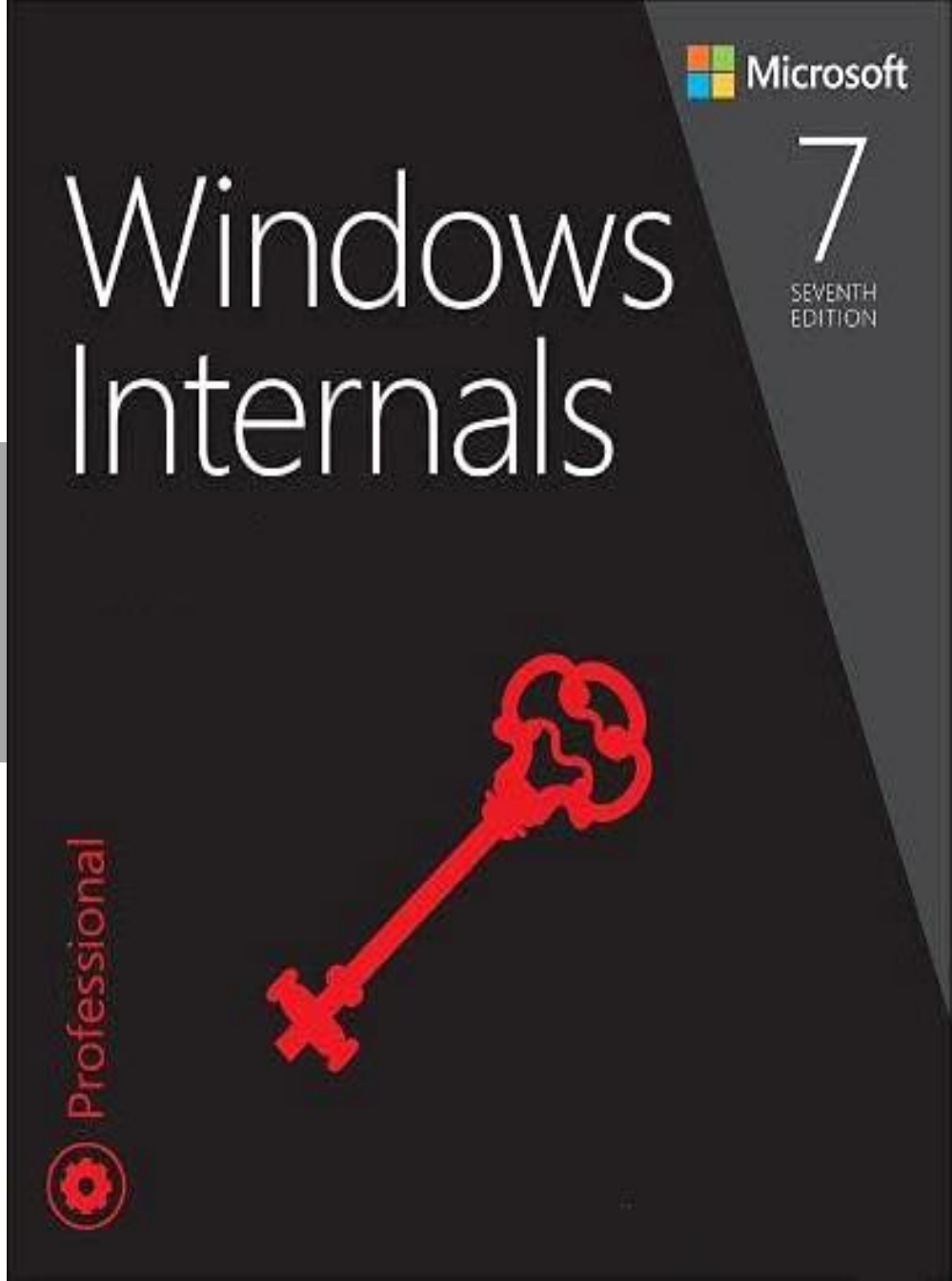
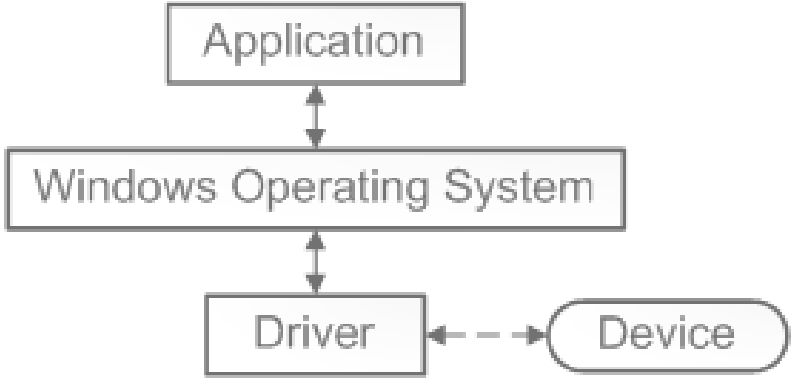
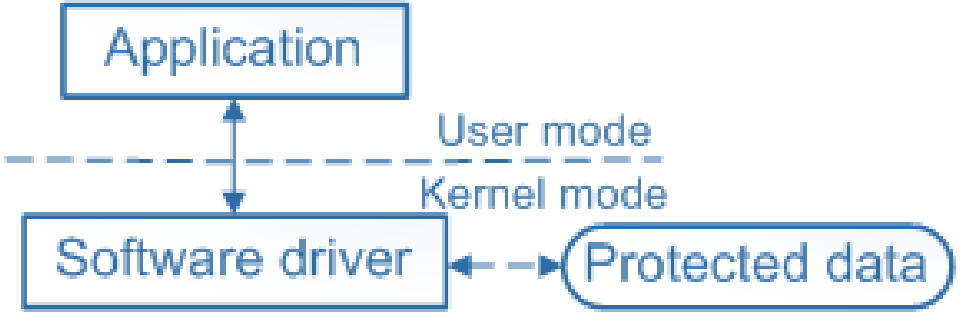
01) Threads

