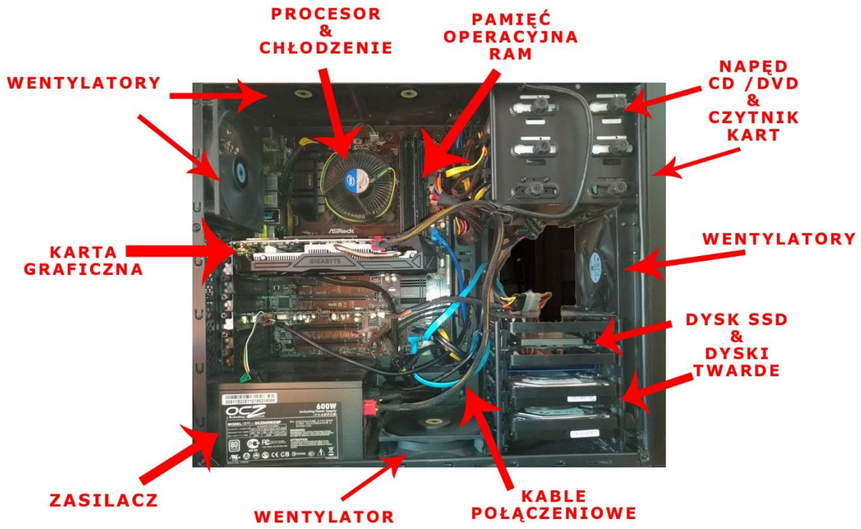
Zestaw komputerowy

Dane wejściowe to te, które są przekazywane do systemu, a dane wyjściowe to te, które z systemu są wysyłane.

Urządzenia wejścia:

- klawiatura,
- mysz komputerowa,
- kamera internetowa,
- mikrofon.



Urządzenia wyjścia:

- monitor,
- drukarka,
- głośniki,
- słuchawki.

Jednostka centralna

- płyta główna, procesor, pamięć RAM, zasilacz, pamięć masowa, karta graficzna etc.

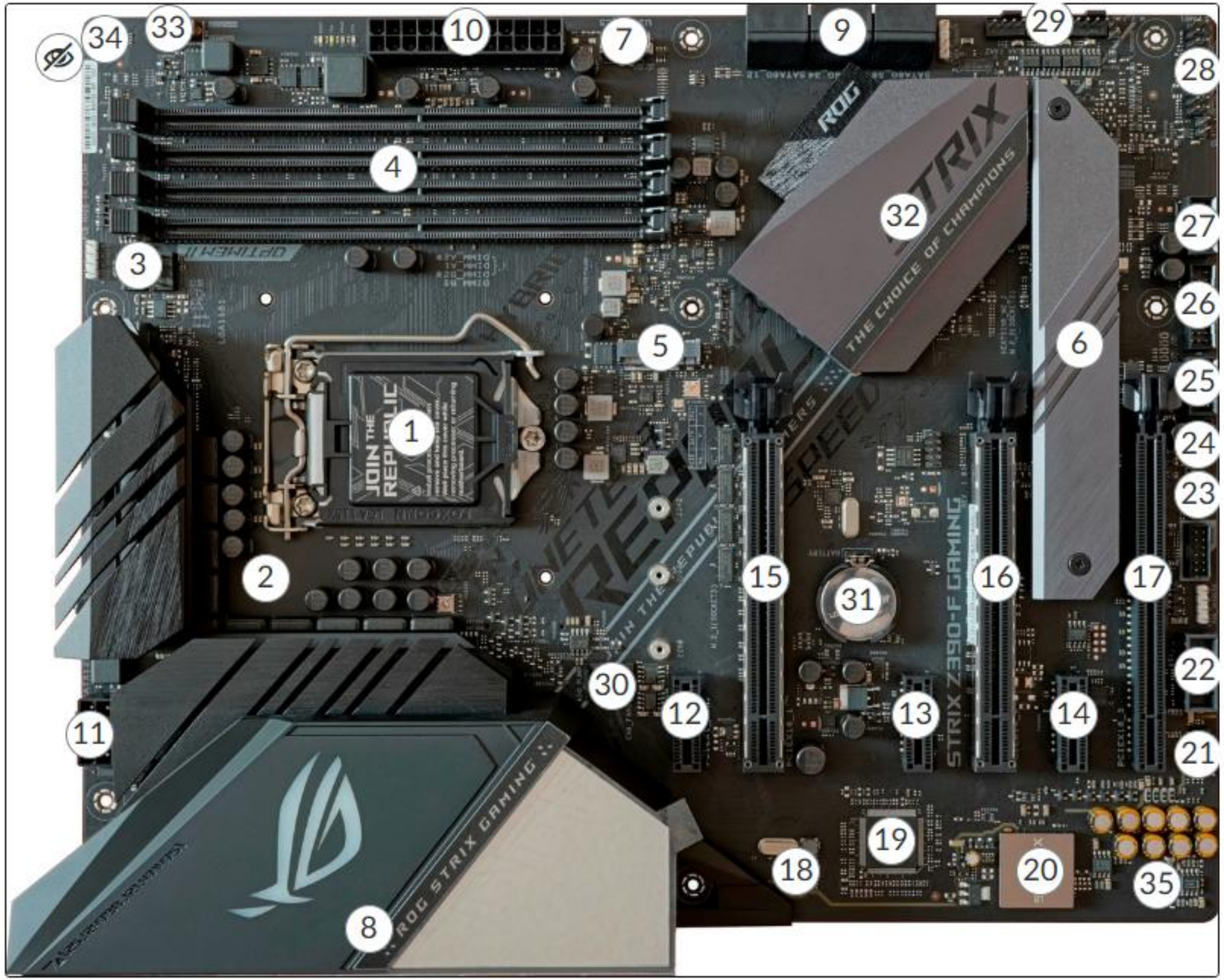
Płyta główna

Najważniejszy moduł komputera.

