

Enigma 2005

Wojciech Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
<http://mazurczyk.com>

Możliwości wykorzystania watermarkingu do zabezpieczenia telefonii IP

Warszawa 01.06.2005

Plan Prezentacji

- Wprowadzenie
- Telefonia IP a bezpieczeństwo – istotne usługi ochrony informacji i komunikacji w sieci
- Klasyczna architektura bezpieczeństwa vs. nowe rozwiązania
- A może watermarking?
- Cechy cyfrowego znaku wodnego z punktu widzenia telefonii IP
- Watermarking w telefonii IP – możliwe scenariusze

Enigma 2005

Wprowadzenie

- SIP, H.323, H.248/Megaco, Skype... ??
- Po co szukać nowych rozwiązań bezpieczeństwa?
- Grupy problemów bezpieczeństwa telefonii IP:
 - protokół sygnalizacyjny
 - pakiety „z głosem” (np. RTP)
 - środowisko sieciowe (IP)
- **Konieczność zabezpieczania protokołu sygnalizacyjnego**

Kryterium bezpiecznego systemu

- Aby system telefonii IP uznać za bezpieczny należy zapewnić:

- UWIERZYTELNIENIE

- POUFNOŚĆ

- INTEGRALNOŚĆ

(wiadomości sygnalizacyjnych i pakietów „z głosem”)

- Dotychczasowe rozwiązania bezpieczeństwa
- Dlaczego nie stosuje się mechanizmów zabezpieczeń?

A może WATERMARKING?

- Fala popularności watermarkingu – tylko zabezpieczanie praw autorskich?



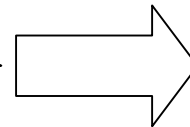
Enigma 2005

Cechy cyfrowego znaku wodnego

- Składa się z dwóch algorytmów:
 - **Wbudowującego** (*ang. Embedding Algorithm*)
 - **Ekstrakcji** (*ang. Extraction Algorithm*)

Najistotniejsze cechy znaku wodnego:

- | | |
|-------------------|---------------|
| - Żywotność | - Pojemność |
| - Bezpieczeństwo | - Złożoność |
| - Niewykrywalność | - Weryfikacja |



