Mariusz Szczerba
Informatyka IV rok

Porównanie systemów operacyjnych pod względem bezpieczeństwa

1. System operacyjny

System operacyjny[1] z angielskiego: operating system (OS) jest to oprogramowanie zarządzające systemem komputerowym, tworzące środowisko do uruchamiania i kontroli zadań.

System operacyjny zajmuje się:

- planowaniem oraz przydziałem czasu procesora poszczególnym zadaniom
- kontrolą i przydziałem pamięci operacyjnej dla uruchomionych zadań
- dostarczaniem mechanizmów do synchronizacji zadań i komunikacji pomiędzy zadaniami
- obsługą sprzętu oraz zapewnieniem równolegle wykonywanym zadaniom jednolitego, wolnego od interferencji dostępu do sprzętu

Dodatkowe zadania, którymi może, ale nie musi, zajmować się system operacyjny to:

- ustalanie połączeń sieciowych,
- zarządzanie plikami.

Jako że system operacyjny tworzy środowisko niezbędne do uruchamiania i kontroli zadań, musi on udostępniać interfejs pozwalający na wykonanie pewnych operacji.

Robi to poprzez dostarczanie metod pozwalających na uruchomienie lub zatrzymanie wskazanego zadania. Najczęściej poprzez udostępnienie w tym celu zestawu funkcji zwanych API (Application Programming Interface) lub wywołań systemowych.

System może zawierać również interfejs użytkownika. Dzięki niemu możliwa jest bezpośrednia interakcja użytkownika z komputerem. Należy przy tym zwrócić uwagę, że o ile interfejs programowy jest elementem koniecznym, o tyle interfejs użytkownika jest elementem opcjonalnym.

2. Rodzaje i podział systemów operacyjnych

Systemy operacyjne można podzielić na kilka sposobów, ze względu na:[2]

Rodzaj architektury:

- monolityczne - o najprostszej strukturze i jednozadaniowe, czyli gdy system może jednocześnie wykonywać tylko jedno zadanie
- warstwowe - o hierarchicznej strukturze poleceń systemowych, system może już wykonywać w tym samym czasie kilka poleceń
- klient- serwer - o bardzo rozbudowanej strukturze, gdzie serwery pełnią nadzór nad podrzędnymi systemami zainstalowanymi w poszczególnych komputerach sieci

[1] https://pl.wikipedia.org/wiki/System_operacyjny
[2] http://informatyka.2ap.pl/ftp/technik_inf/podz_pojecia.pdf dostęp 17.11.2020

Sposób komunikowania się z użytkownikiem (interfejs):

- tekstowe (DOS, UNIX/Linux)
- graficzne (Windows, UNIX/Linux, MacOS)

Ilość możliwych do uruchomienia programów:

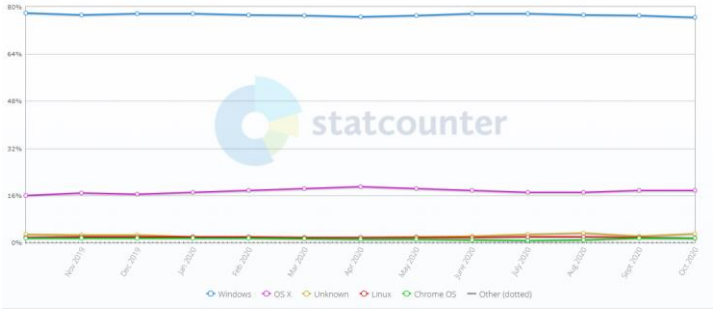
- jednozadaniowych – jeden proces w tym samym czasie (DOS)
- wielozadaniowych – wiele procesów w tym samym czasie (Windows, UNIX/Linux, MacOS)

Rodzaj jądra:

- monolityczne (Linux, OpenBSD, FreeBSD)
- mikrojądra (Amoeba, QNX, BeOS , Haiku)
- hybrydowe (Windows, MacOs)

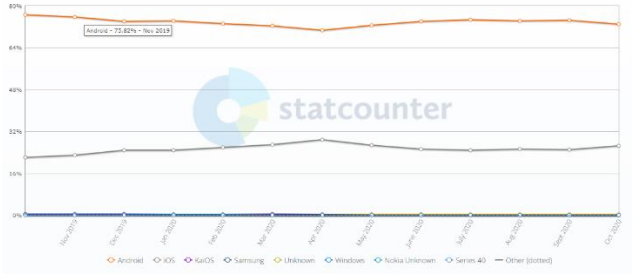
3. Popularność systemów operacyjnych:

Według danych dostępnych na gs.statcounter.com, najpopularniejszym systemem desktopowym jest Windows. Używa go prawie 80% użytkowników, zaś na 2gim miejscu plasuje się system od Apple, to jest OS X.



