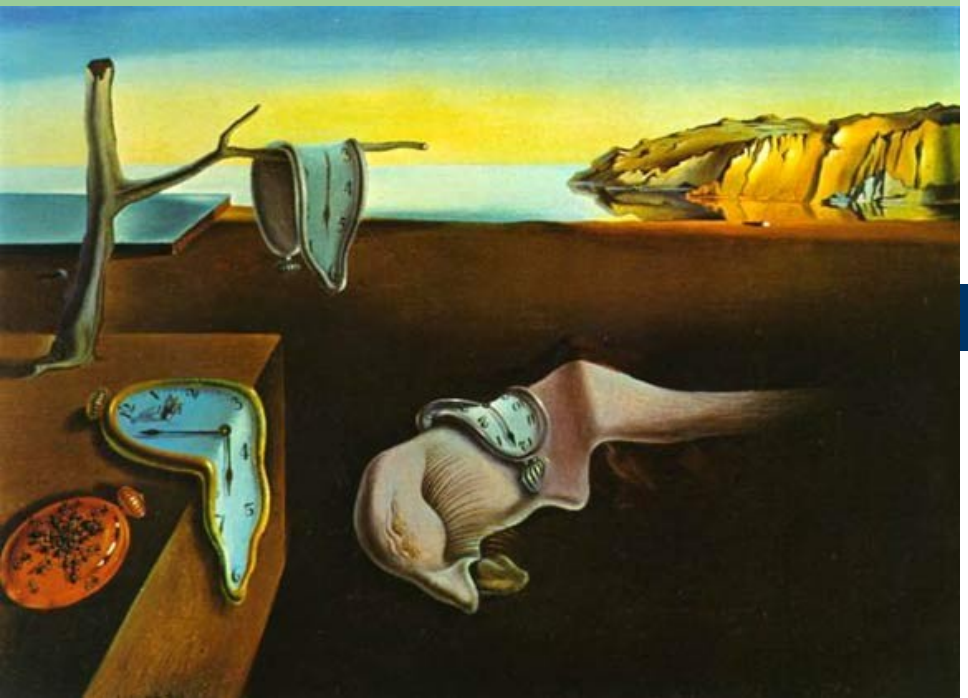
Zdalna identyfikacja systemów operacyjnych i komputerów



Nowe techniki oparte na błędach zegarów

3 kwietnia 2005

Opracował:
Paweł Pokrywka
Promotor:
dr Tomasz Surmacz
Prowadzący seminarium dyplomowe: **prof. Wojciech Zamojski**

Plan prezentacji

- Co to jest FP?
- Klasyczne metody FP.
- Metoda oparta na błędzie zegara.
- Praca dyplomowa i jak się do niej ma FP.

- Dyskusja.

Zdalny fingerprinting (FP)

- Rozpoznawanie obiektów na odległość za pomocą ich cech charakterystycznych (fingerprint - odcisk palca)
- FP systemów operacyjnych polega na rozpoznawaniu systemu z wykorzystaniem sieci komputerowej oraz protokołów komunikacyjnych.
- Dojrzała dziedzina bezpieczeństwa komputerowego

Rodzaje FP

- Aktywny
  - Wymagana interakcja ze zdalnym systemem.
- Pasywny
  - Monitorowanie transmisji.
- Semi-pasywny
  - Modyfikacja transmisji w sposób trudno zauważalny dla badanego systemu.

Klasyczne metody i narzędzia

- Banery (netcat, amap).
- Niestandardowe icmp i udp (xprobe).
- Protokół TCP:
  - Wysyłanie niestandardowych segmentów (nmap, queso).
  - Monitorowanie segmentów kontrolnych (p0f).
  - Monitorowanie częstotliwości powtórzeń (ring).
  - Analiza ISN.

Fingerprinting oparty na czasie

- Rozpoznawanie konkretnego urządzenia.
- Ta metoda pozwala rozróżnić dwie maszyny pracujące pod kontrolą tej samej wersji systemu operacyjnego.
- Kluczowym wymaganiem jest możliwość uzyskania czasu zdalnego systemu (niekoniecznie rzeczywistego).

