



Jay Lala

Raytheon

Panel Discussion – Industry Perspectives:
What Industry Problems Motivate Research
on Scientific Foundations?



Air
Land
Sea
Space
Cyberspace

Innovation. In all domains.

2012 Science of Security Community Meeting: Panel Discussion

Dr. Jay Lala
Principal Engineering Fellow
30 November 2012

Applications of SoS

- It is gratifying to see progress in defining the much needed foundations of cyber security.
- What's the grander purpose of Science?
 - Often times, Science is propelled purely by the quest for human knowledge, e.g., looking for life on Mars or physical evidence of Higgs Boson
 - Other times, Science is driven by practical needs, e.g., to fly faster, higher, farther
- SoS has a very immediate application: How to engineer secure systems?
 - Having a clearly identified need can also focus SoS research

SoS research & its engineering application can proceed in a symbiotic relationship.

Engineering Secure Systems

- DoD Weapon System Acquisition Policies, Requirements and Specs
- Architect, Design, Model & Simulate Phases
- Test & Evaluation

SoS can help in full life-cycle of engineering secure systems.

Acquisition Policies, Requirements & Specs



PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE

3015 DEFENSE PENTAGON
WASHINGTON, DC 20301-3015

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

JUL 18 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Document Streamlining – Program Protection Plan (PPP)

Excerpts from Program Protection Plan Memo

5.0. Threats, Vulnerabilities, and Countermeasures

- Summarize any identified threats and vulnerabilities to CPI and critical functions/components in Table 5.0-1 below. Also identify any countermeasures selected to mitigate risks of compromise.

5.2. Vulnerabilities

- What vulnerabilities have been identified to date?
- How will the program identify new vulnerabilities (both system-level and in the development environment) to the CPI and mission-critical functions and components? Who is responsible for doing this, and with what frequency? Include the responsible person in the table in Section 1.2.
- How often will vulnerabilities be re-assessed?
- How will identified vulnerabilities be mitigated?

Example SoS Questions wrt PPP

- Can SoS provide a foundation for a *taxonomy of vulnerabilities*?
- Is *identification of vulnerabilities* in CPI (Critical Program Information) and critical functions/components, followed by *definition of countermeasures*, the way to engineer secure systems?
- Would we modify this approach with the added knowledge of SoS?
- If yes, what might the new process look like?

Cyber Test & Evaluation



**Test Capabilities for
Cyber Defense Test and Evaluation**

Workshop 1

Deputy Assistant Secretary of Defense,
Developmental Test and Evaluation



DASD, DT&E Perspective



“Requirements for test and evaluation in the defensive cyber domain for MDAP and MAIS programs are not fully understood.”

“Thorough cyber testing needs to be incorporated into weapon system and operational support system development.”

-- DT&E FY2011 Annual Report to Congress



Cyber Defense Test Capability Features

- **Operational network environments including GIG services**
- **Realistic threat portrayals**
- **Representations of network defense capabilities**
- **Protection against collateral damage outside test**
- ***Ability to do the mission in a contested cyber environment* during test events**
- **Evaluation results that identify system vulnerabilities**

Example SoS Questions wrt Cyber T&E

- Can SoS provide a foundation for a *taxonomy of threats* that can be used for *realistic threat portrayals*?
- How does one *model network defenses*?
- What are the critical parameters that capture a *contested cyber environment*?
- How does one estimate *residual system vulnerabilities*?



Phil Venable

Goldman-Sachs

Panel Discussion – Industry Perspectives:
What Industry Problems Motivate Research
on Scientific Foundations?