Kernel Threads

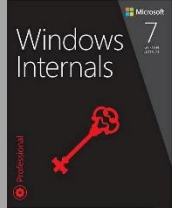


What is a driver?



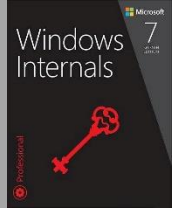


Kernel-Mode Drivers



- Loadable Kernel Modules (.sys files)
  - Under System Process
  - RegPath: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- Driver Frameworks
  - Windows Driver Model (Now Legacy)
  - Windows Driver Foundation (WDF)
    - Kernel Mode Driver Framework (KMDF)
    - User Mode Driver Framework (UMDF)
- Universal Windows Drivers (Since Windows 10)

Kernel Thread Functions




```
NTSTATUS PsCreateSystemThread(
  [out]           PHANDLE            ThreadHandle,
  [in]            ULONG              DesiredAccess,
  [in, optional]  POBJECT_ATTRIBUTES ObjectAttributes,
  [in, optional]  HANDLE             ProcessHandle,
  [out, optional] PCLIENT_ID         ClientId,
  [in]            PKSTART_ROUTINE    StartRoutine,
  [in, optional]  PVOID              StartContext
);
```

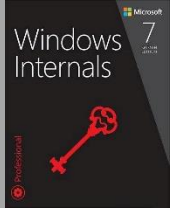
```
__kernel_entry NTSYSCALLAPI NTSTATUS NtClose(
  [in] HANDLE Handle
);
```

Thread Termination:

```
NTSTATUS PsTerminateSystemThread(
  [in] NTSTATUS ExitStatus
);
```

```
void KstartRoutine(
  [in] PVOID StartContext
)
{...}
```

Waiting for Thread in Kernel

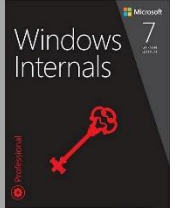



```
NTSTATUS
KeWaitForSingleObject (
    PVOID Object,
    KWAIT_REASON WaitReason,
    KPROCESSOR_MODE WaitMode,
    BOOLEAN Alertable,
    PLARGE_INTEGER Timeout
    );
```

