Least Privilege Separation Kernel (LPSK)

Accomplishments and Current Work
Outline

- Why are we talking about this here?
- What is a separation kernel?
- What is the LPSK?
- Progress with the LPSK
- Future work
- Demo
Digression…

- I think PowerPoint (and its ilk) are greatly misused.
- Therefore…
What is the relevance?
What is a Separation Kernel?
Partition Flow
As a VMM

<table>
<thead>
<tr>
<th>OS #1</th>
<th>OS #2</th>
<th>OS #3</th>
<th>OS #4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Separation Kernel
Separation Kernel Protection Profile (SKPP)

Click to edit Master subtitle style
Least Privilege Separation Kernel (LPSK)
Phase 1 LPSK Architecture
LPSK Config (1)

- **Audit**
  - Enabled?
  - Size of internal audit buffer
  - Action when audit is full

- **Run-time LPSK**
  - How shall kernel use the screen?
  - Reserved memory locations
LPSK Config (2)

- **Partitions**
  - Round robin duration for all partitions
  - For each partition
    - Active?
    - Percent of round robin duration
    - Percent of system RAM
  - Partition with initial I/O focus
  - Partition to handle SAK
Partition flow rules

- Processes in Partition ‘x’ can access Partition ‘y’ (RO or RW)
- Acyclic flow rules
LPSK Config (4)

- Imported files from disk
  - Location on disk
  - Home partition
  - Assigned PL
  - Audited events
LPSK Config (5)

- RAM segments
  - Size
  - Home partition
  - Assigned PL
  - Audited events
LPSK Config (6)

- **Devices**
  - Data channel or control channel
  - Home partition
  - Multiplexed or dedicated
  - Device specific attributes (e.g., keyboard buffer size)
  - Audited events
LPSK Config (7)

- **Processes**
  - Home partition
  - % of partition time slice

- **Subject definitions**
  - Code location and PL assignment
  - Kernel APIs allowed to use
  - Subject-to-resource flows allowed
  - (e.g., subject x can access device y)
  - Audited events
Funded Objective

Click to edit Master subtitle style
Progress Report

Click to edit Master subtitle style
What the Prototype has now

- Kernel config options
- Multitasking processes
- Segmented memory
- Device drivers for:
  - Disk drives (PATA/SATA)
- Inter-process communication using:
  - Eventcounts
  - Sequencers
  - Signals
  - Shared memory
- Kernel event auditing
- I/O focus
Outside the LPSK

Click to edit Master subtitle style
Future Work
Demo

Click to edit Master subtitle style