Cloud Computing Security: What Changes with Software-Defined Networking?

José Fortes
Center for Cloud and Autonomic Computing
Advanced Computing and Information Systems Lab

ARO Workshop on Cloud Security

March 11, 2013

* Work done with Mauricio Tsugawa and Andrea Matsunaga

Outline

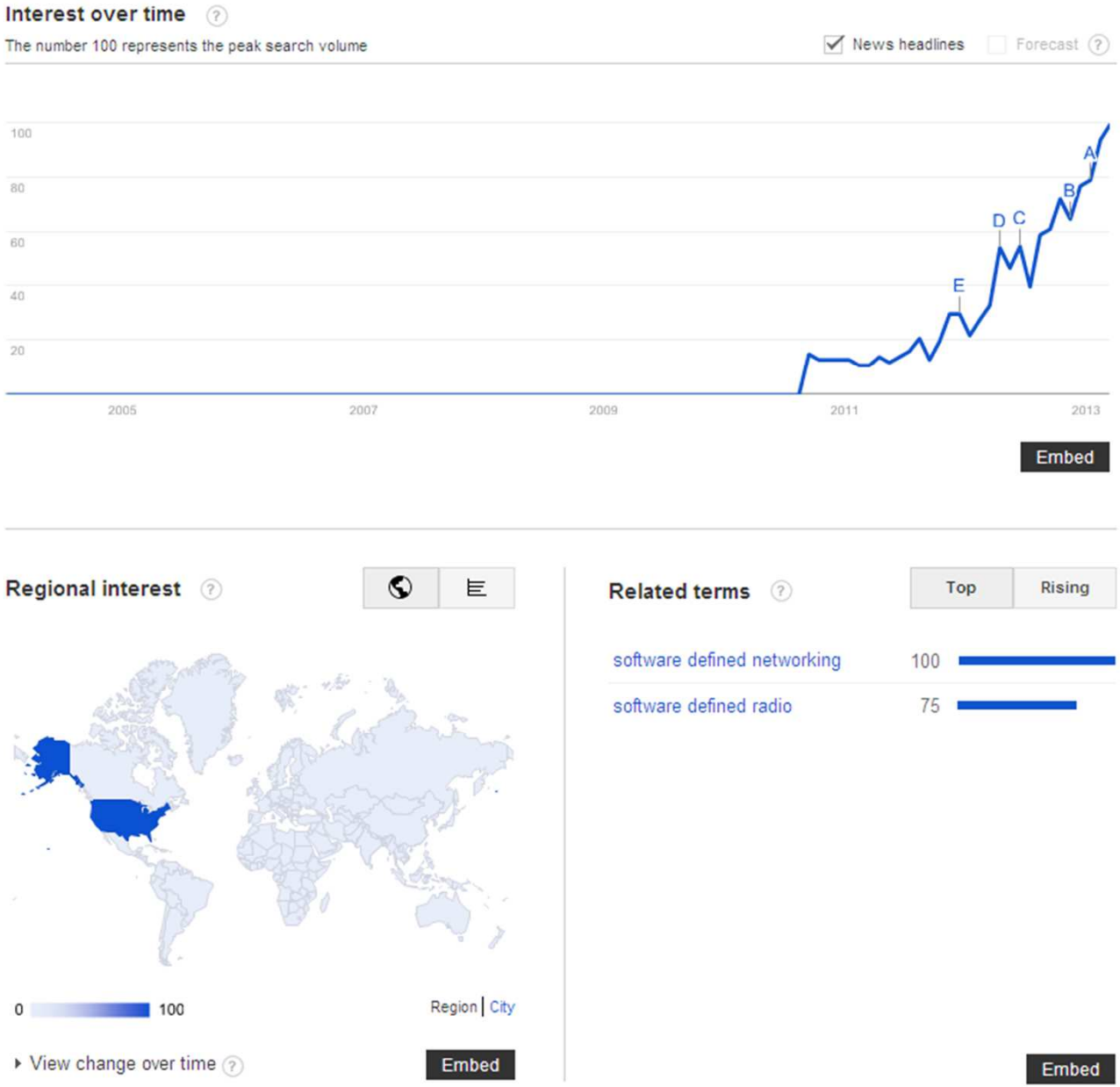
- Quick introduction to SDN
- SDN and Cloud Computing
- Cloud Security with SDN
  - Opportunities
  - Vulnerabilities
- Needed SDN R&D for Cloud Security
- Conclusions

What is Software-Defined Networking?

