Zakład Fizyki Budowli i Komputerowych Metod Projektowania
Instytut Budownictwa
Wydział Budownictwa Lądowego i Wodnego
Politechnika Wrocławska

Technologie informacyjne
- wykład 6 -

Prowadzący: dr inż. Łukasz Nowak , Grzegorz Dmochowski
Konsultacje: Pn C-7 9-11, Nd C-7 11-12,
Piątek, 15-16, s.13 ZOD JG
e-mail: g.dmochowski@pwr.wroc.pl
www: z2.ib.pwr.wroc.pl

Bezpieczeństwo systemów i zestawów informatycznych

- cz. 2 -

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Złośliwe oprogramowanie

ang. *malware* = *malicious* + *software*

Są to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Rodzaje złośliwego oprogramowania 1/9

- **Wirus – program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika. Dzielą się na:**
  - **gnieżdżące się w sektorze rozruchowym twardego dysku (ang. *boot sector viruses*),**
  - **pasożytnicze (ang. *parasitic viruses*),**
  - **wieloczęściowe (ang. *multi-partite viruses*),**
  - **towarzyszące (ang. *companion viruses*),**
  - **makro wirusy (ang. *macro viruses*).**

Wirus albański ☺

Drogi Odbiorco!

Jestem albańskim wirusem komputerowym, ale z uwagi na słabe zaawansowanie informatyczne mojego kraju nie mogę nic ci zrobić. Proszę, skasuj sobie jakiś plik i prześlij mnie dalej.

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Rodzaje złośliwego oprogramowania 2/9

- **Robak – podobne do wirusów, rozmnażające się tylko przez sieć. Nie potrzebują programu "żywiciela". Często powielają się pocztą elektroniczną.**

- **Trojan – nie rozmnaża się jak wirus, ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak**

Rodzaje złośliwego oprogramowania 3/9

- **Backdoor – przejmuje kontrolę nad zainfekowanym komputerem umożliwiając wykonanie na nim czynności administracyjnych łącznie z usuwaniem i zapisem danych, wykonuje zadania wbrew wiedzy i woli ofiary**

- **Wabbit – program rezydentny nie powielający się przez sieć - wynikiem działania jest jedna określona operacja wykonywana w kółko (np. kopiowanie pliku)**

Rodzaje złośliwego oprogramowania 4/9

- **Program szpiegujący (ang. *spyware*) – oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody, takie jak informacje o odwiedzanych witrynach, hasła dostępowe**

- **występuje często jako dodatkowy, ukryty komponent większego programu, odporne na usuwanie i ingerencję użytkownika**
- **mogą zmieniać wpisy do rejestru systemu operacyjnego i ustawienia użytkownika**
- **może pobierać i uruchamiać pliki pobrane z sieci**

Rodzaje złośliwego oprogramowania 5/9

- scumware – żargonowe, zbiorcze określenie oprogramowania, które wykonuje w komputerze niepożądane przez użytkownika czynności.

- stealware/parasiteware - służące do okradania kont internetowych,

- adware - oprogramowanie wyświetlające reklamy,

Rodzaje złośliwego oprogramowania 6/9

- **Hijacker Browser Helper Object - dodatki do przeglądarek, wykonujące operacje bez wiedzy użytkownika.**

- **Exploit – kod umożliwiający bezpośrednie włamanie do komputera ofiary,**

  - **do dokonania zmian lub przejęcia kontroli wykorzystuje się lukę w oprogramowaniu zainstalowanym na atakowanym komputerze.**
  - **mogą być użyte w atakowaniu stron internetowych, systemów operacyjnych lub aplikacji**

Rodzaje złośliwego oprogramowania 7/9

- **Keylogger – odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika**
  - **Istnieją keyloggery występujące w postaci sprzętowej zamiast programowej.**

- **Dialer – programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika, najczęściej są to numery o początku 0-700 lub numery zagraniczne**
  - **szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych ISDN**