Magistrala – zestaw przewodów, łączący różne elementy systemu (procesor, pamięć, urządzenia wejścia/wyjścia).

Wyróżniamy:
Magistralę danych, adresową oraz sterującą.

Magistrala danych - przesyła dane użytkowe pomiędzy urządzeniami komputera;
Magistrala adresowa - nazywana szyną adresową, wskazuje urządzenia lub komórki pamięci, z których, lub do których będą przesyłane dane;
Magistrala sterująca – nazywana szyną sterującą, określa, czy dane są zapisywane, czy odczytywane z urządzeń lub komórek pamięci.



1. Gniazdo CPU
2. Mocowanie chłodzenia CPU
3. Złącza wentylatora CPU
4. Złącza pamięci typu DIMM x4 – pamięć RAM
5. Złącze M.2 – dysk SSD
6. Złącza M.2
7. USB
8. Złącza do podłączenia do urządzeń peryferyjnych
9. Złącza SATA
10. Złącze zasilacza 24-pinowe
11. Złącze zasilacza 8-pinowe
12. 13, 14, 15, 16, 17 - PCI Express – złącze do kart zewnętrznych np. graficznych.
18. Zintegrowana karta sieciowa
19. Układ Super I/O
20. Układ dźwiękowy audio
21. Złącza audio panelu przedniego
22. Złącze portu szeregowego
23. Złącze modułu TPM
24. Dodatkowe złącza wentylatora CPU i pompy chłodzenia wodnego AiO
25. Złacze USB 2.0
26. Złacze USB 3.1
27. Złacze USB 2.0
28. Złącze panelu przedniego (do podłączenia diod, resetu, zasilania)
29. 30 Złącza wentylatora CPU i pompy chłodzenia wodnego AiO
31. Bateria pamięci CMOS (NVRAM)
32. Chipset Intel
33. Przycisk MEMOK


ROG STRIX GAMING
JOIN THE REPUBLIC
Install processor first then remove and keep the cover. We'll place this cover while removing processor or returning motherboard.
LGA1151
STRIX Z390-F GAMING
THE CHOICE OF CHAMPIONS
ROG
STRIX
SupremeFX
nuvoton

Procesor

Procesor – CPU (ang. Central Processing Unit)

Cyfrowy układ scalony, pobierający dane z pamięci i wykonujący wszystkie obliczenia.

Zadania Procesora:
Wykonywanie poleceń programów;
Przetwarzanie danych;
Kontrola pracy innych podzespołów.

Podstawowe parametry jakimi opisywane są procesory to:
Liczba rdzeni - każdy rdzeń wykonuje zadania niezależnie. Im więcej rdzeni tym szybszy procesor
Częstotliwość taktowania,
Rozmiar cache (pamięci podręcznej) - szybka pamięć w procesorze.

Procesor

Taktowanie – czyli jak szybko procesor wykonuje instrukcje.

Taktowanie mierzone w hercach – Hz, gdzie:
1 Hz = 1 cykl na sekundę;
1 GHz = 1 miliard cykli na sekundę.

Procesor działa w rytmie cykli zegara.
W każdym cyklu może wykonać część instrukcji lub przygotować się do następnej.

Czyli Taktowanie (Hz) mówi, ile cykli wykona procesor w ciągu sekundy.

Pamięć

Pamięć operacyjna:

ROM – pamięć stała, umieszczona na płycie głównej. Zapis wszystkiego co komputer „umie” po włączeniu zasilania.

RAM – pamięć o swobodnym dostępie, która przechowuje aktualnie wykonywane zadania wraz z danymi. Resetuje się po wyłączeniu zasilania.

Pamięć

Pamięć zewnętrzna:

Pamięci zewnętrzne służą do przechowywania dużych ilości danych i programów. Są to wszelkiego rodzaju nośniki danych. Po wyłączeniu komputera pamięć zewnętrzna nie traci swej zawartości i po ponownym włączeniu można z niej odczytać dane.

Do pamięci zewnętrznych możemy zaliczyć:

Dyski twarde HDD - urządzenia pamięci z krążkami pokrytymi warstwą magnetyczną.
Nośniki optyczne - płyty CD, DVD.
Pendrive'y - urządzenia przenośne, nazywane również pamięciami flash , które podłączamy do portu USB.
Dyski SSD - podobne w konstrukcji jak pendrive'y, ale o większej pojemności, stosowane są w komputerach jako dyski twarde.

