When Two Languages Are Simpler Than One
Lessons for SES from Cajita, Original-Caja, and Valija

Mark S. Miller
Simultaneous Problems

D = Defensive code problem
O = Offensive code problem
T = Legacy tools problem
C = Legacy code problem
Simultaneous Solution?

D = Defensive code problem
O = Offensive code problem
T = Legacy tools problem
C = Legacy code problem

Original-Caja       dOTc       Secure Linux/Windows
Cajita             DOT        Secure microkernel OS
Don’t try this at home (or at all)

D = Defensive code problem
O = Offensive code problem
T = Legacy tools problem
C = Legacy code problem

Original Caja dOTc Secure Linux/Windows
Cajita DOT Secure microkernel OS
Separate Solutions

D = Defensive code problem
O = Offensive code problem
T = Legacy tools problem
C = Legacy code problem

Cajita
DOT
Secure microkernel OS
Valija
OTC
Virtual Machine
Layered Solutions

\[ \begin{align*}
D &= \text{Defensive code problem} \\
O &= \text{Offensive code problem} \\
T &= \text{Legacy tools problem} \\
C &= \text{Legacy code problem} \\
V &= \text{Virtualizability problem}
\end{align*} \]

<table>
<thead>
<tr>
<th>Cajita*</th>
<th>DOT V</th>
<th>Secure microkernel OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valija</td>
<td>OTC</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>+ Valija on Cajita</td>
<td>DOTCV</td>
<td>VMM + policy glue logic</td>
</tr>
</tbody>
</table>
Lessons for SES

D = Defensive code problem
O = Offensive code problem
T = Legacy tools problem
C = Legacy code problem
V = Virtualizability problem

<table>
<thead>
<tr>
<th>SES</th>
<th>DOT</th>
<th>V</th>
<th>Secure microkernel OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>~Harmony-strict</td>
<td>OTC</td>
<td></td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>+</td>
<td>DOTCV</td>
<td></td>
<td>VMM + policy glue logic</td>
</tr>
</tbody>
</table>
Proposed SES Goals

- SES is smallest secure subset of ~Harmony-strict without loss of functionality.
- SES is a good target for a multiply instantiable embedding of ~Harmony-strict.

<table>
<thead>
<tr>
<th>SES</th>
<th>DOT V</th>
<th>Secure microkernel OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>~Harmony-strict</td>
<td>OTC</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>+ Safer scripting</td>
<td>DOTCV</td>
<td>VMM + policy glue logic</td>
</tr>
</tbody>
</table>
Questions?
Freeze Primordials
Hide Sharp Objects = Cajita
Cajita + Implementation
Replace with per-gadget toy knives
Valija on Cajita Impl
Valija Impl on Cajita Impl