Rodzaje złośliwego oprogramowania 8/9

- **Rootkit – jedno z najniebezpieczniejszych narzędzi hackerskich**
  - **ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych**
  - **zostaje wkompilowany lub wstrzyknięty w istotne procedury systemowe**
  - **z reguły jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja**
  - **jego zainstalowanie jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja**

Rodzaje złośliwego oprogramowania 9/9

- **Hoax – fałszywe wiadomości wysyłanymi przez pocztę elektroniczną, które ostrzegają użytkowników przed nieistniejącymi wirusami.**

- **celem jest rozsiewanie plotek, wywołujących panikę i strach wśród adresatów**
- **czasami te powiadomienia zawierają terminy techniczne, aby zmylić użytkowników.**
- **w wielu przypadkach zawierają instrukcję usuwania "wirusa", zalecając usunięcie określonych plików, które zwykle są niezbędne do pracy na komputerze.**
- **odbiorca bywa zachęcany do masowego rozsyłania "ostrzeżenia"**

Co to jest zapora sieciowa?

Zapora sieciowa (ang. *firewall*) to jeden ze sposobów zabezpieczenia sieci i systemów komputerowych przed intruzami.

Może to być:

- **dedykowany sprzęt komputerowy wraz ze specjalnym oprogramowaniem**
- **samo oprogramowanie blokujące niepowołany dostęp do komputera.**