- Broad Definition
  - Open Network Foundation: “an architecture that enables direct programmability of networks”
  - Internet Engineering Task Force: “an approach that enables applications to converse with and manipulate the control software of network devices and resources” – *Internet Draft, Sep. 2011 by T. Nadeau*
- OpenFlow
  - An approach to SDN with physical separation between control and data planes
  - Provides open interfaces (APIs)
  - Myth: SDN is OpenFlow

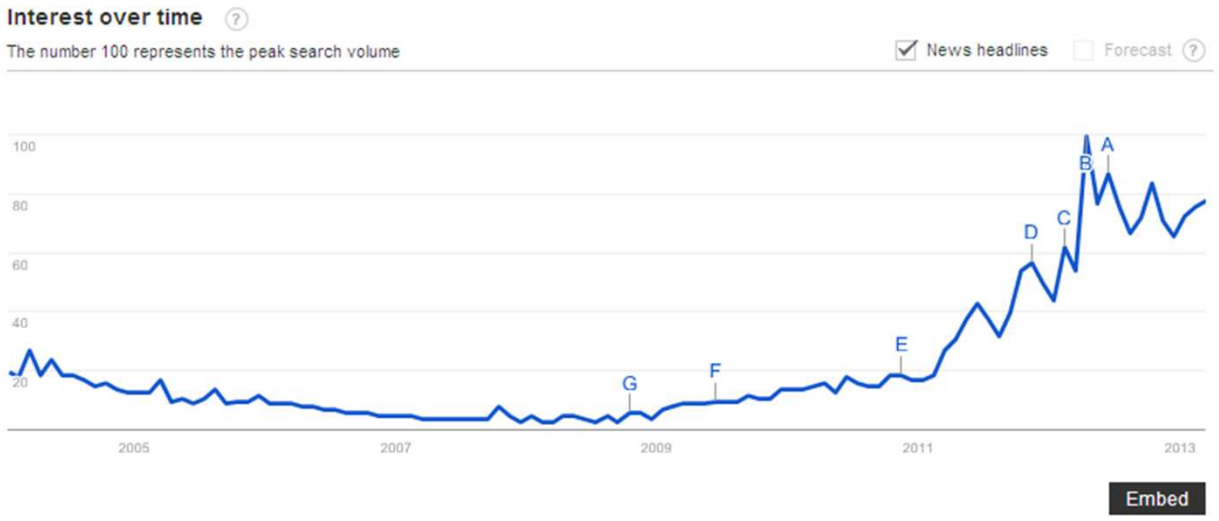
Software-Defined Networking

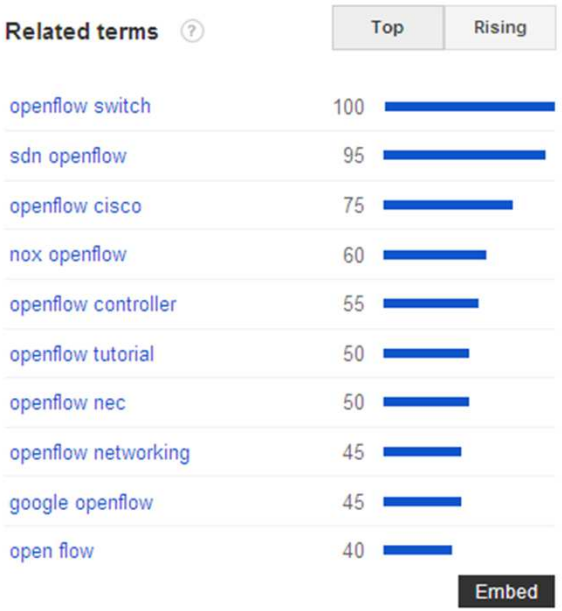
- Google Trends
  - Software-Defined Networking



