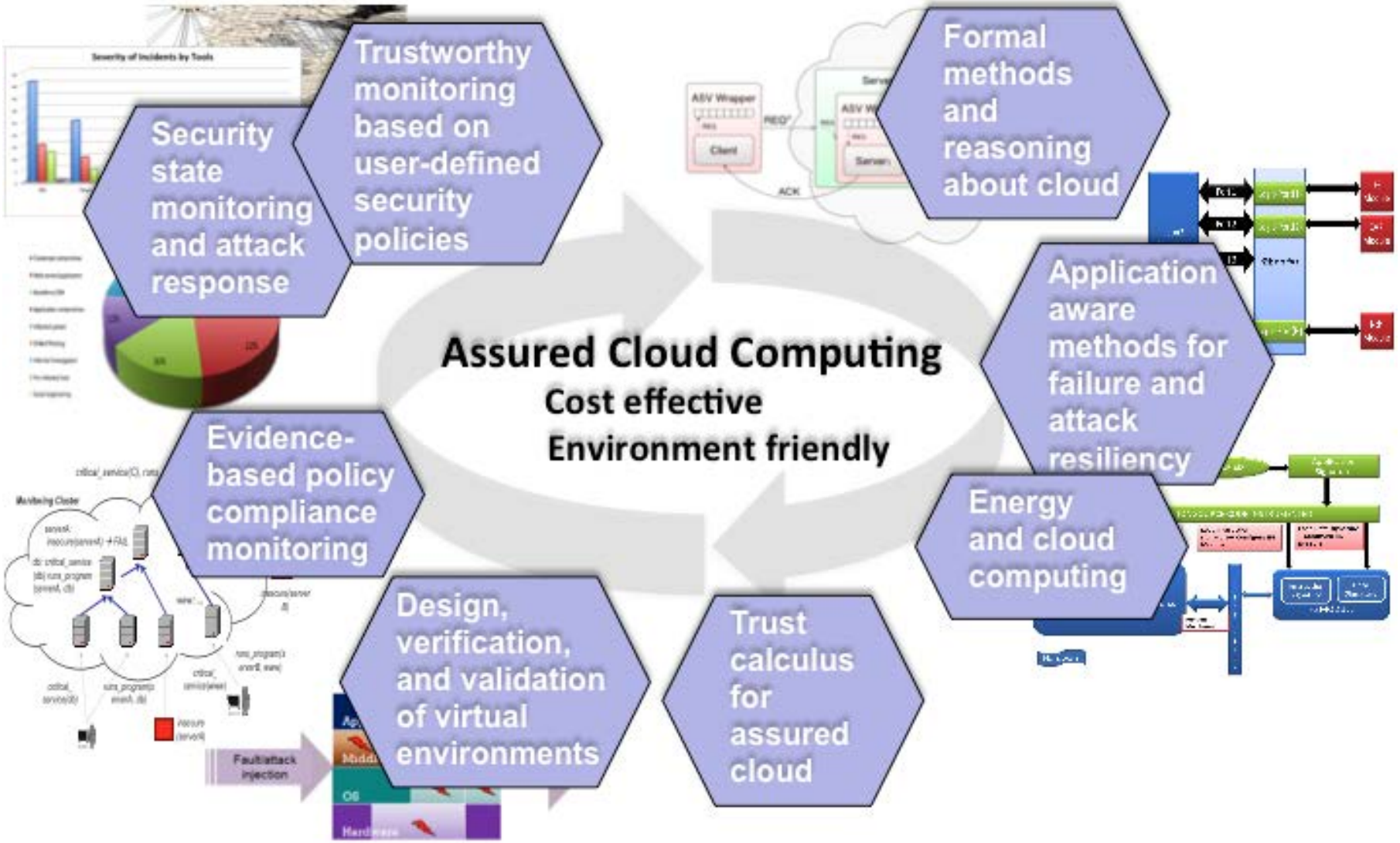
Software Defined Cloud Security Architectures

Roy Campbell

October 8th 2014 , AFRL, Rome, NY

U.S. AIR FORCE

Towards Assured Clouds: Our Approach



U.S. AIR FORCE

Concerns

- Software Defined Networks
- Virtual Machines and Virtualization
- Virtual Appliances. Component reuse.
- Software Defined Compute and Storage Engines
- Virtual Machine Introspection
- Digital Forensics
- Sensing and monitoring
- Integration of Techniques and Fusion of Sensing Information
- Trusted Bootstraps applied to distributed systems
- Transformational way of building security for Cloud Services.

