# Bezpieczeństwo

**Wykład 11**

# Zakres

- Zagrożenia bezpieczeństwa
- Ochrona
- Włamywacze
- Oprogramowanie agresywne
- ...

# Zagrożenia bezpieczeństwa

- Wymagania systemów komputerowych związane z bezpieczeństwem:
  - Poufność (ang. Confidentiality) – Informacje w systemie komputerowym powinny być dostępne do odczytu tylko stronom upoważnionym. Ten typ dostępu obejmuje drukowanie, wyświetlanie i inne formy przedstawiania informacji , w tym proste ujawnianie istnienia obiektu.
  - Integralność (ang. Integrity) – Aktywa systemu powinny być modyfikowane tylko przez strony upoważnione. Modyfikacja obejmuje zapis, zmianę treści, zmianę statusu, usunięcie i utworzenie.
  - Dostępność (ang. Availability) – Aktywa systemu powinny być dostępne stronom upoważnionym.
  - Autentyczność (ang. Authenticity) – System umożliwia weryfikację tożsamości użytkownika.

# Rodzaje zagrożeń

- System komputerowy jest dostawcą informacji
  - Realizowany jest przekaz danych z punktu źródłowego do punktu przeznaczenia

- Rodzaje ataków:
  - Przerwanie przepływu informacji (ang. Interruption)
    - Aktywa systemu komputerowego ulegają zniszczeniu, stają się niedostępne lub nieużyteczne. Jest to atak na *dostępność* aktywów *(ang. availability)*. Przykładem może być zniszczenie elementów sprzętu np. dysku, przecięcie linii komunikacyjnej lub unieruchomienie systemu zarządzania plikami.
  - Przechwycenie informacji (ang. Interception)
    - Strona nieupoważniona uzyskuje dostęp do aktywów (*jest to atak na poufność).* Może być to osoba fizyczna, program lub komputer. Chodzi tutaj np. o podłączenie się do sieci w celu przechwytywania danych lub nielegalne kopiowanie plików czy programów
  - Modyfikacja informacji (ang. Modification)
    - Strona nieupoważniona nie tylko uzyskuje dostęp do aktywów, ale również je narusza. Jest to atak na *integralność* (ang. integrity). Przykładem może być zmiana programu (zmiana jego zachowania) lub modyfikacja zawartości komunikatów przekazywanych siecią
  - Sfałszowanie informacji (ang. Fabrication)
    - Strona nieupoważniona wprowadza do systemu sfałszowane obiekty. Jest to atak na autentyczność (ang. authenticity). Przykłady obejmują wprowadzenie do sieci fałszywych komunikatów lub dodanie zapisów do pliku

# Bezpieczeństwo: Zagrożenia i aktywa

| | Dostępność | Poufność | Integralność/ Autentyczność |
|---|---|---|---|
| Sprzęt | Wyposażenie zostało skradzione/uszkodzone stąd blokada usługi | | |
| Oprogramowanie | Programy skasowano, odmowa dostępu użytkownikom | Wykonanie nielegalnej kopii oprogramowania | Działający program zmodyfikowano w celu wywołania błędu w czasie wykonania lub dla realizacji nieplanowanego zadania |
| Dane | Pliki skasowano, odmowa dostępu użytkownikom | Wykonanie nieupoważnionego odczytu danych. Analiza statystyczna ujawnia odpowiednie dane. | Istniejące pliki zmodyfikowano lub wygenerowano pliki sfałszowane |
| Linie komunikacyjne | Komunikaty zniszczono lub skasowano. Linie i sieci są zablokowane. | Odczytano komunikat. Obserwowany jest rozkład ruchu sieciowego | Komunikaty zmodyfikowano, opóźniono, zmieniono ich kolejność lub powielono je. Generowane są fałszywe komunikaty. |

# Ataki na sprzęt

- Głównym zagrożeniem jest sprzęt
- Najbardziej podatny na ataki, najmniej poddaje się zautomatyzowanej kontroli
- Zagrożenia
  - Przypadkowe lub świadome uszkodzenia
  - Kradzieże
- Potrzebne środki ochrony fizycznej i administracyjnej

# Ataki na oprogramowanie

- Atak na dostępność
  - Oprogramowanie, zwłaszcza aplikacyjne, jest bardzo łatwe do usunięcia, zmiany lub uszkodzenia
    - Ważne jest staranne zarządzanie konfiguracją oprogramowania , w tym tworzenie kopii zapasowych większości jego aktualnych wersji, ułatwia utrzymanie wysokiego poziomu dostępności
  - Większym problemem jest modyfikacja oprogramowania, które nadal funkcjonuje, ale zmienia się jego zachowanie
    - Na przykład: ataki wirusów komputerowych i innych podobnych programów
  - Poufność
    - Mimo pewnych istniejących środków zaradczych, kwestia nieuprawnionego kopiowania oprogramowania nie została rozwiązana

