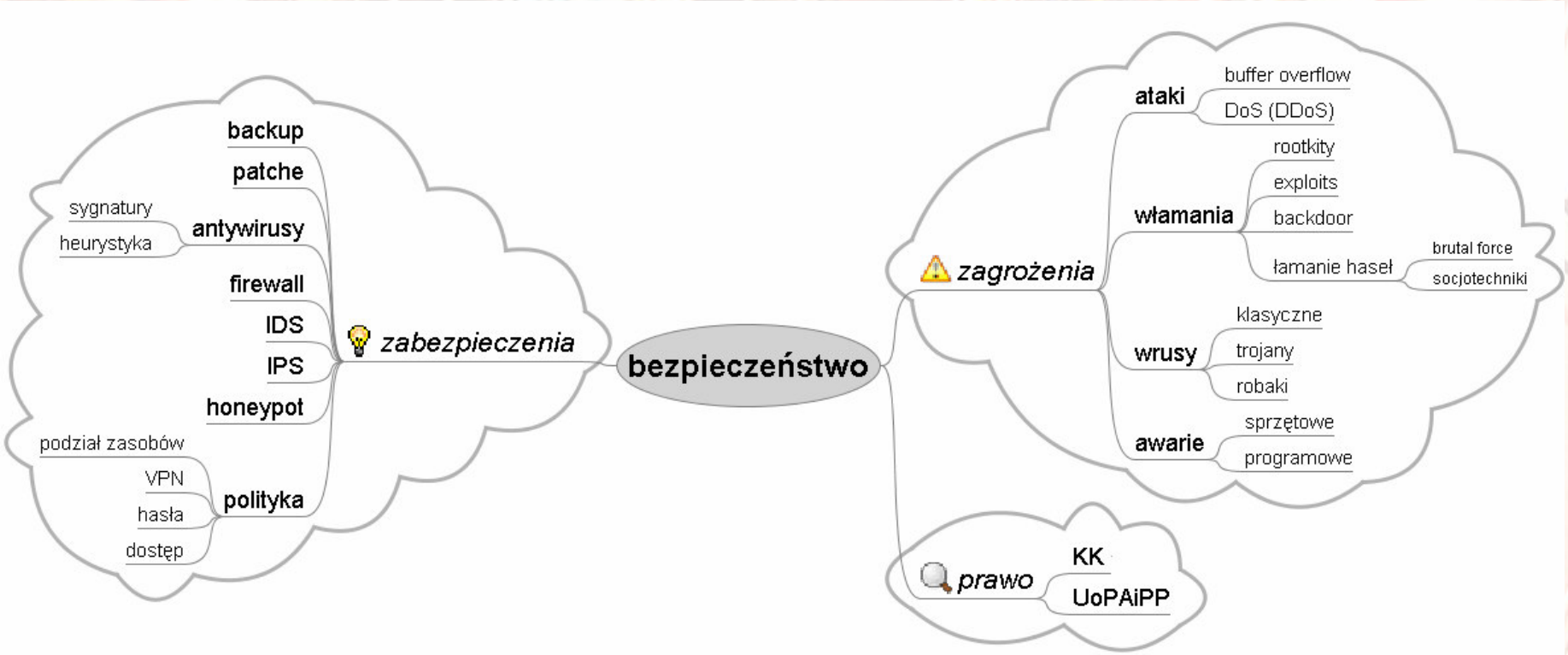
Systemy operacyjne



Bezpieczeństwo systemów.

mgr inż. Krystian Dobrzyński, Wydział Elektroniki i Informatyki, Politechnika Koszalińska, 2005

Ogólne zagadnienia bepieczeństwa.



HASH (*jednokierunkowe*)

- DES3
- MD5
- SHA1

przechowywanie haseł

sumy kontrolne

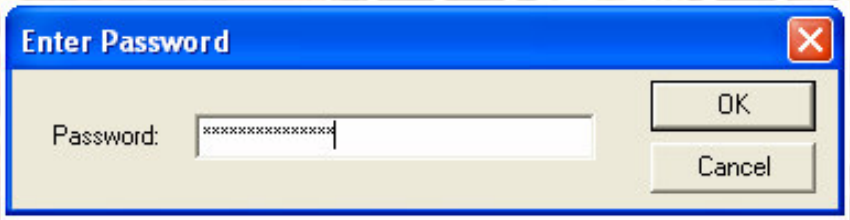
CRYPTO (*dwukierunkowe*)

- RSA
- RC1-5
- Kerberos

kodowanie transmisji

podpis elektroniczny

Szyfrowanie: hasła w systemach UNIX





Szyfrowanie – DES3

aVF32seDFXx2a

wyszukiwanie

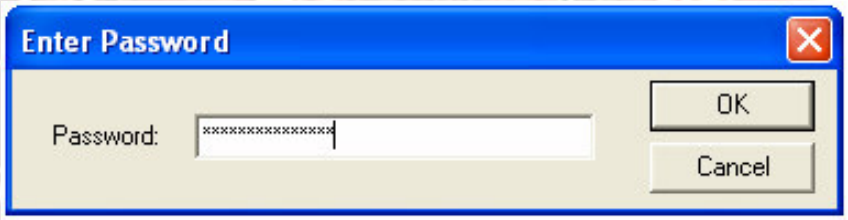
```
lolek:aSF45WSsag1h5::::::
macius:SDoIK9.OFd45s::::::
alina:oei65EEss/432::::::
pawel:5RDeW67)ws31A::::::
robcio:sOGhf.kl3p78A::::::
dzidzia:aVF32seDFXx2a:::::
antoni:sD23Q).kjd3sx::::::
```

dzidzia - autoryzacja

Łamanie haseł: metoda brutalna

ania
ala
asia
agnieszka
alicja
alina
aleksandra
andzelika
boguslawa
bogna
basia
barbara
czesia
celina
dorota
dagmara
dosia
dzesika
eliza
elzbieta
ela
elwira
elizabet







czy jest dostęp ??