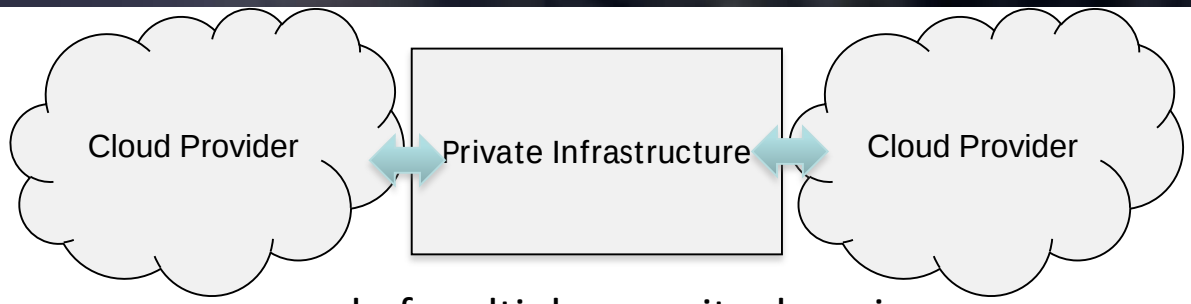
Defense in Depth-Network

- SDN
  - Toolbox for constructing security architecture for a network (FRESCO)
  - Separation of traffic, layering, secure, isolated data flows
  - Virtual network/flows associated with distributed architecture of virtual appliances (virtual cluster)
  - Modular applications in high-level languages written above controllers

ACC Results

- Distributed Monitoring (distributed policy, distributed checking, authenticated results)
- Trust Model for Clouds
- Virtual Appliances
- Virtual Machine Inspection within Clouds
- Remote Digital Forensics
- Integrating virtual networking with virtual appliances

Motivation: Multi-Domain Monitoring

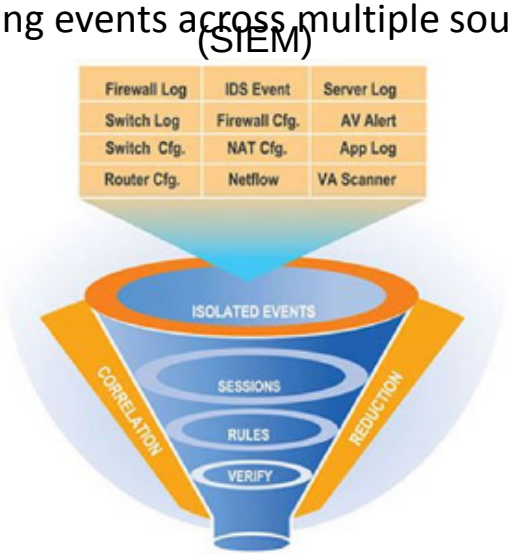


- Modern systems are composed of multiple security domains
  - Cloud Computing
  - Hybrid Clouds
  - Intercloud-Multi-cloud
  - Critical Infrastructure Systems
- Advantages
  - Economy of scale for cloud computing
  - Ability to select which services to use without binding to a single provider for multi-cloud/inter-cloud

EVENT TYPE	SOURCE	SECURITY DOMAIN	DESCRIPTION
runsCriticalService	Deployment software,SNMP agents	Cloud user	critical services run on a specific instances
instanceAssigned	Openstack	Cloud provider	instances are assigned to specific physical servers
badTraffic	IDS, Network monitoring	Cloud provider	malicious traffic detected from specific physical server