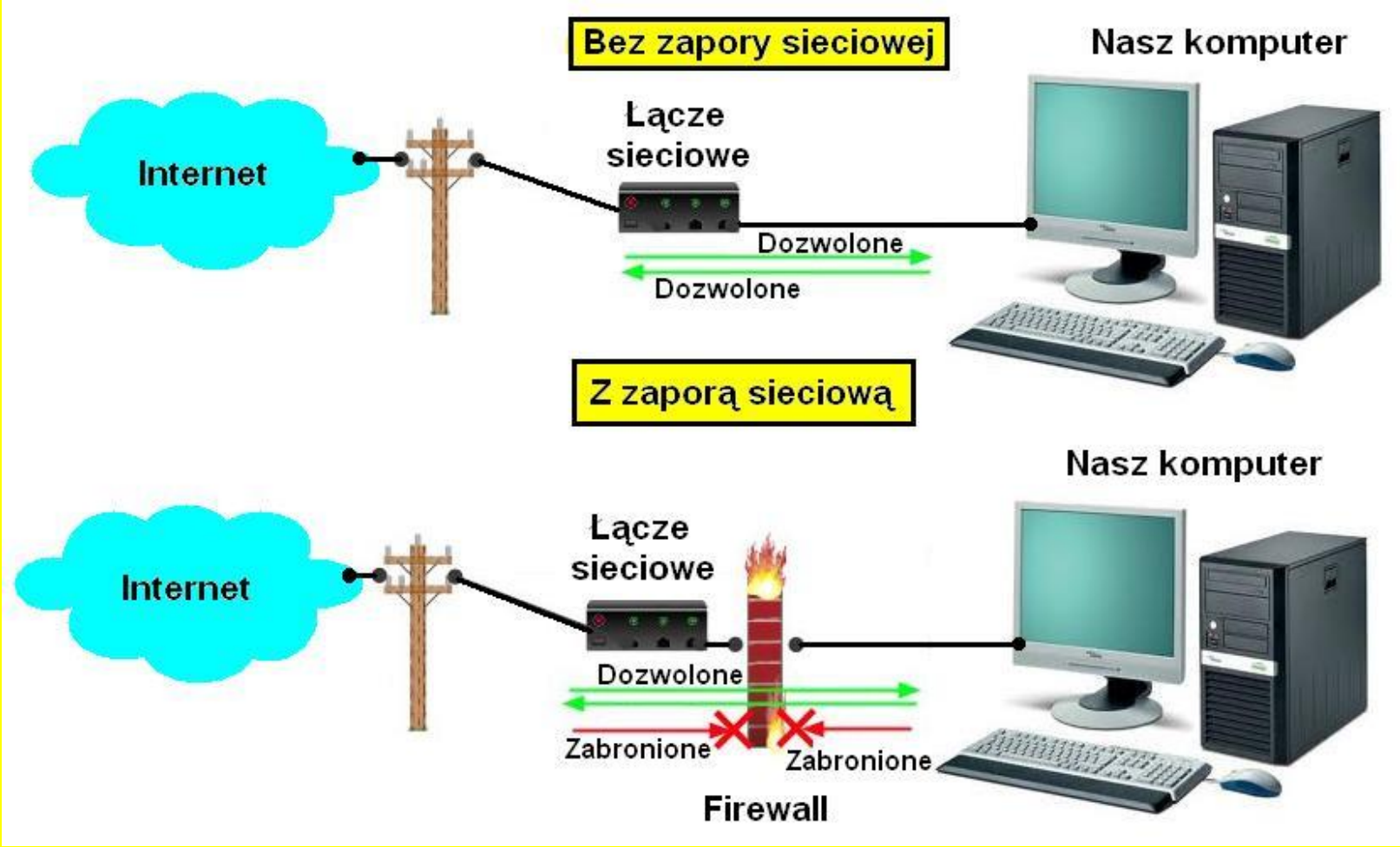
Zadania zapory sieciowej

Podstawowe zadania to:

- **ochrona sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, Internetu,**
- **ochrona przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.**
- **częściowe lub całkowite blokowanie dostępu do określonych miejsc w sieci publicznej**

które odbywają się poprzez filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

Schemat zapory sieciowej



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Zapory sieciowe – mechanizmy działania

- filtrowanie pakietów
- translacja adresów IP
- usługi proxy

Zapory filtrujące 1/2

