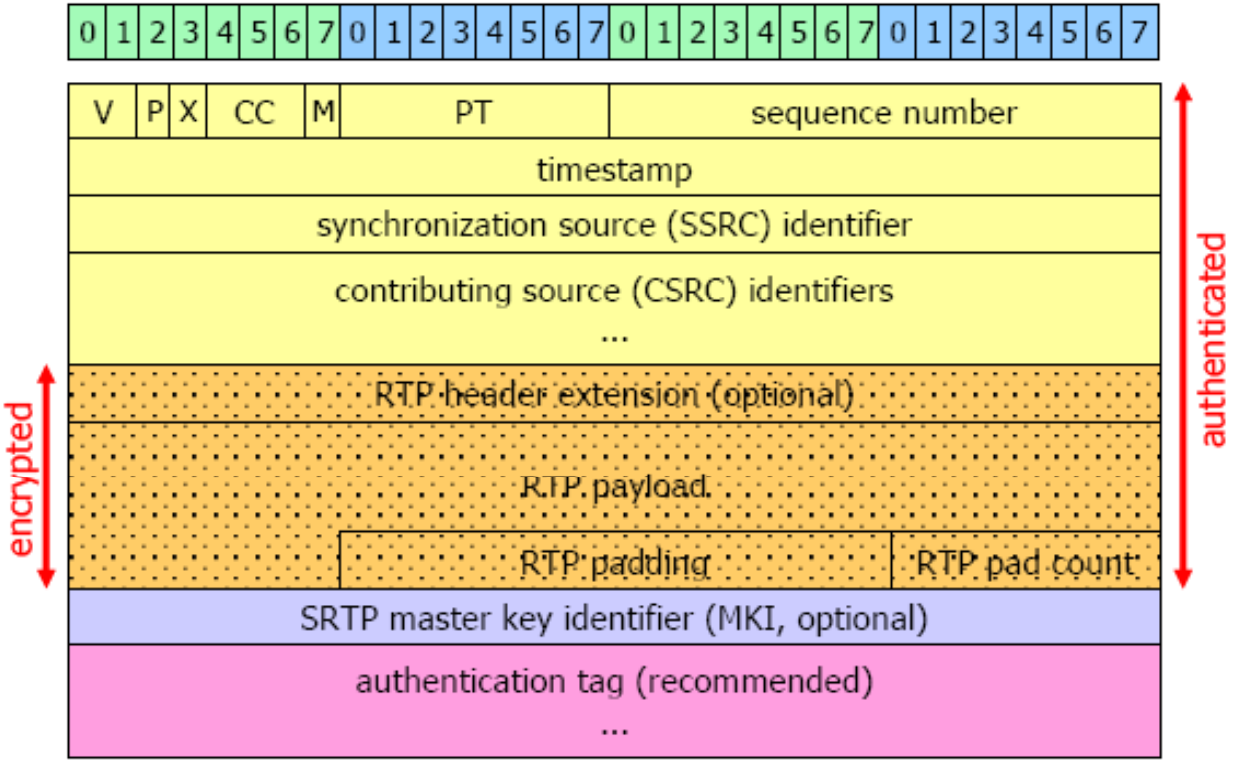
OS – Odbiorca steganogramu

Klasyfikacja metod steganografii w VoIP



Modyfikacja pól pakietu - przykład

- Wykorzystanie wolnych/nieużywanych pól protokołów sieciowych VoIP np. RTP



Modyfikacja zależności czasowych pomiędzy pakietami - przykład

Modyfikacja czasu odstępu między pakietami

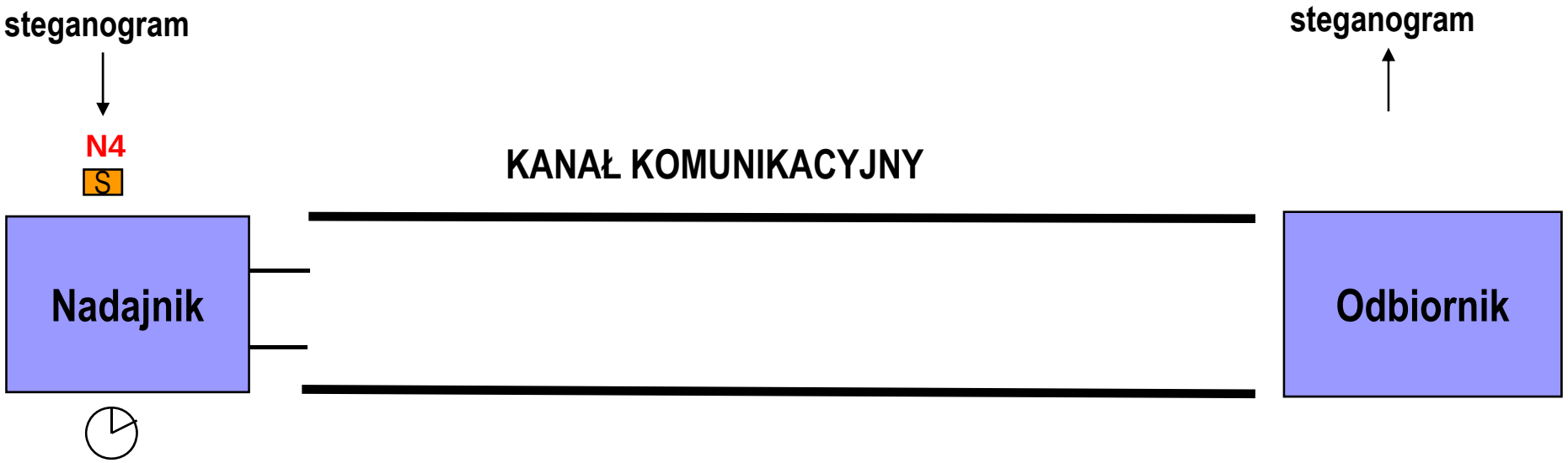
1, 2 Dwie szybkości generowania pakietów RTP