Sharing Only need-to-know Information

- How do we know that the system is working correctly as a whole?
- Integrating events across domains to detect complex security problems and attacks
  - Security Information and Event Management Systems (SIEM) are successful because they are capable of integrate monitoring events across multiple sources



- However, monitoring provides critical information about systems to external organizations which opens the system to attacks
  - *Network topology, network traffic, configurations, installed programs, vulnerable programs, user bahaviors, services, critical machines*

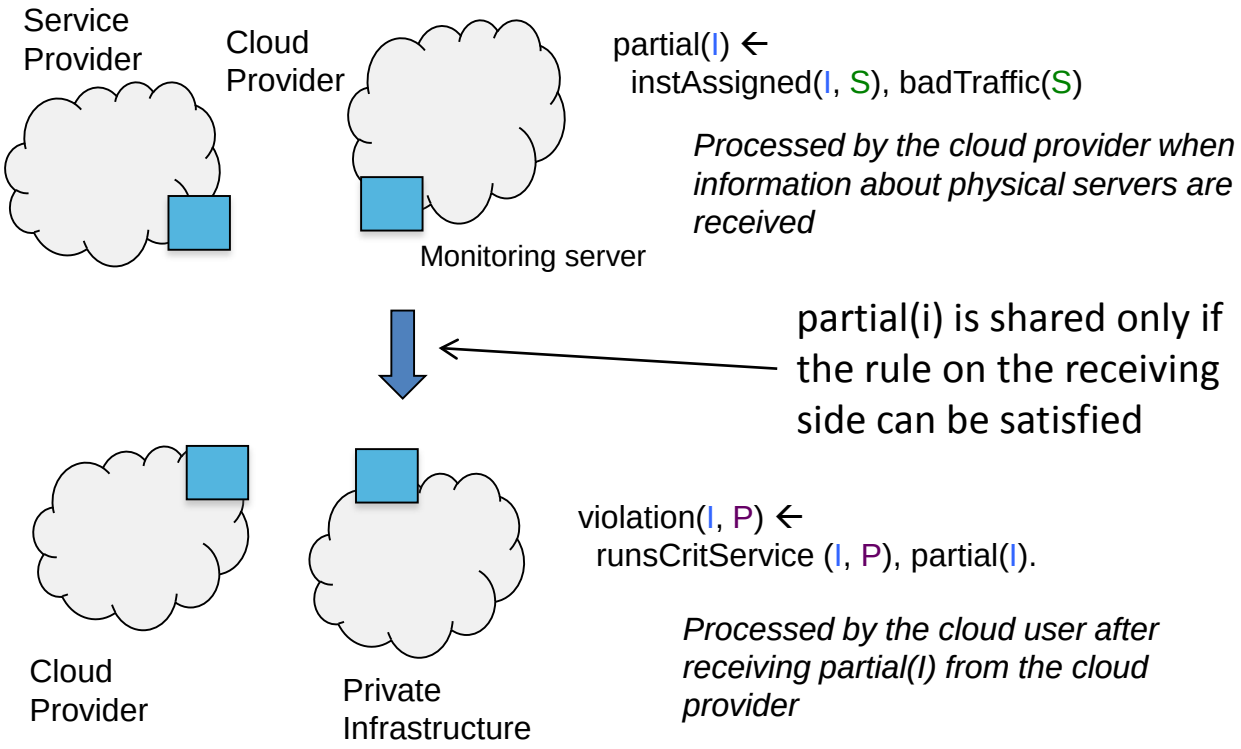
Goal: Share only *need-to-know* information across organizations to detect problems

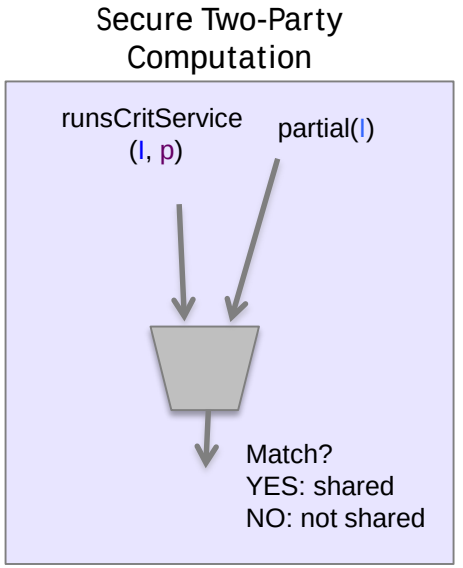
Policy-based Distributed Monitoring System