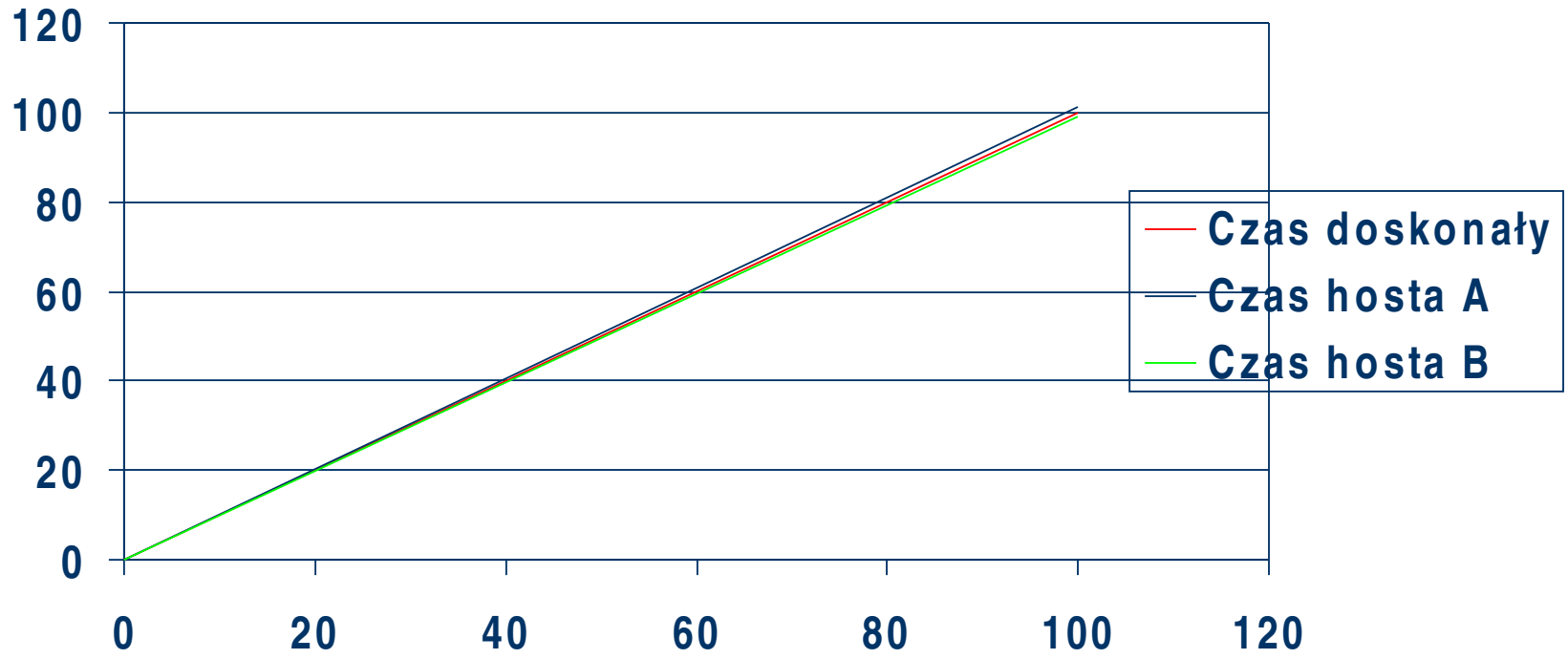
Metody zdalnego odczytu czasu

- W zależności od metody pomiaru otrzymany czas ma różne właściwości:
  - TCP Timestamp (względny)
  - ICMP (rzeczywisty)
  - Protokoły warstw 7 i „8”