- monitorują przepływające przez nie pakiety sieciowe i przepuszczają tylko zgodne z regułami ustawionymi na danej zaporze (zapora pracująca dodatkowo jako router)
- w niewielkich sieciach jest zapora sprzętowa bądź wydzielony komputer z systemem operacyjnym Linux - najczęściej wykorzystywana metoda filtrowania w Linuksie to reguły oparte na *iptables* (filtr pakietów)
- np. zapora systemu Windows XP Service Pack 2

Zapory filtrujące 2/2

Zalety

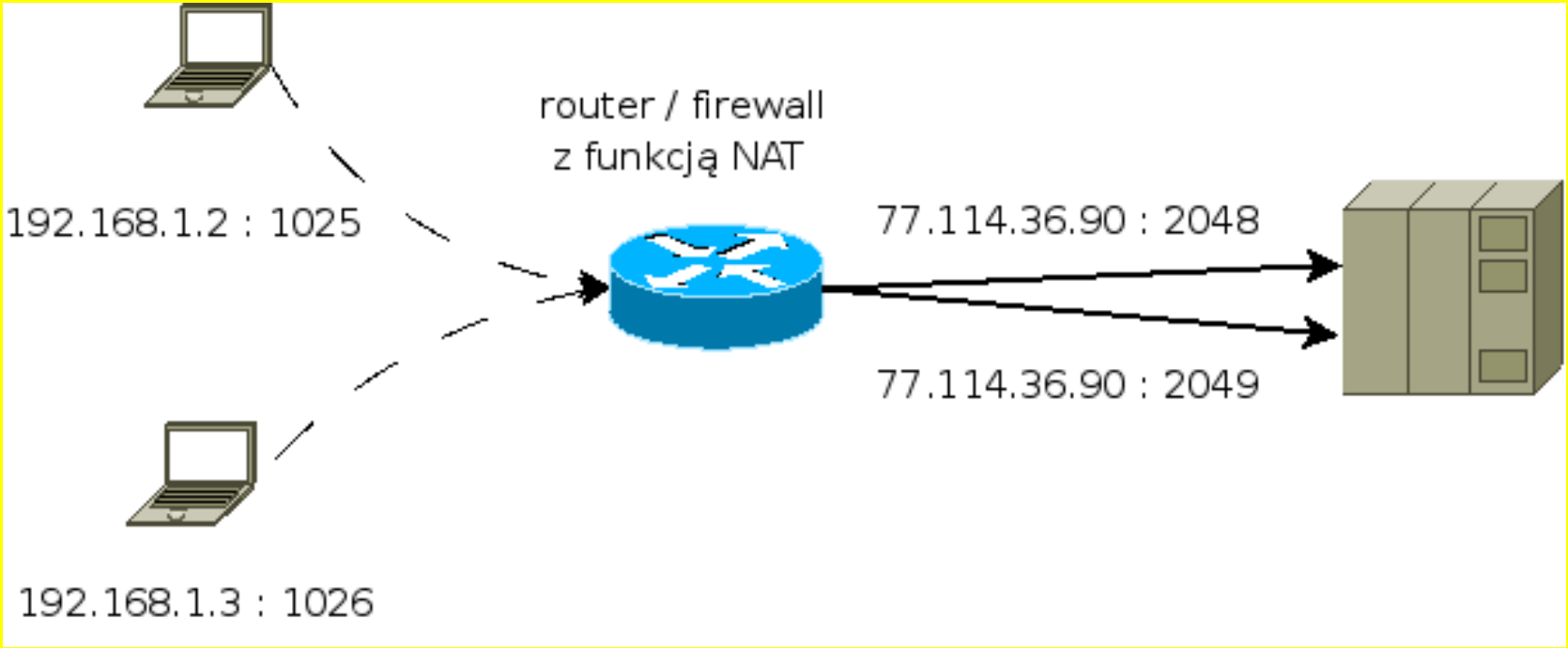
- możliwość zabezpieczenia sieci prywatnej z jednego centralnego punktu
- możliwość wykrycia i odrzucenia nieporządanego ruchu
- możliwość wykrycia spoofingu z sieci lokalnej