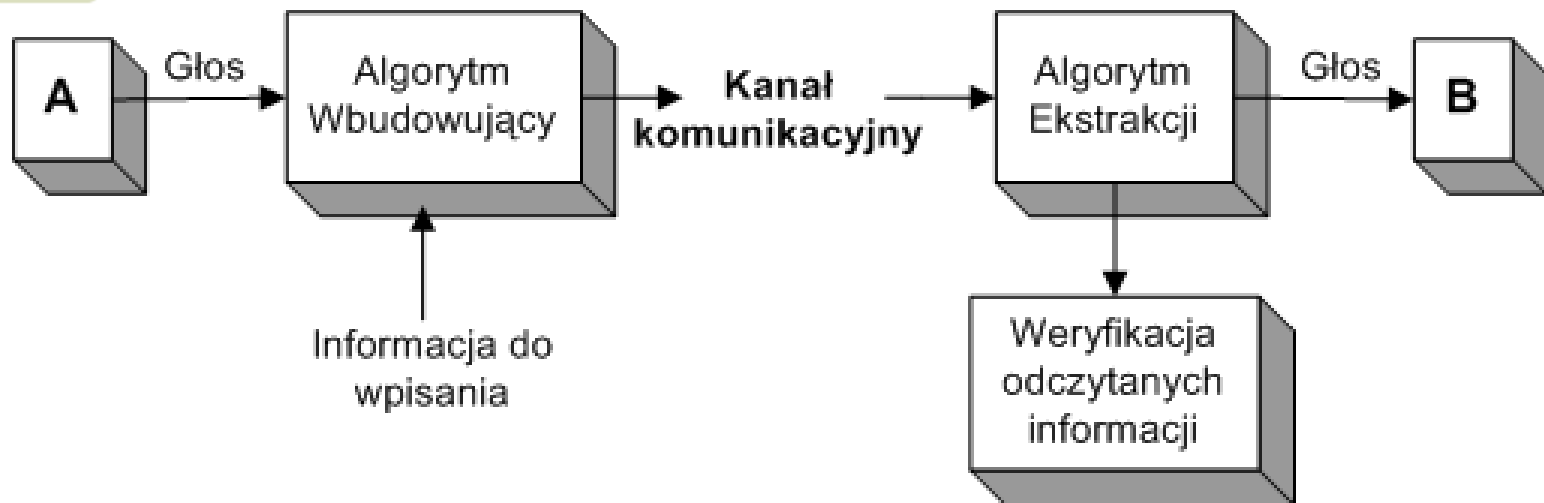
UWIERZYTELNIENIE

INTEGRALNOŚĆ

BRAK POUFNOŚCI

Enigma 2005

Ogólny schemat systemu z watermarkingiem



Warszawa 01.06.2005

Watermarking – możliwe scenariusze

- **Zabezpieczanie audio:**
 - Uwierzytelnienie dzwoniącego
 - Wpisanie cech przesyłanego głosu
- **Zabezpieczanie sygnalizacji:**
 - Uwierzytelnienie i integralność wiadomości sygnalizacyjnych
- **Zabezpieczanie audio i sygnalizacji:** oba powyższe

Watermarking – zabezpieczanie audio

- **Zabezpieczanie audio:**

- Uwierzytelnienie dzwoniącego
- Wpisanie cech przesyłanego głosu

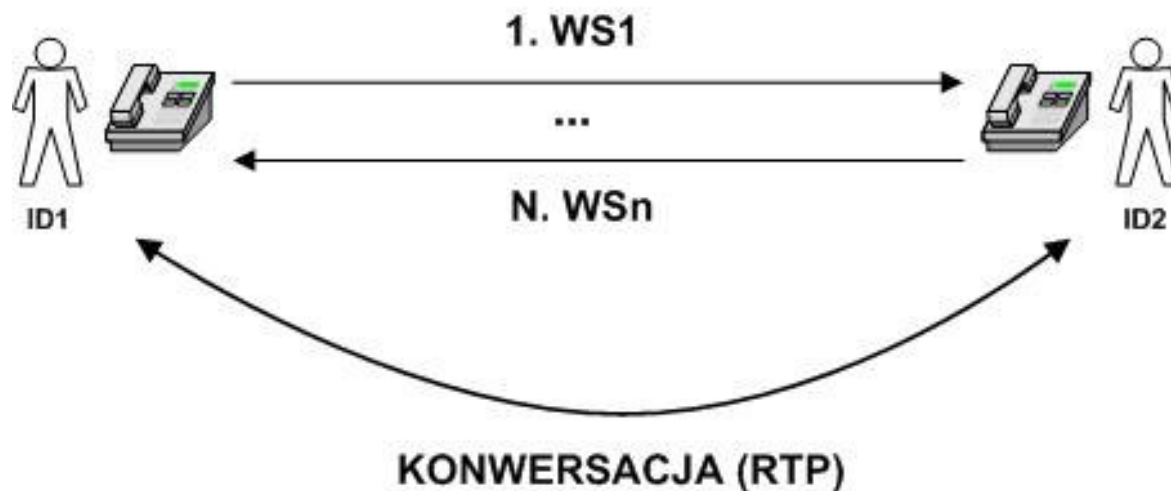
- Weryfikacja wpisanych danych przy ekstrakcji
- Dotychczas powstało kilka algorytmów do zabezpieczania komunikacji głosowej w czasie rzeczywistym

(np. rozwiązanie zaproponowane przez Fraunhofer Institute)

Watermarking – zabezpieczanie sygnalizacji

- **Zabezpieczanie sygnalizacji** - uwierzytelnienie i integralność wiadomości sygnalizacyjnych