Macro Challenges – “Silicon”

“Silicon”

Distributed Policy Specification and Enforcement

Federated Monitoring and Policy Verification

Data Level Entitlements Policy Enforcement

Distributed Interoperable Data Protection

Predictably Secure Systems and Service Development

Dynamic Zone Least Privilege

Massive Scale Behavioral Surveillance

Macro Challenges - “Carbon”

“Carbon”

Behavioral Economics and Incentives

Behavioral Psychology and Education

Security and Usability / User Experience

Opportunities from Augmented Reality

Risk Ontology, Measurement and Metrics

Human Readable Policy Expression

Fail-Secure/Fail-Safe Design Principles Education



Bret Hartman

Cisco

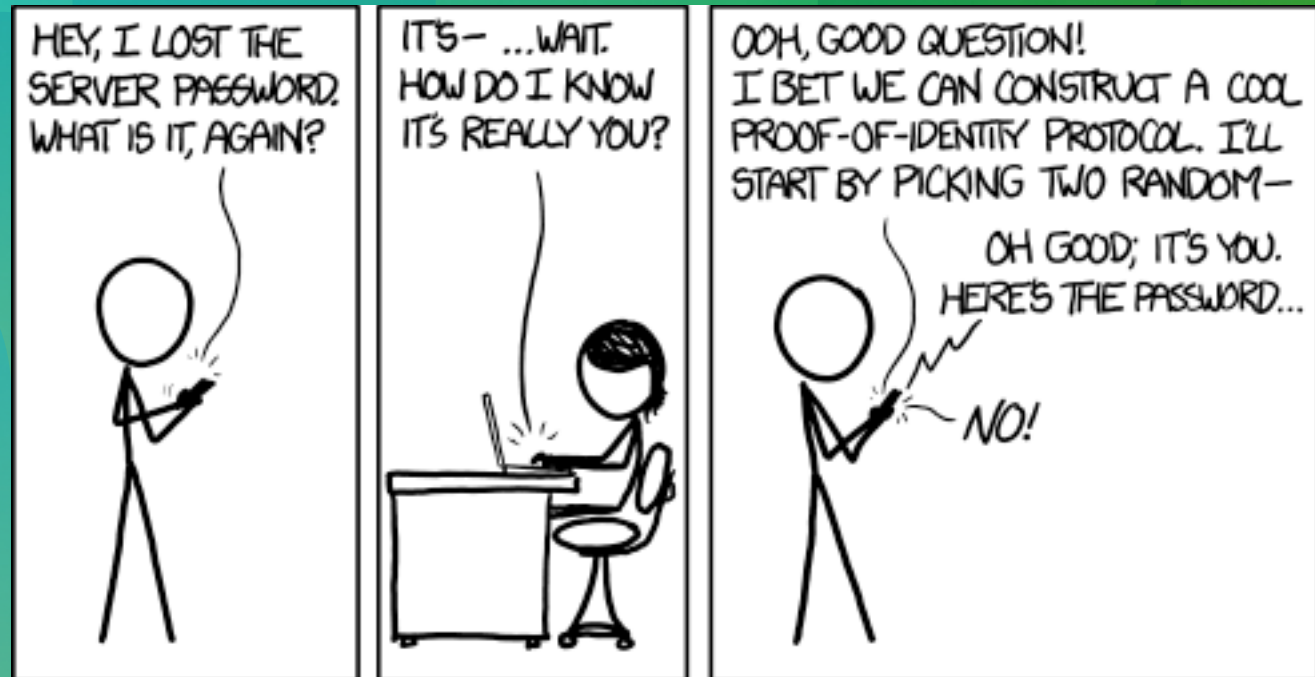
Panel Discussion – Industry Perspectives:
What Industry Problems Motivate Research
on Scientific Foundations?

Science of Security: Thoughts from the Networking World

Bret Hartman
VP & CTO

Security and
Government Group

November 2012



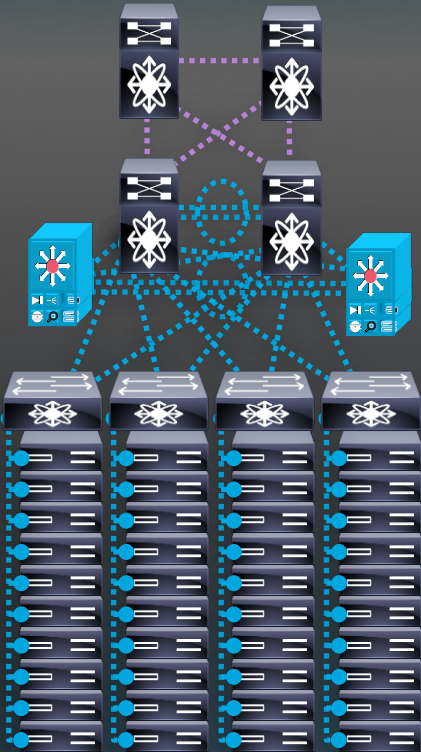
We're all moving to the cloud – but...

