

Real-time Protocol Shepherds

Cyber Security Division 2012 Principal Investigators' Meeting

11 Oct 2012

Ron Watro
Lead Engineer
BBN Technologies
rwatro@bbn.com
617-873-2551 (office)
781-710-5016 (cell)

TTA 5 Overview

TTA #5: Secure, Resilient Systems and Networks

- TTA 5 addresses survivable and time-critical systems
 - Survivable = fulfills mission in presence of adversity
 - Time critical = needs faster-than-human response
- Recognition that today's systems are constantly under attack
- Interest in applicability to critical infrastructure services

Project Team

Ron Watro

Dan Wyschogrod

David Mandelberg

Bill Mackiewicz

RePS Overview

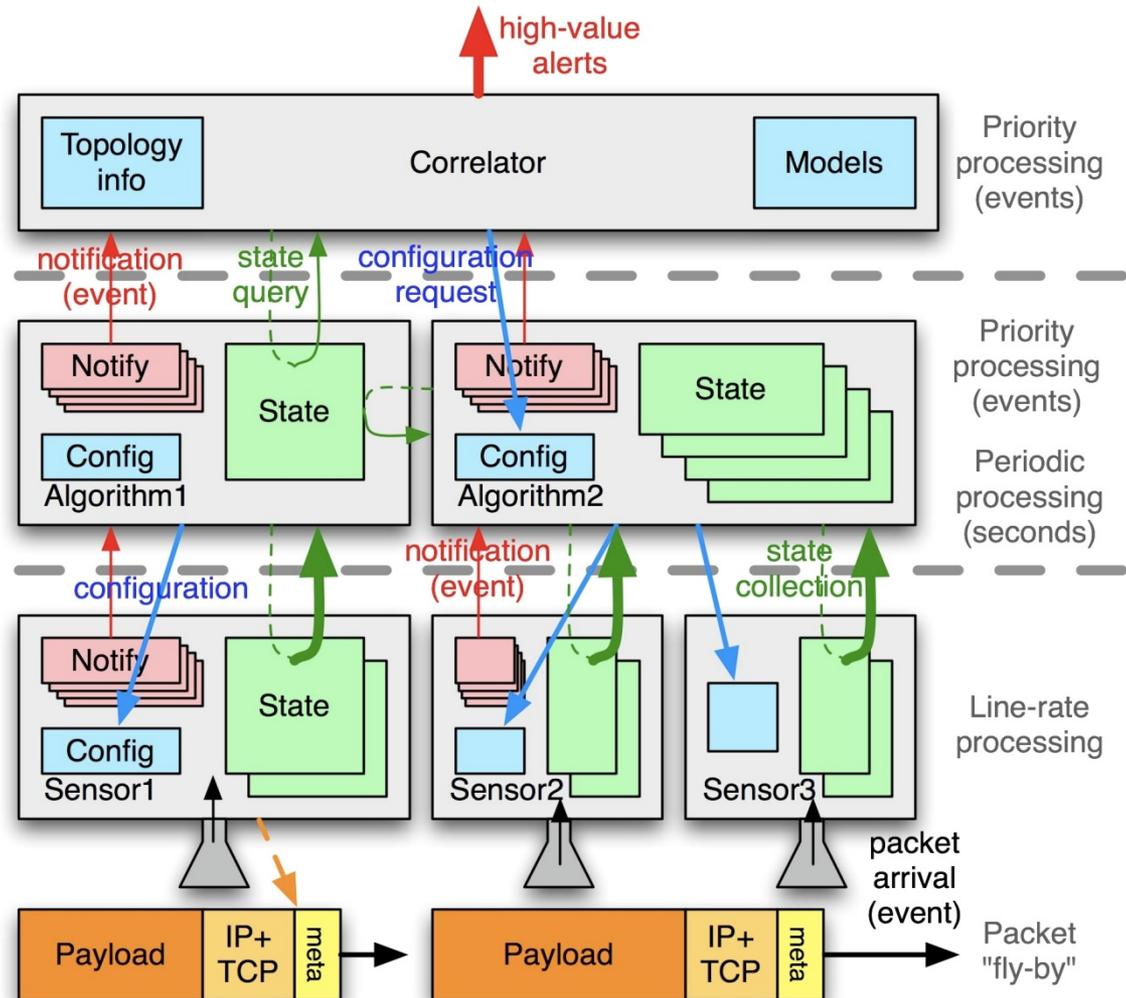
- RePS is a 1-year, Type III (Mature Technology) project
- RePS is based on the completed BBN SMITE project
- SMITE = Scalable Monitoring in the Extreme
- SMITE was the key project in the Scalable Network Management (SNM) program at DARPA
- **RePS and SMITE are NIDS**
 - NIDS = Network-based Intrusion Detection Systems
 - NIDS are often signature-based or anomaly-based
 - RePS/SMITE is an alternate approach based on behavior against a model (as opposed to trained behavior)
 - SMITE focused on fast (up to 100 Gb/sec) networks
- **RePS adds response actions to SMITE and refits it on open source tools**

