Overview

• Motivation and Goal
• Terminology
• Architectural Overview
• Surrogate Selection and Automated Provisioning
• Current Results
• Use Cases
• Next Steps and Future Work
• Questions
Team

Jeff Boleng, PhD – CMU SEI
Grace Lewis – CMU SEI
Vignesh Shenoy – CMU INI
Varun Tibrewal – CMU INI
Manoj Subramaniam – CMU INI
Sebastian Eschevarria – CMU SEI
Ben Bradshaw – CMU SEI

CMU: Carnegie Mellon University
SEI: Software Engineering Institute
INI: Information Networking Institute
Motivation and Goal

Goal
A secure and assured digital container format for mobile computing components

Technical Challenges
Myriad of languages, architectures, platforms, APIs, etc. create an exponential challenge for software portability, interoperability, security, and assurance

Key Idea
Define software portability execution characteristics and an accompanying digital container format to enable secure and assured mobile computing components

Impact
Agile software components which can be trusted and executed to provide results across the spectrum of computing platforms
Goal (expanded)

Mobile computing components that are

- Automatically provisioned
  - JIT provisioned
  - Technology agnostic
  - Dependency fulfillment
- Secure
  - Trusted computing component
  - Trusted computing provider
- Assured
  - Input and output format validation
  - Pre/post conditions
  - Run-time invariants
Approach and Assumptions

Demonstrate full end to end solution
  • Each component may be sub-optimal

Digital container for computing components
  • Extend DMTF OVF file format

OVF format
  • Xml descriptor with packaged components (tar)

Proper packaging is critical

Ultimately demonstrate composability
Elements of the Solution

Automatically provisioned

- JIT provisioning → todays details
- Technology agnostic → run time environment specified
- Dependency fulfillment → prototype using Docker and LXC

Secure

- Trusted computing component → OVF code signing
- Trusted computing provider → Certificates and TLS

Assured

- Input and output format validation → using MIME types and Tika
- Pre/post conditions → ??? Proof carrying code ???
- Run-time invariants → ??? Proof carrying code ???
Terminology

Mobile Device
  • Self explanatory

Client Application
  • Application running on the mobile device communicating to the Application Server

Offload Element
  • Computing component that migrates to the surrogate

Surrogate Client
  • Service running on the mobile device for discovery, provisioning, and offload

Validation Service
  • I/O and assurance validation

Surrogate
  • Infrastructure server (cloud or cloudlet)

Surrogate Server
  • Service running on the surrogate for discovery, provisioning, and offload

Application Server
  • Run-time instantiation of the offload element

Sandbox
  • Computing environment the application server executes in
Architecture Overview
1. Discovery and Provisioning
   a) **Surrogate Server** beacons availability
   b) **Surrogate Client** contacts **Surrogate Server** and establishes TLS connection
      - Surrogate checks Mobile Device certificates
      - Mobile Device checks Surrogate certificates
   c) **Surrogate Client submits requirements to Surrogate Server and keeps TLS connections alive**
   d) **Surrogate Selection**
   e) Surrogate Client selects best Surrogate, terminates all other TLS connections
   f) Surrogate Client sends payload to selected **Surrogate Server**
   g) **Surrogate Server** verifies payload integrity via code signing in metadata
   h) **Surrogate Server** provisions an execution **Sandbox** for payload based on the execution type in the metadata (bytecode, script, vm, etc.)
Provisioning, Deployment, and Execution

i) Surrogate Server provisions the execution Sandbox with the Offload Element

j) Surrogate Server provisions the execution platform with Validation Service (currently using Apache Tika) and satisfies dependencies

k) Surrogate Server passes back IP address and port of Validation Service back to Surrogate Client

l) Surrogate Client starts Client Application with IP and Port

m) Client Applications sends data to Validation Service on Surrogate

n) Validation Service enforces data input format

o) Validation Service passes data to Application Service

p) Application Service executing in Sandbox on Surrogate computes result and passes it back to Validation Service on the Mobile Device