Gniazda i złącza

Wyróżniamy:

D-SUB (VGA) - tandardowe złącze analogowe sygnału wideo

DVI - Służy do wysyłania sygnału wideo, zarówno cyfrowego, jak i analogowego (w zależności od typu DVI).

HDMI - multimedialne złącze cyfrowe stosowane nie tylko w kartach graficznych komputerów, ale również szeroko wykorzystywane w wielu urządzeniach codziennego użytku.

USB typu C

USB 3.1

RJ – 45 - typ złącza stosowany do połączenia komputera z siecią internetową za pomocą kabla sieciowego

Jack - złącze transmitujące sygnały analogowe, wykorzystywane głównie do połączeń audio.

DisplayPort - następca HDMI, umożliwia przesyłanie wysokiej jakości obrazu oraz dźwięku z komputera.

Rys. 1.1. Model systemu komputerowego

System komputerowy

układ współdziałających ze sobą (według pewnych zasad) dwóch składowych: sprzętu komputerowego (hardware) oraz oprogramowania (software).

Warstwy systemu komputerowego:

- warstwa sprzętowa
- system operacyjny
- programy narzędziowe
- programy użytkowe
- użytkownicy

Zanim załaduje się system operacyjny

BIOS

zapisany w pamięci stałej zestaw podstawowych procedur pośredniczących pomiędzy systemem operacyjnym, a sprzętem. Jest on integralną częścią każdej płyty i nie może być wymieniany pomiędzy innymi różnymi płytami.

Zadania Biosu:

- przeprowadzenie po restarcie testów podstawowych układów urządzeń systemów zwanych autotestem po włączeniu zasilania (POST)
- inicjalizacja pracy systemów
- zapewnienie w postaci programów obsługi przerwań, procedur obsługi, podstawowych i standardowych urządzeń systemu
- niwelacja z punktu widzenia systemu operacyjnego, różnic konstrukcyjnych.

Wejście do BIOSu odbywa się poprzez naciśnięcie odpowiedniego klawisza tuż po włączeniu komputera - przed włączeniem systemu Windows.

Zanim załaduje się system operacyjny

UEFI

interfejs pomiędzy systemem operacyjnym, a oprogramowaniem. Jest on następcą BIOSu w komputerach osobistych. Został opracowany przez firmę Intel.

Kluczowe cechy i zalety UEFI:

- Szybszy rozruch: Uruchamia system operacyjny znacznie szybciej niż tradycyjny BIOS.
- Wsparcie dla dużych dysków: Potrafi obsługiwać dyski twarde o pojemności większej niż 2 terabajty.
- Bezpieczne uruchamianie (Secure Boot): Funkcja zabezpieczająca, która zapobiega uruchomieniu złośliwego oprogramowania.
- Graficzny interfejs użytkownika: Zapewnia bardziej przyjazny i intuicyjny interfejs, często sterowany myszą.
- Rozszerzalność i elastyczność: Pozwala na łatwiejsze aktualizacje i modyfikacje firmware.
- Zarządzanie energią: Umożliwia optymalizację zużycia energii i konfigurację zachowania komputera po utracie zasilania.

System operacyjny

System operacyjny - podstawowe oprogramowanie komputera (lub telefonu, konsoli, tabletu itd.), które zarządza całym sprzętem i umożliwia uruchamianie innych programów.

Zadania systemu operacyjnego

Komunikacja z użytkownikiem

- Wyświetlanie okien, ikon, menu;
- Umożliwienie obsługi komputera.

Zarządzanie danymi

- Tworzenie, przechowywanie, kopiowanie, przenoszenie, kasowanie plików.

Zarządzanie procesami

- planowanie oraz przydział czasu procesora
- kontrola i przydział pamięci operacyjnej

Zarządzanie sprzętem

- Obsługa urządzeń wejścia/wyjścia (klawiatura, mysz, drukarka, mikrofon);
- Optymalizacja pracy sprzętu.

Warstwy systemu operacyjnego

Przyjmuję się podział na trzy główne elementy budowy systemu operacyjnego:

Jądro (ang. Kernel)

jest to warstwa odpowiedzialna za wykonywanie podstawowych zadań systemu operacyjnego, tj. zarządza pamięcią, procesami, urządzeniami i plikami.;

Powłoka (shell)

jest to specjalny program służący do komunikacji użytkownika z systemem operacyjnym;