- 30 years of increasing security challenges
 - Security research has been ineffective in defending us from the acceleration of ever larger compromises and more serious breaches
- Securing the cloud is a massive transition
 - Add-on -> embedded -> cloud
 - Diminishing effectiveness of device and data center security
 - Protection burden is shifting to service providers
 - Service providers are ill-equipped to deal with the threats
- Increased risks in the cloud
 - Centralized services are consolidated targets
 - Questionable isolation and multi-tenancy
 - Expansion of DDoS as a component of a multi-pronged attack

Software Defined Networking (SDN) is the next wave – and security is not ready

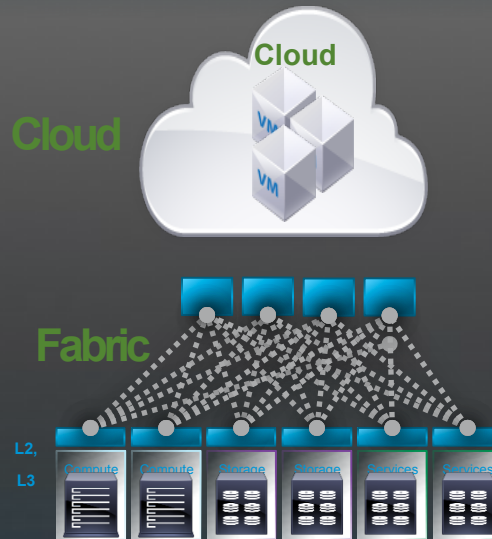
Evolution of Data Center

Distributed



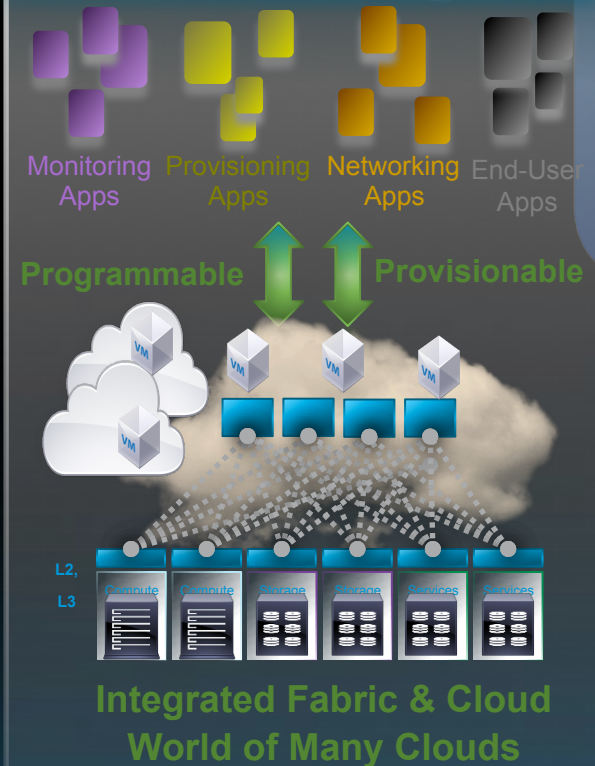
- Manual Provisioning
- Limited scaling
- Rack-wide VM mobility

Fabric Based



- Policy-based Provisioning
- Scale Physical & Virtual/Cloud
- DC-wide/Cross-DC VM Mobility

