stegano.net

HICCUPS

system ukrytej komunikacji dla „zepsutych" sieci

Krzysztof Szczypiorski
Instytut Telekomunikacji PW
ksz@stegano.net

VII Krajowa Konferencja Zastosowań Kryptografii Enigma'2003
Warszawa, 9 oraz 12-14 maja 2003

stegano.net

Plan prezentacji

- Idea działania
- Cechy środowiska sieciowego dla systemu
- Kanały ukrywania informacji wykorzystywane przez system
- Schemat działania systemu
- Elementy systemu
- Zarys przykładowej implementacji dla WLAN IEEE 802.11
- Przykłady zastosowań
- Stan prac i perspektywy rozwoju

stegano.net

HICCUPS

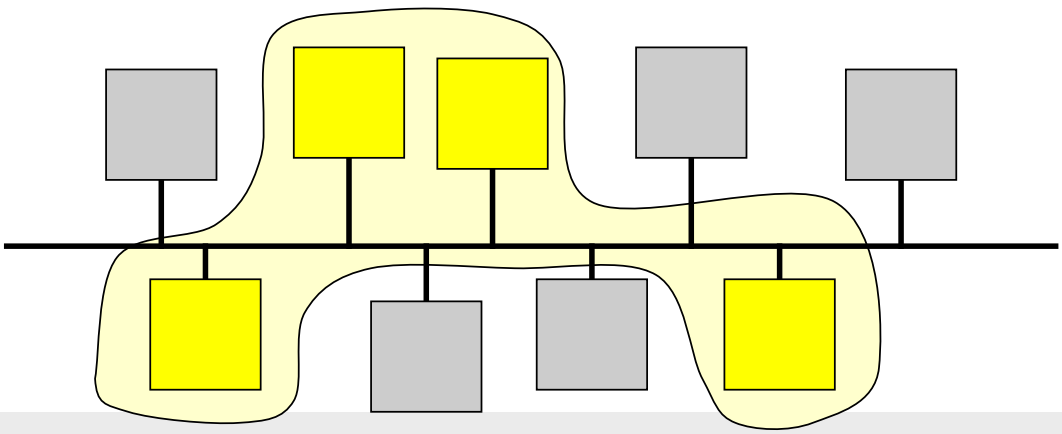
- **HICCUPS** = Hidden Communication System for Corrupted Networks
- system ukrytej komunikacji dla „zepsutych” („skorumpowanych”) sieci
- oryginalny system opracowany w Instytucie Telekomunikacji PW
- **czkawka** «urywane odgłosy wydawane w następstwie ostrych wdechów, spowodowanych okresowymi, nagłymi, krótkimi skurczami przepony»

  Słownika języka polskiego PWN – http://sjp.pwn.pl/

stegano.net

Idea działania cz. 1

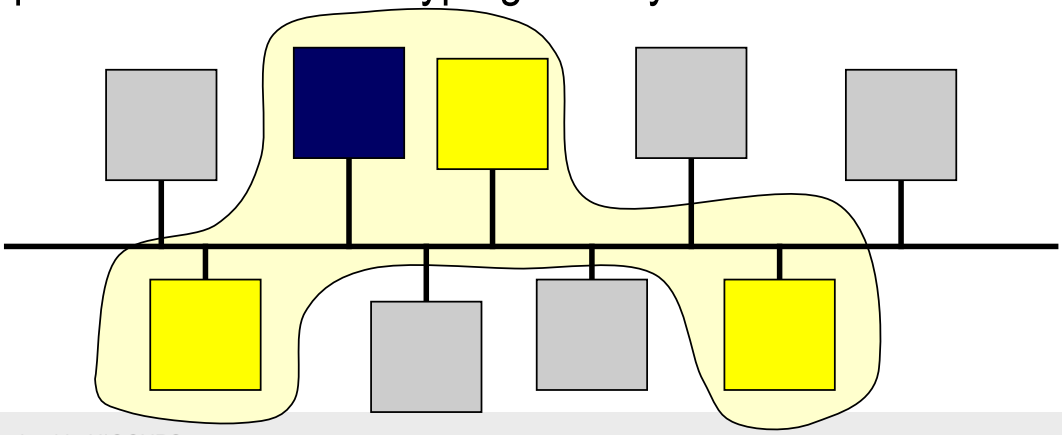
- wykorzystanie sieci, w której stacje „nasłuchują” współdzielonego medium np. powietrza
- normalna praca systemu steganograficznego polega na wykorzystaniu kanałów o niskiej przepływności ok. 1% pasma (np. opcjonalnych pól protokołów sieciowych)



