Introdução a Windows Drivers

Objetivo

O objetivo deste curso é preparar os alunos que queiram entender, testar, complementar ou construir drivers para Windows empregando os conceitos da plataforma Windows NT, identificando e apresentando as informações essenciais para o entendimento do papel de um driver e de como ele interage com o resto do sistema operacional.

Os conceitos e práticas apresentados neste curso são requisitos mínimos para o perfeito entendimento dos cursos de WDM Drivers e de File Systems Drivers. Técnicas de acesso ao hardware não são abordados, sendo elas parte integrante do curso de WDM Drivers.

Público alvo

Este curso é destinado aos desenvolvedores ou estudantes que precisam entender os conceitos fundamentais sobre implementação de drivers para Windows, técnicas de depuração de drivers de Kernel tais como *Live Debug* e análises de dump do sistema, e instalação de drivers.

Pré-requisitos

- Os estudantes deverão ter sólidos conhecimentos da linguagem C tais como estruturas, ponteiros, heap, utilização da pilha, alocação dinâmica de memória e listas. O uso de linguagem C++ não será empregado neste curso. Os estudantes também deverão conhecer conceitos de depuração de software.
- Conhecimentos básicos da API do Windows tais como lidar com arquivos, handles, eventos, threads e processos.
- Conceitos básicos de Sistemas Operacionais.

Metodologia

Os tópicos são abordados de maneira simples e gradativa de forma a colocar em prática cada novo tópico apresentado. O curso é repleto de atividades práticas que despertam novas dúvidas enquanto o estudante ainda está em curso, tendo assim a oportunidade de consultar um profissional da área. O curso é todo apresentado em slides e acompanha material impresso.

Tópicos abordados

1) Visão Geral da Arquitetura do Sistema
    a) Processos e Threads
    b) Memória Virtual
        i) Address Spaces
        ii) Page Fault
        iii) Paginação
        iv) MDL
        v) Section
    c) Kernel-Mode x User-Mode
    d) Subsistemas e API nativa
    e) I/O Manager
        i) File Objects
        ii) Driver Objects
        iii) Device Objects
        iv) IRP
    f) Pilha de dispositivos
    g) Object Manager
    h) Registry
    i) Camada de abstração de Hardware (HAL)
    j) Tipos de Drivers
        i) Legacy
        ii) WDM
        iii) WDF (KMDF e UMDF)
        iv) File Systems
        v) Minifilters

2) Ambiente (obtenção, instalação e utilização)
    a) Windows Driver Foundation Kit
    b) Microsoft Visual Studio Express
    c) Microsoft Debugging Tools for Windows
    d) Símbolos
    e) Máquinas Virtuais

3) Escrevendo um Driver
    i) DriverEntry
    ii) DriverUnload
  b) Compilando o Driver
  c) Instalando o Driver (Legacy)
    i) Dependências
    ii) Grupos
    iii) Load Order
  d) Depurando o Driver
    i) Configurando o Sistema
    ii) Instalações Checked Build
    iii) Driver Verifier
    iv) Mapeando Imagens
    v) Máquinas Virtuais
  e) Iniciando o Driver
  f) Strings e Conversões
  g) Alocando Memória
    i) Pools de Alocação
    ii) Tags
    iii) Listas
  h) Criando Device Object
  i) Symbolic Links
  j) I/O Request Packets
    i) Parâmetros de uma IRP
    ii) Completando IRPs
  k) Objetos, Handles e Ponteiros
  l) Create, Cleanup e Close
  m) Implementando Dispatch Routines
    i) Buffered I/O
    ii) Direct I/O
    iii) Neither I/O
  n) IOCTLs e DeviceIoControl
  o) Contexto Arbitrário
  p) IRQLs, APCs, DPCs
    i) Alertas

4) Escrevendo Filtros
  a) Filtros para Drivers Legacy
  b) Repassando IRPs
  c) Stack Locations
  d) I/O Completion Routines

e) Tratamento de IRPs Pendentes
    i) Filas de Sistema
    ii) Filas Customizadas
f) Cancelamento de IRPs
g) Criando IRPs para outros Drivers
    i) Alocando/Reutilizando IRPs
    ii) Drivers de Alto Nível
    iii) IRPs Síncronas/Assíncronas

5) Miscelaneous
    a) Notificações
        i) Shutdown
        ii) Processos/Threads
        iii) Imagens
    b) System Threads e WorkItems
    c) Dispatch Objects
        i) Evento
        ii) Mutex
        iii) Semáforo
        iv) Timer
        v) Thread
    d) Esperando Objetos
    e) Sincronismo
        i) Critical Region
        ii) ERESOURCE
        iii) Spin Locks
        iv) Fast Mutex
        v) Interlocked Actions

6) Instalações
    a) Service Control Manager
    b) Criando um arquivo INF
    c) Instalando um Driver
    d) Desinstalando um Driver

7) Referências
    a) Web Sites
    b) Grupos de discussão
    c) Livros