q) Validation Service on Mobile Device enforces result format

r) Validation Service passes result (or error) to Client Application

s) Loop to M or end
# Run-time Environment

## Software execution characteristics

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>Components are portable across computing platforms and architectures using virtual machine, either with a host OS or a hypervisor</td>
</tr>
<tr>
<td>Emulation</td>
<td>Components are portable by running on a machine emulator</td>
</tr>
<tr>
<td>Platform</td>
<td>Components are portable by running in a common, standards based platform, such as a web browser (potentially enables byte code and interpreted portability)</td>
</tr>
<tr>
<td>Byte code</td>
<td>Portability is achieved through prior or just-in-time compilation to a common byte code and VM layer (e.g. JVM, CLR, Flash, etc.)</td>
</tr>
<tr>
<td>Interpreted</td>
<td>Portability is achieved with a common interpreter running on multiple computing platforms</td>
</tr>
<tr>
<td>API</td>
<td>Portability is achieved via source code re-compilation using a standard API (e.g. OpenGL, Qt, DirectX, etc.)</td>
</tr>
<tr>
<td>Distribution</td>
<td>Portability is achieved via package distribution and repositories supporting various computing platforms, either by binary distribution (e.g. rpm, apt, etc.) or source code distribution (e.g. gentoo/portage)</td>
</tr>
<tr>
<td>Binary</td>
<td>Binary executables run natively on different platforms with no recompilation (could require supporting OS, e.g. Portable Apps, or run as an embedded system), static vs. dynamic linkage</td>
</tr>
<tr>
<td>Service</td>
<td>Existing cloud service exists to provide a solution and connectivity to it is available and secure</td>
</tr>
</tbody>
</table>
Software execution landscape (notional)

- **Component Size**: Large, Small
- **Ubiquity**: Low, High

- **Distribution**
- **Interpreted API**
- **Byte Code**
- **Emulation**
- **VM**

*Requires secure and assured infrastructure access*
Surrogate Selection

- Component creator determine minimum and optimal execution parameters when packaging
  - Currently memory, CPU, and disk
  - Assigns weights (1-100) that must total 100
- Multiple offload elements and multiple surrogates
- Mobile sends requirements for container execution
- Surrogate determines if it can execute component
- Surrogate calculates capability score
- Mobile calculates final performance score and selects Surrogate

Note: Investigating effects of caching
Capability Score

\[ SC_i = \frac{(C_i - R_i)}{R_i} \]

\[ \varphi = \sum (SC_i \times W_i) \]

SC\(_i\) – Surplus Capability of Surrogate for the resource ‘i’
C\(_i\) – Capability of surrogate for resource ‘i’ (or optimal requirement*)
R\(_i\) – Requirement of the offload element for resource ‘i’
W\(_i\) – Weight associated with resource ‘i’
\( \varphi \) – Capability score of the surrogate for the particular offload element

*ensures Surrogate cannot “cheat” and capture all offload elements
Size Benefit

\[ sb = \frac{\text{Max Size} - \text{Size}}{\text{Max Size}} \times 100 \]

- \textit{Max Size} – Size of the biggest offload element
- \textit{Size} – Size of the offload element in consideration
Performance Score

$$\rho = \phi + (x \ast sb)$$

- $\rho$ – Final performance score of the Surrogate for the Offload Element
- $\phi$ – Capability score of the Surrogate for the particular Offload Element
- $x$ – Network performance factor
- $sb$ – Size benefit of the Offload Element
Testing Approach

Face detection
• Java and python containers

Prime number calculation
• Java, python, and C executable containers

\[ \text{Time-to-Result} = \text{Surrogate Discovery Time} + \text{Surrogate Selection Time} + \text{Offload and Deploy time} + \text{Input/Output communication time} + \text{Input/Output Validation time} \]
Sample Timing (prime number calculation)
Testing Scenario

- Select correct offload element for surrogate capability
- Select offload element with smallest weight if all capability scores were equal
- Select best surrogate with differing capability scores
- Still experimenting with TTR
# Initial Test Results