# Ataki na Dane

- Kwestie bezpieczeństwa w odniesieniu do danych:
  - dostępność (możliwość przypadkowego lub celowego uszkodzenia plików danych)
  - poufność
    - nieupoważniony odczyt plików z danymi/baz danych → przedmiot najszerszych badań jeśli chodzi o zagadnienia bezpieczeństwa systemów komputerowych
    - analiza danych, przejawiająca się w wykorzystaniu tzw. statystycznych baz danych
      - W miarę wzrostu popularności statystycznych baz danych zwiększa się ryzyko ujawnienia informacji osobistych
      - Problem ten nasila się ze względu na rosnącą tendencję łączenia zbiorów danych
  - integralność (modyfikacje plików danych mogą mieć skutki o różnej skali, od niewielkich po katastrofalne)

# Ataki na linie komunikacyjne i sieci (1)

- Ataki pasywne (ang. Passive attack) – polegają na podsłuchiwaniu lub monitorowaniu transmisji, celem atakujących jest przejęcie przesyłanej informacji
  - Ujawnienie zawartości komunikatu – rozmowa telefoniczna, e-mail, transfer pliku mogą zawierać informacje wrażliwe lub poufne, celem jest zapobieżenie możliwości przejęcia treści tych transmisji przez atakujących
  - Analiza ruchu sieciowego –
    - Nawet jeśli mamy możliwość maskowania (np. kodowania) zawartości pakietów, to można obserwować rozkład tych komunikatów, określić lokalizację i dane identyfikacyjne komputerów oraz częstotliwość i długość wymienianych komunikatów. Na podstawie tych informacji można stwierdzić, jaki jest charakter komunikacji
  - Ataki pasywne trudno wykryć, gdyż nie są one związane z żadną zmianą danych. Nacisk w tym przypadku położono bardziej na zapobieganie, niż na wykrycie.

# Ataki na linie komunikacyjne i sieci (2)

- Ataki aktywne (ang.)
  - Ataki aktywne polegają na dokonaniu modyfikacji strumienia danych (lub na wygenerowaniu fałszywego strumienia danych) i mogą być podzielone na cztery grupy: maskowanie, odtwarzanie, modyfikacja zawartości komunikatów i blokada usługi.
  - Maskowanie (udawanie, symulowanie, ang. masquerade)- zachodzi, gdy jeden podmiot podszywa się pod dane identyfikacyjne innego podmiotu
    - Atak maskowania zazwyczaj obejmuje jedną lub więcej form ataku aktywnego
    - Na przykład sekwencja uwierzytelniania może zostać przechwycona i odtworzona później, gdy pełna sekwencja zostanie zrealizowana, co umożliwi podmiotowi upoważnionemu z ograniczonymi uprawnieniami symulowanie uprawnień większych
  - Odpowiadanie (ang. Replay) – polega na pasywnym przejęciu jednostki danych i późniejszej jej transmisji w celu uzyskania nieupoważnionego efektu

# Ataki na linie komunikacyjne i sieci (3)

- Ataki aktywne (ang.)
  - Modyfikacja zawartości komunikatów –
    - Pewna część prawidłowego komunikatu została zmieniona
    - Komunikaty są opóźniane albo jest zmieniana ich kolejność
  - Blokada usługi –
    - Uniemożliwia lub blokuje normalne korzystanie lub zarządzanie komunikacją
    - Atak ten może mieć konkretny cel. np. napastnik może kasować wszystkie komunikaty kierowane do określonego adresu (np. do usługi odpowiedzialnej za kontrolowanie stanu bezpieczeństwa)
    - Inną możliwością jest zakłócenia pracy całej sieci przez jej zablokowanie lub przeciążenie komunikatami tak, by ją w praktyce całkowicie zablokować