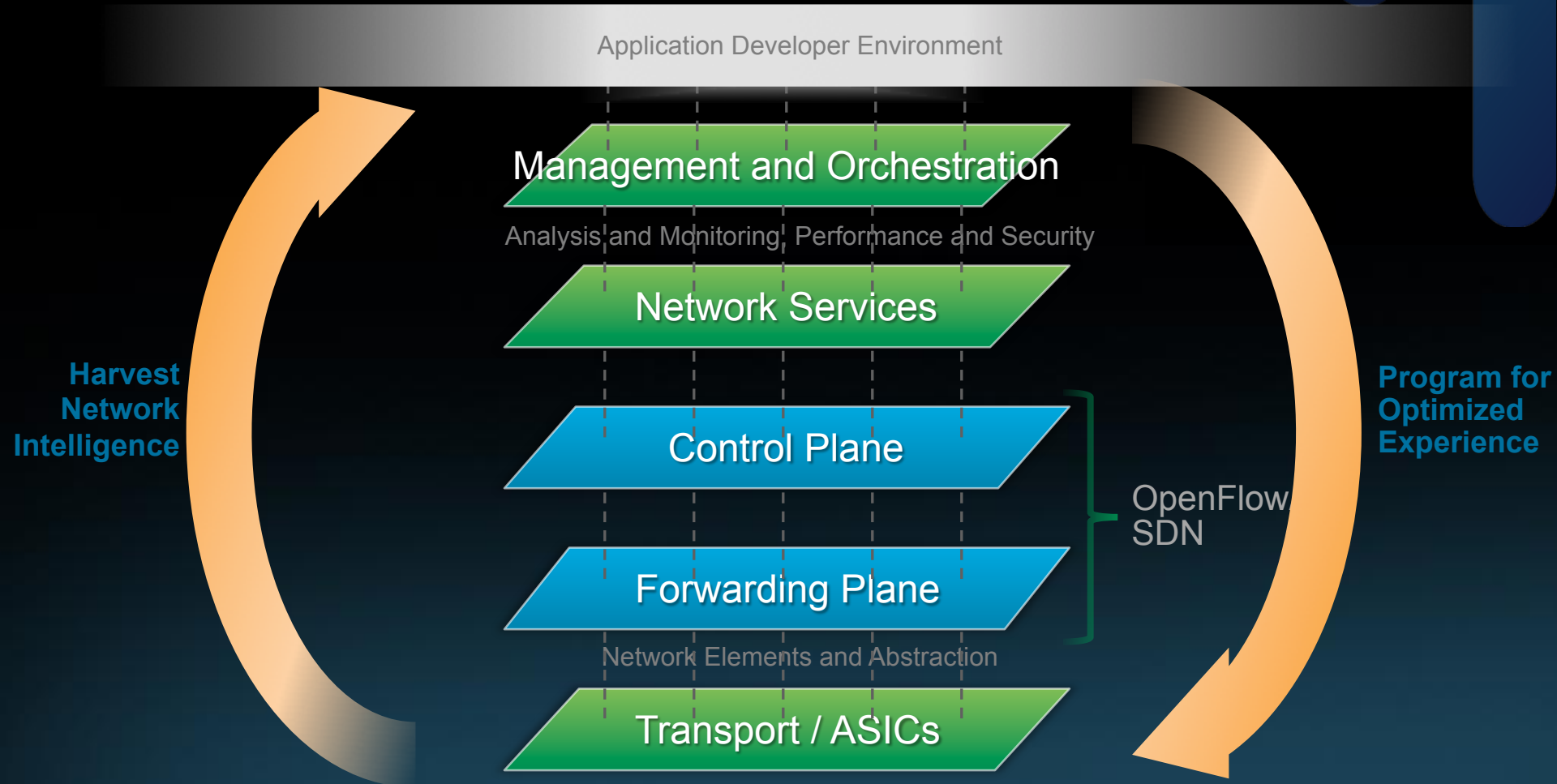
Application Driven



- Service-centric Provisioning
- Flexible – Anywhere, Anytime
- Cross-cloud VM Mobility

