SciGuard: A Security Architecture for Science DMZ based on SDN and NFV

A collaborative project between Clemson and ASU

Clemson: Hongxin Hu, Richard Brooks, Kuang-Ching Wang, Nuyun Zhang
ASU: Gail-Joon Ahn, Dijiang Huang, Adam Doupe

Presented at NSF CC* PI Workshop Panel on Securing the Science DMZ
Research as a Service (RaaS) Model

- Customizable R&D and Education Support
- Data Services
- Federated IDM & Isolation
- Distributed & Federated Cloud
- Security Policy Enforcement
- Heterogeneous Hardware Farm

- Cloud
- Meta-Data
- FISMA MODERATE
- HIPPA COMPLIANT
- RESTful API
- RAW DATA SOURCE (.bam, .vcf, .cds, .fastq)
- STORAGE FEDERATION

- Research as a Service / RaaS Schema

-Jay Etchings, Research Computing Senior Architect, Arizona State University
Support Entrepreneurs and Spin-offs

<table>
<thead>
<tr>
<th>Key Metrics</th>
<th>FY 2015 (YTD)*</th>
<th>FY 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intellectual Property Disclosures</td>
<td>248</td>
<td>261</td>
</tr>
<tr>
<td>Issued US Patents</td>
<td>54</td>
<td>56</td>
</tr>
<tr>
<td>Exclusive Licenses/Options</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>Nonexclusive Licenses/Options</td>
<td>30</td>
<td>27</td>
</tr>
<tr>
<td>Start-ups</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>AzTE Assisted Industry Sponsored Research (ISR) Awards</td>
<td>$9.6M**</td>
<td>$12.7M</td>
</tr>
<tr>
<td>Gross Revenue</td>
<td>$2.0M***</td>
<td>$4.3M</td>
</tr>
</tbody>
</table>

* May 29, 2015
** Includes agreement modifications and amendments facilitated by AzTE, through March 2015
*** Includes Sanford Harmony FY2015 (YTD) EULA income
Browser + Internet: No software setup hassle

A Cloud-Based Virtual Laboratory for Cybersecurity Education
Science DMZ

Science DMZ: a high performance network environment to support big data transfer and access to high-performance computation

- Typically deployed at the edge of a university’s network
- Simple Science DMZ
Science DMZ Security Challenge

- **Institutional firewalls** are ill-suited to high-performance science environments
  - Designed to support a large number of small traffic flows rather than the small number of large flows in data-intensive science

- The Science DMZ model proposed by **Esnet** suggests to use router/switch **ACLs (access control lists)**
  - Stateless
  - Static rules
    - Proactively installed
    - Memory cost
    - Performance impact
  - Per-packet processing
    - Performance bottlenecks
SciGuard

A Security Architecture for Science DMZ based on SDN and NFV

- Task 1: SDN firewall application for securing science DMZ
- Task 2: NFV-based virtual IDS for securing science DMZ
- Task 3: Cloud-based Federation for the science DMZ
SciGuard

Task 1: Developing an SDN Firewall Application for Securing Science DMZs

FlowGuard Firewall Overview

- **High scalability**
  - Stateless: Per-flow processing
  - Stateful: Per-connection processing

10-millisecond latency
FlowsGuard Firewall Overview
SciGuard

Task 2: Building an NFV-based **Virtual IDS** for Securing Science DMZs

- Quickly instantiated and elastically scaled to deal with attack traffic variation

**Research Challenges**
- Traffic winnowing
- Flow correlation
- Safe state migration
- Optimal provision
SciGuard

Task 3: Cloud-based Federation for the Science DMZ

- Security Policy Automatic Testing
- Security Intelligence Sharing
- Customizable user research/education management platform
SciGuard

Thank you!