NIDS Comparisons

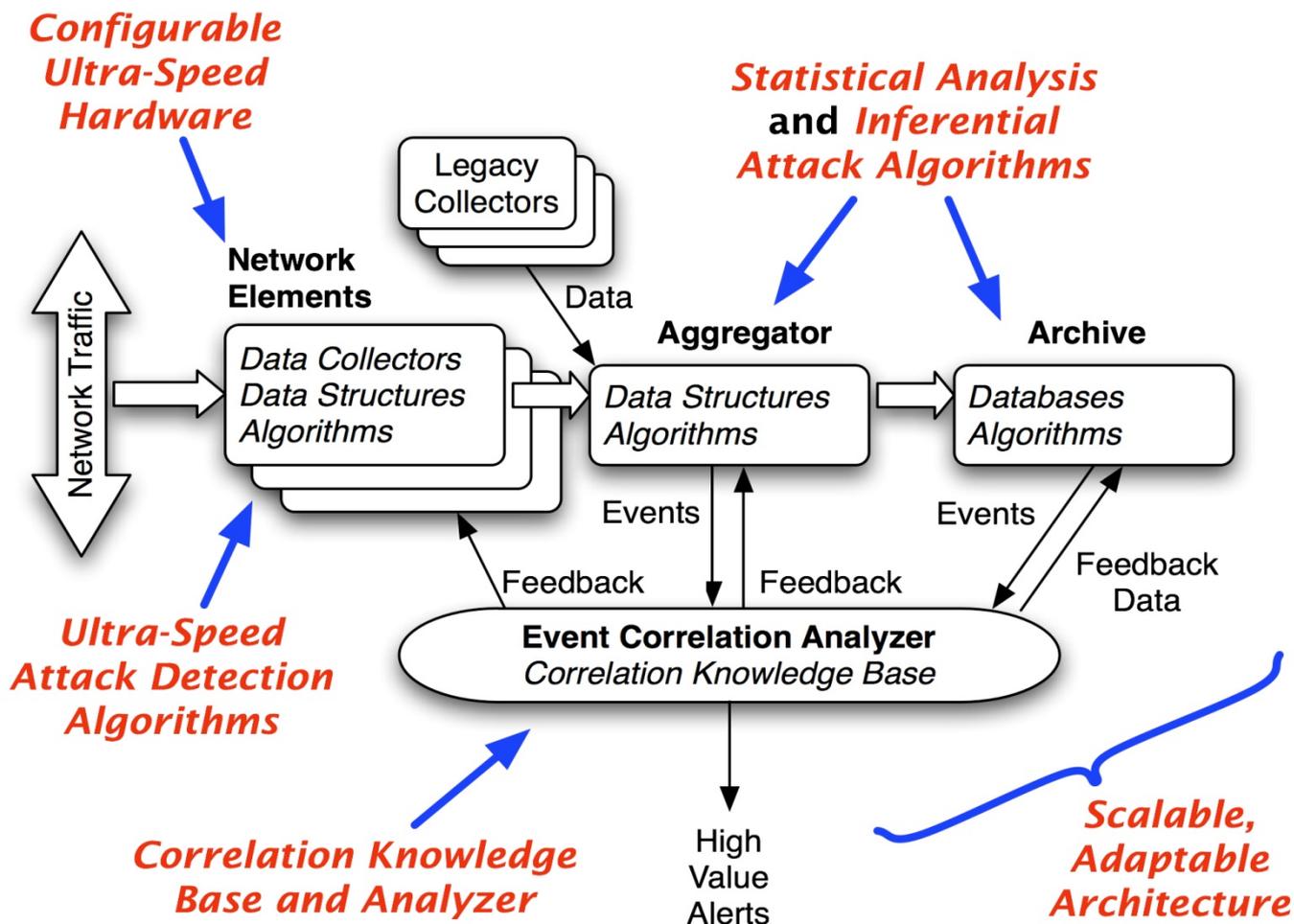
	Signature	Anomaly	SMITE
Coverage			
Known signatures	✓		
Deviations from trained	N/A	✓	N/A
Deviations from normal		✓	✓
Encrypted attacks		Some	Some
Extensible	✓		✓
Scales w/ population	✓		✓
Scales w/ traffic			✓
Scales w/ attack type	✓		✓
Detection score	Tunable		
False Alarm score			
High Bandwidth	No	No	Yes
Zero Day Attacks	Few	Some	More!
Identify Attack	Specific	General	General

SMITE Architecture

- Correlation Engine
 - False positive filter
- Algorithms
 - Alert generation
- Sensors
 - Hardware feature extraction
- Meta-header
 - Inter-sensor communication



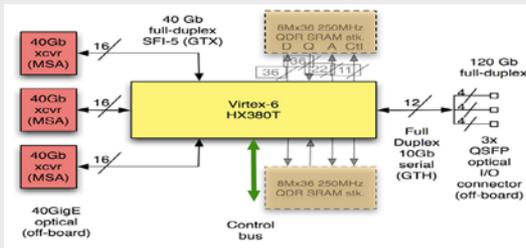
SMITE Functional View



SMITE "Eagle100" Sensor Hardware

I/O BLADE

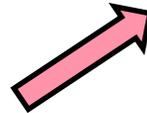
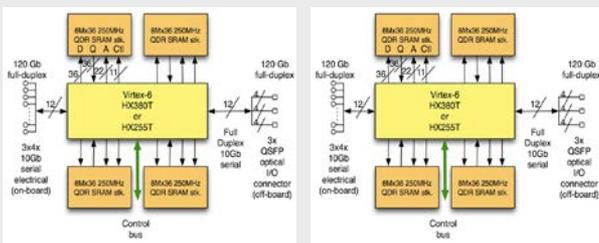
I/O BLADE



