Windows Internals Course – University of Tokyo – July 2003

LPC Exercises

Adrian Marinescu – 2003/07/18a

The first experiment models the behavior of a system process (e.g. csrss, which performs tasks on behalf of some clients). The second experiment builds a server which communicates with both user-process and kernel-mode components at the same time. The third is an experiment regarding thread injection from a debugger to a target process.

Local Procedure Call (LPC)

Windows NT system uses LPC mechanism for high speed inter-process communication. The mechanism can be used for message passing between user-mode components or between kernel components and user-mode processes. Message passing via LPC is generally used by system processes (csrss, smss, lsass) to communicate with client processes. RPC uses LPC as one of its transports for local communication.

LPC Ports

The LPC ports are objects used to control the communication process between two or more components. A server creates a server connection port, which is a named port object that other processes see exposed in the global namespace. A client can request a connection to a port by supplying the connection port name to an NT interface.

Question: *How can you see what LPC objects are created in the system?*

Experiment 1: Write a minimal LPC server and client application, which would allow a privileged server to call a system API on behalf of an unprivileged client (e.g. reading a few bytes from a file protected from ordinary user).

Experiment 2: Modify the same LPC server application to receive, beside the messages from the client process, also the exception messages that system sends to the process's ExceptionPort. Terminate the client process and verify that LPC_CLIENT_DIED message is received.

Experiment 3: Study the side effects of attaching a debugger to the client process. What happens in the server process when you break into the debugger in the client and resume execution?

Question: *The server received a single connection request from the client. How did the system manage to send the LPC_CLIENT_DIED notification too?*

Question: *Why does LPC need separate port objects for passing messages between user-mode processes and doesn't use the same mechanism used for dispatching exceptions?*