Rysunek 1: popularność systemów desktopowych

Na platformach mobilnych najpopularniejszym systemem jest Android z udziałem prawie 80%.



Rysunek 2: Procent udziału systemów na platformach mobilnych

Zaś jak spojrzeć całościowo Android i Windows używa podobna rzesza klientów, co czyni je najpopularniejszymi systemami.

4. Bezpieczeństwo systemów:

a. Microsoft Windows
· Co to jest?

Microsoft Windows[3] (ang. windows „okna") jest to rodzina systemów operacyjnych stworzonych przez firmę Microsoft. Systemy rodziny Windows działają na serwerach, systemach wbudowanych oraz na komputerach osobistych, z którymi są najczęściej kojarzone.

Prezentację pierwszego graficznego środowiska pracy z rodziny Windows firmy Microsoft przeprowadzono w listopadzie 1984. Wówczas była to graficzna nakładka na system operacyjny MS-DOS. Nakładka, a później system operacyjny Windows po pewnym czasie zdominowała światowy rynek komputerów osobistych.

Jest on dostępny dla laptopów i komputerów stacjonarnych, tabletów, smartfonów, innych produktów Windows oraz dla konsoli Xbox One.

- Bezpieczeństwo

Windows w opinii użytkowników pod względem bezpieczeństwa zajmuje zazwyczaj ostatnie miejsce. *Spowodowane jest to dużą liczbą jego użytkowników, co sprawia, że jest on doskonałym celem do* ataków. Chociaż ostatnio posiada oprogramowanie chroniące przed złośliwym oprogramowaniem, które jest często aktualizowane.
Poza tym w Windowsie w kwestii bezpieczeństwa, znajdziemy miedzy innymi takie usługi jak:

- zapora systemu Windows
- ochrona przed złośliwym oprogramowaniem
- ochronę konta użytkownika

Windows posiada trzy podstawowe kryteria poddziału zagadnień bezpieczeństwa:

a. Funkcje tożsamości i kontroli dostępu:

Historycznie kontrola dostępu stanowi proces, na który składają się trzy komponenty:[4]

- identyfikacja – przedstawienie unikalnych cech obiektu przy próbie dostępu do komponentów systemu operacyjnego
- uwierzytelnianie – potwierdzenie tożsamości obiektu po zakończeniu identyfikacji
- autoryzacja – określenie praw i/lub uprawnień do zasobów na podstawie porównania listy kontroli dostępu i uwierzytelnionego obiektu

Weryfikacja powyższych składowych zapewnia ochronę tożsamości a tym samym umożliwia powstrzymanie przed atakami, które mają na celu dostęp do poufnych danych. Dzięki mechanizmowi wymuszającemu potwierdzenie tożsamości, dostęp do danych może być zagwarantowanych dla właściwych powierników.

W Windows 10 utworzono w tym celu wiele rozwiązań, takich jak np.:

- Windows Hello z zastosowaniem urządzeń do weryfikacji biometrycznej
- funkcja Dynamic Access Control
- mechanizm Single Sign-On
- funkcja BitLocker z ochroną przed atakami typu brute-force
- Microsoft Passport z opcją uwierzytelniania wieloskładnikowego

[3] https://pl.wikipedia.org/wiki/Microsoft_Windows
[4] https://csirt.gov.pl/cer/zalecenia-konfiguracyj/microsoft-windows/903,Przewodnik-Zabezpieczen-systemu-Windows-10.html dostęp 17.11.2020

b. Ochrona informacji

Systemy takie jak Encrypted File system (EFS), BitLocker. Są to usługi zapewniające szyfrowanie zawartości podsystemów dyskowych.

c. Ochrona przed złośliwym oprogramowaniem

UEFI Secure Boot, funkcje wirtualizacji (np. Intel VT-x), funkcje ochrony pamięci procesora (np. Intel VT-d), ELAM (antymalware), moduł TPM oraz sensory biometryczne.

b. Linux

Co to jest?

Linux[5] jest to rodzina uniksopodobnych systemów operacyjnych opartych na jądrze Linux. Linux jest jednym z przykładów wolnego i otwartego oprogramowania (FLOSS): jego kod źródłowy może być dowolnie wykorzystywany, modyfikowany i rozpowszechniany. Jako że Linux to też Android Os, to jest on najpopularniejszym systemem operacyjnym na świecie. Jeżeli brać pod uwagę wszystkie urządzenia.