PROCESSING BLADE

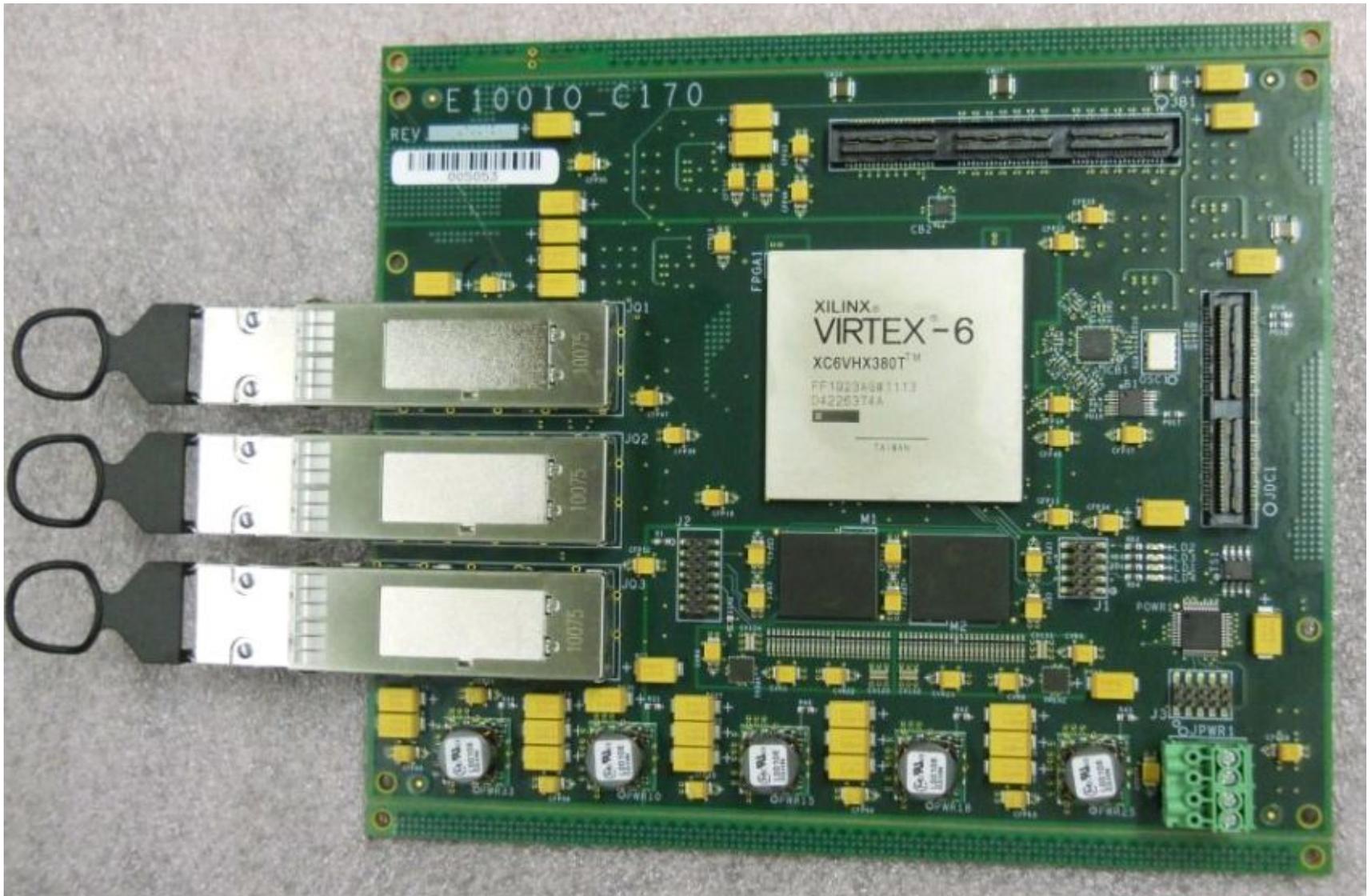
PROCESSING BLADE

PROCESSING BLADE

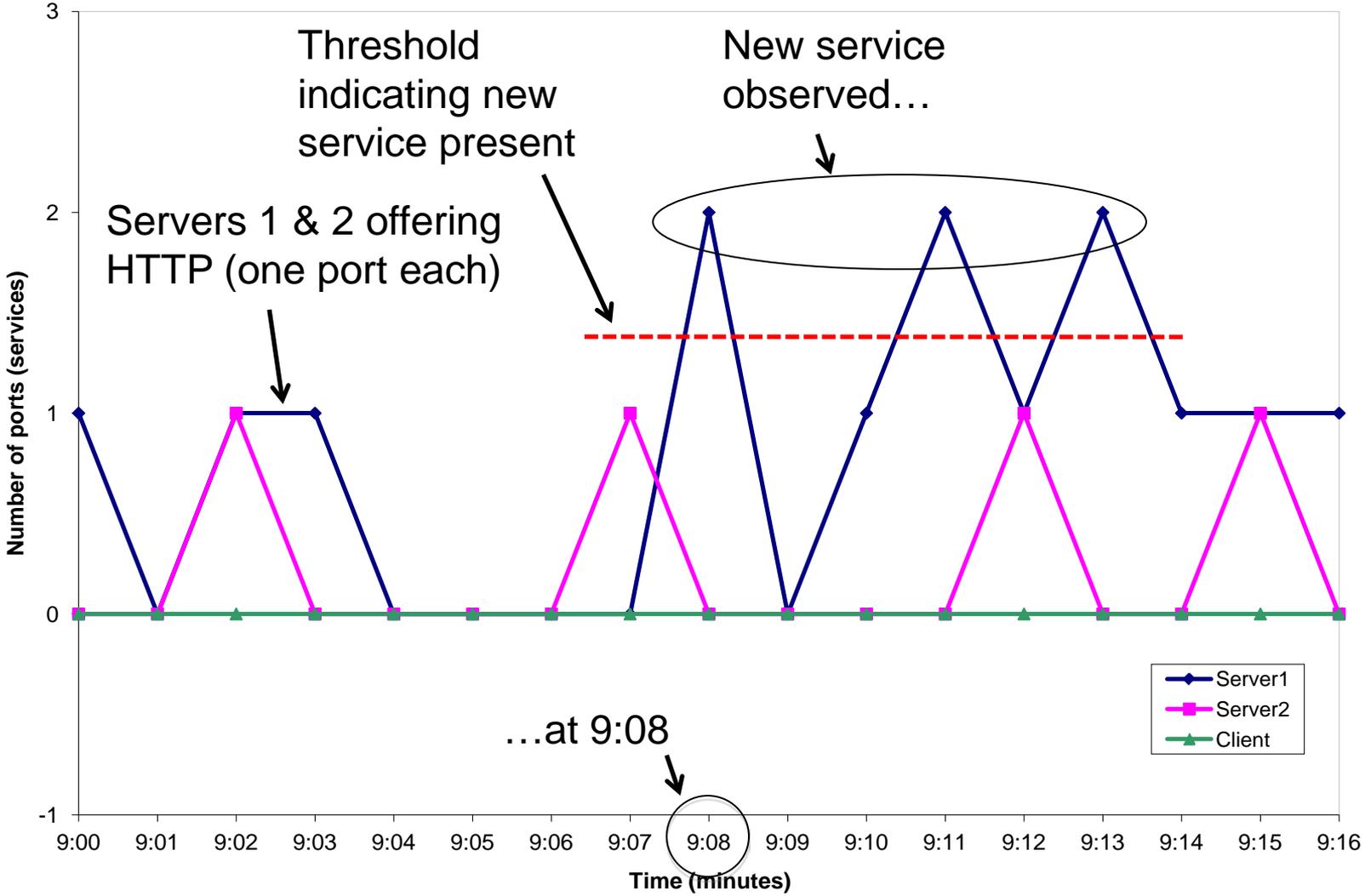


**Performance Series
14 Slot ACTA Chassis**

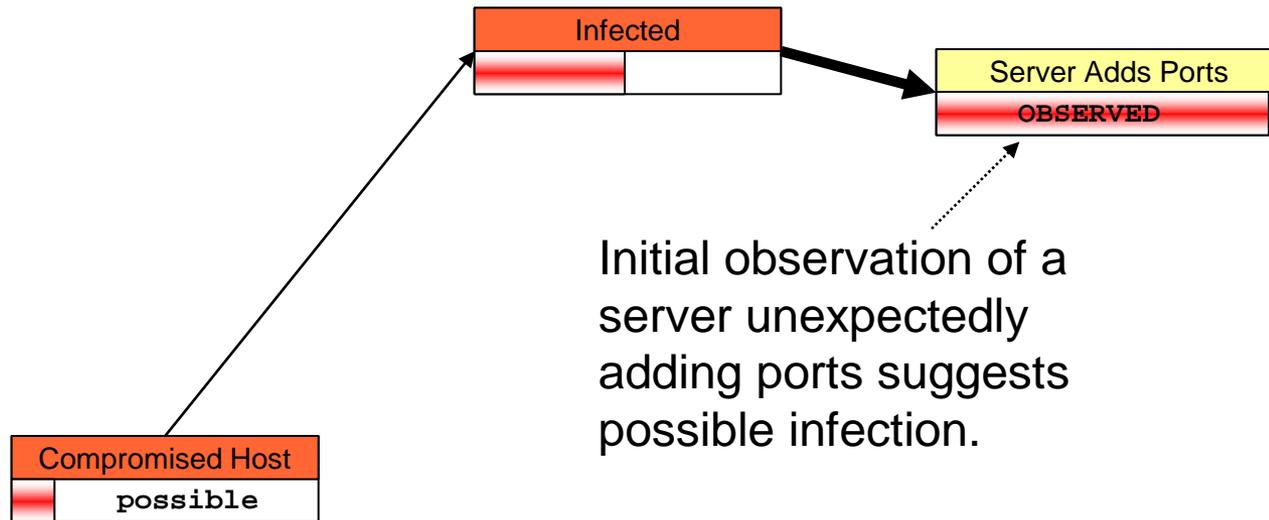