Drivers should set this value to **Executive**

Drivers should specify **KernelMode**

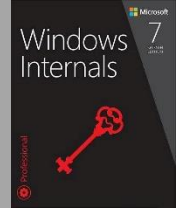
Getting Object by Handle



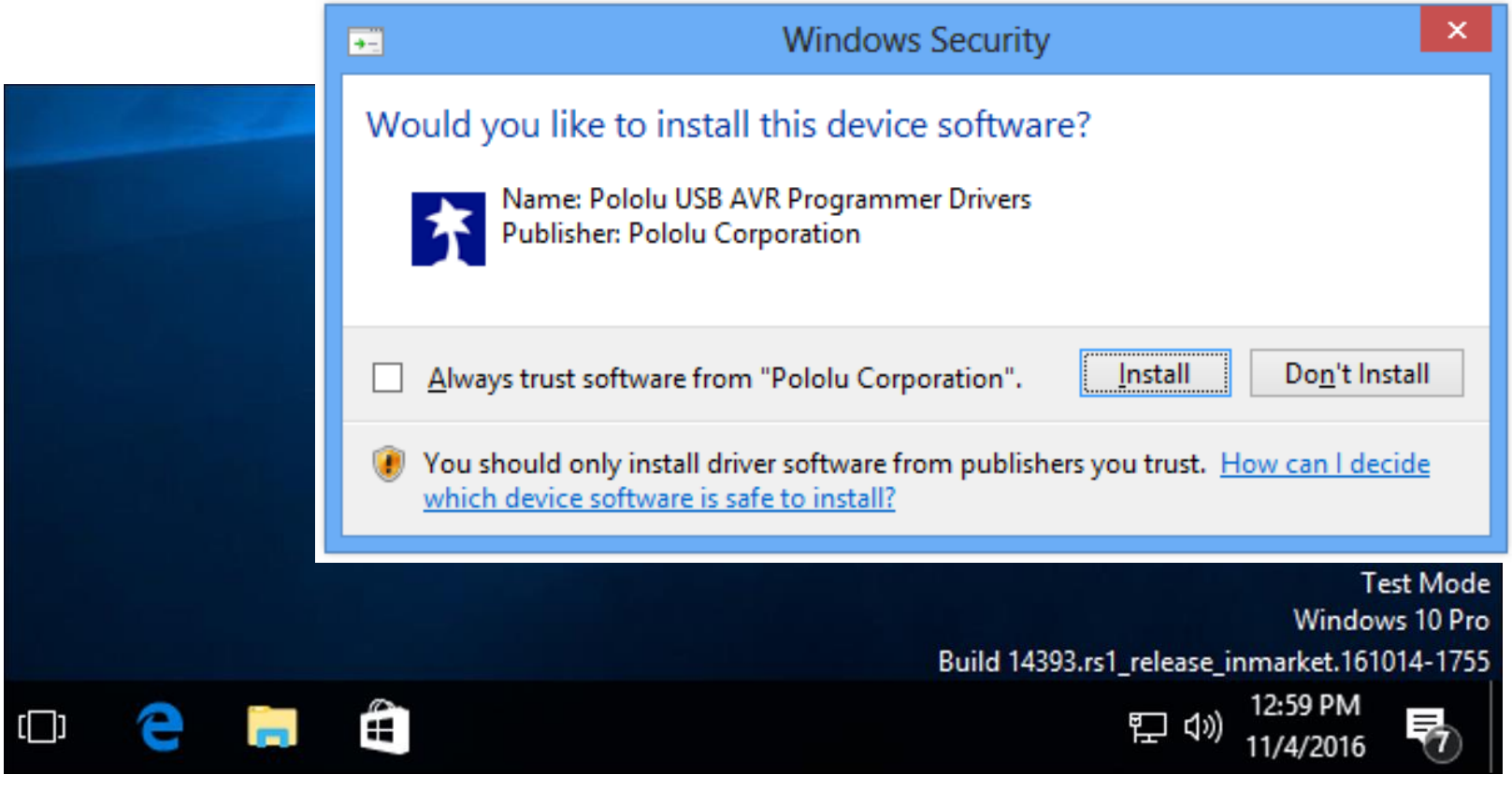

```
NTSTATUS ObReferenceObjectByHandle(
  [in]           HANDLE                     Handle,
  [in]           ACCESS_MASK                DesiredAccess,
  [in, optional] POBJECT_TYPE               ObjectType,
  [in]           KPROCESSOR_MODE            AccessMode,
  [out]          PVOID                      *Object,
  [out, optional] POBJECT_HANDLE_INFORMATION HandleInformation
);
```

```
void ObDereferenceObject(
  [in]  a
);
```

Driver Signing




```
Bcdedit.exe -set TESTSIGNING ON
```



CODING TIME