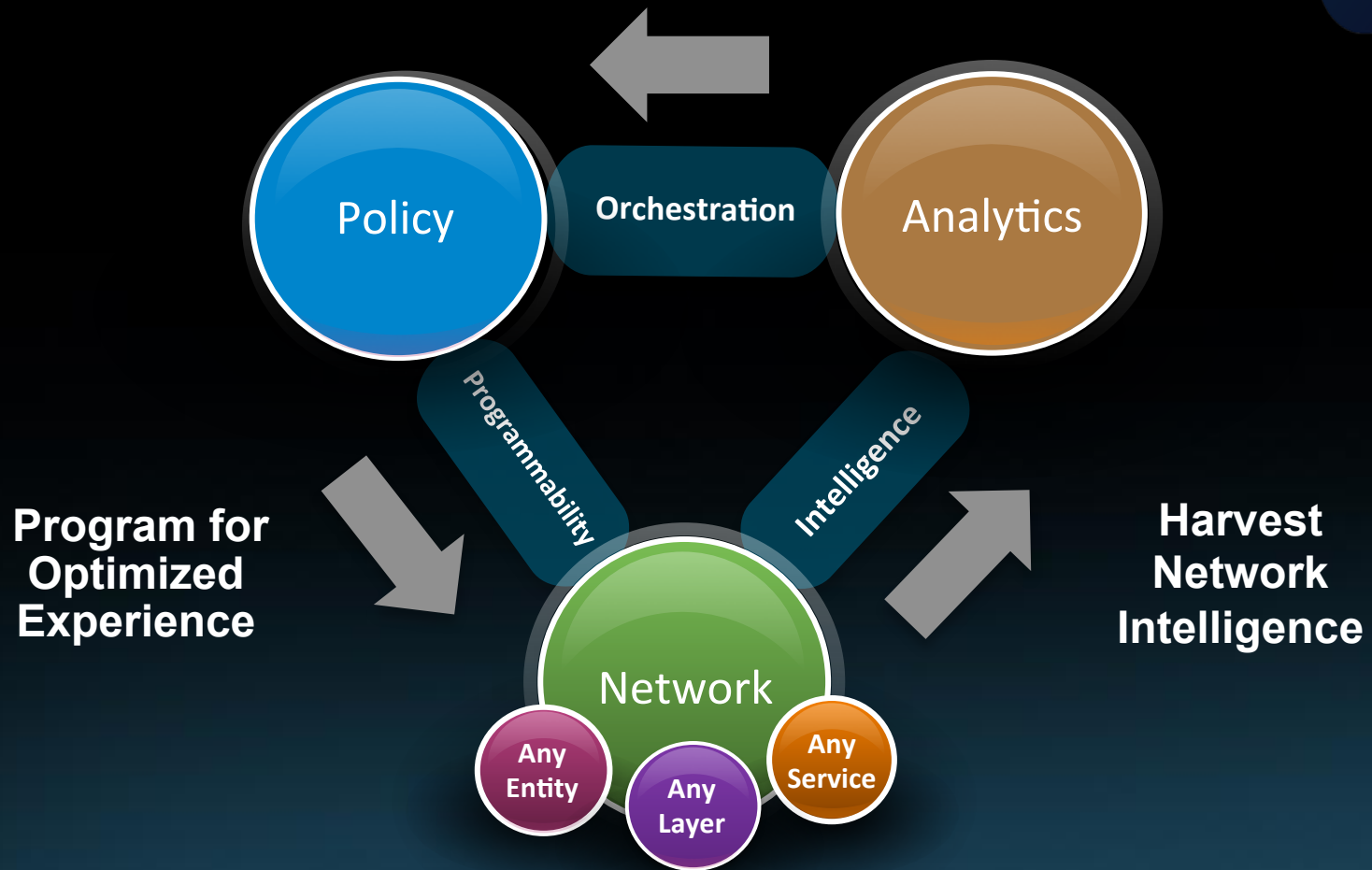
Programmability at Multiple Layers of the Network

Flexibility in Deriving Abstractions



Network as a Service

Application Driven, Adaptable



SDN and Security Research Topics

- Securing the SDN

Ensure that the security policy defined by the applications is enforced by the SDN stack

Chain of trust from network devices, controllers, and applications

Interoperable security policy enforcement across multiple vendors

- SDN delivering security services

Network virtualization provides new opportunities to segment traffic end-to-end

Network intelligence provides unprecedented potential intelligence analytics

- Can we rely on the Service Providers to protect all of us?

Transparency vs. privacy

Assurance vs. cost