Eagle100 I/O Card



Example - An initial alert



Correlator Notified

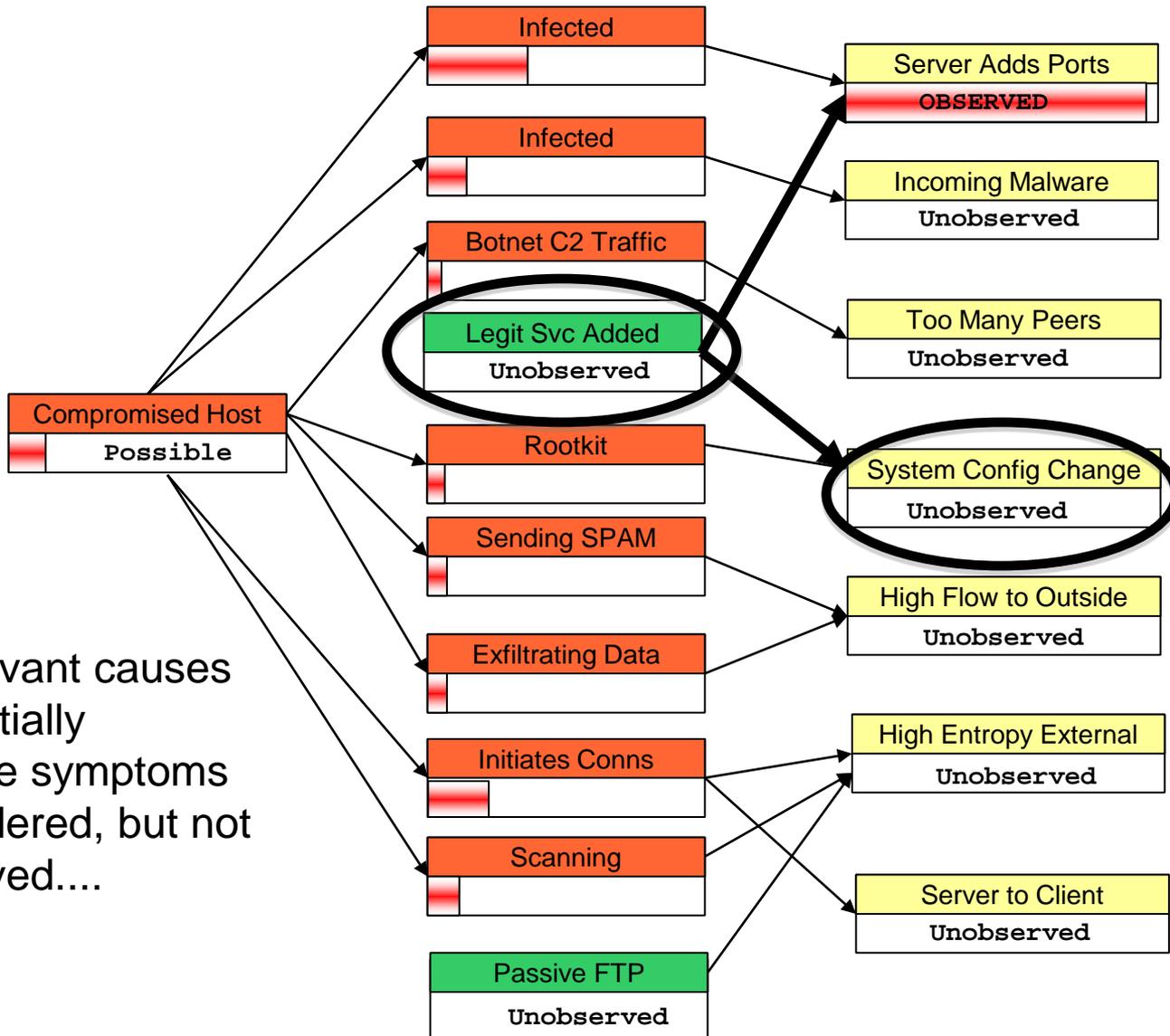


Initial observation of a server unexpectedly adding ports suggests possible infection.