Łamanie haseł: metoda słownikowa

```
ania
ala
asia
agnieszka
alicja
alina
aleksandra
andzelika
boguslawa
bogna
basia
barbara
czesia
celina
dorota
dagmara
dosia
dzesika
eliza
elzbieta
ela
elwira
elizabet
```



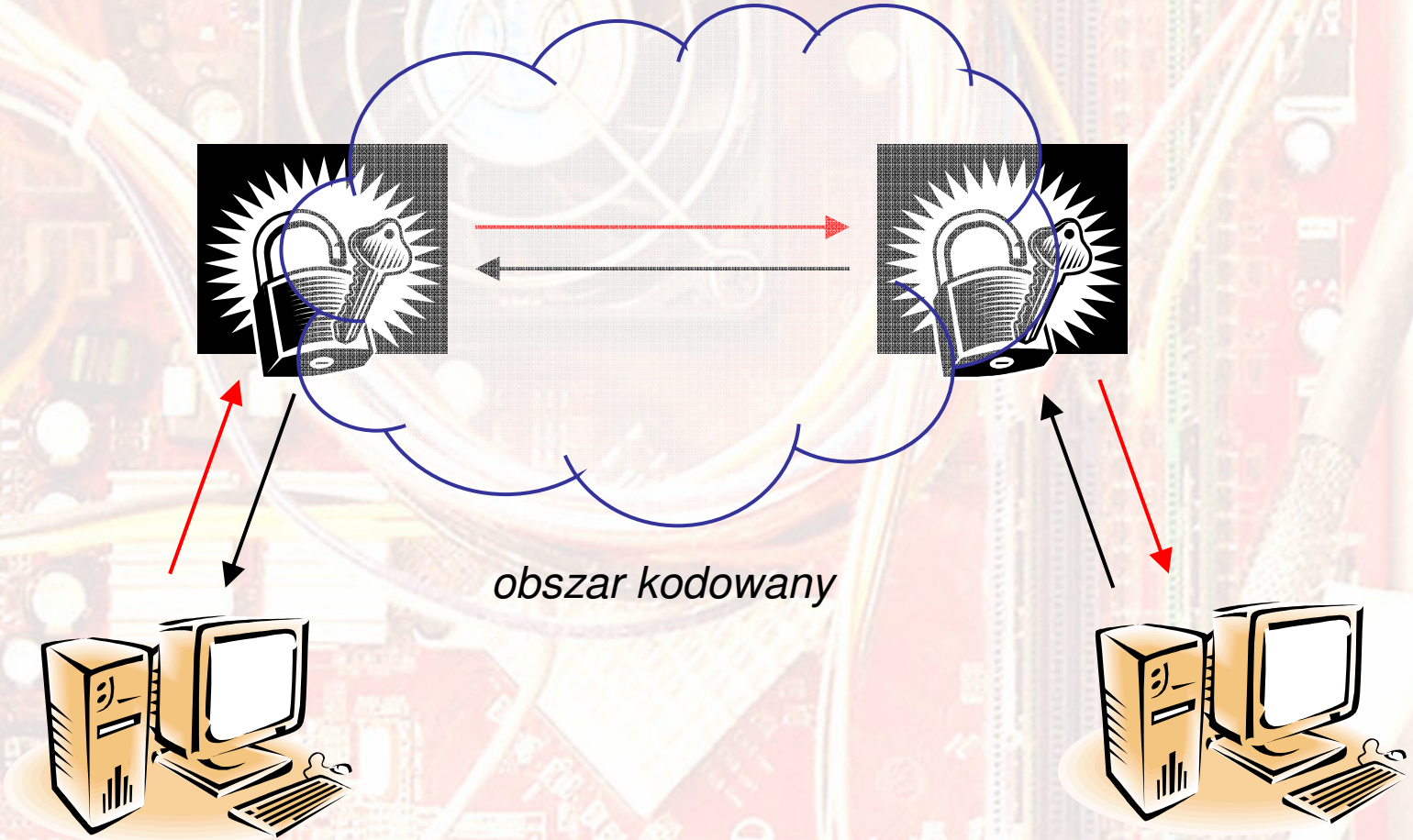
kodowanie

aVF32seDFXx2a

szukanie

```
lolek:aSF45WSsag1h5:::::
macius:SDoIK9.OFd45s:::::
alina:oei65EEss/432:::::
pawel:5RDeW67)ws31A:::::
robcio:sOGhf.kl3p78A:::::
dzidzia:aVF32seDFXx2a:::::
antoni:sD23Q).kjd3sx:::::
```

Szyfrowanie: symetryczne (z jednym kluczem)



Szyfrowanie: asymetryczne (z parą kluczy)

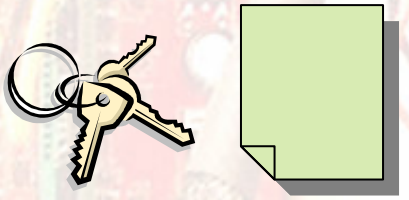


generowanie kluczy



prywatny publiczny

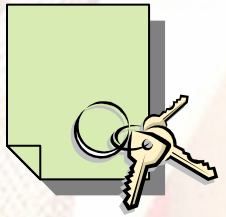
przekazanie klucza publicznego



publiczny dane jawne

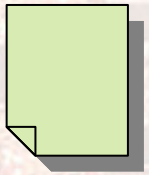
kodowanie danych

przekazanie zakodowanych danych





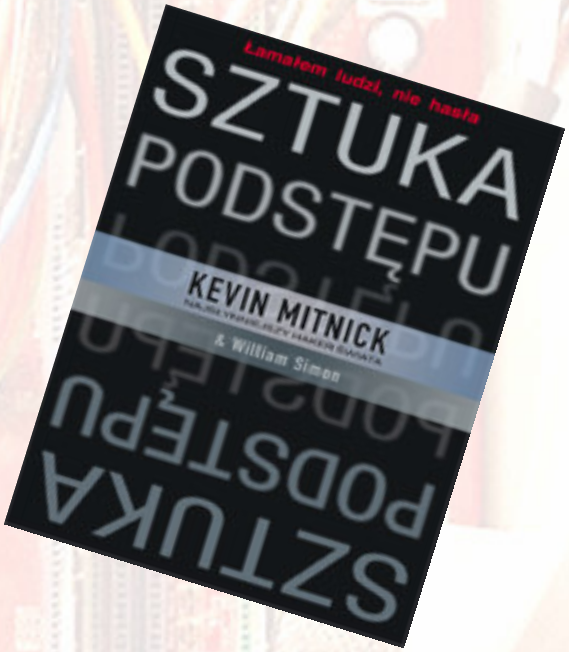
dekodowanie danych



dane jawne

Łamanie haseł: socjotechniki (inżynieria społeczna)