OpenFlow

- Google Trends
  - OpenFlow



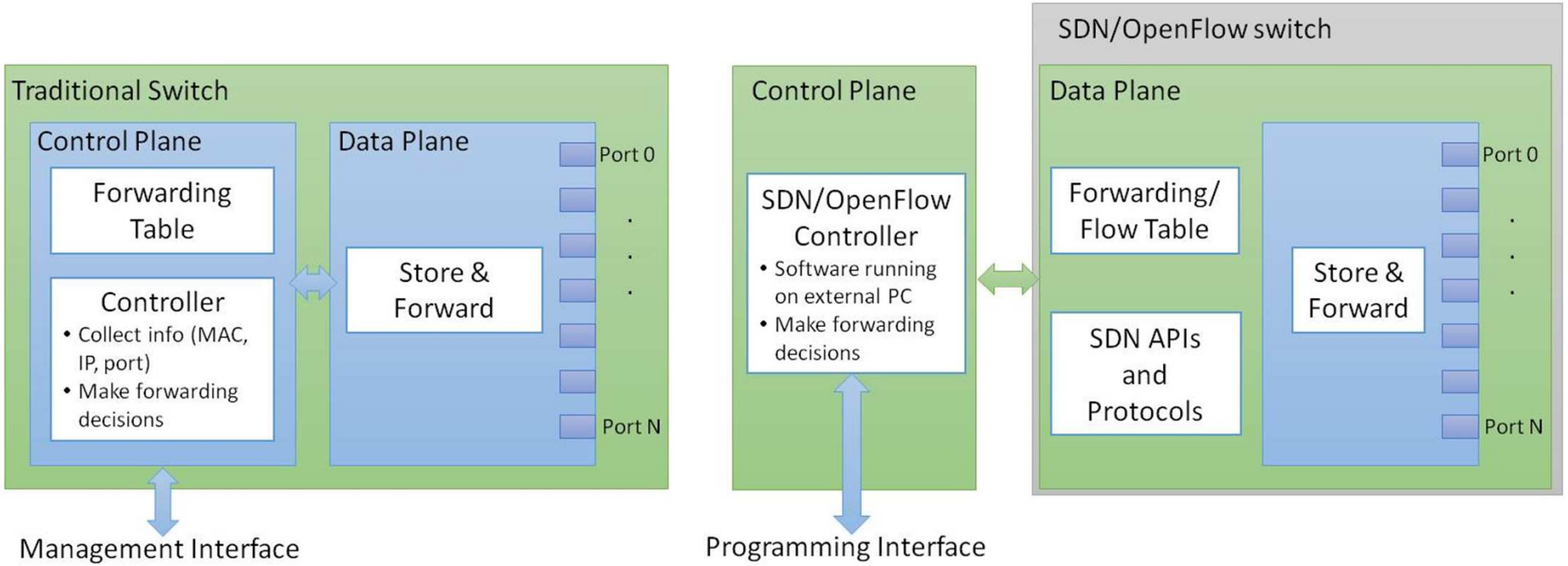


Need for SDN

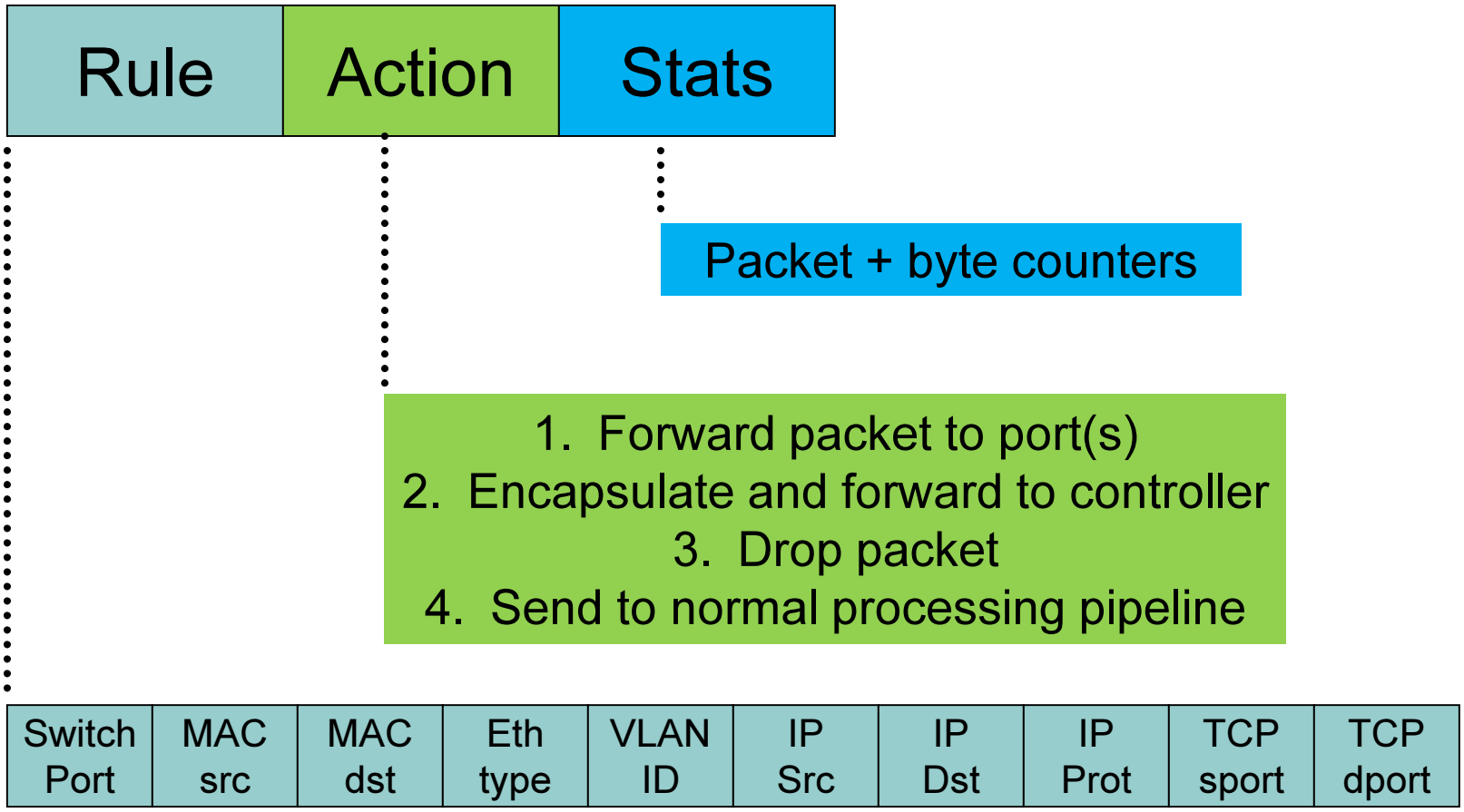
- Network infrastructure “ossification”
  - Large base of devices and protocols
  - Networking experiments cannot compete with production traffic
  - No practical way to test new network protocols in realistic settings
- Closed systems
  - Vendor lock-in
  - Proprietary management interfaces – lack of standard or open interfaces
  - Hard to establish collaborations