Nowa metoda steganografii dla VoIP: LACK

- **LACK** (*Lost Audio PaCKets Steganography*)
- Została zgłoszona przez Politechnikę Warszawską do Urzędu Patentowego RP, jako **wynalazek**

  (zgłoszenie nr 384940 z 15 kwietnia 2008)
- Do ukrytej komunikacji wykorzystuje **celowo opóźniane** w nadajniku pakiety RTP, które w odbiorniku uznawane są za **stracone**

LACK – zasada działania

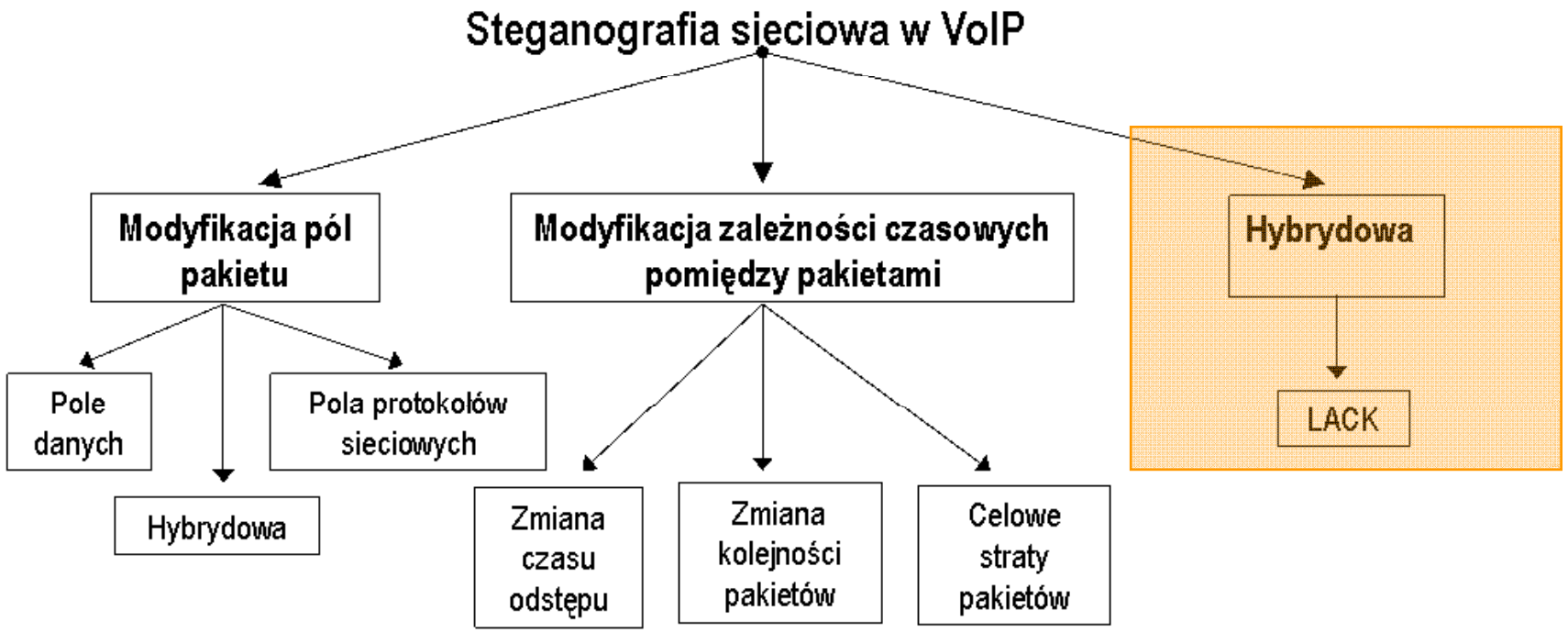


N*X*	Numer sekwencyjny pakietu
P*Y*	Kolejność skompresowanych danych głosowych

Cechy LACK

- Rozwiązanie **hybrydowe**
- Połączenie **zalet** obu grup steganografii sieciowej dla VoIP
- **Znaczna przepływność** przy **trudniejszej steganalizie**
- **Brak konieczności synchronizacji** nadajnika z odbiornikiem
- **Prosty w implementacji**
- Koszt: możliwość **pogorszenia jakości rozmowy**