system plików

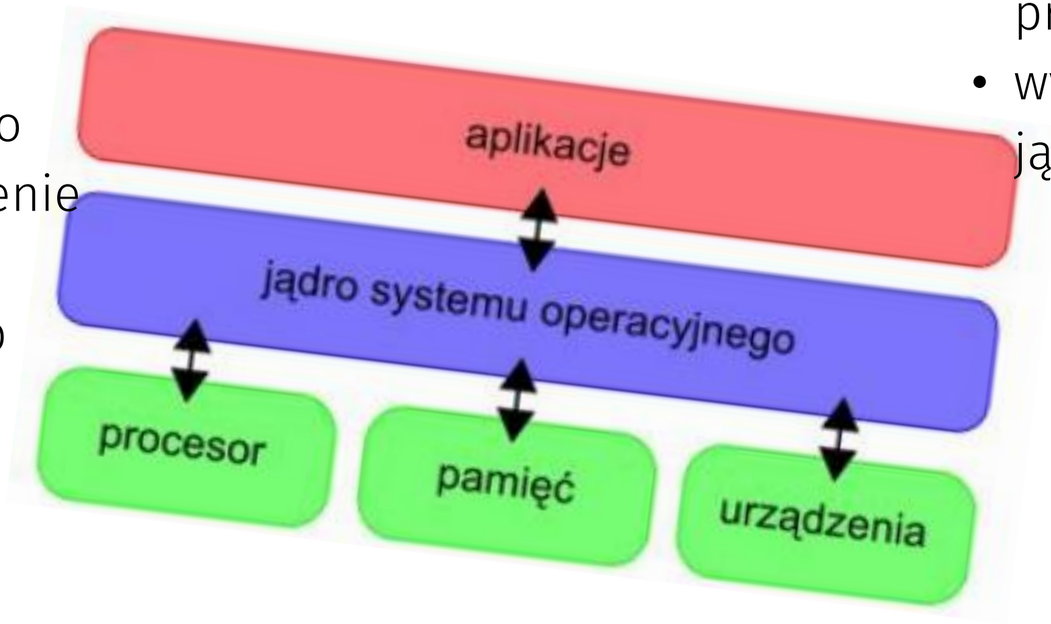
jest to warstwa odpowiedzialna za sposób organizacji danych na nośniku.

Cechy jądra systemu operacyjnego:

- wielozadaniowość (możliwość równoczesnego uruchamiania wielu procesów)
- wielowątkowość (wykonywanie wielu niezależnych wątków w ramach jednego procesu)
- wywłaszczalność (zdolność jądra do wstrzymania aktualnie wykonywanego zadania, aby umożliwić przeprowadzenie innego zadania)
- skalowalność (możliwość rozwoju lub miniaturyzacji sprzętu)

Zadania jądra systemu:

- przydział czasu procesora
- przydział obszarów pamięci
- obsługa plików



Zadania powłoki

- zgłoszenie gotowości systemu
- pośredniczenie między jądrem, a użytkownikiem
- analiza poleceń i zlecenie jądru uruchomionego programu użytkowego
- wyświetlenie odpowiedzi jądra

System operacyjny	Opis	Języki użyte do budowy
Windows	Najpopularniejszy na PC, używany w biurach i grach.	C, C++, C#
Linux	Darmowy, otwarto-źródłowy, stosowany na serwerach i komputerach	C, asembler
macOS	System Apple dla komputerów Mac, stabilny i zintegrowany ze sprzętem.	Objective-C, Swift, C
Android	Mobilny system Google (telefony, tablety, TV).	Java, Kotlin, C, C++
iOS	Mobilny system Apple dla iPhone/iPad.	Objective-C, Swift, C
Unix	Starszy, stabilny system, baza dla innych SO	
CChrome OS	Lekki system oparty na przeglądarce, dla laptopów	C, C++, JavaScript

Windows

Zalety

- Wydajny system z szerokim wsparciem dla oprogramowania i gier.
- Intuicyjny interfejs graficzny, ułatwiający obsługę nawet mniej zaawansowanym użytkownikom.
- Regularne aktualizacje poprawiające bezpieczeństwo i funkcjonalność.
- Duża społeczność użytkowników i dostęp do wsparcia technicznego.

Wady

- Płatny
- Wymaga mocnego sprzętu
- Mniej stabilny niż Linux
- Mniejsza możliwość personalizacji w porównaniu z Linuxem

Linux

Zalety

- Otwarte systemy pozwalają na modyfikację kodu źródłowego.
- Zoptymalizowany system działający efektywnie nawet na starszym sprzęcie.
- Wysoka odporność na wirusy i ataki.
- Duże możliwości personalizacji i konfiguracji.

Wady

- Mniejsza dostępność niektórych programów komercyjnych.
- Wyższy próg wejścia dla nowych użytkowników.
- Ograniczone wsparcie dla niektórych urządzeń peryferyjnych.

macOS

Zalety

- Elegancki interfejs z intuicyjną nawigacją.
- Wysoka wydajność i stabilność działania.
- Doskonała integracja z innymi urządzeniami Apple.

Wady

- Dostępny tylko na sprzęcie Apple, który jest droższy.
- Ograniczona kompatybilność z niektórymi aplikacjami i grami.
- Mniejsze możliwości personalizacji w porównaniu z Linuxem.

iOS vs. Android

iOS

- Stabilny i szybki
- Regularne aktualizacje
- Bardzo bezpieczny
- Spójny ekosystem Apple
- Łatwy w obsłudze

- Tylko na iPhone/iPad
- Drogi sprzęt
- Mała personalizacja
- Mniej aplikacji darmowych niż Android

Android

- Darmowy
- Ogromna liczba aplikacji
- Działa na wielu urządzeniach
- Możliwość modyfikacji
- Obsługa kart pamięci i wielu standardów

- Fragmentacja (różne wersje na różnych telefonach)
- Reklamy i złośliwe aplikacje
- Często wolniejsze aktualizacje
- Może zwalniać po czasie

Podział programów komputerowych

Języki programowania

- Narzędzie pozwalające formułować instrukcje dla komputera, określając jakie zadania ma wykonać. Jest to system reguł, który definiuje sposób tworzenia programów, zarówno pod kątem logicznej struktury (semantyka), jak i ich pisowni (składnia).