Suspicion level may be:

- * unlikely
- * possible
- * likely

But Benign Hypothesis Present

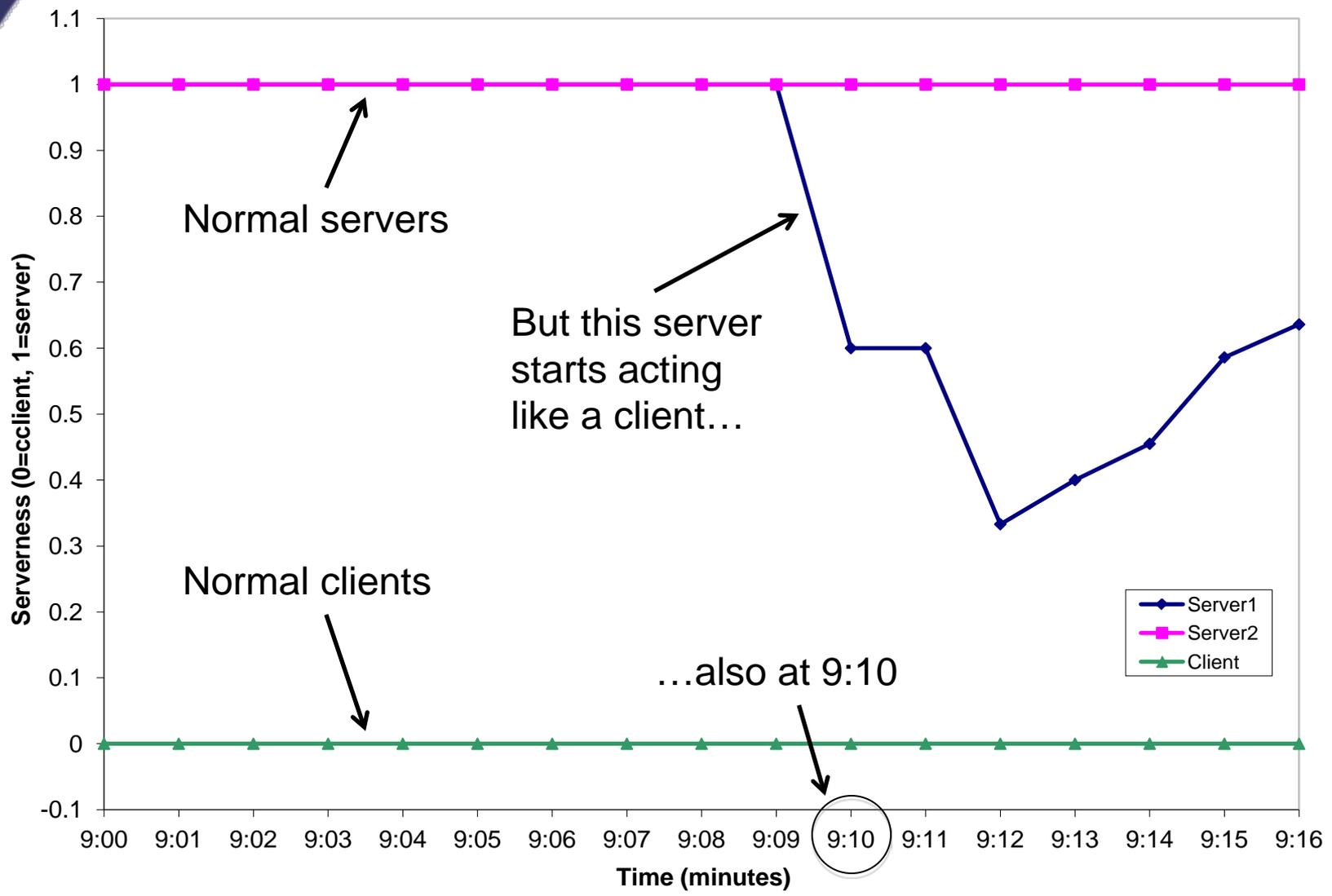


Other relevant causes and potentially observable symptoms are considered, but not yet observed....

Entropy (Connectivity Diversity)