stegano.net

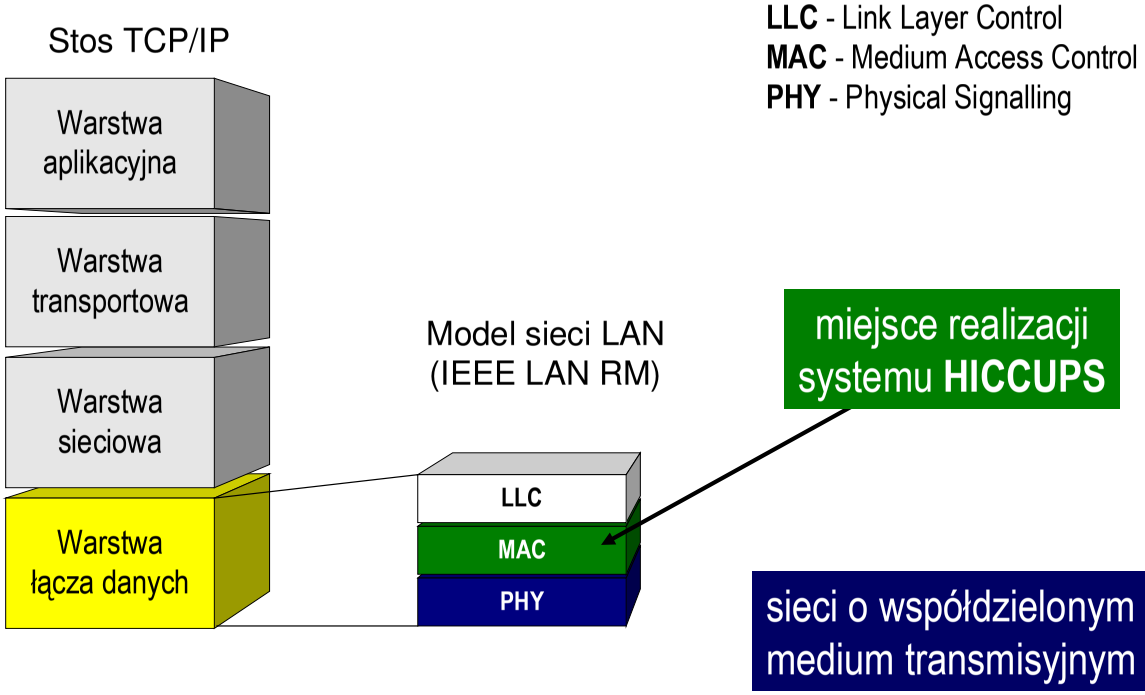
Idea działania cz. 2

- po otrzymaniu od wybranej stacji pakietu o ustalonej zawartości pozostałe stacje ukrytej grupy przechodzą w tryb „uszkodzonych ramek” – dostępna przepływność sięga 100%; opuszczenie tego stanu – pakiet o ustalonej zawartości
- dodatkowo: wykorzystanie sieci zabezpieczonej już uprzednio metodami kryptograficznymi



stegano.net

IEEE LAN RM a stos TCP/IP



stegano.net

Cechy środowiska sieciowego

- **C1:** dostęp do współdzielonego medium transmisyjnego dającego możliwość kopiowania wszystkich ramek z medium transmisyjnego np. sieć lokalna o topologii szyny
  - CSMA (Carrier Sense Multiple Access) - Aloha
  - CSMA/CD (CSMA with Collision Detection) - Ethernet
  - CSMA/CA (CSMA with Collision Avoidance) - WLAN
  - Token Bus
- **C2:** jawna metoda inicjacji parametrów szyfrów np. za pomocą wartości, wektorów inicjujących
- **C3:** kontrola poprawności szyfrogramów za pomocą sum kontrolnych (np. funkcje skrótu, cykliczne kody nadmiarowe – Cyclic Redundancy Code – CRC)