- Python, C++, Java, JavaScript, C#, SQL

Programy użytkowe

- Programy służące do wykonywania konkretnych zadań dla użytkownika. Do kategorii tej zaliczają się programy biurowe (edytory tekstu, arkusze kalkulacyjne), programy graficzne, przeglądarki internetowe, odtwarzacze multimediów, aplikacje komunikacyjne, a także wyspecjalizowane programy dla poszczególnych branż,

Programy narzędziowe

- Specjalistyczne oprogramowanie systemowe, które wspiera zarządzanie, optymalizację, konserwację i bezpieczeństwo komputera oraz urządzeń inteligentnych. W tej kategorii znajdują się narzędzia do czyszczenia systemu (np. CCleaner), zarządzania dyskami, odzyskiwania danych, monitorowania system.

Pliki

- Plik komputerowy to uporządkowany, nazwany zbiór danych o skończonej długości, przechowywany na urządzeniu pamięci masowej (np. dysku) i służący do rejestrowania informacji takich jak tekst, obrazy, muzyka, wideo czy programy

Nazwa pliku

- Składa się z dwóch członów: nazwy oraz rozszerzenia, np.
  - Plik.exe

Rozszerzenie pliku

- Określa typ i zwykle wskazuje program, w którym utworzono plik.

Rozszerzenie	Typ pliku
Exe, com	Plik wykonywalny przez system Windows (uruchomienie skutkuje wykonanie zawartego w nim programu).
bat	Tzw. Plik wsadowy czyli plik tekstowy wykonywalny, po jego uruchomieniu wykonywane są instrukcje zapisane wewnątrz.
Sys, dll	Pliki składowe systemu operacyjnego i oprogramowania (biblioteki z kodem)
txt	Plik tekstowy
Rtf, foc, docs	Plik tekstowy (np. Ms. Word)
odt	Plik tekstowy standardu OpenDocument

Rozszerzenie	Typ pliku
pdf	Plik dokumentów elektronicznych
Zip, rar	Pliki zarchiwizowane
Sys, dll	Pliki składowe systemu operacyjnego i oprogramowania (biblioteki z kodem)
Jpg, gif, png, bmp	Pliki graficzne bitmapowe
Cdr, svg	Pliki graficzne wektorowe
Wav, mid, mp3	Plik muzyczne
Htm, html, htmlx	Pliki hipertekstowe

Rozszerzenie	Typ pliku
Ppt, pptx	Plik prezentacji
Xls, xlsx	Pliki excel

Bezpieczeństwo pracy w systemie i sieci

Ochrona dostępu

- Pamiętaj o silnym haśle!
- Ustaw automatyczną blokadę;
- Używaj konta użytkownika, a nie administratora.

Aktualizacje

- Pamiętaj o aktualizacji systemu i sterowników!

Ochrona przed złośliwym oprogramowaniem

- Pamiętaj o włączeniu antywirusa!
- Nie otwieraj podejrzanych linków, załączników, obrazów;
- Uważaj na podejrzane wiadomosci oraz phishing;
- Pobieraj jedynie z zaufanych źródeł.

Kopie zapasowe

- Zapisuj ważne dane w chmurze, bądź na dysku zewnętrznym.

Ataki na systemy komputerowe

Atak na system komputerowy jest to działanie mające na celu przeniknięcie do chronionego systemu komputerowego w celu przechwycenia, zniszczenia lub zmodyfikowania przechowywanych tam informacji.

Ataki możemy podzielić ze względu na:

1. Miejsce ich przeprowadzania:

Zewnętrzne (zdalne) - ataki przeprowadzane są z systemów znajdujących się poza atakowaną siecią
Wewnętrzne (lokalne) - ataki przeprowadzane są z systemów znajdujących się w atakowanej sieci

2. Zamiar:

Zamierzony - atakujący zdaje sobie sprawę z tego, co robi i jakie konsekwencje mogą z tego wyniknąć, na przykład atak w celu uzyskania konkretnie wytyczonych informacji.
Niezamierzony - atakujący przypadkowo i nieświadomie dokonuje ataku, na przykład jeden z użytkowników serwera przez błąd programu obchodzi system autoryzacji uzyskując prawa administratora.

3. Aktywność:

Aktywny - w wyniku ataku system komputerowy traci integralność, na przykład atak włamywacza, który usuwa pewną ilość ważnych danych oraz powoduje zmianę działania programów. Atakiem aktywnym może być także modyfikowanie strumienia danych lub tworzenie danych fałszywych.