Kevin Mitnick: *Łamałem ludzi, nie hasła…*

Włamania: exploits

exploit

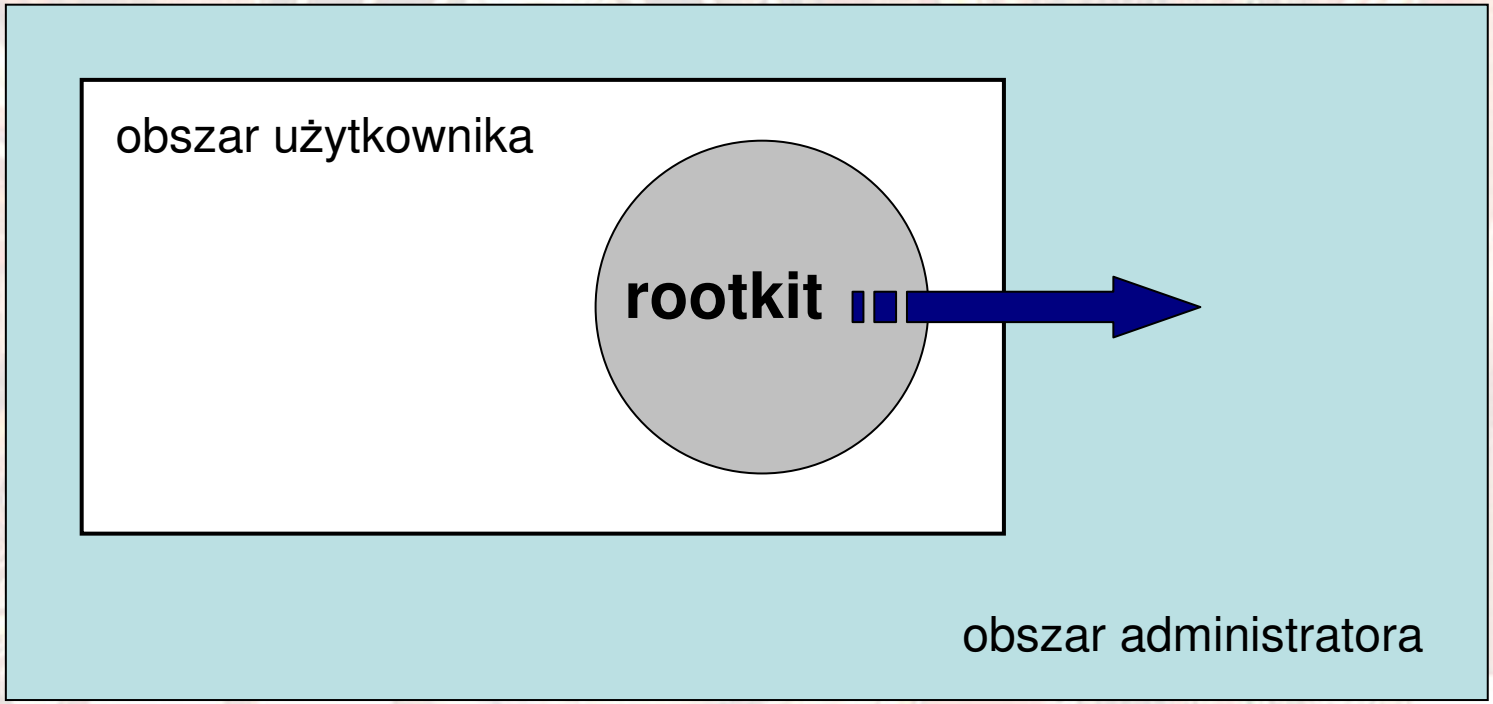




awaria systemu lub usługi

osłabienie zabezpieczeń

uzyskanie praw uprzywilejowanych




```
Bash :> id
uid=125 (somebody) gid=45 (clients)
Bash :> myrootkit
Waiting to apply rootkit…
Done!
Bash :> id
uid=0 (root) gid=1 (admins)
```

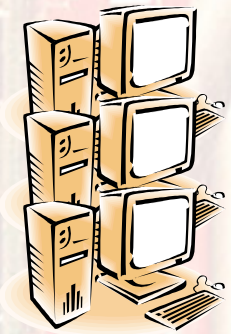
Atak ‘buffer overflow’