- **C1**: cecha nieodzowna

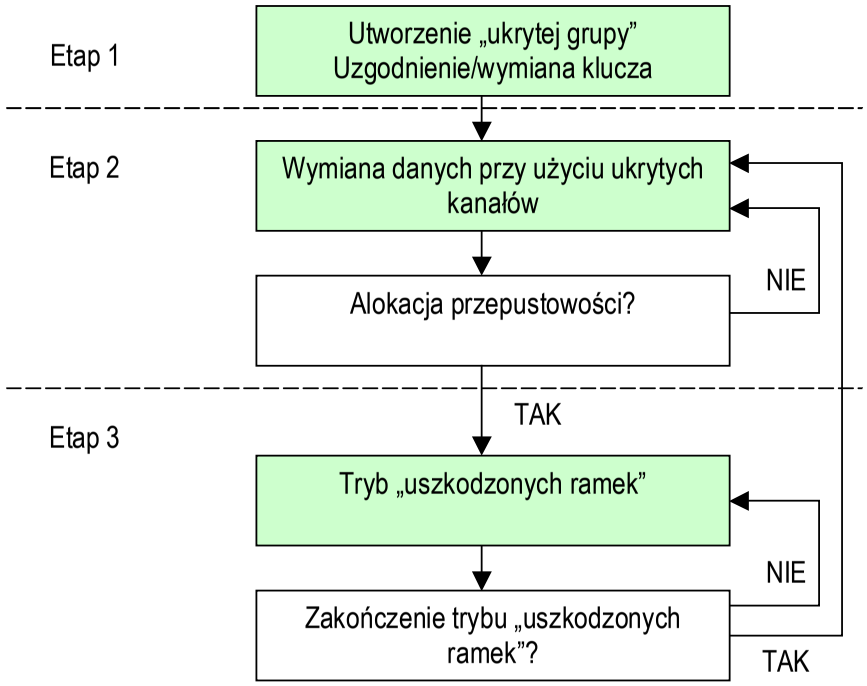
stegano.net

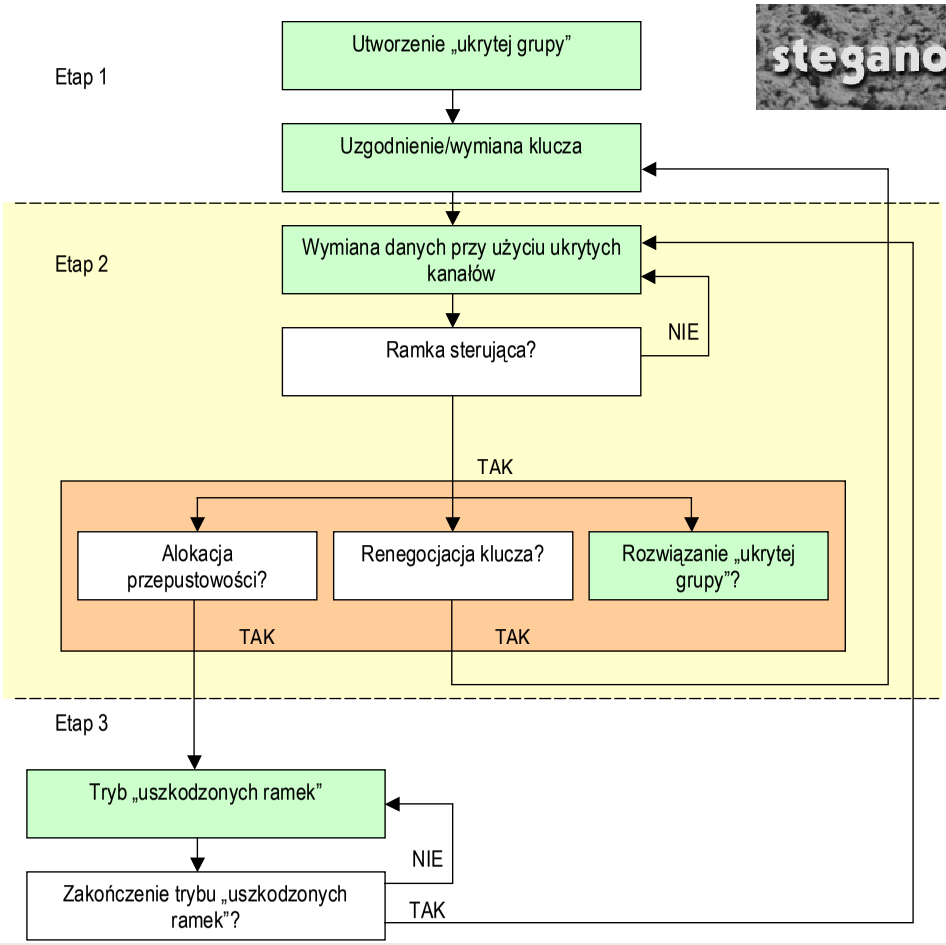
Kanały ukrywania informacji

- **K1:** kanał oparty na wartościach inicjujących szyfry
- **K2:** kanał oparty na adresach sieciowych MAC (np. adresach źródła i przeznaczenia)
- **K3:** kanał oparty na sumach kontrolnych
- dla sieci posiadających wyłącznie **C1**: tylko **K2** i **K3**