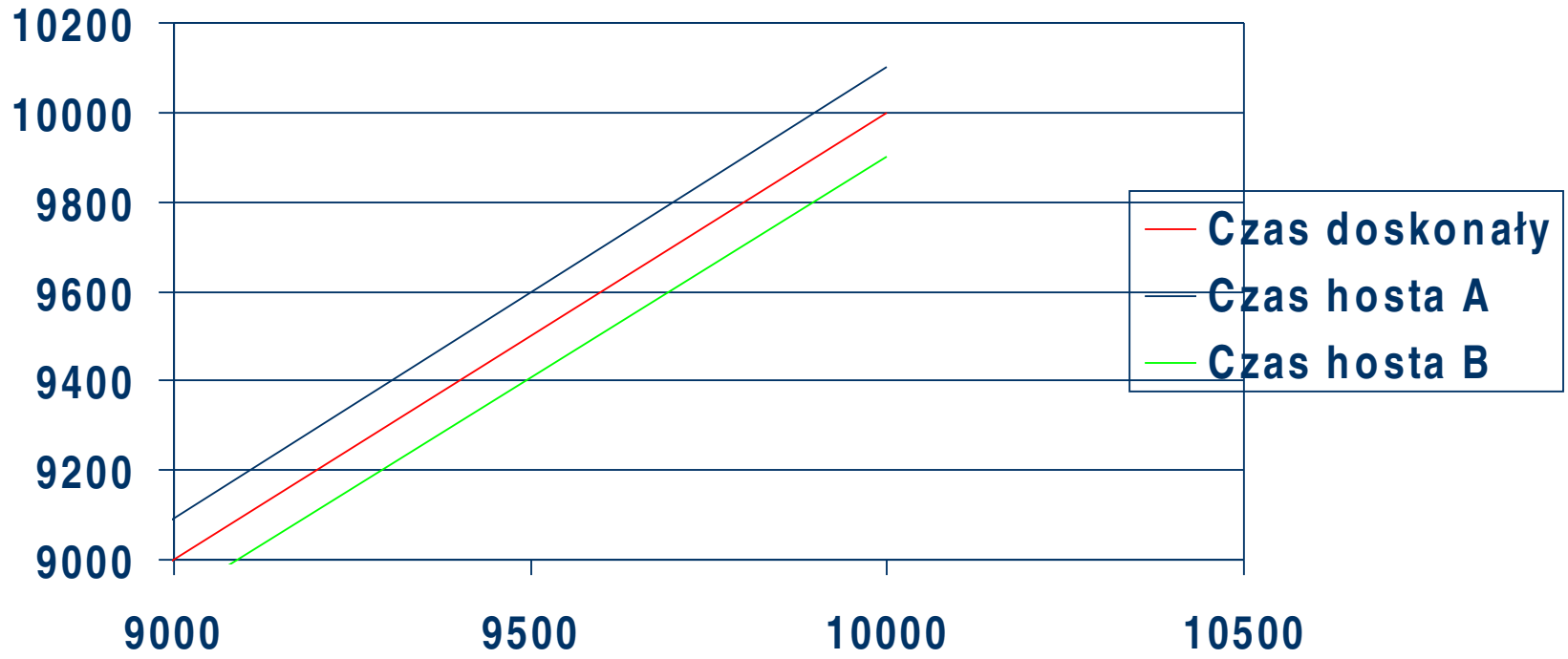
Błąd zegara

- Czas doskonały
- Czas obarczony błędem
- „Śpieszenie" i "spóźnianie"

Wykorzystanie błędu zegara do FP



Wykorzystanie błędu zegara do FP



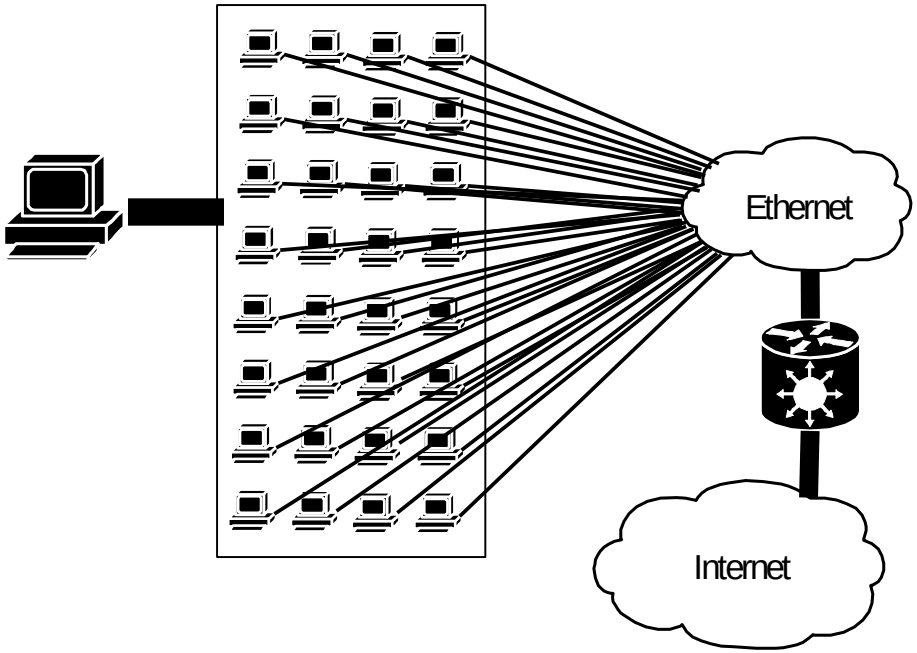
Zastosowania nowej metody FP

- Wykrywanie wirtualizacji (honeyd, vmware itd.).
- Wykrywanie liczby maszyn za NATem.
- Śledzenie konkretnych maszyn.
- Dowody sądowe („antydowody”).
- Likwidowanie bariery anonimowości.

Praca dyplomowa

- Wykorzystywanie słabości uwierzytelniania użytkowników w sieci.
  - System *multispoof*
- Metody detekcji nadużyć.
- Metody prewencyjne.

multispoof: idea



multispoof: detekcja

- Zdalny FP systemów operacyjnych i urządzeń
  - Ciągłe badanie stanu sieci i komputerów użytkowników (pasywne i/lub aktywne).
  - Jeśli zbyt wiele systemów nagle ulegnie zmianie, to jest to sygnał alarmowy.
- „Odwrotna" detekcja NAT
  - Do tej pory detekcja NAT zawsze była ukierunkowana na znalezienie użytkownika, który udostępnia swoje łącze kilku komputerom.
  - Trzeba wykryć sytuacje, kiedy w jednej chwili jeden komputer korzysta z kilku adresów.

Prewencja

- Autoryzujące serwery proxy
- VPN
- Inteligentne przełączniki sieciowe
  - Statyczne przypisania MAC - port
  - 802.11x
- Inna technologia sieci

Literatura

- Opracowano na bazie artykułu:
  - T. Kohno, A. Broido, kc claffy, "Remote physical device fingerprinting", http://www.caida.org/outreach/papers/2005/fingerprinting/

Dziękuję za uwagę.