ofiara

bufor sesji

bufor połączeń

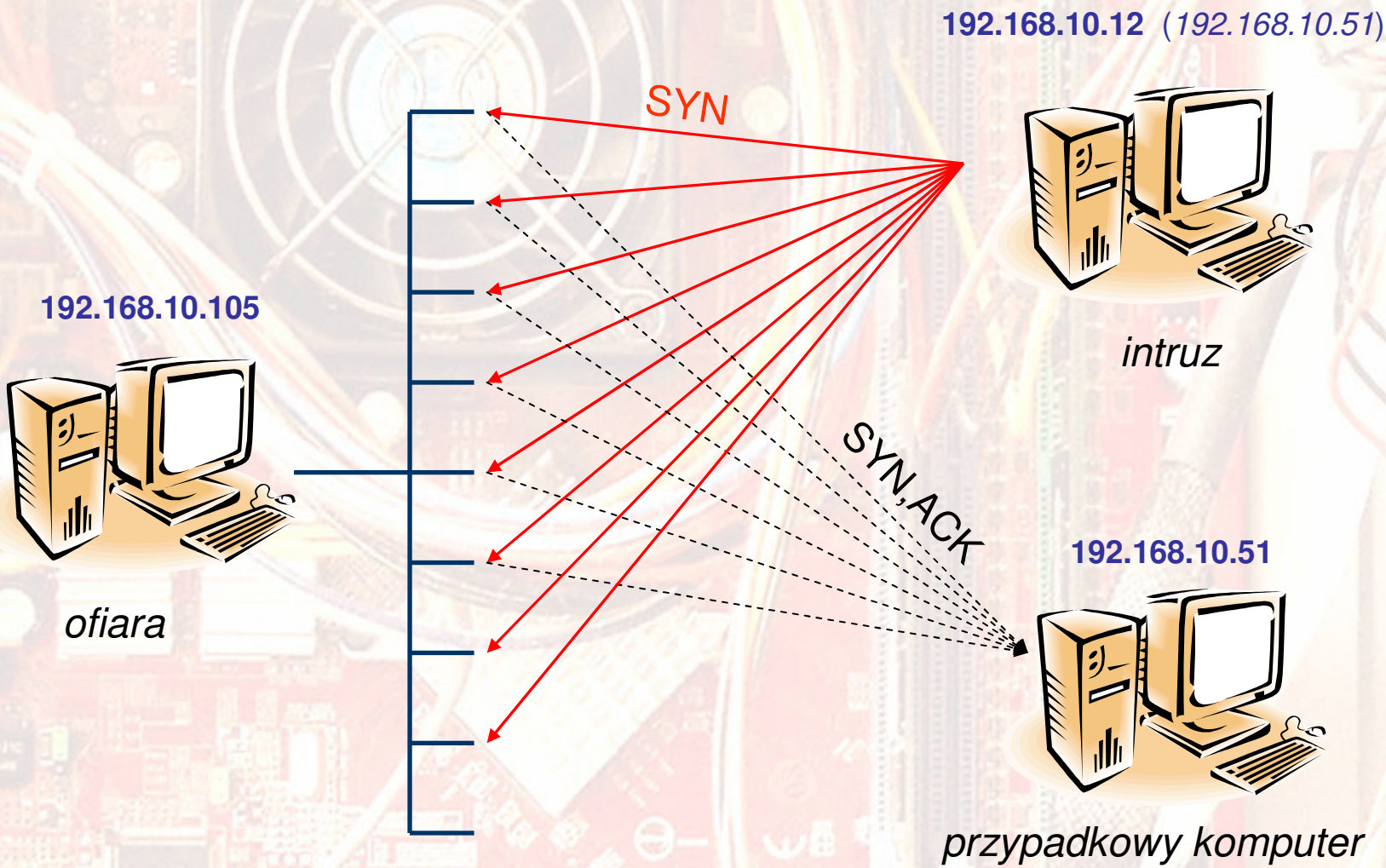


intruzi

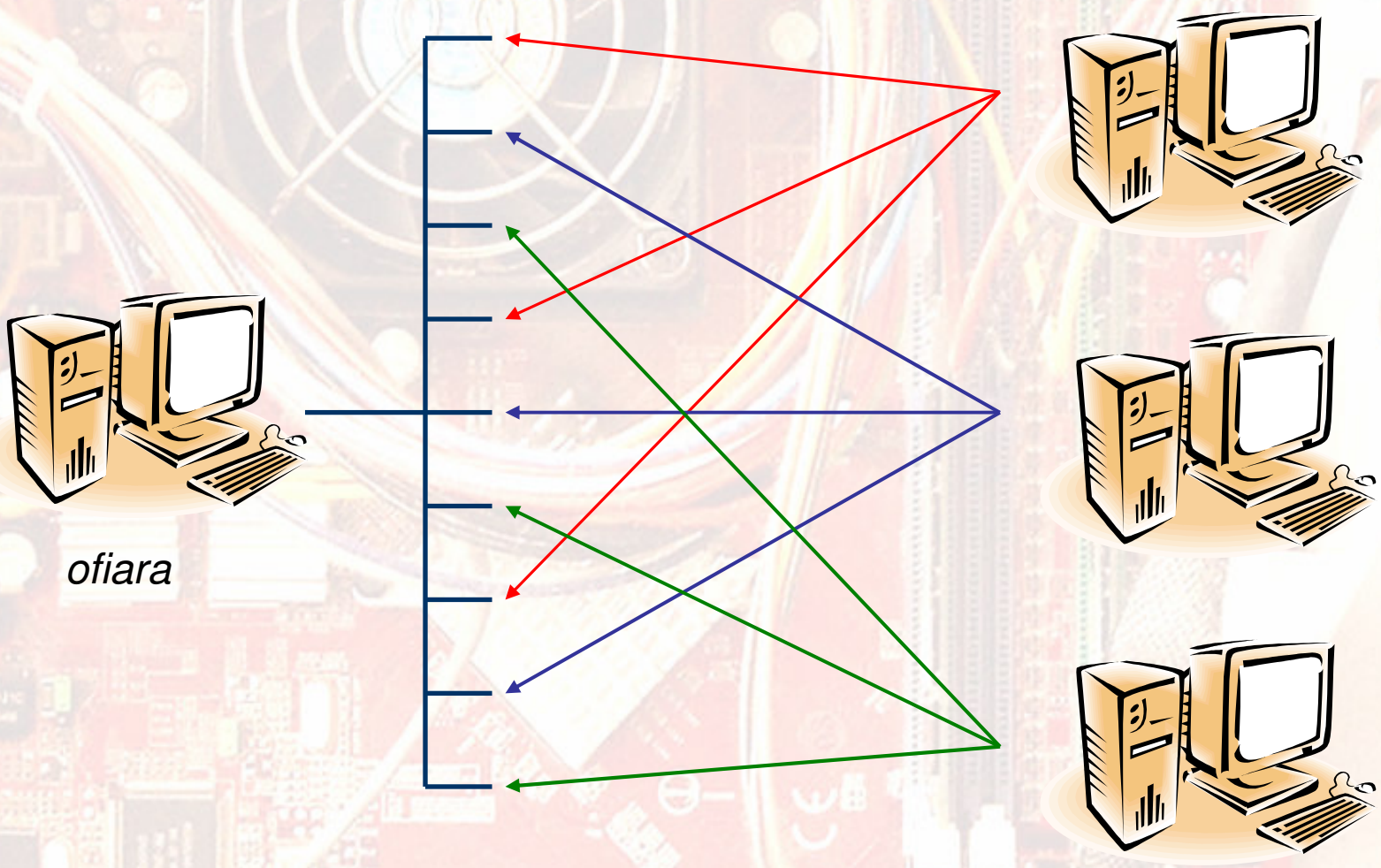
OBSŁUGA SESJI


SYN
SYN,ACK
ACK
…transmisja…
FIN
FIN,ACK
ACK

Atak typu SYNflood - DoS