Uogólniona postać ramki MAC dla sieci posiadających **C1** - **K2** i **K3**

Schemat działania





stegano.net

Podstawowe elementy systemu

- **E1:** interfejs sieciowy pracujący w danej technologii sieciowej np. IEEE 802.11b(g), umożliwiający modyfikację kanałów K1-K3 oraz pełne sterowanie polem użytkowym w ramce MAC, oraz
- **E2:** system zarządzania, który zajmuje się modyfikacją kanałów i pola użytkowego

stegano.net

System zarządzania

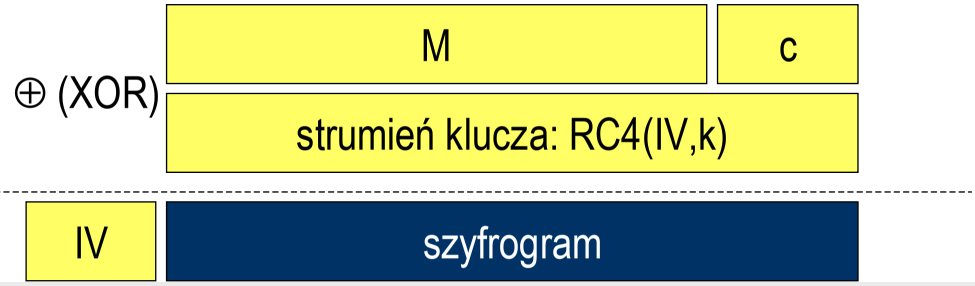
- System zarządzania (E2) może zostać zrealizowany sprzętowo lub programowo i powinien zapewniać następujące funkcję:
  - dołączanie się do „ukrytej grupy”
  - odłączenia się od „ukrytej grupy”
  - interfejs dla warstw wyższych umożliwiający sterowanie kanałami K1-K3 i polem użytkowym
- a rozszerzając funkcjonalność systemu o dystrybucję klucza – dodatkowo:
  - uzgadnianie/wymianę klucza
  - odświeżanie klucza
  - realizację poufności

stegano.net

Przykładowa implementacja

WLAN IEEE 802.11

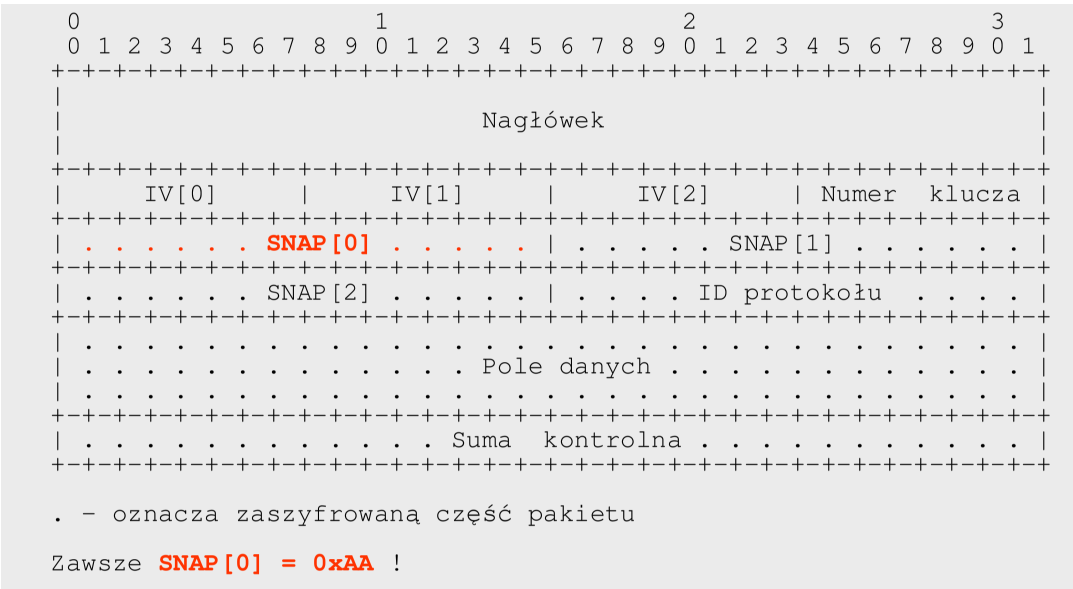
- Idea działania - WEP - Wired Equivalent Privacy
  - bazuje na **RC4** z kluczem 64-bitowym (efektywnie 40-bitowym)
  - użycie **RC4** z kluczem 128-bitowym (efektywnie 104-bitowym) jest rozwiązaniem niestandardowym
  - nadawca i odbiorca dzielą tajny klucz – **k**
  - wektor inicjujący – **IV**
  - wiadomość – **M**
  - przekształcenie **RC4(IV,k)** generujące strumień klucza
  - suma kontrolna c realizowana za pomocą **CRC-32**
  - manualna dystrybucja klucza