Pasywny - atak ten polega na wejściu do systemu bez dokonywania żadnych zmian, na przykład atak włamywacza, który kopiuje pewną ilość ważnych danych nie powodując zmian w działaniu programów. Atakiem pasywnym może być także podsłuchiwanie lub monitorowanie przesyłanych danych. W tym przypadku celem osoby atakującej jest odkrycie zawartości komunikatu. Ataki pasywne są bardzo trudne do wykrycia, ponieważ nie wiążą się z modyfikacjami jakichkolwiek danych.

4. Przepływ informacji:

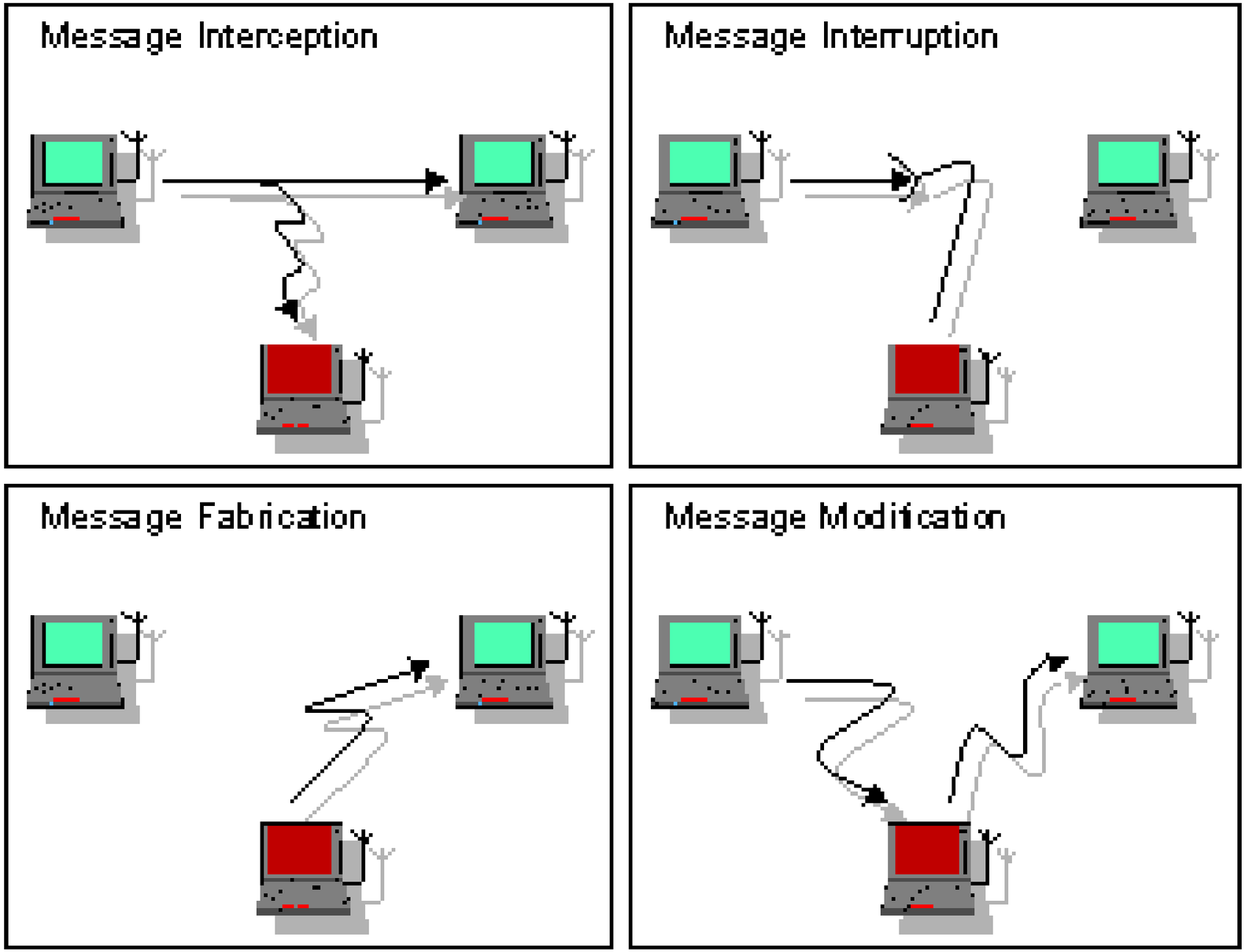
Przerwanie (interruption) - jest atakiem na dyspozycyjność polegającym na częściowym zniszczeniu systemu lub spowodowaniu jego niedostępności (niezdolności do normalnego użytkowania). Przykładem tutaj może być fizyczne zniszczenie fragmentu komputera lub sieci, np. uszkodzenie dysku, przecięcie linii łączności między komputerem a drugim obiektem, lub uniemożliwienie działania systemu zarządzania plikami.

Przechwycenie (interception) - jest atakiem opierającym się na poufności i występuje wtedy, gdy ktoś niepowołany uzyskuje dostęp do zasobów naszego systemu komputerowego. Przykładem tutaj może być podsłuch pakietów w celu przechwycenia danych w sieci i nielegalne kopiowanie plików lub programów.