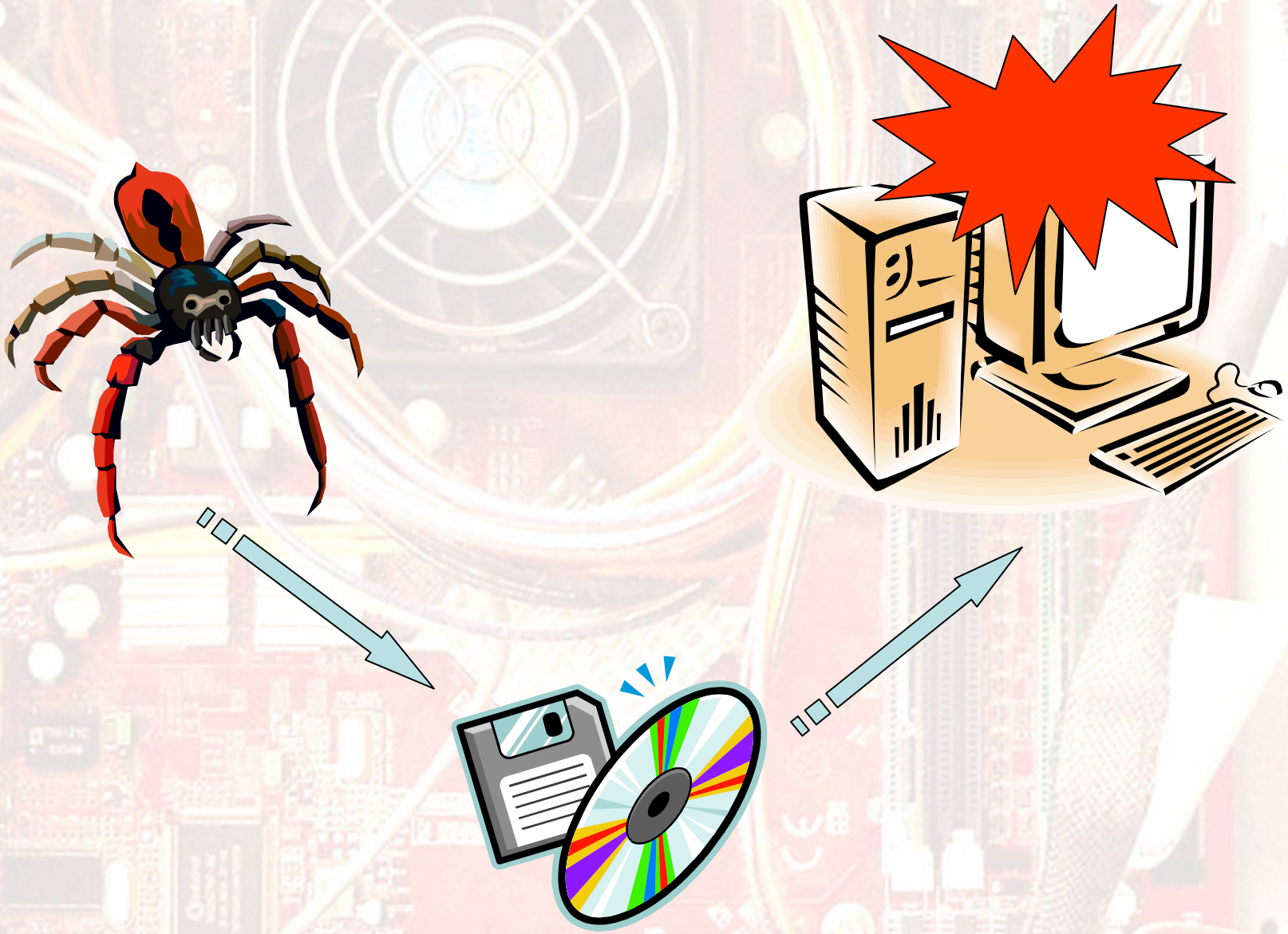


Atak DDoS



ofiara

Wirusy: klasyczne



skanowanie



C:\

D:\



Dokumenty

```
ania@cos.pl
ktostam@server.com
alej@yahoo.fr
wrota@o2.pl
test@maszyna.org
```