**Test Case 1:**

<table>
<thead>
<tr>
<th>Selected Cloudlet</th>
<th>Discovery Time</th>
<th>Deploy Time</th>
<th>Average IO Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java 1.0GHz, 4096MB</td>
<td>270</td>
<td>100</td>
<td>280</td>
</tr>
<tr>
<td>Java 3.0GHz, 1000MB, 2.0</td>
<td>240</td>
<td>100</td>
<td>260</td>
</tr>
<tr>
<td>Cloudlet 3</td>
<td>180</td>
<td>100</td>
<td>220</td>
</tr>
<tr>
<td>Java 2.0, 3072MB</td>
<td>60</td>
<td>100</td>
<td>140</td>
</tr>
<tr>
<td>CPU:10,RAM:90</td>
<td>150</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>CPU:20,RAM:80</td>
<td>120</td>
<td>100</td>
<td>180</td>
</tr>
<tr>
<td>CPU:40,RAM:60</td>
<td>60</td>
<td>100</td>
<td>140</td>
</tr>
<tr>
<td>CPU:50, RAM:50</td>
<td>30</td>
<td>100</td>
<td>120</td>
</tr>
</tbody>
</table>

**Java 1.0GHz, 4096MB**

- **CPU:20,RAM:80**
  - Discovery Time: 240
  - Deploy Time: 180
  - Average IO Time: 1

- **CPU:40,RAM:60**
  - Discovery Time: 180
  - Deploy Time: 160

- **CPU:50, RAM:50**
  - Discovery Time: 150
  - Deploy Time: 150

- **CPU:60, RAM:40**
  - Discovery Time: 120
  - Deploy Time: 120

- **CPU:80, RAM:20**
  - Discovery Time: 60
  - Deploy Time: 60

- **CPU:90, RAM:10**
  - Discovery Time: 30

(Selected data only changes as shown)

**RAM - min-512MB Max-2048MB**

**CPU - min-1GHz Max 2GHz**

(Selected Cloudlet score, final performance score considering the size of the package)
## Use Cases

### Compute Rqmts
- Available Memory: XXX
- Available Disk: YYY
- Platform: ZZZ
- Connected to Cloud?: Yes/No

### Signature & ID

### I/O formats

### Dependencies

### Assurance Rqmts

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Emulation</th>
<th>Platform</th>
<th>Byte code</th>
<th>Interpreted</th>
<th>API</th>
<th>Distribution</th>
<th>Binary</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAMCC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloudlet Metadata</th>
<th>Available Memory</th>
<th>Available Disk</th>
<th>Platform</th>
<th>Connected to Cloud?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XXX</td>
<td>YYY</td>
<td>ZZZ</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

| Team A              |                 |               |          |                    |

<table>
<thead>
<tr>
<th>Cloudlet Metadata</th>
<th>Available Memory</th>
<th>Available Disk</th>
<th>Platform</th>
<th>Connected to Cloud?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XXX</td>
<td>YYY</td>
<td>ZZZ</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connected to Cloud?</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use Cases

- Cyber foraging
- Rapid re-configuration of deployed sensors
- Distribute search logic in large scale distributed databases
- Interoperability or translation for existing or legacy systems
- Service market place of composable computing components
  - Image processing
  - Speech recognition
- Crowd analysis
  - Extend MIT “mood meter” with offload elements and mobile devices
  - POI location via face detection and recognition
Next Steps and Future Work

• Finish prototype using Docker and all other existing components
• More testing
  • Dependency satisfaction
  • Input/Output validation
    • Need to get output validation functioning on mobile device
  • Wide range of offload elements
  • Wide configuration of Surrogates
• Open source the solution
• Propose formal extensions to DMTF OVF (tentative)
• Demonstrate component composability
• Examine deeper assurance solutions (e.g. DNS Server component)
  • Pre/post condition specification and enforcement
  • Run-time invariant specification and enforcement
• Populate project artifacts on SATURN blog
Questions and Feedback

Thank you for your time and attention.

We welcome feedback and collaboration.

Please contact me at jlboleng@sei.cmu.edu with questions or feedback.