Exploring research collaborations between University of Puerto Rico and Brazil

José R. Ortiz-Ubarri  
Computer Science Department  
University of Puerto Rico

Collaborators: Edusmildo Orozco, Rafael Arce, Humberto Ortiz, Francis Castro, CSLab students

SwitchOn Workshop 2015
Puerto Rico is right here!
My path to Sao Paulo!!!

from SJU to MIA
My path to Sao Paulo!!!

- from SJU to MIA
- from MIA to GRU
University of Puerto Rico
Rio Piedras Campus

Computer Science
Department

- 9 full time professors
- Undergraduate program
- Working on a graduate program
Our work

- Educational projects to improve CS curriculum and the way computer science is taught at the University of Puerto Rico

- Application of High Performance Computing to solve computationally intensive scientific problems

- Computer and Network security
Educational work

- Educational projects to improve CS curriculum and the way computer science is taught at the University of Puerto Rico
  - J. Ortiz-Ubarri, R. Arce-Nazario, I. Rubio. *Development of engaging and readily transferable laboratory experiences for the introductory programming course*. National Science Foundation under Grant No. DUE-1245744.
Application of HPC

- Application of High Performance Computing to solve computationally intensive scientific problems
  - Periodic Arrays for application in multiple target recognition, optical orthogonal codes, and digital watermarking
  - Enumeration of permutation polynomials for applications in cryptography
  - Scientific data analysis and visualization
Costas problem example

- The enumeration of two-dimensional Costas arrays is a problem with factorial time complexity and has been solved for sizes up to 29 using computer clusters.
- Costas arrays of higher dimensionality have recently been proposed and their properties are beginning to be understood.
- We presented the first implementations for enumerating these multidimensional arrays in GPUs and FPGAs, as well as the first discussion of techniques to prune the search space and reduce enumeration run time.
Both GPU and FPGA implementations rely on Costas array symmetries to reduce the search space and perform concurrent explorations over the remaining candidate solutions.
Computer and Network security

- With our undergraduates we have been working in applications for network monitoring for situational awareness and computer and network forensics

  - **Tools to monitor our Science DMZ**

  - **Web based network visualizations**
    - Toa, a web based application for network situational awareness

  - **Computer forensics tools**
Toa features

• Web implementation based on bootstrap.
  • main web interface fits nicely in tablets and smartphones

• Interactive charts capable of listening to events.
  • used to connect charts to plugins

• Query the sensor data in the database and generate graphs.

• Parallel implementation of the parser and the grapher.
Generic data preparation process

For each sensor:

Raw data → Filter → Render vis → Vis

http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf
Toa data preparation process

Raw data collector -> Filter guided by sensors configured in DB parser -> For each sensor Render vis grapher -> Vis Web interface
Toa: Overview

Cron triggers the parser and grapher every 5 minutes.

System configuration and parsed data.

Parser → Grapher → GUI

Collector stores NetFlows in a FS.

User clients connect to the TOA web service.
The web GUI presents users with the following network traffic visualization options:

- per network (interface, Autonomous System [AS], or network block (CIDR)) traffic,
- per-port traffic for each network,
- network to network traffic.
By Network: RRP

RRP Interface Graphs by Day

- Octets
By Network: RRP

- Octets
- Packets
By Network: RRP

- Octets
- Packets
- Flows
By Network: RRP, port 22 (ssh)

- Octets
- Packets
- Flows
- Combined
From Network 2 Network

- Octets
- Packets
- Flows
- Combined
## Top 100

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Flows</th>
<th>Octets</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>188.145.101.15</td>
<td>72.88-KB</td>
<td>89.37-MB</td>
<td>64.00-bytes</td>
</tr>
<tr>
<td>186.145.182.24</td>
<td>181.12-KB</td>
<td>31.25-MB</td>
<td>94.21-KB</td>
</tr>
<tr>
<td>186.145.182.21</td>
<td>200.90-KB</td>
<td>25.03-MB</td>
<td>22.28-KB</td>
</tr>
<tr>
<td>186.145.138.238</td>
<td>12.87-KB</td>
<td>16.26-MB</td>
<td>11.00-bytes</td>
</tr>
<tr>
<td>186.145.186.198</td>
<td>6.34-KB</td>
<td>8.78-MB</td>
<td>1.00-bytes</td>
</tr>
<tr>
<td>186.145.180.150</td>
<td>6.23-KB</td>
<td>5.97-MB</td>
<td>594.00-bytes</td>
</tr>
<tr>
<td>186.145.87.47</td>
<td>6.64-KB</td>
<td>5.12-MB</td>
<td>574.00-bytes</td>
</tr>
<tr>
<td>186.145.180.118</td>
<td>5.63-KB</td>
<td>4.97-MB</td>
<td>29.00-bytes</td>
</tr>
<tr>
<td>186.145.182.11</td>
<td>48.37-KB</td>
<td>2.94-MB</td>
<td>5.88-KB</td>
</tr>
<tr>
<td>186.145.196.137</td>
<td>3.21-KB</td>
<td>2.20-MB</td>
<td>508.00-bytes</td>
</tr>
<tr>
<td>186.145.239.180</td>
<td>21.35-KB</td>
<td>2.67-MB</td>
<td>2.77-KB</td>
</tr>
<tr>
<td>186.145.180.200</td>
<td>4.82-KB</td>
<td>3.25-MB</td>
<td>821.00-bytes</td>
</tr>
<tr>
<td>186.145.239.179</td>
<td>24.30-KB</td>
<td>2.60-MB</td>
<td>3.34-KB</td>
</tr>
<tr>
<td>186.145.180.154</td>
<td>1.91-KB</td>
<td>2.22-MB</td>
<td>496.00-bytes</td>
</tr>
</tbody>
</table>
### Top 100 Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Flows</th>
<th>Octets</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>221.80-KB</td>
<td>62.35-MB</td>
<td>41.80-KB</td>
</tr>
<tr>
<td>80</td>
<td>309.99-KB</td>
<td>25.80-MB</td>
<td>36.64-KB</td>
</tr>
<tr>
<td>49135</td>
<td>18.00-KB</td>
<td>17.49-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>465</td>
<td>9.86-KB</td>
<td>11.72-MB</td>
<td>31.00-byte</td>
</tr>
<tr>
<td>26181</td>
<td>7.54-KB</td>
<td>10.44-MB</td>
<td>2.00-byte</td>
</tr>
<tr>
<td>59040</td>
<td>7.37-KB</td>
<td>8.36-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>5001</td>
<td>3.47-KB</td>
<td>5.09-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>65199</td>
<td>2.04-KB</td>
<td>8.07-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>18514</td>
<td>2.00-KB</td>
<td>4.17-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>50078</td>
<td>2.43-KB</td>
<td>3.36-MB</td>
<td>2.00-byte</td>
</tr>
<tr>
<td>36766</td>
<td>1.46-KB</td>
<td>2.00-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>41130</td>
<td>1.28-KB</td>
<td>1.68-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>55443</td>
<td>1.10-KB</td>
<td>1.00-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>26181</td>
<td>1.26-KB</td>
<td>1.51-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>30039</td>
<td>1.04-KB</td>
<td>1.44-MB</td>
<td>2.00-byte</td>
</tr>
</tbody>
</table>
Graph Events

- A dialog generated when the user clicks a time point.
Cube Example
Example of Possible Threats

- Network scan
- Port scan
Graph Example
References:


Thanks!

jose.ortiz23@uprrp.edu