KLONY



Wirusy: trojany



wykorzystanie „tylnych drzwi”



przesyłanie danych

Inicjowanie połączeń, dialing



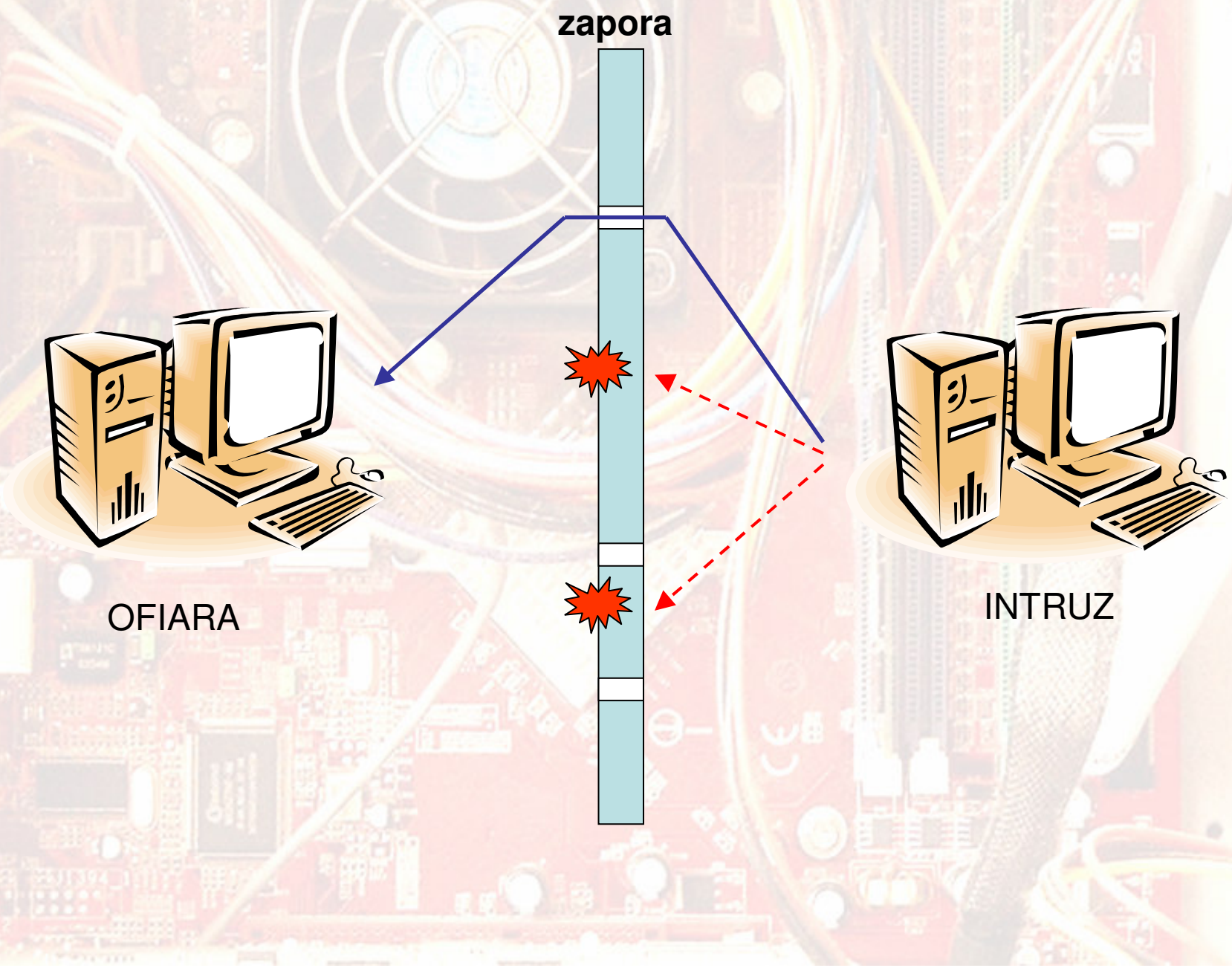


logowanie klawiatury

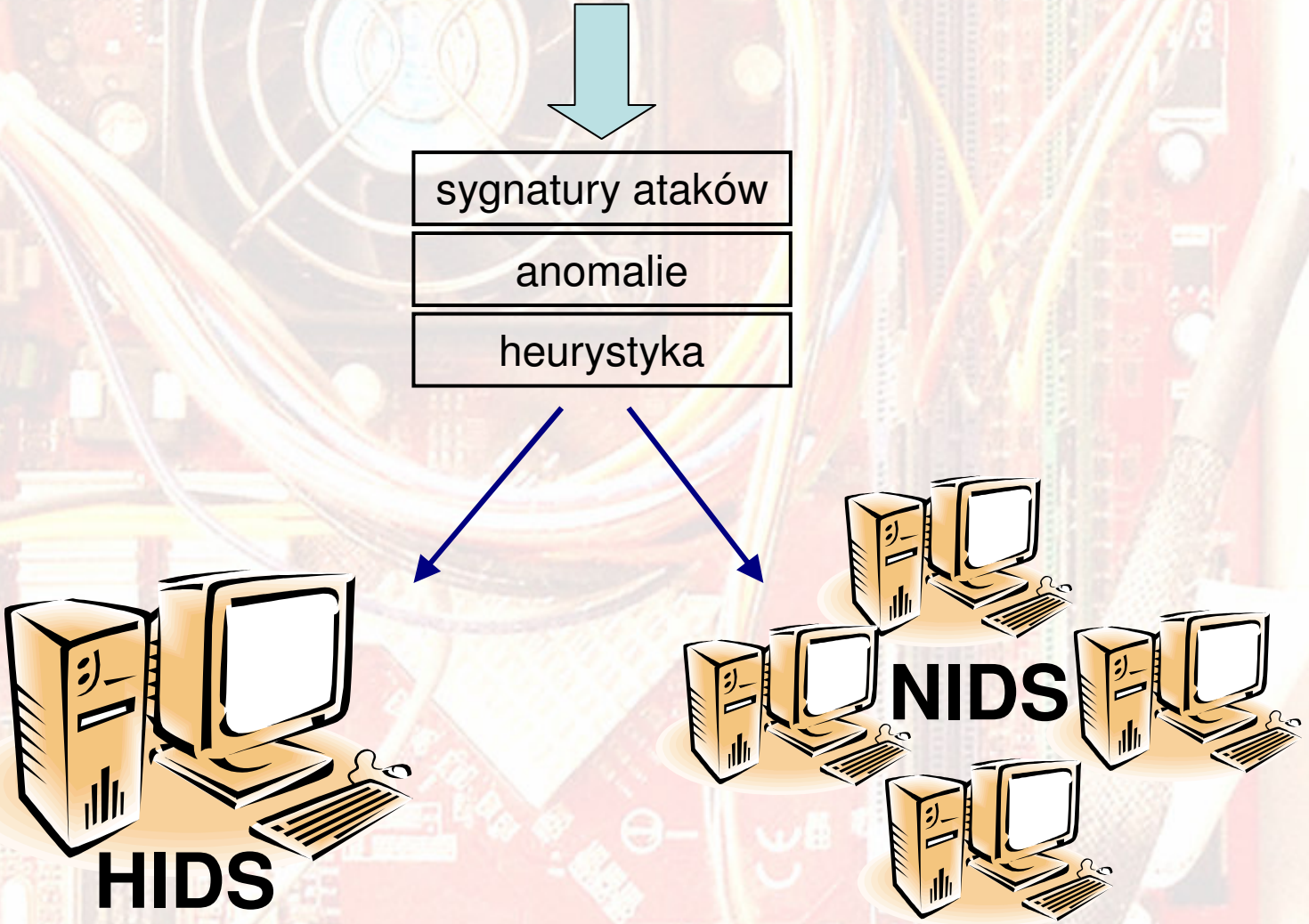
INTRUZ

OFIARA

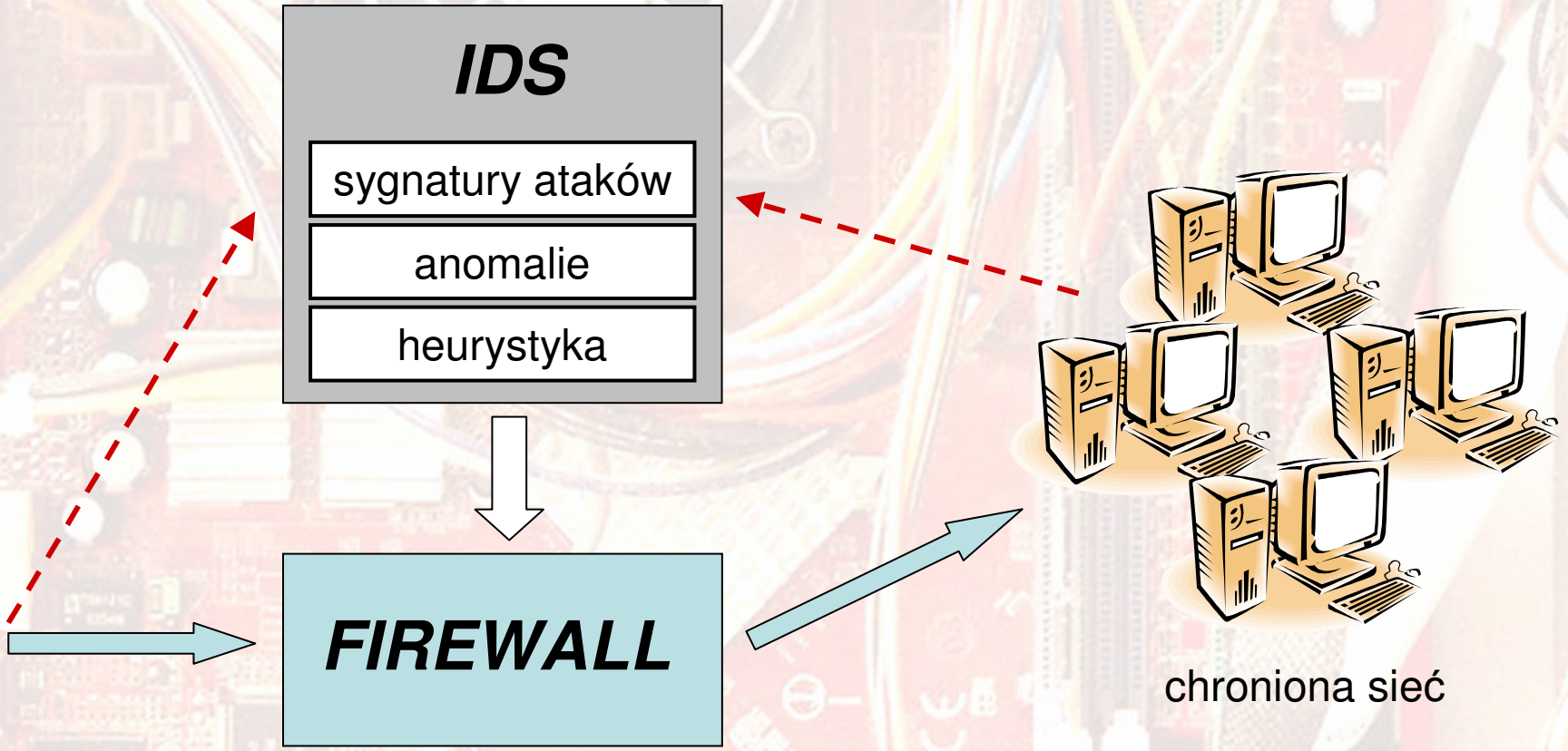
Ochrona: firewall, zapora ogniowa



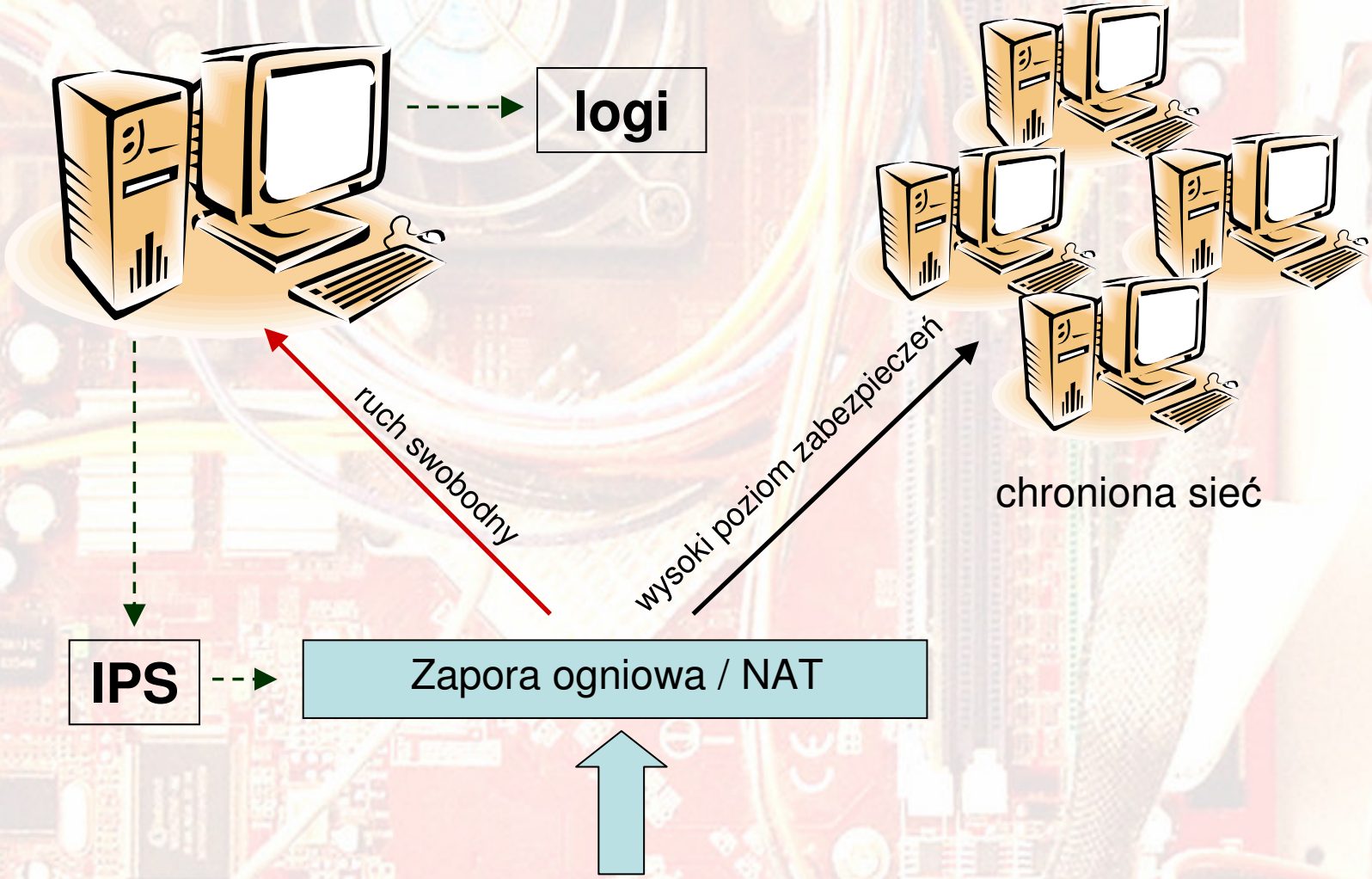
Ochrona: IDS (Intrusion Detection System)



Ochrona: IPS (Intrusion Prevention System)



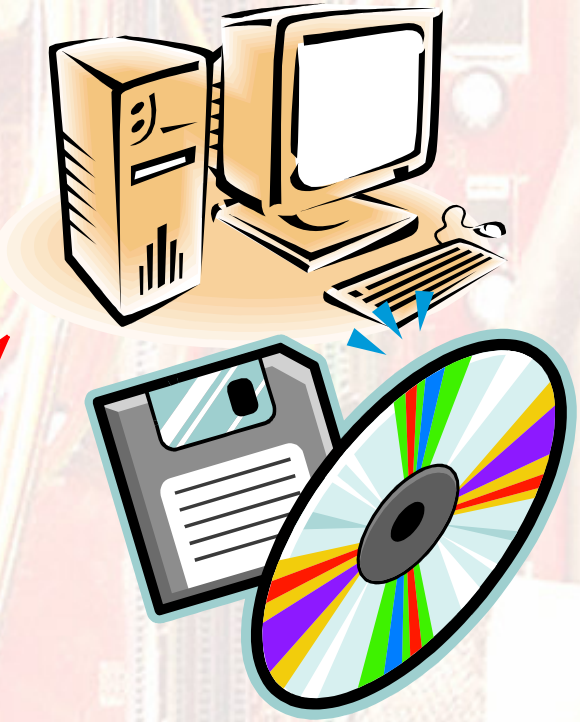
Ochrona: Honeypot – lep na muchy