OpenFlow Architecture

- Separate control plane and data plane
  - Run control plane software on general purpose hardware
  - Programmable data plane



OpenFlow Flow Table Entry



Source: Nick McKeown, "Why Can't I Innovate in My Wiring Closet?", MIT CSAIL Colloquium, April 2008

SDN and Cloud Computing

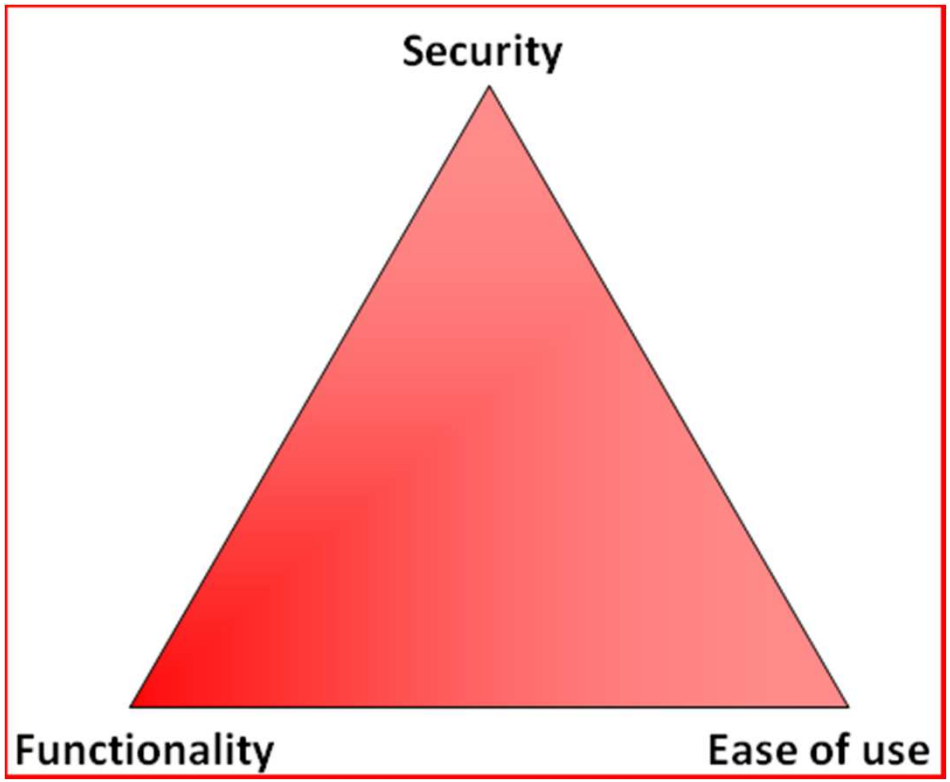
- Cloud Computing
  - Dynamic environment: resources (physical and virtual), users, and applications frequently come and go
  - Large scale infrastructure
  - Need efficient mechanisms to change how networks operate
- Without SDN
  - Rely on vendor-provided and in-house software to manage the network
  - Manually generated or semi-automatically generated configurations
  - Only cloud/network administrators can interact with network equipment

SDN and Cloud Computing

- With SDN
  - Network “programming” instead of network configuration
  - Potentially open to all users/applications
- From a security stand point, how do SDN-based clouds compare to pre-SDN clouds?
  - Can SDN address pre-SDN security vulnerabilities?
  - Does SDN expose new vulnerabilities?
  - What needs to be developed or reused to secure SDN-based clouds?