Wady

- przygotowanie bardziej rozbudowanej polityki bezpieczeństwa dla zapory nie jest łatwym zadaniem
- dodatkowe zadanie dla routera (przy kilkudziesięciu Mbps ruchu obciążenie jest już zauważalne)
- w przypadku popełnienia błędu w konfiguracji może być trudno go znaleźć

Zapory z translacją adresów sieciowych (*NAT*) 1/4

Translacja adresów



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Zapory z translacją adresów sieciowych (*NAT*) 2/4

- ang. *network address translation* - polega na dokonywaniu zamiany adresu IP hosta wewnętrznego w celu ukrycia go przed zewnętrznym monitorowaniem (inaczej maskowanie adresu IP)
- możliwa większa anonimowość (serwery nie mogą zidentyfikować konkretnego hosta po samym adresie IP)
- możliwość dostępu do Internetu dla większej ilości komputerów niż ilość dostępnych publicznych adresów IP
- np. iptables (Linux), software do Livebox'a (TP S.A.)

Zapory z translacją adresów sieciowych (*NAT*) 3/4

Wyróżniamy dwie metody działania translacji adresów NAT:

- **statyczna – dla każdego adresu sieci prywatnej przydzielony jest konkretny adres sieci publicznej**
- **dynamiczna – dla grupy adresów, lub dla całej sieci prywatnej przydzielony jest jeden lub więcej adres publiczny.**

Zapory z translacją adresów sieciowych (*NAT*) 4/4

Zalety

- możliwość zbudowania rozległej sieci, posiadając ograniczoną ilość publicznych adresów IP
- oszczędność publicznych klas adresowych (RIPE bardzo niechętnie rozdaje adresy IP, providerzy podobnie)

Wady

- NAT może być problemem jeśli chcemy korzystać z IPsec, ponieważ nagłówek może być szyfrowany i/lub sprawdzana jest jego suma kontrolna
- w przypadku bardziej skomplikowanych protokołów (np. FTP) NAT musi go rozumieć, aby prawidłowo tłumaczyć ukryte w nich adresy IP

Zapory pośredniczące (*proxy*)