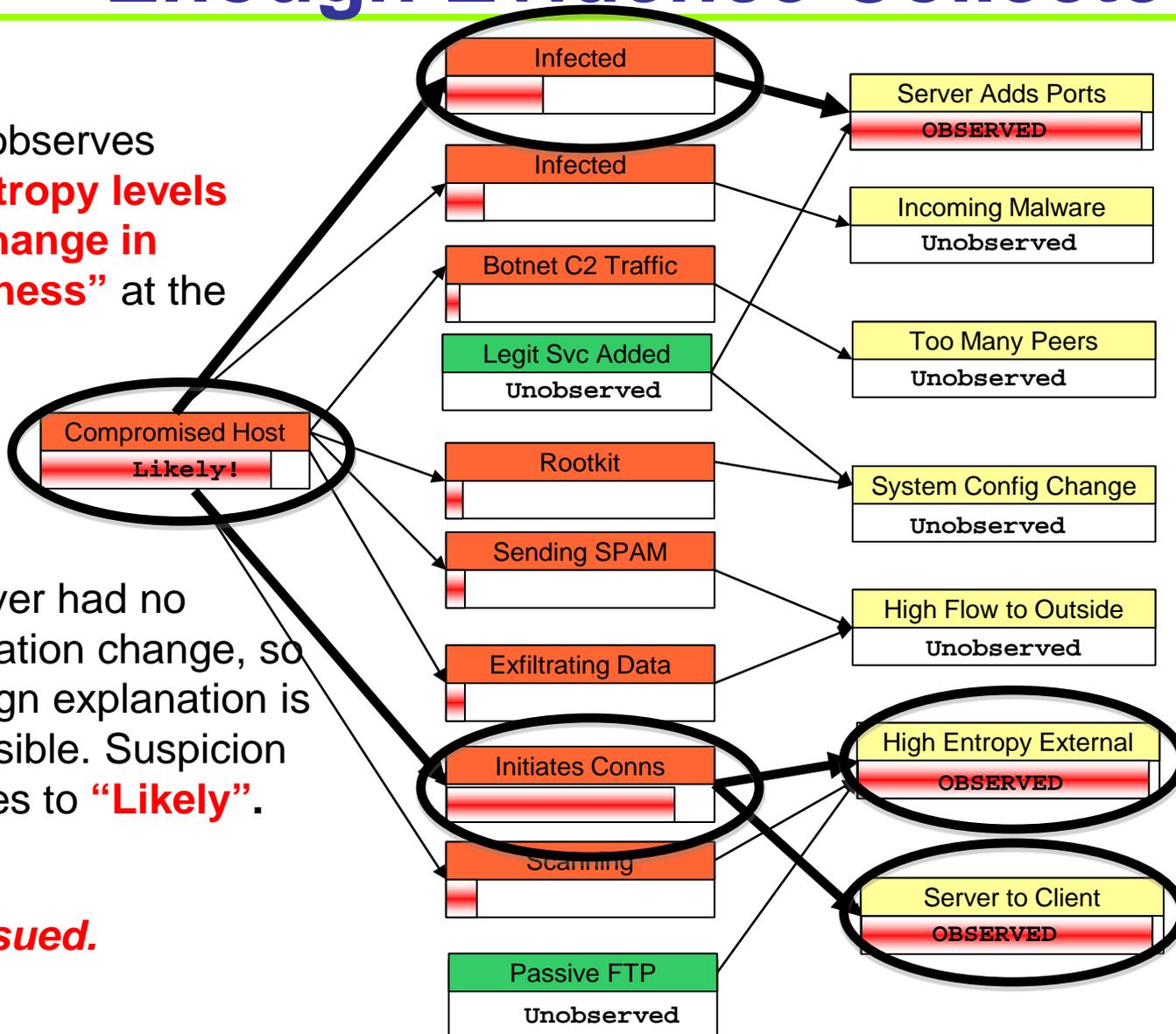


Server Acts Like Client



Enough Evidence Collected

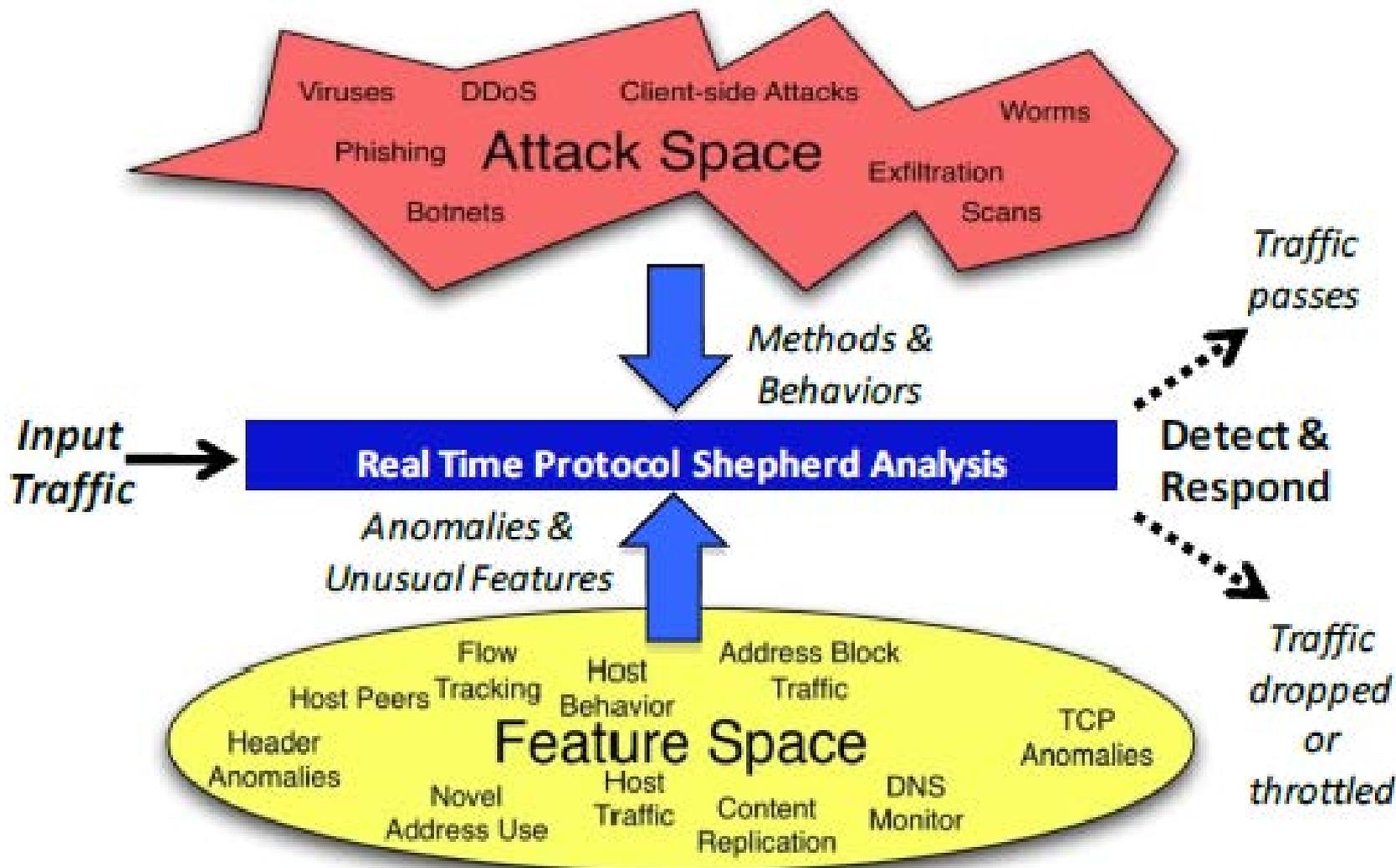
SMITE observes **high entropy levels** and a **change in “serverness”** at the server.



The server had no configuration change, so the benign explanation is not plausible. Suspicion level rises to **“Likely”**.

Alert issued.