Security-Functionality-Usability

- OpenFlow and current SDN movement started as an academic project
  - Originally intended for campus networks
  - Now, many wish to apply it everywhere (including WAN)
  - Main focus on functionality (programmability of networks)



Source: Andrew Waite. InfoSec Triads: Security/Functionality/Ease-of-Use. June 12, 2010.

Cloud Security with SDN

- Opportunities
  - SDN-promoted open interfaces:
    - Large community of developers
    - Open-source culture
  - Develop vendor-independent security mechanisms
- Vulnerabilities
  - Multiple points of action/entry available for malicious users
  - Low level access to network programming can enable attacks considered impractical in the past (pre-SDN)

Network Management Complexity

- Network programming/configuration is an error-prone activity
  - SDN will not simplify network programming
  - High barrier for cloud users (as IaaS clouds shift VM/OS management to users, SDN can shift network management to users)
- SDN promotes open interfaces
  - Programs more readable
    - Easier debugging
    - Facilitate change in personnel
  - Define network programming best practices

Network Management Model

- Traditional Autonomous Systems (AS)
  - A domain/site/cloud focuses on protecting its own systems
  - Interaction with a limited number of neighboring AS
- SDN logically centralized management
  - A controller (or a collaborating set of controllers) operate network devices potentially in multiple domains
  - Need a well-defined model for collaboration and federation
  - Need to be included in the inter-cloud security discussion

Restricted vs. Open Access to Management

- Traditional management networks
  - Physically isolated from production traffic
  - Many insecure mechanisms to configure network devices, but only administrators can access
  - Access to SDN interfaces can be restricted to administrators
- SDN advocates direct network programming
  - Need to define what, how, and who can program
  - Need to develop AAA mechanisms
  - Some features starting to appear in OpenFlow controllers (e.g., NOX [1], and FlowVisor[2])

[1] NOX OpenFlow Controller. http://www.noxrepo.org
[2] R. Sherwood, G. Gibb, K.-K. Yap, *et al.*, "Can the Production Network Be the Testbed," In Proceedings of the Usenix Symposium on Operating System Design and Implementation (OSDI), 2010

Users/Tenants Isolation

- Several techniques used to achieve isolation among multiple tenants
  - Provider-controlled firewalls
  - VLANs
- SDN interfaces enable cleaner implementations
  - Quickly detect possible DoS by exhaustion attacks and direct attack traffic to low priority links
  - Program switches so that a tenant (group of VMs) minimally shares network paths with other tenants

Response to Attacks

- SDN can be programmed to act (reconfigure the network) when attacks are detected
  - Every SDN switch can be used to detect suspicious activity (e.g., match a rule and generate an event for a controller)
  - Wide range of actions – anything that an SDN program can do (as opposed to disabling a switch port or email to administrator of a traditional IDS)
- How to recast existing IDS mechanisms and algorithms in SDN environments?
- Can new algorithms be implemented with SDN?

Network Statistics Monitoring

- Traditional network statistics data (counters on switches via SNMP) rarely available to end users
- SDN switches collect statistics data per flow
  - Data exposed through programming interfaces
  - Can be used by SDN controller to adjust paths based on the statistics
    - Cloud providers can minimize SLA violations
  - Can be used by end users
    - Verify SLA violations
    - Reconfigure network to improve application performance

Data Confidentiality

- SDN does not offer encrypted communication
  - Unlikely to be implemented in the future
  - VPN-like functionality may be possible
    - Users need to trust the encryption software (VPN client) and provider-owned switch/routers (VPN server) to have access to plain data
- True end-to-end confidentiality accomplished only when secrets are only known to communication parties
  - Many application-level protocols can be used (SSL, GSI, etc)

VM Migration

- VM migration is used to improve resource management intra- and inter-clouds
  - Requires complex network reconfigurations
  - Reconfiguration complexity increases with migration distance: within rack < across racks < across server rooms < across buildings < across administrative domains
  - As SDN evolves and gets deployed, more network programs supporting VM migration will be made available
- SDN will not improve the security of VM migration