- **wykonują połączenie z serwerem w imieniu użytkownika**
- **zamiast uruchomienia sesji http:// bezpośrednio do zdalnego serwera WWW, uruchamiana jest sesja z zaporą i dopiero stamtąd uruchamiane jest połączenie z systemem zdalnym - cała komunikacja na serwer http przechodzi przez proxy, które może filtrować ruch**
- **zabezpieczające działanie zapory polega na blokowaniu wybranej treści (ang. *content filtering*), aby nie dotarła ona do klienta**
- **np. TIS Internet Firewall Toolkit, SOCKS, Microsoft Internet Information Server, Netscape Commerce Server**

Darmowe firewall’e (freeware)

- PC Tools Firewall Plus Free Edition

- ZoneAlarm Free Firewall

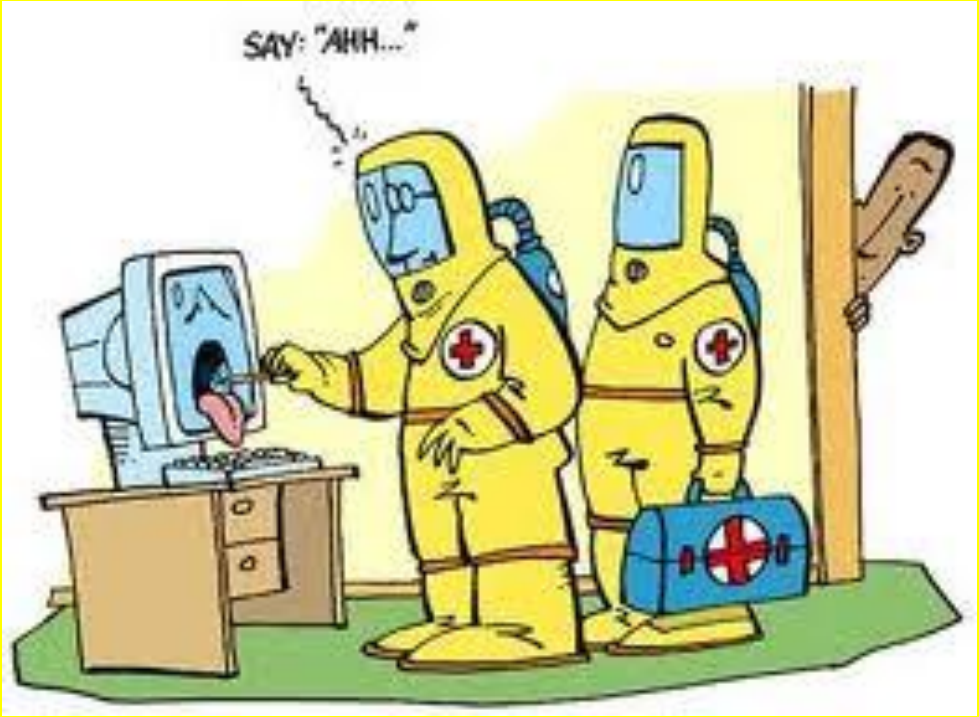
- Comodo Internet Security

- SyGate

- Zapora systemowa Windows

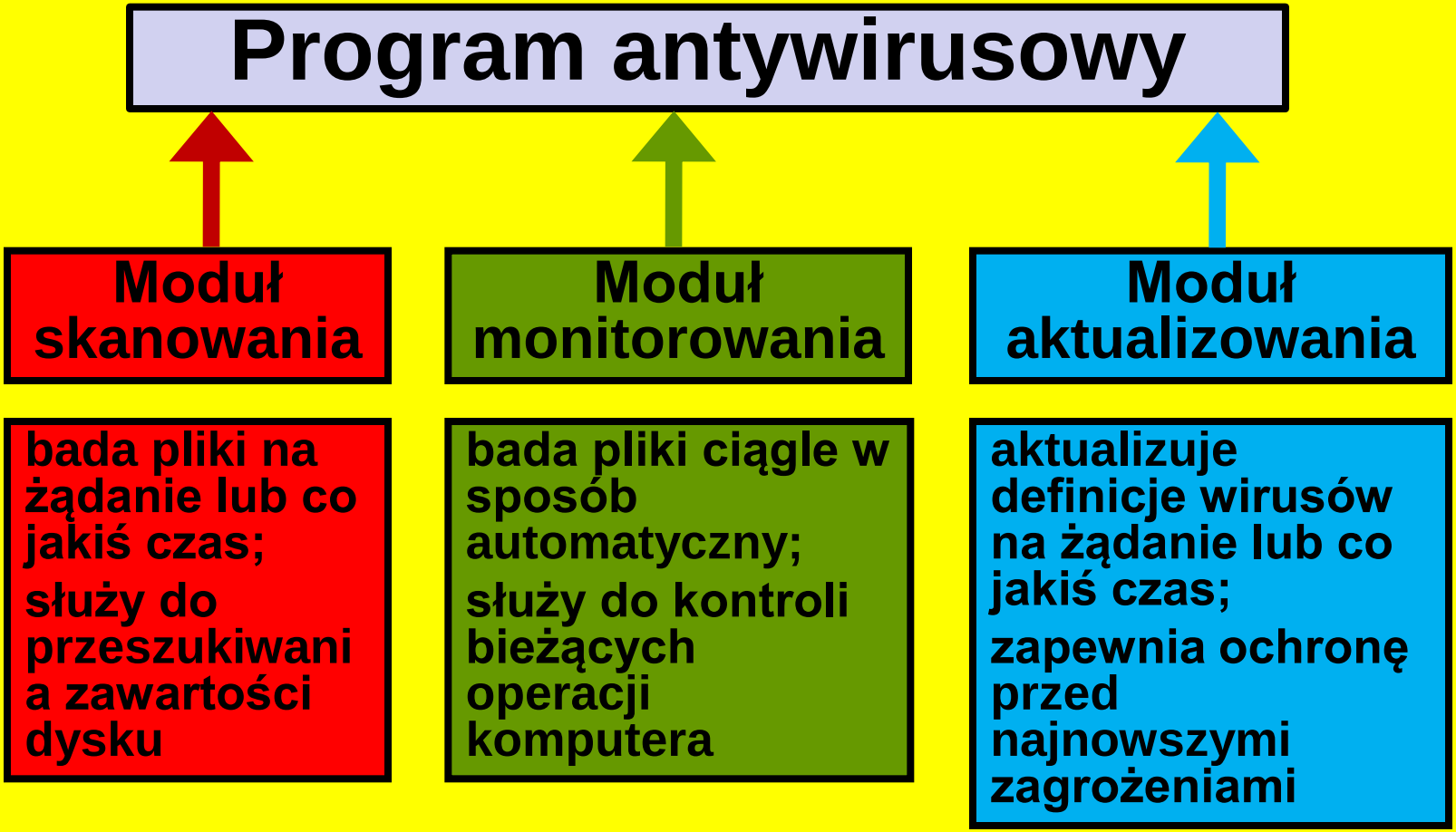
Program antywirusowy

Program antywirusowy jest to program, którego celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Program antywirusowy - budowa



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Program antywirusowy - moduły

Skanery

- najstarszy i najprostszy sposób ochrony antywirusowej
- ich działanie polega na wyszukiwaniu określonej sekwencji bajtów w ciągu danych (tzw. sygnatury wirusa), dzięki której możliwe jest odnalezienie wirusa w pamięci lub w zarażonej ofierze
- skuteczność skanera antywirusowego zależy od charakterystyczności tej sekwencji (bardzo specyficznego napisu lub ciągu bajtów)
- wraz z pojawieniem się wirusów polimorficznych (ich różne próbki nie wyglądają tak samo) znaczenie skanerów trochę zmalało, jednak nadal jest to najważniejsza metoda walki z wirusami