Modyfikacja (modification) - jest atakiem opierającym się na nienaruszalności polegającym na zdobyciu dostępu do zasobów przez niepowołaną osobę, która wprowadza do nich jakieś zmiany w celu uzyskania wyższych praw lub utrzymaniu dostępu do danego systemu. Przykładem tutaj może być zmiana wartości w pliku z danymi, wprowadzenie zmiany w programie w celu wywołania innego sposobu jego działania lub modyfikacja komunikatów przesyłanych w sieci.

Podrobienie (fabrication)

- podrobienie jest atakiem opierającym się na autentyczności, podczas przesyłania danych z jednego do drugiego komputera trzeci komputer blokuje uniemożliwiając mu dalszy przesył, a sam wprowadza do systemu drugiego komputera fałszywe obiekty. Przykładem tutaj może być wprowadzenie nieautentycznych komunikatów do sieci lub dodanie danych do pliku.



Przykłady ataków:

1. **Skanowanie** - skaner to program automatycznie wyszukujący luki w systemie.

Co skaner może?

odnaleźć komputer lub sieć
wykryć obsługiwane przez serwer usługi
zdiagnozować je
scharakteryzować system operacyjny
scharakteryzować strukturę sieci komputerowej

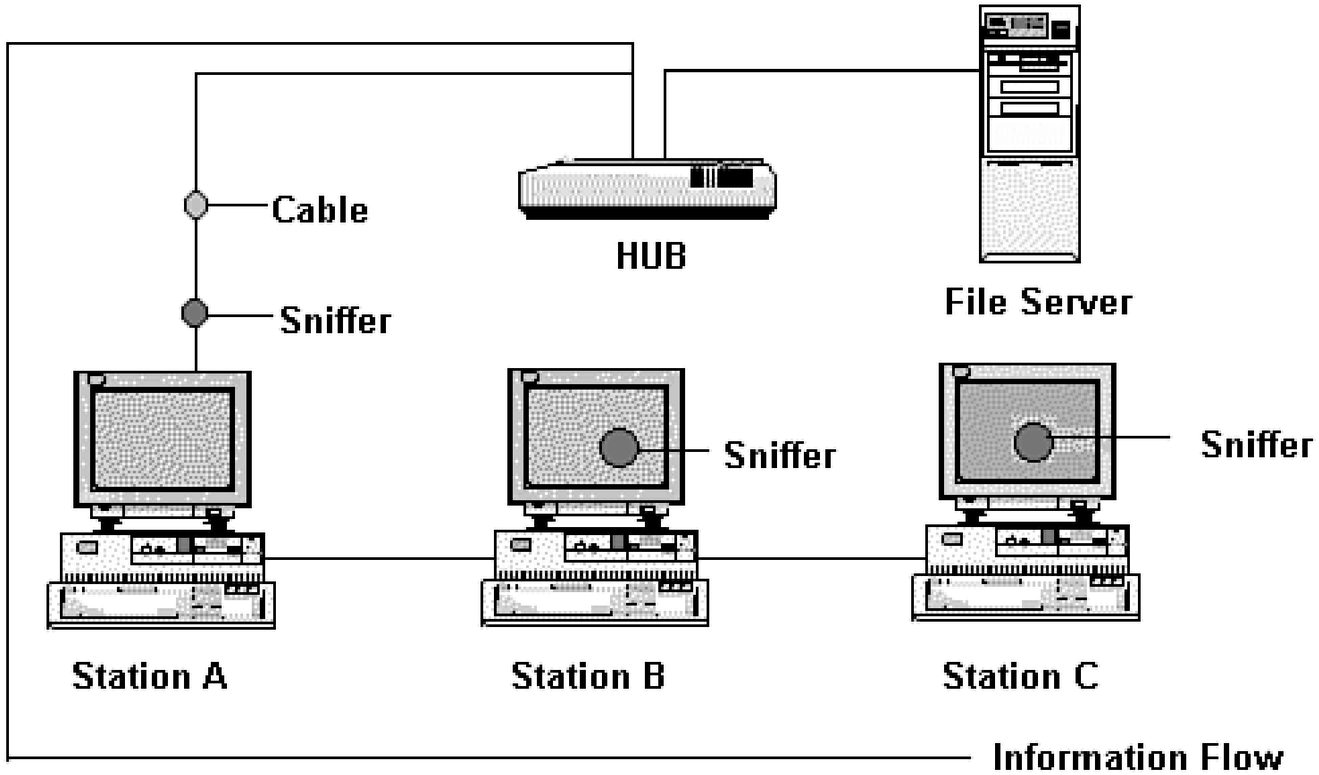
Co więc haker robi?

W pierwszej kolejności wykonuje skanowanie zdalnej maszyny pod kątem otwartych portów, a następnie próbuje uzyskać informacje o rodzaju i wersji oprogramowania odpowiedzialnego za obsługę tych portów, a także informacje o architekturze i systemie operacyjnym. Większość wykorzystywanych przez hakerów dziur w systemach jest zależna od oprogramowania zarządzającego daną usługą, bądź nawet od wersji całego systemu. Posiadając już wszelkie informacje, haker może odwiedzając stronę internetową z listą dostępnych exploitów, ściągnąć z niej odpowiedni program i przeprowadzić atak.

Przykłady ataków:

2. Sniffing - technika przechwytywania, monitorowania i analizowania ruchu sieciowego za pomocą specjalnego oprogramowania lub urządzenia zwanego **snifferem**.