FAZA SYGNALIZACYJNA

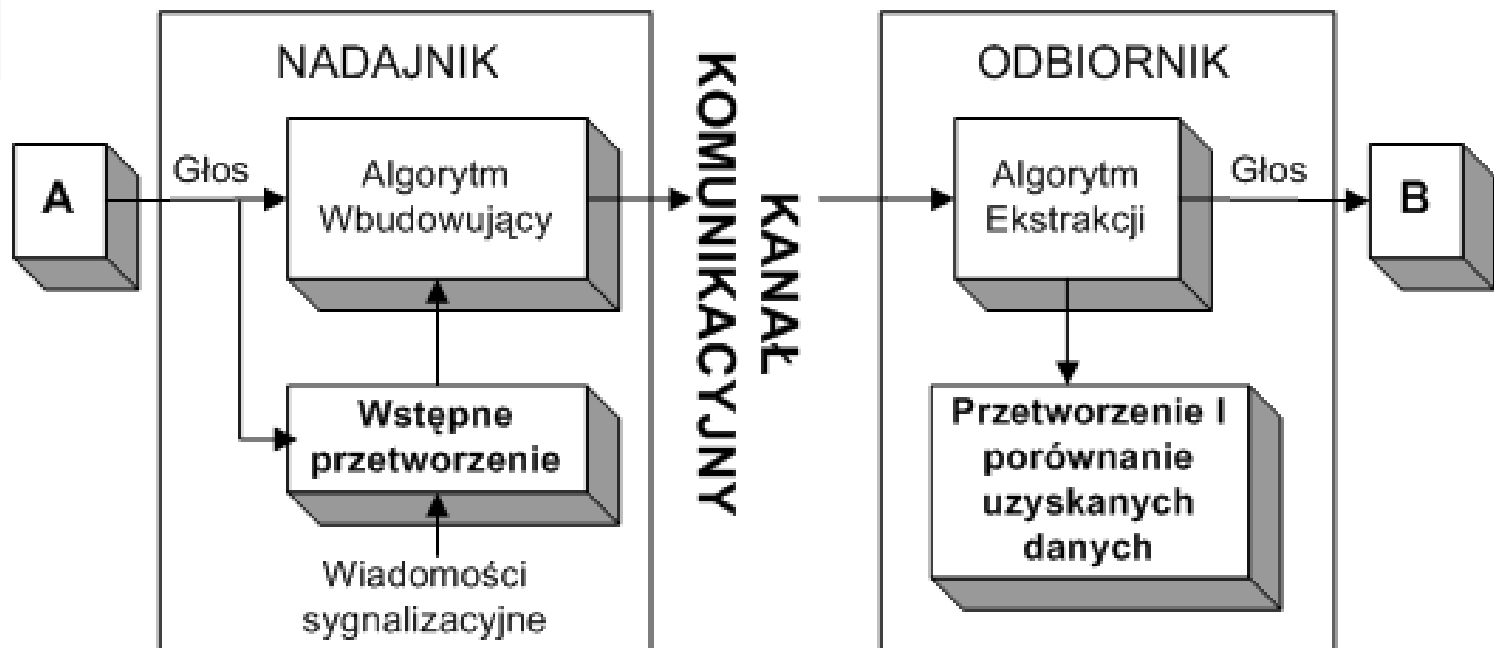


WATERMARK(H(H(WS1),H(WS2),...,H(WSn),TS, IDx, PASS))

