Neuromorphic Data Microscope
CLSAC’16
October 28, 2016
David Follett
Founder, CEO
Lewis Rhodes Labs (LRL)
david@lewis-rhodes.com
978-273-0537
Vision

Neuromorphic Processing Units (NPUs)

*stunningly power efficient at pattern matching*

Data Center & Cloud Impact

*profoundly changes economics*
Why Neuromorphic?  
**Power/op & Cost/op**

- **>500 IDS Servers**
  - 500,000 W
  - 14,000 lbs
  - $2,500,000

- **5 FPGA Neuromorphic Cyber Microscopes**
  - 2,500 W
  - 200 lbs
  - $125,000

- **1 ASIC Neuromorphic Cyber Microscope**
  - 50 W, 1 lb
  - $500

- **All 4,036 “Emerging Threats” PCREs (1/16)**
  - Pervasive examination (no directives)

**Performance Gains**
- **Power/op:** > 1M
- **Cost/op:** > 1M
Neuromorphic is very Different

Legacy Von Neumann Architecture (CPU)
- **Complex processor**
  - Extraordinarily flexible
  - Data processing via sequential instructions
- **Simple memory**

Neuromorphic Processing Unit (NPU)
- **Simple processor**
  - Massively parallel integrators
- **Complex memory**
  - Data processing via efficacy & temporal/spatial mapping
  - Processing is multi-dimensional
Computer Science Perspective

(Un)Structured Input Stream(s) → Neuromorphic Processor → Policy Recognition: Find $E_x^n$, n >> 1

Behavioral: Find $!E_x^n$, n >> 1

Structured Output → Metadata → Stream

- Behavior
- Match
- Classification
- Filter
- Prediction
- Pipeline
Some Interesting Features

❖ NPU integrates key mission requirements, ex.,
   ➢ Context switching
   ➢ Dynamic programmability
   ➢ Behavioral characterization
   ➢ Time & Order invariance
   ➢ Pervasive analysis
   ➢ Basic statistical operations

❖ Current device uses a single neuron type
   ➢ Can extend HW architecture through novel neurons
   ➢ Example: more complex statistical operations
Scalability

**Device**
Bandwidth x Expressions = Constant

<table>
<thead>
<tr>
<th>Device</th>
<th>Bandwidth</th>
<th>Expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPGA</td>
<td>2.5 Gb/s</td>
<td>≈ 1,000</td>
</tr>
<tr>
<td></td>
<td>5 Gb/s</td>
<td>≈ 500</td>
</tr>
<tr>
<td></td>
<td>10 Gb/s</td>
<td>≈ 250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>etc.</td>
</tr>
<tr>
<td>ASIC</td>
<td>20 Gb/s</td>
<td>≈ 20,000</td>
</tr>
<tr>
<td></td>
<td>40 Gb/s</td>
<td>≈ 10,000</td>
</tr>
<tr>
<td></td>
<td>80 Gb/s</td>
<td>≈ 5,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>etc.</td>
</tr>
</tbody>
</table>

**System**
Arbitrary Depth & Width

- Input Stream
- Control
- Output Stream
- Output
Latest Product

Intrusion Detection System
ex. WaterSlide, Proprietary

Commodity Server

PCRE Compiler

IDS Patches

DMA Driver

Neuromorphic Data Microscope
Version 4.0

Neuromorphic Processor
PCIe
Standards Hide Complexity

Application (Suricata, etc.)

APIs
- Result
- Cmd & Cntl
- Config

Neuro Compiler

Compiled Elements
- A=[a.1,a.2,a.3…]
- B=[b.1]
- C=[c.1,c.2,c.3]
- ...

PCI Card

NPU

DMA Driver

Loader

PCIe Bus

Data Stream

Cmd & Cntl

Config

Signatures
- Regex, etc. {A,B,C,…}

Compiler

Sandia ported to Quiz Kid (aka WaterSlide)
Throughput Efficiency

Note 1: Theoretical Max bounded by context switching
Note 2: Un-optimized generic Altera DMA Interface
Note 3: CUDA style DMA planned for next generation
Graph Analytics Scaling Example

Parallel Application Support
- Applications completely Independent
  - No performance degradation
- Integrated cloud extremely scalable
CYBER APPLICATION
Exemplar Intel Community IDS

Facility B

NAS
Blade Servers

Software Sensors

Facility A

NAS
Blade Servers

Network Security

Policy Control
Suricata, etc.