# Ochrona

# Współdzielenie zasobów

- Wprowadzenie wieloprogramowości stworzyło możliwości współdzielenia zasobów przez użytkowników, która obejmuje:
  - Procesor, Pamięć, Urządzenia I/O (np. dyski i drukarki), Programy, Dane
- Współdzielenie zasobów stwarza potrzebę ich ochrony przed nieupoważnionym dostępem
- System operacyjny jest w stanie zapewnić ochronę w następującym zakresie:
  - Tryb bez ochrony: Ma uzasadnienie, gdyż ważne procedury wykonywane są w wydzielonym czasie
  - Izolacja: Powoduje, że każdy proces realizowany jest niezależnie od innych, bez współdzielenia czy komunikacji – ma swoją przestrzeń adresową , swoje pliki i inne obiekty
  - Współdzielić wszystko lub nic: Właściciel obiektu (np. pliku czy pamięci) deklaruje go jako publiczny lub prywatny. W pierwszym przypadku każdy proces ma dostęp do danego obiektu., w drugim tylko procesy właściciela.
- Współdzielenie przez ograniczenie dostępu: System operacyjny sprawdza uprawnienia użytkownika przy każdej próbie dostępu do danego obiektu
- Współdzielenie dynamiczne: Jest to rozszerzenie koncepcji kontroli dostępu, dopuszczające dynamiczne tworzenie praw dostępu do obiektów
- Ograniczone wykorzystanie obiektu: Ta forma ochrony ogranicza nie dostęp, ale sposób korzystania z obiektu. Np. użytkownik może mieć prawdo do przeglądania dokumentu, ale nie do jego wydrukowania lub użytkownik może mieć dostęp do bazy danych w celu uzyskania informacji statystycznej, ale nie do uzyskiwania konkretnych wartości danych.

# Ochrona pamięci

- Kluczowe znaczenie w środowisku wieloprogramowym – zapewnia poprawne funkcjonowanie aktywnych procesów, a także bezpieczeństwo
- Możliwość wykonania przez proces zapisów w przestrzeni adresowej innego procesu może zakłócić jego pracę
- Separacja przestrzeni adresowej jest łatwa do przeprowadzenia – stronicowanie i segmentacja zapewniają efektywne środki zarządzania pamięcią główną
- Jeśli potrzebna jest pełna separacja, to system operacyjny musi zapewnić, że każda strona (czy segment) jest dostępna tylko dla tego procesu, do którego jest przypisana
- Jeśli współdzielenie ma być dostępne, wtedy ten sam segment lub strona może występować w więcej niż jednej tablicy.

# Przykład sprzętowej obsługi ochrony pamięci

- Komputery rodziny IBM System 370, pracujące pod systemem OS/390
- Z każdą ramką strony pamięci operacyjnej jest związany 7-bitowy klucz sterujący pamięci, który może być ustawiany przez system operacyjny
- Dwa z tych bitów wskazują, czy były odwołania do strony zajmującej daną ramkę i czy strona ta była modyfikowana, Są one wykorzystywane przez algorytm wymiany stron.
- Pozostałe bity są wykorzystywane przez mechanizm ochrony: 4-bitowy klucz sterujący dostępu i bit ochrony pobrania.
- Odwołania procesora do pamięci (i odwołania I/O DMA) aby uzyskać pozwolenie dostępu do strony muszą stosować odpowiedni klucz.
- Bit ochrony pobrania (ang. fetch. protection bit) wskazuje, czy dany klucz sterujący dostępu należy uwzględnić tylko przy operacjach zapisu, czy także odczytu.
- W procesorze istnieje słowo statusu programu (PSW, ang. program status word), które mieści w sobie informacje sterujące, dotyczące aktualnie wykonywanego procesu (z 4-bitowym kluczem PSW).
  - Gdy proces próbuje uzyskać dostęp do danej strony lub zainicjować dla niej operację DMA, aktualny klucz jest porównywany z kodem dostępu.
  - Zapis jest dozwolony tylko wtedy, gdy kody są zgodne.
  - Gdy bit ochrony pobrania jest ustawionym, wtedy w przypadku operacji odczytu klucz PSW musi być zgodny z kodem dostępu.

# Kontrola dostępu zorientowana na użytkownika

- Środki kontroli dostępu użytkownika są często nazywane uwierzytelnieniem (ang. authentication).
- Najpowszechniejsza technika: logowanie – podanie identyfikatora oraz hasła
  - System pozwala się zalogować tylko wtedy, gdy rozpozna identyfikator oraz hasło do niego przypisane
  - Jest to szczególnie zawodna część kontroli dostępu, użytkownicy mogą zapominać lub ujawniać hasła, włamywacze sprawnie uzyskują informacje na temat identyfikatorów, plik zawierający identyfikatory i hasła jest narażony na penetrację