Program antywirusowy - moduły

Monitory

- zainstalowany jest jako TSR (ang. *Terminate and Stay Resident*) lub sterownik SYS, który – poprzez monitorowanie odpowiednich funkcji DOS i BIOS – pozwala na wykrywanie wszystkich wykonywanych za pomocą tych funkcji odwołań do dysków
- to, czy monitor będzie działał prawidłowo zależy często od momentu, w którym przejął on kontrolę nad systemem (przed działaniem wirusa czy po)
- dużą wadą jest to, że powodują czasami fałszywe alarmy - użytkownik po kolejnym potwierdzeniu jakiejś zwykłej operacji dyskowej staje się mniej uważny a nawet usuwa program antywirusowy z pamięci

Program antywirusowy - moduły

Programy autoweryfikujące

- służą do sprawdzania czy dany program nie został w jakiś sposób zmieniony przez wirusa.
- sprawdzanie to jest możliwe poprzez dodanie do wskazanego pliku określonego, krótkiego programu - dodawany kod dopisuje się do pliku wykorzystując te same mechanizmy co wirusy i pozwala na autoweryfikację
- programy tego typu najczęściej nie są odporne na technikę ukrywania kodu wirusa *stealth* i w systemie zainfekowanym przez wirusa używającego tej techniki okażą się całkowicie nieefektywne

Program antywirusowy - moduły

Programy zliczające sumy kontrolne

- polega na obliczaniu odpowiednich sum kontrolnych (ang. *checksum*) dla żądanego pliku lub plików za pomocą określonych algorytmów
- zliczane sumy kontrolne są przechowywane w osobnych plikach, tworzonych po pierwszym uruchomieniu programu
- ogromną wadą jest to, że pliki przechowujące obliczone sumy kontrolne nie są wcale chronione (niektóre wirusy potrafią zarazić określony plik i obliczyć dla niego nową sumę kontrolną)

Program antywirusowy - moduły

Szczepionki

- programy skierowane przeciwko konkretnym wirusom
- po odpowiedniej analizie kodu wirusa można zdefiniować tzw. sygnatury i wykrywa się kolejne kopie wirusa, a nawet czasami na wyleczenia plików
- szczepionki to zwykle rozbudowane programy, które potrafią wykryć i usunąć kilka tysięcy określonych wirusów
- dla nowych wirusów szczepionki nie są efektywne

Darmowe antywirusy (freeware)