- Our Distributed Monitoring System
  - Policy-based
  - Detects violations of global policies while limiting event exposure
  - Identifies "need-to-know" events and shares only those

1. Policy rewritten to identify cross-domain sharing
2. Events shared only if they can create a violation

violation(I, P) ←
runsCritService (I, P), instAssigned(I, S), badTraffic(S)





Virtual Network/Virtual Appliances

- Science DMZ
- Secure End to End systems
- Overlay networks (research, academics, public)
- Monitoring of virtual appliances
- Introspection/forensics tools
- Policies for and monitoring of data flow between networks

SDN Facilities

- New Lab
- Latest wired and wireless switches/routers
- Integrated with experimental cloud
- Can simulate two campuses and multiple data centers
- Virtualization via Open Daylight Controller

U.S. AIR FORCE

Matrix Integration Lab

Virtual Campus 1

- HP12900 VIRTUALIZED DC
- HP5900 DATA CENTER
- HP5406 CAMPUS SWITCH
- HP3800 * BLDG/CAMPUS
- HP2570

- HP560 AC AP

Virtual Campus 2

- HP12900 VIRTUALIZED DC
- HP5900 DATA CENTER
- HP5406 CAMPUS SWITCH
- HP3800 *BLDG/CAMPUS
- HP2570

- HP560 AC AP

OPEN DAYLIGHT CONTROLLERS

U.S. AIR FORCE

12900 VIRTUALIZED DATA CENTER

High 10GbE, 40GbE and 100 GbE density across 36 Tb/s switch fabric

Defense in Depth-Virtualization

- Both metal and hypervisor based software stacks – appliances. Management of images (real or virtual)
- Separation of control (set up, configuration, security provisions) from function (processing, data)
- Introspection and monitoring of components.
- Secure slices of the Cloud representing different aspects of same application: auditing/introspection

U.S. AIR FORCE

Cloud Security References

1. Yao, F., et al. (2014). CryptVMI: a Flexible and Encrypted Virtual Machine Introspection in the Cloud. Proceedings of the Second International Workshop on Security in Cloud Computing. Kyoto, Japan, ACM New York: 11-18.
2. Huang, J., et al. (2014). Denial-of-Service Threat to Hadoop/YARN Clusters with Multi-Tenancy. 2014 IEEE Second international Congress on Big Data (BigData Congress 2014). Anchorage, AK, USA, IEEE.
3. Montanari, M., et al. (2013). Limiting Data Exposure in Monitoring Multi-domain Policy Conformance. TRUST. Imperial College, London, IEEE: 65-82.
4. Montanari, M., et al. (2013). Distributed security policy conformance. Computers & Security. **33:** 28-40.
5. Malik, M. S., et al. (2013). Towards SDN enabled network control delegation in clouds. 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Budapest, Hungary, IEEE: 1-6.
6. Huh, J. H., et al. (2013). An empirical study on the software integrity of virtual appliances. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13. New York, New York, USA, ACM Press: 231-231.
7. Montanari, M., et al. (2012). Multi-Organization Policy-based Monitoring. IEEE POLICY, IEEE.
8. Montanari, M., et al. (2012). Evidence of log integrity in policy-based security monitoring. IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012), IEEE: 1-6.
9. Montanari, M., et al. (2012). Multi-organization Policy-Based Monitoring. 2012 IEEE International Symposium on Policies for Distributed Systems and Networks, IEEE: 70-77.
10. Montanari, M. and R. H. Campbell (2012). Confidentiality of event data in policy-based monitoring. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), IEEE: 1-12.