# Kontrola dostępu zorientowana na dane

- Procedura kontroli dostępu użytkownika umożliwia powiązanie go z profilem określającym dozwolone operacje i dostęp do plików → system operacyjny może realizować zasady operacji oparte na profilu użytkownika
- Ogólny model kontroli dostępu, realizowany przez systemy zarządzania plikami (lub bazami danych) korzysta z macierzy dostępu (ang. access matrix). Jego podstawowe elementy to:
  - Podmiot (ang. Subject): Jednostka realizująca dostęp do obiektów. Ogólnie koncepcja podmiotu odpowiada idei procesu. Dowolny użytkownik (lub aplikacja) uzyskuje dostęp do przedmiotu za pomocą środków w ramach procesu, który go reprezentuje.
  - Przedmiot (ang. Object): Wszystko, do czego dostęp podlega kontroli np. pliki, części programu, segmenty w pamięci
  - Prawa dostępu (ang. Access rights): Sposób, w jaki podmiot realizuje dostęp do przedmiotu np. operacje odczytu, zapisu czy realizacji
- Jeden wymiar macierzy to zidentyfikowane podmioty (zwykle użytkownicy i grupy, ale mogą też to być terminale, hosty czy aplikacje).
- Drugi wymiar macierzy stanowi lista przedmiotów, do których można uzyskać dostęp.
  - Np. rekordy, pliki, bazy danych
  - Na najniższym poziomie szczegółowości mogą być poszczególne pola danych.

# Kontrola dostępu zorientowana na dane (2)

- W praktyce macierz dostępu jest implementowana dwiema metodami:
  - Rozkład kolumnowy – powstają lisy kontroli dostępu (ACL) określające dla danego przedmiotu prawa dostępu wszystkich użytkowników
  - Rozkład wierszowy – znaczniki uprawnień, określają one przedmioty i operacje dostępne dla danego użytkownika
    - Każdy użytkownik ma szereg takich znaczników i może być upoważniony do ich pożyczania lub przekazywania innym
    - Ponieważ informacje te mogą być rozproszone w całym systemie, z punktu widzenia bezpieczeństwa stanowią większy problem niż listy kontroli dostępu.

# Włamywacze

# Rodzaje włamywaczy

- Ukryty – osoba, która nie upoważniona do korzystania z komputera, ale penetruje system kontroli dostępu w celu wykorzystania kont uprawnionych użytkowników
- Nadużywający – znany w systemie użytkownik korzystający z danych, programów i zasobów, do których nie ma uprawnionego dostępu, lub posiadający odpowiednie prawa dostępu, ale używający ich niewłaściwie
- Tajny użytkownik – osoba, która przejmuje kontrolę na całym systemem i korzysta z uzyskanych możliwości w celu uniknięcia skutków działań ochronnych lub wstrzymania rejestracji zapisów kontrolnych

# Techniki włamań

- Ochrona pliku z hasłami:
  - Szyfrowanie jednokierunkowe – system zapisuje hasła jedynie w postaci zaszyfrowanej
  - Kontrola dostępu – dostęp do pliku haseł jest możliwy tylko z jednego lub niewielu kont
- Różne metody odnajdywania haseł
  - (hasła domyślne, krótkie, listy słów prawdopodobnych, podsłuchiwanie linii łączącej użytkownika zdalnego z hostem, stosowanie konia trojańskiego)

# Oprogramowanie agresywne

# Ogólna klasyfikacja

- Wymagające programu nosiciela
  - Tylne drzwi
  - Bomby logiczne
  - Trojany
  - Wirusy
- Niezależne
  - Robak
  - Zombie
- Wirusy, Robaki, Zombie – mają możliwość replikacji

# Tylne drzwi

- Jest to kod w programie rozpoznający pewną szczególną sekwencję wejściową
- Tylne drzwi do programu umożliwiają poinformowanej osobie uzyskać dostęp do jego opcji bez przechodzenia przez procedurę bezpieczeństwa
- Stosowane od lat do testowania i debugowania programów
- Zagrożenie w rękach pozbawionych skrupułów programistów

# Bomba logiczna

- Jedno z najstarszych zagrożeń programowych, poprzedzające wirusy i robaki – jest to kod zapisany wewnątrz programu, który „eksploduje”, jeśli zajdą pewne warunki (np. obecność lub brak pewnych plików, dzień tygodnia, data, konkretny użytkownik uruchamiający aplikację)

# „Konie trojańskie”

- Koń trojański, trojan – pozornie przydatny program lub skrypt, zawierający ukryty kod, który po wywołaniu wykonuje zbędne lub szkodliwe działania
- Programy takie mogą być używane do wykonywania funkcji, których użytkownik bez odpowiednich uprawnień nie może wykonać.
- Np. aby uzyskać dostęp do plików innego użytkownika w systemie wielodostępnym, dany użytkownik mógłby stworzyć odpwiedniego „trojana”,
  - Po wywołaniu program taki zmienia uprawnienia do plików użytkownika, który go wywołuje, że stają się one dostępne do odczytu przez dowolną osobę.
  - Autor może skłaniać użytkowników do użycia swojego programu
  - Inne zastosowanie trojana: niszczenie danych, kasowanie plików użytkownika