- AVG Anti-Virus Free

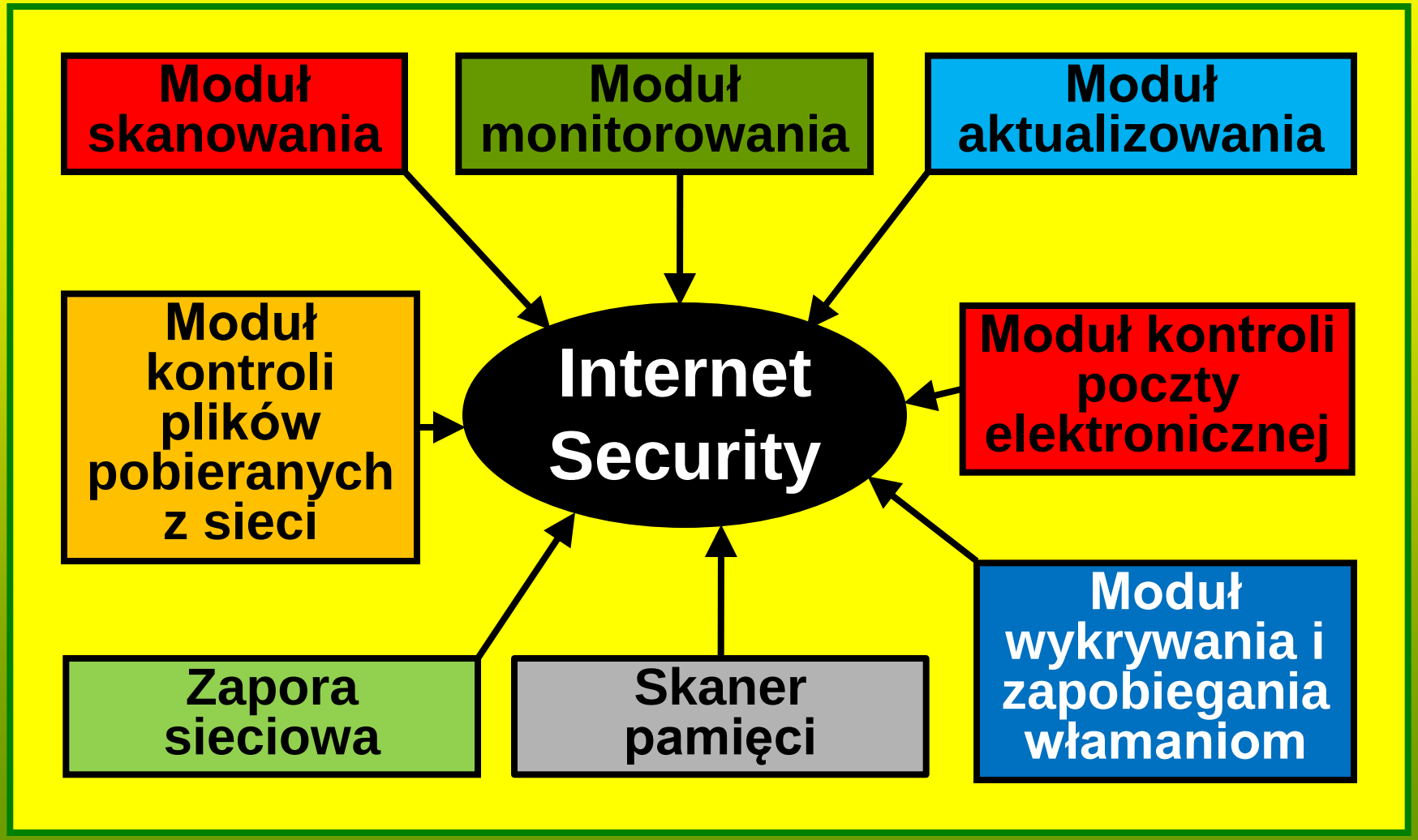
- avast! Free Antivirus

- Avira AntiVir Presonal

- Panda Cloud Antivirus

- Comodo Antivirus

Programy Internet Security



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Przykłady programów typu Internet Security

- Norton Internet Security
- Kaspersky Internet Security
- Avast Internet Security
- Comodo Internet Security
- AVG Internet Security

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Zasady bezpiecznego korzystania z komputera i internetu 1/3

- instalacja oprogramowania antywirusowego,
- włączona zapora sieciowa (firewall) z modułem HIPS (np. DefenseWall HIPS), która zapobiega włączeniu zagrożeń typu zero day,
- aktualizacje oprogramowania,
- nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia,

Zasady bezpiecznego korzystania z komputera i internetu 2/3

- **nieinstalowanie oprogramowania „niewymaganego” (np. toolbar’y, screensaver’y),**
- **czytanie okien instalacyjnych aplikacji, a także ich licencji,**
- **wyłączenie makr w plikach MS Office nieznanego pochodzenia,**
- **regularne całościowe skany systemu programem antywirusowym i antymalware,**

Zasady bezpiecznego korzystania z komputera i internetu 3/3

- **przy płatnościach drogą elektroniczną upewnienie się, że transmisja danych będzie szyfrowana (banking mode),**

- **użytkowanie środowisk systemów operacyjnych niepodatnych lub mało podatnych na złośliwe oprogramowanie (np. systemy UNIX, GNU/Linux, MacOS X).**

Dziękuję za uwagę

Zakład Fizyki Budowli i Komputerowych Metod Projektowania
Instytut Budownictwa
Wydział Budownictwa Lądowego i Wodnego
Politechnika Wrocławska

Technologie informacyjne
- wykład 6 -

Prowadzący: dr inż. Łukasz Nowak, Grzegorz Dmochowski
Konsultacje: Pn C-7 9-11, Nd C-7 11-12,
Piątek, 15-16, s.13 ZOD JG
e-mail: g.dmochowski@pwr.wroc.pl
www: z2.ib.pwr.wroc.pl