Linux na urządzenia desktopowe ma wiele różnych odmian, które mogą znacznie różnić się funkcjonalnością. Jak i jest on używany przez dużą rzesze osób doświadczonych w kwestii oprogramowania, którzy też są zaangażowani w kwestie bezpieczeństwa. Do tego w Linuxie system jest oparty o jądro monolityczne, a zwykły użytkownik nie ma dostępu do uprawnień „root", dzięki czemu nie ma dostępu do jądra systemu.

Jak widać podstawowym zabezpieczeniem Linuxa jest sam system, gdyż dostęp do plików systemowych zabezpieczony jest hasłem, a sam system jest odporny na większość istniejących szkodników.

Bezpieczeństwo

Sposoby zabezpieczenia systemu

- dostęp do plików systemowych jest zabezpieczony hasłem
- system jest odporny na większość znanych wirusów ale to nie znaczy że nie istnieją
- regularne aktualizacje systemu dostarczają nowe wersje programów oraz łatają wykryte błędy bezpieczeństwa wszystkich pakietów
- włączona zapora ogniowa zabezpiecza dostęp do zawartości Twojego komputera z zewnątrz do minimum
- program antywirusowy , który jednak nie jest koniecznością jak w innych systemach
- skanowanie systemu plików w poszukiwaniu rootkitów: np.: program chkrootkit, do zainstalowania z repozytorium

c. Systemy mobilne

Android OS

[5] https://pl.wikipedia.org/wiki/Linux

Android[6] jest to system operacyjny z jądrem Linux dla urządzeń mobilnych takich jak telefony komórkowe, smartfony, tablety (tablety PC) i netbooki. Wspomniane jądro oraz niektóre inne komponenty, które zaadaptowano do Androida opublikowane są na licencji GNU GPL. Android nie zawiera natomiast kodu pochodzącego z projektu GNU. Cecha ta odróżnia Androida od wielu innych istniejących obecnie dystrybucji Linuksa. Początkowo był rozwijany przez firmę Android Inc. (kupioną później przez Google), następnie przeszedł pod skrzydła Open Handset Alliance.

IOS

iOS[7] jest to system operacyjny Apple Inc. dla urządzeń mobilnych iPhone, iPod touch oraz iPad. Obecna nazwa funkcjonuje od 7 czerwca 2010, wcześniej system był znany jako iPhone OS. System ten bazuje na systemie operacyjnym Mac OS X 10.5 i tym samym na Darwinie. iOS dostępny jest tylko na urządzeniach firmy Apple.

Zabezpieczenia, porównanie[8]

Od początku system operacyjny Android był mniej bezpieczny niż iOS, między innymi z uwagi na otwartość i możliwość modyfikacji kodu źródłowego systemu. Przez co hakerzy mogą pokusić się o znalezienie luk w bezpieczeństwie.

Jednak w ostatnim czasie Google podejmuje bardzo wiele działań na rzecz zwiększenia bezpieczeństwa systemu operacyjnego Android m.in, ułatwiając producentom smartfonów wprowadzanie kolejnych aktualizacji zabezpieczeń na autorskich nakładkach.

Tak czy inaczej w kwestii bezpieczeństwa zdecydowanie wygrywa iOS, chociażby ze względu na fakt, że Apple nie przechowuje danych osobowych użytkowników, a wszelkie inne informacje są szyfrowane. System operacyjny iOS jest również o wiele bardziej odporny na cyberatak.

Jednym z wyznaczników bezpieczeństwa może być poziom trudności znalezienia krytycznych luk bezpieczeństwa i sposobów wykorzystania ich. Według największych firmy zajmujące się bezpieczeństwem trudność zhakowania wyceniana jest na 1,5 mln dol. za zero days exploits w iOS, podczas gdy znalezienie krytycznej luki w Androidzie na jedyne 200 tys. dol.

Plusy i minusy

a. Android

    + system zarządzania uprawnieniami aplikacji

    + systemy szyfrowania danych

    + tryb piaskownicy

    + Google Play Protect

    - otwartość i ogólnodostępność kodu źródłowego, umożliwiająca modyfikacje

    - brak aktualizacji oprogramowania dla niektórych urządzeń

[6] https://pl.wikipedia.org/wiki/Android_(system_operacyjny)
[7] https://pl.wikipedia.org/wiki/IOS
[8] https://komorkomania.pl/8372,bezpieczenstwo-androida-vs-bezpieczenstwo-ios-a-infografika

b. IOS

+ zaawansowane funkcje bezpieczeństwa systemu i aplikacji ze sklepu

+ zamknięty system

+ trudniej znaleźć luki w oprogramowaniu