Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Implementing a Windows System Service Call

Alexander Schmidt

10 January 2008

Agenda

- A sample service call
- Implementation roadmap
  - Select a kernel module
  - Implement the service call
  - Expand the system service table
  - Provide a library
  - Test the system service

A Sample Service Call

- **AddInteger** service call
- Two integer (long) parameters as input parameters
- One reference integer (long) parameter as output parameter
- Status code (NTSTATUS) as return value
- Prototype

```
NTSTATUS NtAddInteger(
      LONG a,
      LONG b,
      PLONG sum );
```

Where To Implement?

- Select an appropriate kernel module:
  - PS?
  - EX?
  - MM?
  - KE?
  - OB?

Where To Implement?

Select an appropriate kernel module:

- Ex
  - Executive
  - Implements the native API (*NtXxx*)

Implement the Service Call

Most important of all:

- Check parameters!
- Convention/Assumption:
  - Trust the kernel
  - Suspect the user
- Check for
  - Plausibility
  - Validity of addresses

Announce the Service

Announce the service to the system

- ntos\ke\i386\systable.asm
  - System service table
  - Argument table
  - Increment service call number
- ntos\ke\i386\sysstubs.asm
  - System service stub

Compile the Kernel

Modify makefile:

- ntos\ex\BUILD\Makefile

Provide a Library

- Library may implement additional functions
  - add
  - sub
  - mul
- „Calls‟ the kernel
- Evaluates system status values
- Hide kernel details ;-)

Test the Program

A simple test program ...

Thank you for your attention!