Ochrona: oprogramowanie antywirusowe (sygnatury)



wyszukiwanie



usunięcie pliku

dezinfekcja

kwarantanna

Ochrona: oprogramowanie antywirusowe (heurystyka)



odwołania do INT13h

modyfikacje tablicy przerwań

zmiany w plikach systemowych

nieautoryzowane łączenia

nieautoryzowane usługi

Ochrona: oprogramowanie antywirusowe (CSI – Code Sequence Identification)

wersja A



wersja B



.....pamięć operacyjna.....

```
push ebx
push esi
push edi
mov cnt, 0
mov ebx, tbl
mov esi, src
lea edi, dst
mov ecx, fl
add ecx, esi
xor eax, eax
jmp lbl3
```

wzorzec

```
push ebx
push esi
push edi
mov cnt, 0
mov ebx, tbl
mov esi, src
lea edi, dst
mov ecx, fl
add ecx, esi
xor eax, eax
jmp lbl3
```



- *osoby **odpowiedzialne** (oficer bezpieczeństwa)*
- *ocena stanu aktualnego*
- *ocena potrzeb i wymaganego **poziomu bezpieczeństwa***
- *program **ochrony informacji** (IA)*
- *wybór architektury, mechanizmów i technologii*
- *opracowanie budżetu*
- *opracowanie mechanizmów **reakcji na incydenty***