Reliability/Availability

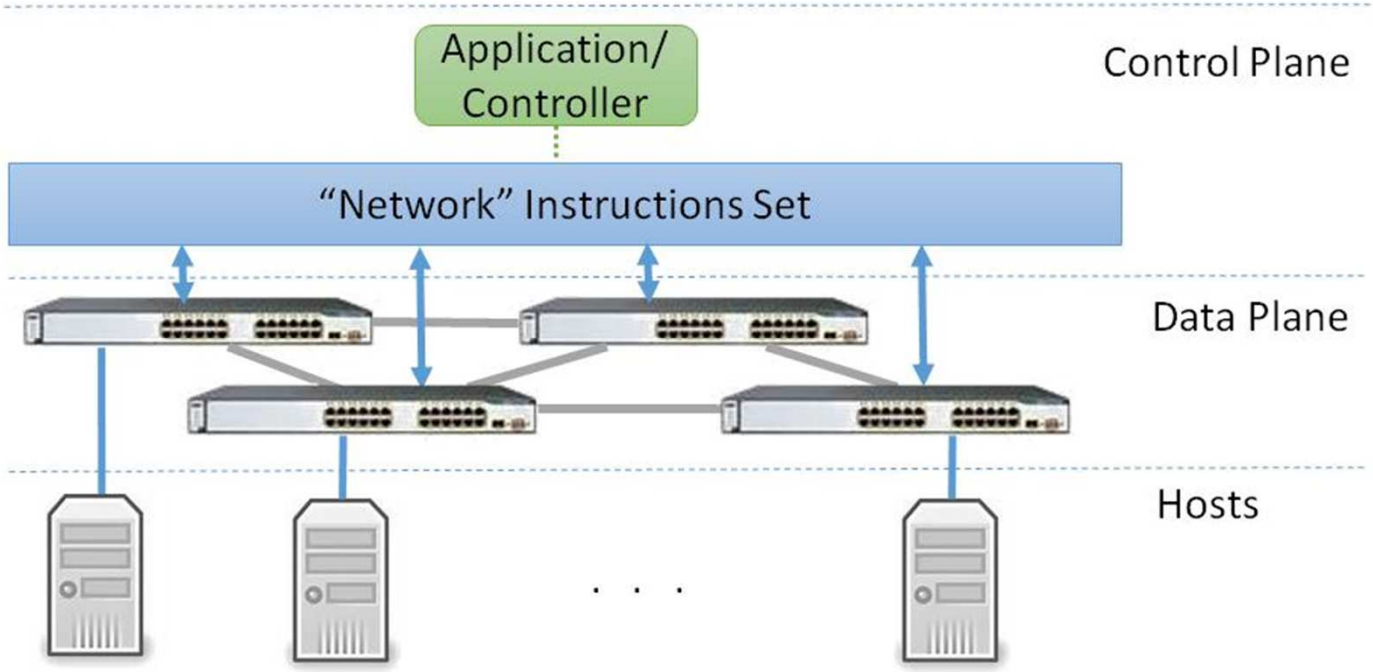
- SDN controller requires high reliability
  - SDN controller crash can cause complete network shutdown
  - Compromised SDN controller gives an attacker full control of the network
- Can existing fault tolerance techniques/mechanisms be applied?
- New vulnerabilities introduced by fault tolerance techniques (e.g., malicious controller taking over by forcing the main controller to go down)?

Opportunities for attackers

- Control and data plane interface/communication needs to be properly secured
- Low-level network interfaces make many attacks easier to accomplish (e.g., man-in-the-middle)
- Controller runs on general purpose computers where known exploits could exist

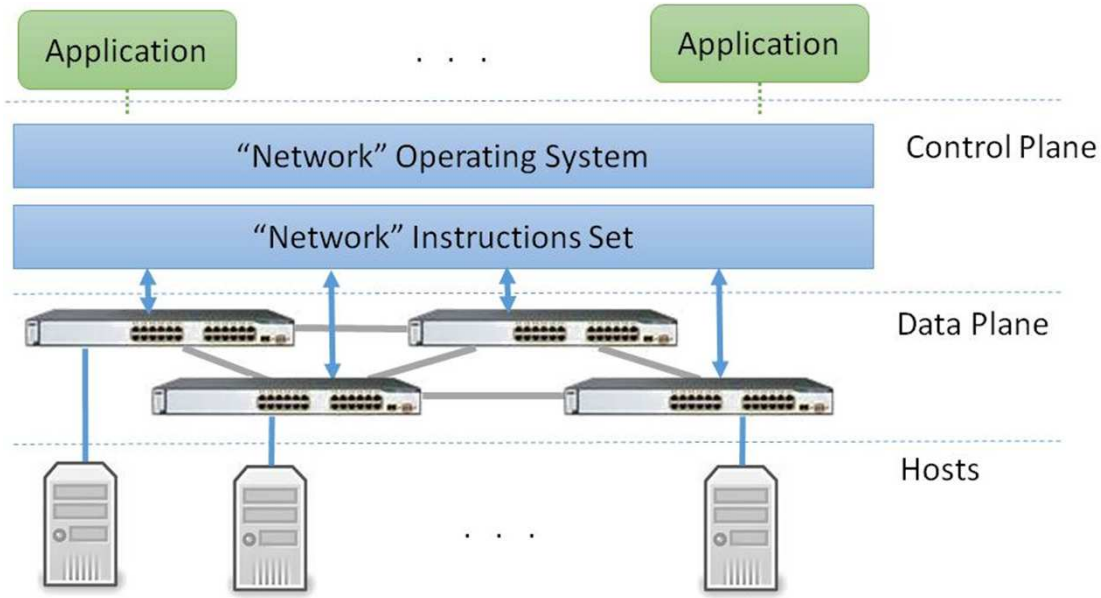
Stand-alone deployment

- Single controller
  - Only administrators can program the network
    - SDN used as a better technology for network management
    - Assuming a very reliable controller running trusted network program, substantial changes to network management security are not expected