Wykrywanie snifferów w sieci jest zadaniem trudnym, bowiem programy tego typu działają pasywnie i nie zostawiają żadnych śladów w logach systemowych.



Przykłady ataków:

3. Spoofing - technika cyberprzestępcza polegająca na podszywaniu się pod inne komputery/adresy, aby oszukać ofiarę i uzyskać dostęp do poufnych informacji, takich jak dane osobowe czy finansowe.

4. Hijacking - wszystkie ataki, w których włamywacz próbuje uzyskać dostęp do istniejącej sesji użytkownika, tzn. takich gdzie identyfikator został już wcześniej przydzielony. Polegają na uzyskiwaniu nieuprawnionego dostępu do systemów komputerowych na skutek przechwycenia sesji legalnego użytkownika.

5. Wirusy - Cechy charakterystyczne:
Powielają się - wirusy rozprzestrzeniają się poprzez pliki wykonywaln.
Do uaktywnienia wirusa niezbędne jest uruchomienie zawierającego go pliku; część wirusów wykorzystuje błędy w oprogramowaniu umożliwiające uruchamianie plików automatycznie (np. REDLOF, różne robaki pocztowe)
Robaki potrafią same rozprzestrzeniać się na inne komputery wykorzystując mechanizmy sieciowe.

Możliwe skutki:

- utrudnianie (czasami uniemożliwianie) pracy na komputerze - w przypadku wielu wirusów jedyny cel
- mogą niszczyć, zmieniać dane i/lub oprogramowanie zawarte na dysku
- mogą wykradać dane
- mogą przenosić i instalować inne typy złośliwych programów, np. konie trojańskie
- istnieją (bardzo rzadkie) wirusy mogące uszkodzić komputer - kasowanie pamięci Flash

Konie trojańskie

Cechy charakterystyczne:

- nie powielają się samoczynnie (ale mogą być roznoszone przez wirusy)
- udają programy użytkowe, narzędziowe, gry (stąd nazwa)
- końmi trojańskimi mogą być także np. strony WWW zawierające odpowiednio spreparowane kontrolki ActiveX
- zazwyczaj ukrywają się w systemie, tak aby ich działania były trudno zauważalne często umożliwiają dostęp z zewnątrz do komputera bez wiedzy użytkownika

Możliwe skutki:

- mogą umożliwiać innym osobom manipulowanie komputerem i znajdującymi się na nim danymi bez wiedzy użytkownika
- mogą wykradać dane, przechwytywać obraz z ekranu, tekst pisany na klawiaturze
- mogą wykorzystywać komputer do rozsyłania spamu lub zdalnych ataków na inne komputery
- mogą pobierać z sieci i instalować inne konie trojańskie lub spyware dialery mogą narazić użytkowników modemów na wysokie koszty

Spyware

Cechy charakterystyczne:

- zawarte w oficjalnych wersjach instalacyjnych wielu różnych "darmowych" programów !!! (np. KaZaA)
- pojawiają się także w postaci kontrolek ActiveX na stronach WWW (np. Gator - "Precision Time")
- podstawowy i jedyny cel - szpiegowanie użytkownika
  (informacja o odwiedzanych stronach WWW, ściąganych plikach itp. - zazwyczaj anonimowa, ale niektóre programy mogą przesyłać dane personalne)
- obecność w programie okienek reklamowych może świadczyć o obecności spyware trudne do odinstalowania, nawet po odinstalowaniu programu - "nosiciela" pozostają w systemie
- skutkiem ubocznym może być nieprawidłowe działanie innych programów
- zazwyczaj niewykrywane przez programy antywirusowe; niezbędne specjalne programy do wykrywania i usuwania spyware (np. Ad-Aware, Spybot Search & Destroy)
- programy użytkowe zawierające spyware często nie działają po jego usunięciu
  funkcje szpiegowskie pełnią czasem także reklamy na stronach WWW

DoS (Denial of Service)

W ogólnym znaczeniu metoda ta polega na częściowym lub całkowitym zablokowaniu dostępu do świadczonych usług. Podatność ośrodków sieciowych na ataki DoS wynika z ograniczenia zasobów każdego serwera/systemu. W przypadku zastosowań WWW ograniczenie to wynika przede wszystkim z przepustowości łącza. Ale nie tylko, innymi ograniczeniami są pamięć operacyjna oraz moc obliczeniowa warunkowana rodzajem stosowanego procesora (procesorów). Celem i konsekwencją ataku DDoS jest uniemożliwienie systemowi świadczenia usług, co osiąga się przez zajęcie jego zasobów "czymś innym".

DoS - oznacza typ cyberataku, w którym hakerzy, zalewając serwer dużą ilością danych, uniemożliwiają jego prawidłowe funkcjonowanie i dostęp dla legalnych użytkowników.
DDoS - rozproszony atak cybernetyczny polegający na masowym wysyłaniu zapytań do celu (strony internetowej, serwera, usługi) z wielu źródeł jednocześnie, aby przeciążyć jego zasoby i uniemożliwić prawidłowe działanie prawdziwym użytkownikom