Steganografia w VoIP („steganofonia”)



Wojciech Mazurczyk and Krzysztof Szczypiorski, information scientists at

the Institute of Telecommunications in Warsaw, Poland, revealed last week that they are developing a "steganographic" system for VoIP networks (www.arxiv.org/abs/0805.2938).

More in a web phone call than meets the ear

THE next time your internet (VoIP) phone call sounds a bit fuzzy, it might not be your ISP that's to blame. Someone could be trying to squeeze a secret message between the packets of data carrying the caller's voice.

Wojciech Mazurczyk and Krzysztof Szczypiorski, information scientists at the Institute of Telecommunications in Warsaw, Poland, revealed last week that they are developing a "steganographic" system for VoIP networks (www.arxiv.org/abs/0805.2938). Steganography is the art of hiding messa

http://www.arxiv.org/abs/0805.2938

them in ordinary communications. For example, a message can be encoded as a string of numbers which are used to modify the brightness and colour of an image. The effect is too subtle to be noticed by unwitting observers but the message can be deciphered with appropriate software by anyone who knows it's there.

Now the Polish researchers have worked out how to use internet phone calls rather than images as the carrier. "The idea is simple," says Mazurczyk: you replace some of the voice data packets that you ar sending with the hidden mess This is possible because VoIP u data transmission routine call User Datagram Protocol (UDP). the more familiar TCP, which delivers nd emails, UDP does not guarantee that packets will arrive in the same order they were sent: they may arrive out of order, be duplicated or simply go missing. The fact that the voice message can survive when VoIP packets are lost means that some of them can be used for another message – the hidden one.

> "The idea is simple: replace some of the voice data with a hidden message"

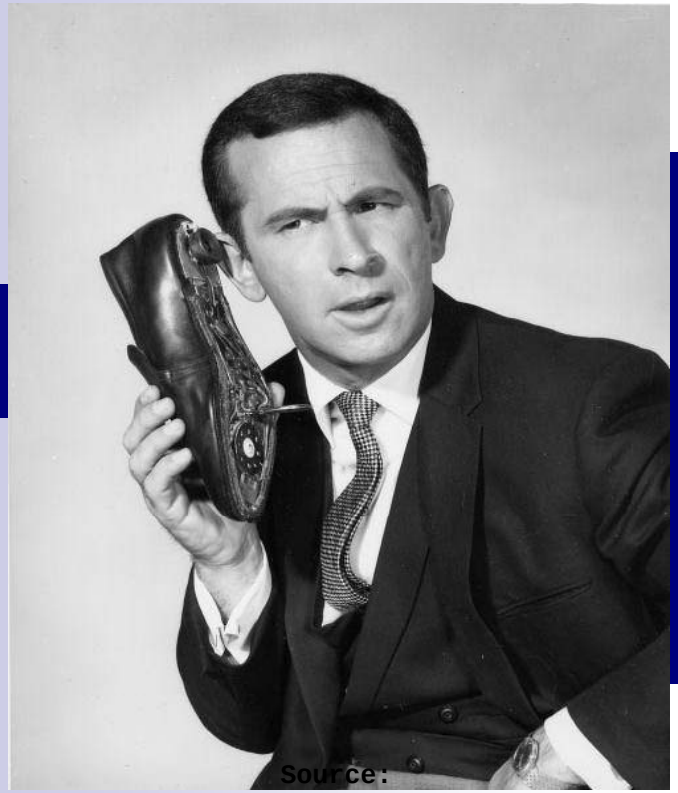
as lost ones," explains Mazurczyk. The researchers are trying to minimise the number of packets used to avoid degradation of audio quality – which could be a giveaway to any eavesdropper who suspects there is a message hidden in the call.

"It's an interesting proposal: it makes sense to hide data in a VoIP payload," says Tyler Moore, a computer security engineer at the University of Cambridge. However, he warns that while the message may be hidden, the identities of the callers aren't – and that's often all a snooper needs to know. Paul Marks ●

28 | New Scientist | 31 May 2008

www.newscientist.com

28 | New Scientist | 31 May 2008



Source:
http://webtown.typepad.com/webtown/2008/06/suspected-terro.html

Dziękujemy za uwagę!