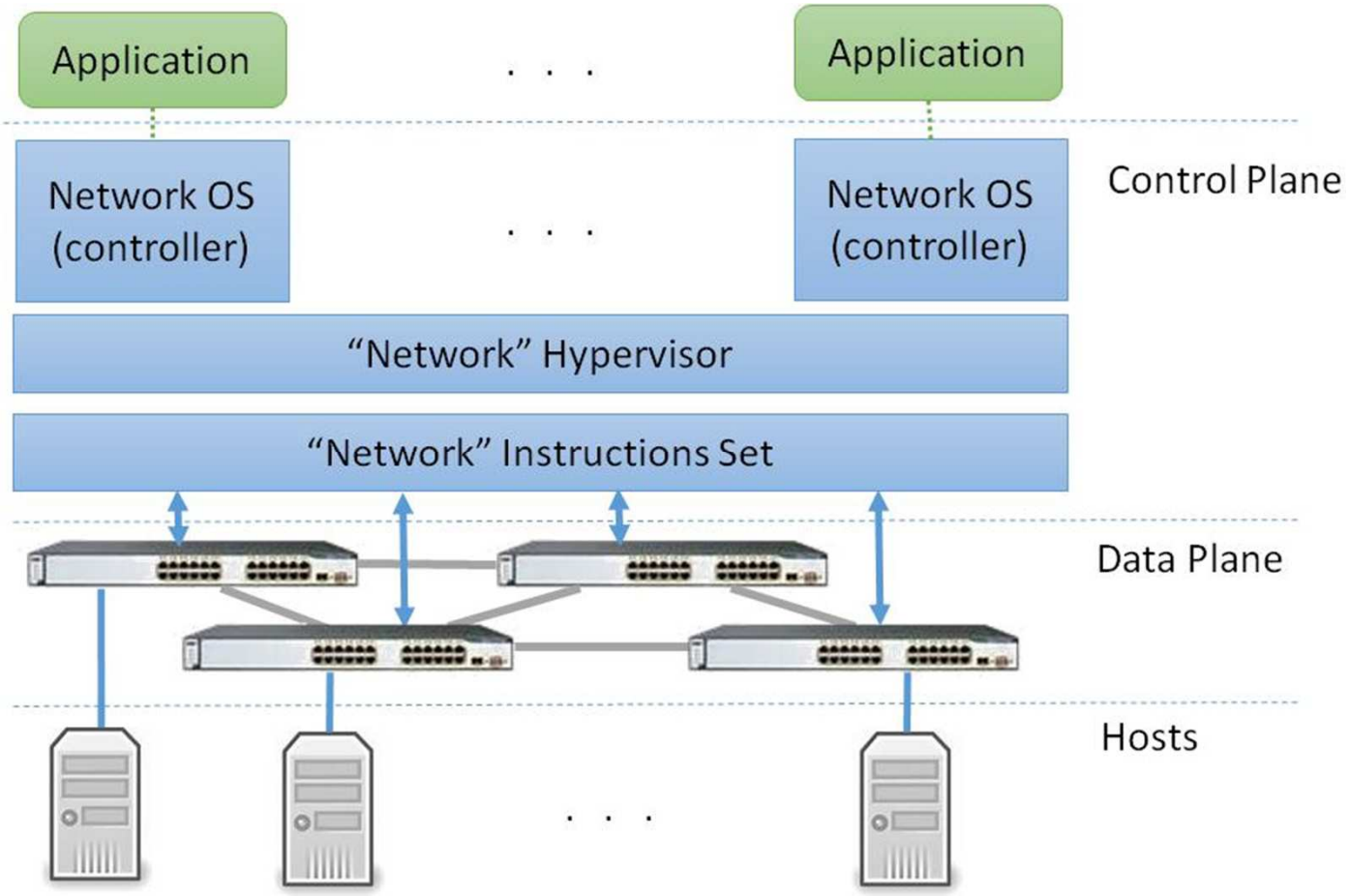
Multiple applications

- Network Operating System
  - Coordinate data plane resources
    - Each application needs to be identified
    - Needs AAA
  - “Network system call”-like interface needed
    - Accommodate conflicting requests
    - Potential vulnerabilities