RePS Concept



Sample Protocol: ICMP

Attack	Description	SMITE Indicators
Traffic redirection	Misuse of ICMP Redirect messages.	Header of an ICMP packet inbound from the Internet shows redirect to an internal address
Malformed packet	Host misprocessing of ICMP messages. Includes undefined or seldom-used message types, and inconsistencies between the ICMP IP header and the message body IP header.	Incoming ICMP Parameter Problem message
Firewall and IDS evasion	Use of ICMP messages to carry attacker communications that easily penetrates firewalls (e.g., ICMP Echo and Timestamp)	Repeated use in traffic crossing the enterprise border in either direction.
Botnet C2	Use of ICMP as a covert C2 channel.	Repeated use in traffic crossing the enterprise border in either direction.
Exfiltration	Use of ICMP messages to carry data through firewalls.	Unusually-large amounts of data are included after the ICMP header and/or the source has a high generation rate of ICMP packets or a significant data throughput of ICMP messages
Reconnaissance	Looking for open server ports or detecting active addresses by examining ICMP responses.	ICMP replies to external hosts; large numbers of ICMP Destination Unreachable messages are seen in either direction
Denial of Service	Use of ICMP messages to misinform host protocol stacks to shut down or misdirect traffic	Unusually-small path MTUs in ICMP Destination Unreachable/Cannot Fragment messages

Deployment Targets

Bro

- Led by Vern Paxson
- NSF funded
- Detection approach very similar to SMITE
- Not in-line with traffic but can actuate with router ACL updates



Suricata

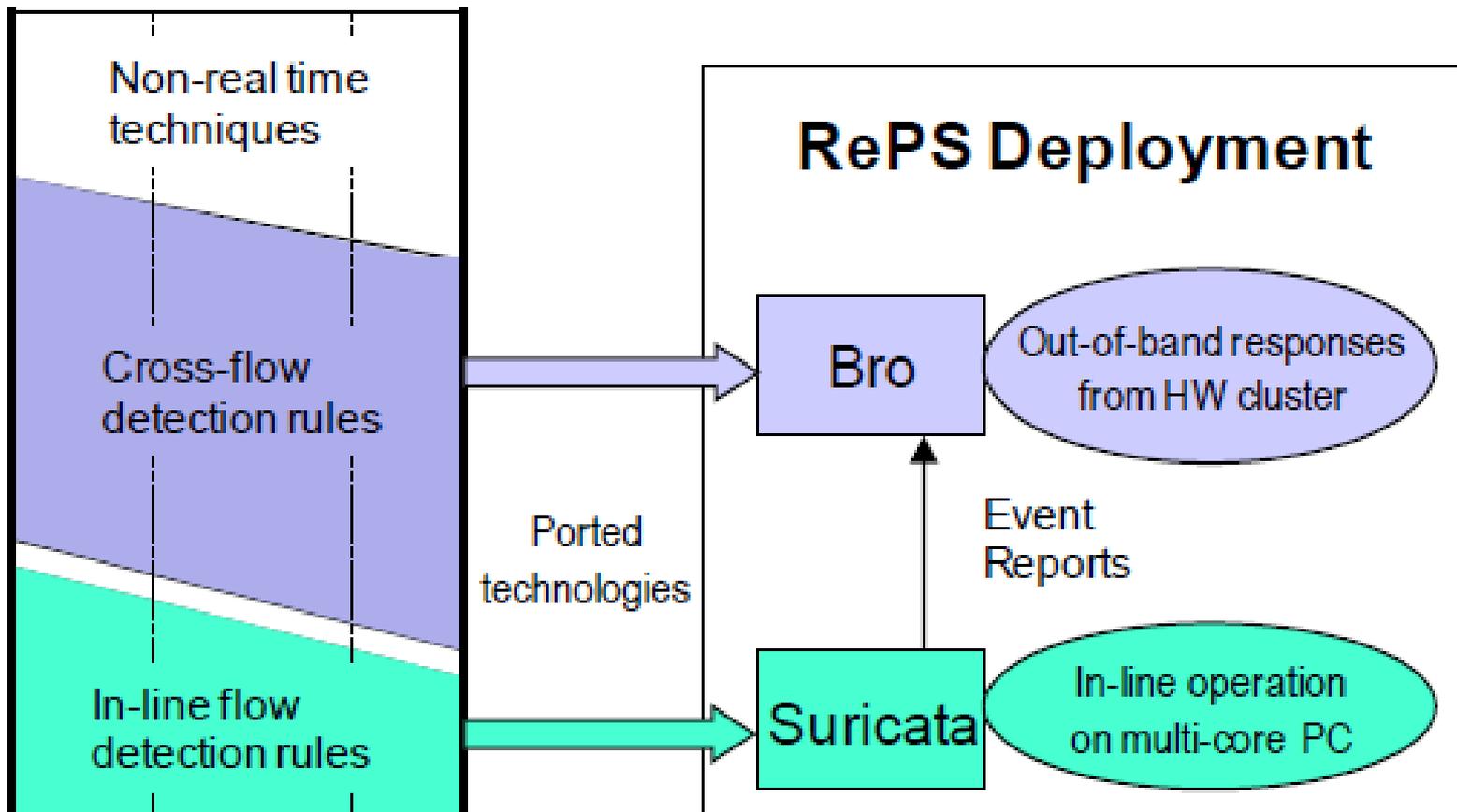
- Led by Matt Jonkman
- Consortium funded
- Snort-style signatures plus more (eg IP reputation)
- Has in-line mode



