Ćwiczenie 6. Śledzenie wykonywania się programów i zmiana ścieżki wykonania

Celem ćwiczenia jest zapoznanie się ze śledzeniem działania programów wykonywalnych bez dostępnego kodu źródłowego i próba wnioskowania o zamysłach autora.

Wprowadzenie

W programie `lab6.exe` prosi się użytkownika o podanie nazwy użytkownika i numeru seryjnego. W przypadku podania poprawnego numeru program wyświetli komunikat informujący o sukcesie. W innym razie pojawią się stosowne komunikaty informujące o porażce.
Ponieważ odgadnięcie numeru seryjnego jest trudne, więc sugeruje się śledzenie wykonania programu i rozpoznanie myśli towarzyszącej autorowi, aby złamać algorytm tworzący/weryfikujący hasło.

Przebieg ćwiczenia

- Uruchomić program `lab6.exe` i zaobserwować działanie
- Uruchomić turbo debugger `td.exe` i próbować wykonać program. Zwrócić uwagę na pojawiający się komunikat. (Okazuje się, że program rozpoznaje obecność debuggera. Zatem w pierwszym kroku należy deaktywować odpowiedni fragment programu.)
- Proponuje się rozpocząć śledzenie wykonywania programu począwszy od adresu `cs:02C2` (początek funkcji `main()`). O obecności debuggera świadczą podmienione wektory przerwać o numerach 1 i 3. Tablica wektorów przerwań mieści się w RAM pod adresem `0000:0000` i zawiera dalekie adresy do funkcji obsługi przerwań.
- Używając narzędzia do edycji plików na dysku (np. `PCTools.exe`) dokonać odpowiednich modyfikacji.
- Ponowić próbę wykonania programu pod debuggerem. Teraz okaże się, że program „w jakiś sposób” rozpoznaje, że wykonuje się za długo. Zatem program zapewne mierzy „jakoś” czas wykonania. Patrz wskazówka nr 1. Po odnalezieniu odpowiedniego fragmentu programu dokonać odpowiednich modyfikacji.
- Teraz już w zasadzie nic nie stoi na przeszkodzie, aby odnaleźć fragment programu odpowiedzialny za sprawdzenie poprawności numeru seryjnego. Pomocna może być wskazówka nr 2.

- Do finałowego odszyfrowania sposobu weryfikacji poprawności numeru seryjnego, można przeczytać wskazówkę nr 3.
- **Dla „Ciekawych świata”**: gdzie się podziały napisy informujące o porażce lub sukcesie?

Wskazówka do programu

1. Do odczytu stanu zegara systemowego (32-bitowa wartość) można użyć funkcję BIOS-u nr 0 w ramach przerwania 1Ah. Funkcja ta wymaga wpisania.
   AH 00h
   Wartości zwracane
   AL znacznik przekroczenia północy
   CX starsze słowo licznika
   DX młodsze słowo licznika

2. Do odczytu sektora dyskowego można użyć funkcję BIOS-u nr 2 w ramach przerwania 13h. Funkcja ta wymaga wpisania.
   AH 02h
   AL liczba sektorów po 512 bajtów
   CH młodsze 8 bitów numeru cylindra
   CL sektor na 6 bitach i 2 starsze bity numeru cylindra
   DH numer głowicy
   DL napęd (80H – pierwszy dysk twardy)
   ES:BX adres bufora na przeczytane sektory
   Wartości zwracane
   ES:BX tu jest wpisana zawartość przeczytanego sektora

   Sektor 1 cylindra zerowego **począwszy od pozycji 27h zawiera numer seryjny dysku** (4 bajty). Numer seryjny dysku można sprawdzić wpisując DOS-owe polecenie DIR.

3. Numer seryjny wymagany w programie zależy od wprowadzonej nazwy użytkownika i od numeru seryjnego dysku.

Warunki zaliczenia ćwiczenia

Zaliczenie ćwiczenia polega na demonstracji działania programu prowadzącemu z prawidłowo podanym hasłem.

Sprawozdanie

Sprawozdanie powinno zawierać opis jak wykonano śledzenie programu i podawać jakich dokonano zmian w kodzie programu wykonywalnego.

Literatura

Kernigham, Ritchie, *Język C*, WNT 1989
Dokumentacja pakietu Borland C 3.1
Wróbel Eugeniusz, *Asembler 8086/88*
Scanlon Leo J., *Assembler 8086/8088/80286*
Kruk Stanisław, *Język Assembler dla początkujących*
Syck Gary, *Turbo Assembler : biblia użytkownika*