AGS Virtual Guard Server (AGS VGS)

- **Guard sanitizes (downgrades) high-level**
  - Available at a lower level, **only** if meet constraints
  - For example, message contain no “dirty words”

- **Low-assurance is complicated & expensive**
  - “Server farms” with separate guard boxes per policy
  - Large monolithic platform & algorithm C&A effort

- **VGS uses COTS GEMSOS Class A1 platform**
  - Run multiple diverse downgrading algorithms on VGS
  - Scalable high performance – multiprocessor RTOS
  - High-assurance each instance is isolated and protected
  - Assured pipelines for messages in and out
  - Dramatic recertification reduction – just downgrading
Notional High-to-Low Guard Architecture

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Read Label</th>
<th>Write Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Process Family</td>
<td>Read: H</td>
<td>Write: H</td>
</tr>
<tr>
<td>Release Process</td>
<td>Read: H</td>
<td>Write: L</td>
</tr>
<tr>
<td>Low Process Family</td>
<td>Read: L</td>
<td>Write: L</td>
</tr>
</tbody>
</table>

- **High Buffer**
  - Label: H
- **Low Buffer**
  - Label: L
- **Message Handler**
- **Trusted Guard Function**
  - (e.g. Dirty Word)
- **Queue Synchronization**
  - (GEMSOS Advance)

- **MAC (MLS)**
- **TCB**
- **Ethernet NICs**
  - Label: H
- **GTNP (GEMSOS)**
- **Clock Disks**
  - Label: L
- **Network Clients**
  - Label: H
AGS Virtual Guard Server (AGS VGS)

- Guard sanitizes (downgrades) high-level

- Low-assurance is complicated & expensive

- VGS uses COTS GEMSOS Class A1 platform
  - Run multiple diverse downgrading algorithms on VGS
  - Scalable high performance – multiprocessor RTOS
  - High-assurance each instance is isolated and protected
  - Assured pipelines for messages in and out
  - Dramatic recertification reduction – just downgrading
A COTS, Virtualized, Adaptable, High-Assurance Guard Server

Dr. Roger R. Schell
Roger.Schell@aesec.com

Mark R. Heckman
mark.heckman@aesec.com

Edwards E. Reed
ed.reed@aesec.com

ACSAC 2011 Work in Progress
Orlando, Florida
December 7, 2011