RePS Deployment Plan

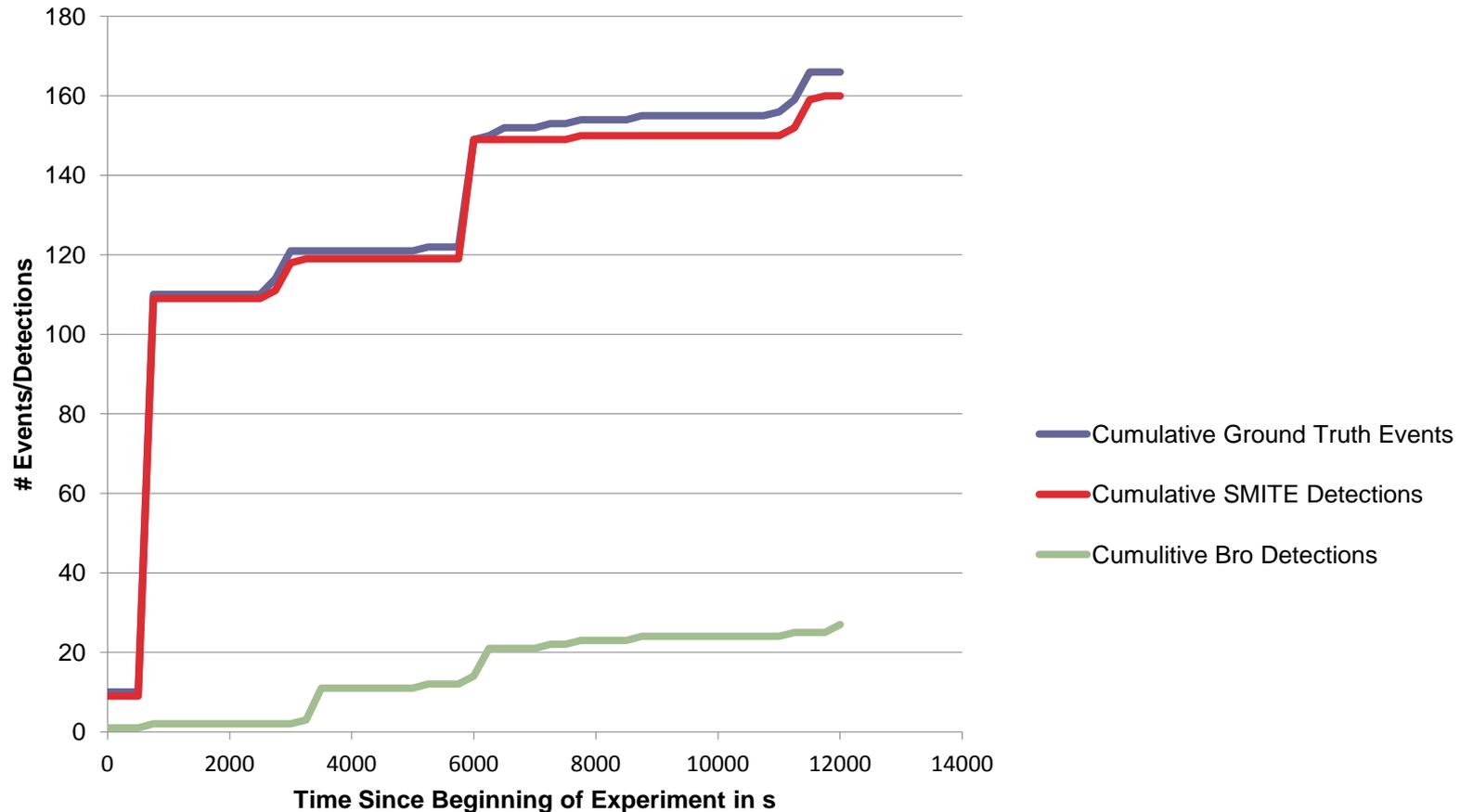
SMITE Technologies

Sensors - Algorithms - Correlation



Cumulative SMITE and Bro Detections vs. Time

Cumulative Detections by SMITE and Bro Compared to Ground Truth

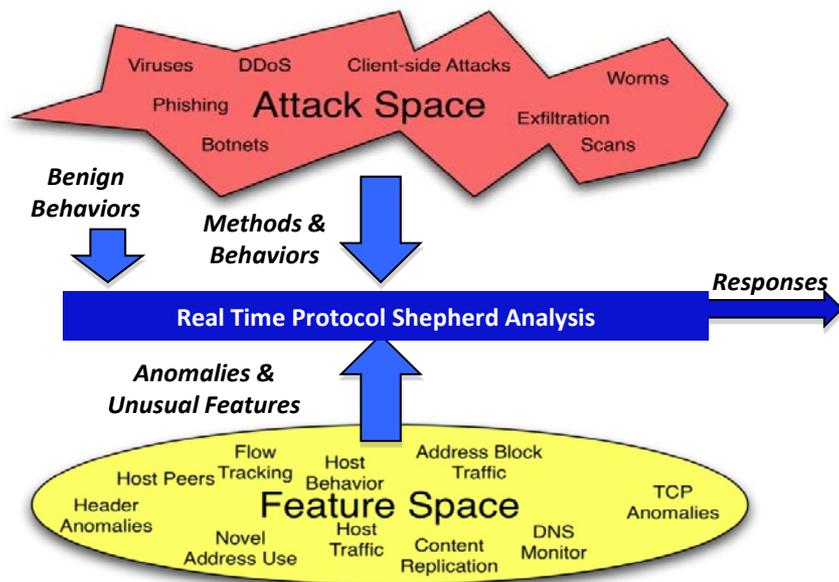


Tech Transfer

- Irvine Sensors Corp (now called ISC8)
 - Built original SMITE hardware
 - Developed an appliance version for commercial sales
 - Currently developing new products in this area
- RePS Open Source Concept
 - Take the real-time actionable portion of SMITE and deploy it across Suricata/Bro
 - Test at BBN and work with the community to generate interest in maintaining and extending the work

Schedule

ID	Task Name	Start	Finish	Q4 12			Q1 13			Q2 13			Q3 13			Q4 13					
				Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec			
1	Infrastcurure	10/1/2012	12/7/2012	█																	
2	Design Update	10/1/2012	12/7/2012	█																	
3	Suricata Coding	11/15/2012	7/26/2013				█														
4	Bro Coding	11/15/2012	7/26/2013				█														
5	Primary test	12/17/2012	7/26/2013				█														
6	Program Management	10/1/2012	7/26/2013	█																	
7	Option: Secondary Test	7/26/2013	11/25/2013													█					
8	Initial System Delivery	1/25/2013	1/25/2013	◆																	
9	Full System	7/26/2013	7/26/2013													◆					
10	Updated System	11/25/2013	11/25/2013	◆																	



Operational Capability

Enhances network-based intrusion prevention (IPS) to detect and respond to attacks such as DNS poisoning

Requires configuration settings but no training on benign traffic. False alarm rate is very low based on testing from previous program

Open-source approach provides low cost of ownership

Built as multi-threaded software to support Bro clusters. Performance on commercial HW expected to support traffic up to 1 Gb/sec with acceptable packet latency

Proposed Technical Approach

Resilient enterprise systems must proactively manage their external interfaces, sensing danger and responding in real time by blocking or throttling targeted traffic

Current IPS have weak support for analysis and response for specific protocols behaviors (ICMP, DNS, TCP, etc)

BBN has developed proven protocol analysis technology as a passive detection scheme for DARPA/SPAWAR

RePS project extends completed DARPA work into open source real time response tools for Bro and Suricata

Schedule, Cost, Deliverables, & Contact Info

Type III Project – Enhancement & Transition of past work

POP: 10 month base; 4 month option for add'l testing

Milestones:

- 1) Design modifications to existing protocol analysis algorithms (month 2)*
- 2) Bro and Suricata deployments (month 4 & 10)*
- 3) Optimized and updated deployment (month 14)*

Deliverables: Open source contributions to Bro and Suricata

PI: Ron Watro, Raytheon BBN Technologies