stegano.net

WEP - Wired Equivalent Privacy

Ramka 802.11 zabezpieczona WEP



stegano.net

Cechy środowiska WLAN IEEE 802.11

- **C1.WLAN:** bezprzewodowa sieć lokalna o topologii szyny z metodą dostępu CSMA/CA
- **C2.WLAN:** jawna metoda inicjacji parametrów szyfru RC4 za pomocą wartości inicjujących
- **C3.WLAN:** kontrola poprawności szyfrogramów za pomocą sum kontrolnych – CRC-32

stegano.net

Kanały ukrywania informacji w WLAN IEEE 802.11

- **K1.WLAN**: kanał oparty na wartościach inicjujących szyfr RC4: 24-bitowy
- **K2.WLAN**: kanał oparty na adresach sieciowych MAC:
  - źródła (Source Address – SA): 48-bitowy
  - przeznaczania (Destination Address – DA): 48-bitowy
  - odbiornika (Receiver Address – RA): 48-bitowy
  - nadajnika (Transmitter Address – TA): 48-bitowy
- **K3.WLAN**: kanał oparty na sumach kontrolnych na poziomie WEP: 32-bitowy

stegano.net

Przykłady zastosowań

- **system monitoringu wizyjnego** oparty na bezprzewodowych kamerach; kamery przekazują obraz różnicowy; w momencie pojawienia się ruchomego obiektu w obszarze pracy wybranej kamery następuje alokacja większej przepustowości, niezbędnej do przesłania większej porcji danych
- **kryptosystem pracujący w środowisku podatnym na podsłuch** (np. bezprzewodowa sieć lokalna o dużym zasięgu np. kilku kilometrów kwadratowych)
- **realizacja systemu uwierzytelniającego** stacje sieciowe działającego niezależnie do mechanizmów zaimplementowanych w danym protokole sieciowym

stegano.net

Stan prac i perspektywy rozwoju

- projekt: **stegano.net**
- symulacja programowa proponowanego systemu w sieciach CSMA/CA
- prace implementacyjne:
  - WLAN IEEE 802.11b(g)
  - CSMA/CD – IEEE 802.3 (Ethernet)
- system zarządzania „prawem głosu”

stegano.net

Koniec

Czy mają Państwo pytania?

Krzysztof Szczypiorski
Instytut Telekomunikacji PW
ksz@stegano.net

stegano.net

Literatura

• Ahsan K., Kundur D.: Practical Data Hiding in TCP/IP. In: Proc. Workshop on Multimedia Security at ACM Multimedia '02, Juan-les-Pins (on the French Riviera), December 2002

• Chmielewski A.: Urządzenie do wytwarzania dodatkowego kanału cyfrowego. Zgłoszenie wynalazku nr P.245442. Politechnika Warszawska, 1985

• Chmielewski A.: Wykorzystanie nadmiarowości kodu transmisyjnego do przesyłania dodatkowego strumienia danych. Rozprawa doktorska, Politechnika Warszawska, 1988

• 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.

• Handel T. and Sandford M.: Hiding Data in the OSI Network Model. In Anderson R., editor, Information Hiding: Proceedings of the First International Workshop, pp. 23–38, Cambridge, U.K., May 30-June 01, 1996, vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc.

• IEEE P802.11i/D3.0 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security

• Rowland C. H.: Covert Channels in the TCP/IP Protocol Suite. Psionics Technologies, November 14, 1996

• Szczypiorski K., Szafran P.: Sposób steganograficznego ukrywania i przesyłania danych dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym oraz układ formowania ramek warstwy sterowania dostępem do medium. Zgłoszenie wynalazku nr P. 359660. Politechnika Warszawska, 2003

• Szczypiorski K.: Bezpieczeństwo lokalnych sieci bezprzewodowych IEEE 802.11. Materiały: VI Krajowa Konferencja Zastosowań Kryptografii Enigma'2002, Warszawa, maj 2002