# Wirusy

- Programy, które mogą infektować inne programy przez ich modyfikację.
- Zmodyfikowany program zawiera kopię wirusa i może kontynuować zarażanie innych.
- Podobnie jak ich biologiczne odpowiedniki, wirusy komputerowe zawierają przepisy na generowanie dokładnych swoich kopii.
- Po wprowadzeniu do komputera, typowy wirus przejmuje czasowo kontrolę nad systemem/aplikacją
- Infekcja może być rozprzestrzeniana z komputera na komputer przez użytkowników
- W środowisku sieciowym możliwość dostępu do aplikacji i usług systemowych na innych komputerach stwarza doskonałe możliwości rozprzestrzeniania się wirusa

# Robaki

- Korzystają z połączeń sieciowych do rozprzestrzeniania się z systemu na system
- Gdy robak jest aktywny, może zachować jak komputerowy wirus: wprowadzić trojana, lub wykonywać dowolne destrukcyjne/szkodliwe działania
- Do replikacji robak korzysta z technologii sieciowej np:
  - Poczty elektronicznej
  - Mechanizmu zdalnego wykonywania programów: Robak wykonuje swoją kopię w innym systemie
  - Mechanizmu zdalnego logowania: Robak loguje się w jednym systemie zdalnym jako użytkownik, a potem kopiuje się do innych systemów

# Zombie

- Program, który w sposób ukryty przejmuje inny komputer podłączony do Internetu i korzysta z niego do przeprowadzania ataków.
- Właściwego autora takich ataków jest trudno ustalić.
- Programy zombie są wykorzystywane do przeprowadzania ataków „blokada usługi”, zazwyczaj przeciwko wybranym stronom WWW.
- Są one wprowadzane do setek komputerów należących do niczego nie podejrzewających osób trzecich, a następnie wykorzystywane do zasypania wybranej strony wygenerowanym zmasowanym ruchem internetowym

# Typy wirusów

- Wirus pasożytniczy – tradycyjny, najpopularniejsza forma wirusa, doczepia się do plików wykonywalnych i podczas realizacji zainfekowanego programu replikuje się, wyszukując do zaatakowania inne pliki wykonywalne.
- Wirus rezydujący w pamięci – Wprowadzony do pamięci głównej jako część rezydentnego programu systemowego. Z tego miejsca infekuje każdy wykonywany program.
- Wirus sektora początkowego – Infekuje główny sektor ładowania początkowego (lub sektor ładowania początkowego) i rozprzestrzenia się, gdy system uruchamiany jest z dysku zawierającego ten wirus
- Wirus utajniony – Forma wirusa zaprojektowana tak, by uniemożliwić wykrycie przez oprogramowanie antywirusowe. Np. wirus stosujący kompresję, by program zainfekowany miał taki sam rozmiar co niezainfekowany
- Wirus polimorficzny – Wirus, który mutuje przy każdym zainfekowaniu, uniemożliwiając wykrycie na podstawie analizy sygnatury.

# Makrowirusy

- Pod koniec 1999 roku, makrowirusy stanowiły 2/3 wszystkich wirusów komputerowych
- Korzystają z możliwości dostępnej w programie Word i w innych aplikacjach biurowych (np. Excel) a mianowicie z makro.
  - Makro – wykonywalny program osadzony w dokumencie edytora tekstu czy pliku innego typu, np. używająca jakiejś formy Basica
- Makrowirusy są szczególnie groźne, gdyż:
  - Są niezależne od platformy. Niemal wszystkie infekują dokumenty edytora Word firmy Microsoft, zainfekowana może być każda platforma i każdy system operacyjny gdzie taki program działa
  - Infekują dokumenty a nie wykonywalne części kodu. Większość informacji w systemie komputerowym ma postać dokumentu, a nie programu.
- Łatwo się rozprzestrzeniają. Powszechne jest wykorzystanie poczty elektronicznej.

# Techniki antywirusowe

- Profilaktyka  - nie dopuścić do instalacji wirusa
- Wykrycie – zlokalizowanie wirusa
- Identyfikacja – okreslenie typu wirusa
- Usunięcie – usunięcie śladów wirusa i odtworzenie oryginalnego stanu systemu.