WSx - wiadomość sygnalizacyjna o numerze

Watermarking – audio i sygnalizacja

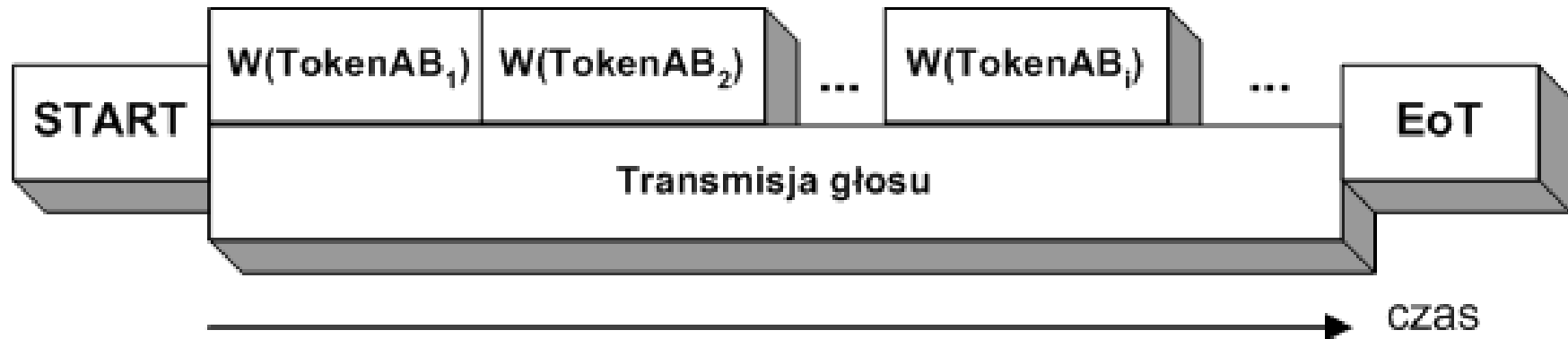
- Zabezpieczanie audio i sygnalizacji



Enigma 2005

A dokładniej...

$$\text{TokenAB} = H \left(H(\text{SM}_s) \parallel \begin{pmatrix} \text{TS} \\ \text{PASS} \\ \text{ID}_A \end{pmatrix} \parallel R \parallel \text{VF}_s \right) \parallel R$$
$$\text{TokenBA} = H \left(H(\text{SM}_R) \parallel \begin{pmatrix} \text{TS} \\ \text{PASS} \\ \text{ID}_B \end{pmatrix} \parallel R \parallel \text{VF}_R \right) \parallel R$$



Parametr LoT i algorytm (dla strony B):

START

```
CL = a; LoTA = x; TA = 0;
StartTimer(TA);
FOR (i = 0; i++; i < End of Transmission)
{
  IF (TokenABi = TokenBAi) THEN
  {
    LoTA ++;
    ResetTimer(TA);
  }
  ELSE (LoTA --);
  IF (LoTA <= CL) OR (TA > k) THEN STOP;
  IF (LoTA = a*x) THEN LoT = x;
}
```

LoT – Level of Trust

CL – Critical Level

T – Timer

i – Time slot

Zalety zaproponowanego rozwiązania:

- Jedna metoda zabezpieczania sygnalizacji i audio w telefonii IP
- Rozwiązanie jest niezależne od zastosowanego protokołu sygnalizacyjnego
- Łączy zabezpieczanie audio i sygnalizacji przez co zapobiega dublowaniu opóźnień i zapotrzebowania na moc obliczeniową (mniejszy koszt)
- Dobre zabezpieczenie w przypadku współpracy protokołów sygnalizacyjnych lub VoIP-PSTN

Enigma 2005

Wady, czyli co należy jeszcze rozważyć:

- Proponowane rozwiązanie posiada pewne **wady**:
 - działanie dopiero **po rozpoczęciu** rozmowy
 - konieczność „sporej” pojemności znaku wodnego
- Dobór właściwego algorytmu watermarkingu jest kluczowy!
- Przypadki skrajne – zdefiniować wymagania na parametry cyfrowego znaku wodnego
- Zbadanie **opóźnień** wprowadzanych przez nowe rozwiązanie w porównaniu do rozwiązań istniejących

Enigma 2005

Podsumowanie:

- Technika watermarkingu na pomoc mechanizmom zabezpieczeń telefonii IP
- Zapewnia dwie z trzech usług ochrony informacji
- Nie mniej jednak może być interesującą uzupełnieniem/alternatywą dla klasycznych mechanizmów zabezpieczania sygnalizacji i audio dla telefonii IP
- Konieczność dalszego rozwijania rozwiązania i dalszych badań - ciągle jest jeszcze dużo do zrobienia 😊

Enigma 2005

Wojciech Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
<http://mazurczyk.com>

Możliwości wykorzystania watermarkingu do zabezpieczenia telefonii IP

Warszawa 01.06.2005