Alerts

Operational Intelligence
Splunk, etc.

analysts

Internet

Neuromorphic Cyber Systems
Practical Considerations

- **Hardware sensor cost extremely high**
  - ex. 10GbE IDS >$100k
  - Cost limits **number & resolution** of HW sensors

- **Software sensors often resource intensive**
  - ex. ROP detectors require most of the CPU
  - Cost limits **number & resolution** of SW sensors

- **Analyst’s priority, reduce False Negatives**
  - Achieved by detuning sensors, ie. large # of False Positives
  - Major source of noise, direct result of sensor cost

- **Detuned sensors are more vulnerable to attack**
  - Spoofing & Flooding are common
Analyst’s Top Priority

Signal/Noise is killing analyst community

False Positives must be Reduced
Root Cause: Resolution

State-of-the-Art Sensors

- **Cost** limits resolution
- **TPs** identified but
- Many **FPs** captured
- Splunk database,
  - Low Accuracy
  - Poor signal/noise ratio
  - It’s still a haystack
- **S/N** is killing the analysts

- True Positives (**TP**)
- Potential False Positives (**FP**)
- Expression Coverage
Neuro: Resolution
Cyber Microscope

Neuromorphic

- Speed creates resolution
  - Same number of **TPs**
  - Dramatically fewer **FPs**
- Greater Accuracy
- Higher Signal/Noise ratio
- Profound impact on analysts

- **True Positives (TP)**
- **Potential False Positives (FP)**
- **Expression Coverage**
Analyst’s Second Priority

Reduce False Negatives

Internet

Network

Servers Cloud

Storage NAS, SAN

Hardware Sensors

Software Sensors

Operational Intelligence Splunk, etc.

analysts

Behavioral Prediction Required

True Positive

False Positive

False Negative

Neuromorphic Cyber Systems
Root Cause: Temporal Variance
Simplest form of behavior prediction

State-of-the-Art Sensors
ex. Suricata

- Temporal variance is common
  - Shifting offsets
  - Re-ordering
  - Easily implemented by attacker

- Very costly to address
  - Pervasive analysis
  - Associative analysis

- True Positives (TP)
- Temporal Variants, Potential (FN)
- Expression Coverage
Neuro: Temporal Variance

**Neuromorphic**
- Pervasive analysis is innate
  - Evaluates every byte
  - Limiting this costs resources
- Associative analysis is innate
  - Metadata reordering
- Reduced False Negatives **FN**
  - Behavioral Prediction
- Profound impact on Analysts

**Temporal Variants**
- True Positives (TP)
- Temporal Variants, Potential (FN)
- Expression Coverage

**Attack Vector Classes**
Neuro Addresses Core Issues

- Internet
- Servers
- Cloud
- Storage
- NAS, SAN
- Network
- Neuro Sensors
- Operational Intelligence
  Splunk, etc.
- analysts
- Increased True Positives
- Reduced False Positives
- Reduced False Negatives

True Positive  False Positive
False Negative
Operational Control

Application

cyber, image/video analysis, novel event detection, graph analytics, speech recognition, etc.

Behavioral
Identify $t_n$, $n >> 1$
ex., syscall graph

Recognition
Find $t_n$, $n >> 1$
ex., signatures

Data Stream(s) → NPU → Result(s)

Neuromorphic Cyber Systems
Cyber Microscope Product Rollout

1\(^{st}\) Generation (FPGA) 2\(^{nd}\) Generation (ASIC) 3\(^{rd}\) Generation (ASIC)

- Intrusion Detection System Acceleration
- Security Alert Management Acceleration
- Host Behavioral Analysis
- IDS
- SAM
- Behavioral
- IDS System on Chip
Conclusions

❖ Neuromorphic will revolutionize cyber defense
  ➢ Dramatic reductions in power/op
    • FPGA, >1,000x
    • ASIC, >1,000,000x
  ➢ Plethora of powerful novel features
    • Order & time invariant, Sessionization, Behavioral prediction

❖ Operational readiness is close
  ➢ Compatible with existing standards & infrastructure
    • Sandia ported Quiz Kid (aka WaterSlide), 4 week effort
  ➢ 4th gen FPGA systems available in November