Fully virtualized clouds

- SDN offers functionality to implement new network virtualization services

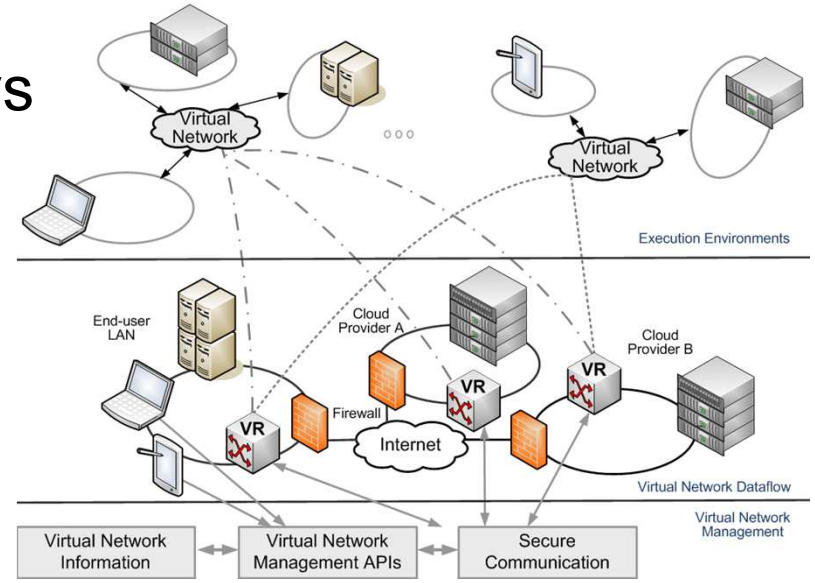


Network Hypervisor

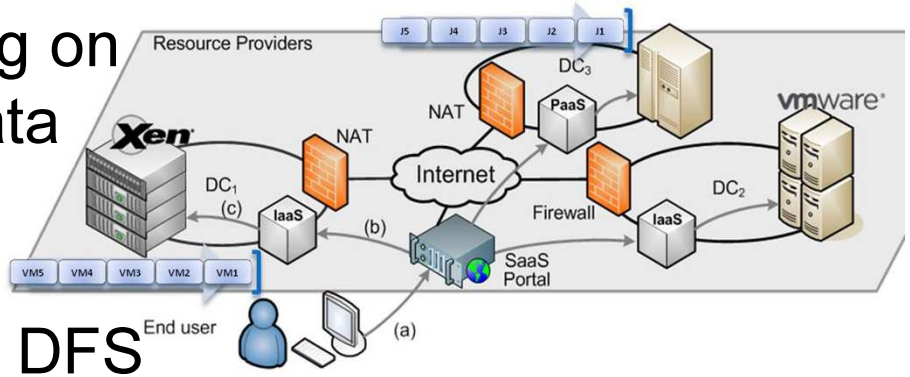
- Expose a partial view of the data plane to different network OS
- Coordinate the execution of multiple network OS
- Sophisticated AAA needed
  - IaaS clouds have a well-defined user-to-VM mappings that can be reused
  - When multiple clouds are involved, solutions for cloud federation/collaboration should be leveraged

Related Research at ACIS/CAC

- ViNe
  - Export APIs to manage IP overlays
  - Investigating mechanisms to integrate ViNe + OpenFlow
    - Transitioning solution, while WAN-SDN is not available
    - Program OpenFlow to use ViNe for WAN transport
    - Program ViNe to establish necessary tunnels



- Resource Usage Estimation
  - Distributed applications running on clouds need network usage data
  - Use SDN network statistics
  - Optimize distribution of tasks
  - Optimize distribution of data in DFS



Related Research at ACIS/CAC

- Role-based access control via delegation mechanisms using short-lived identities
  - Possible solution for needed AAA in SDN
    - SDN accounts/identities with different capabilities are created in Network Operating Systems
    - Cloud users are grouped by roles and mapped to SDN accounts with correct capabilities
    - SDN accounts are recycled when operations finish
    - No need for one-to-one mappings between cloud and SDN users
      - Smaller set of “short-lived” identities needed
      - Easier to integrate multiple user bases (inter-cloud)

Conclusions

- Can SDN address pre-SDN security vulnerabilities?
  - SDN does not simplify network management
  - Many vulnerabilities are expected to be better/cleanly addressed using SDN mechanisms
  - Requires correct network programming
- Does SDN expose new vulnerabilities?
  - Larger number of points where attacks can happen
  - Control plane exposed to attacks
- What needs to be developed or reused to secure SDN-based clouds?
  - Secure and trusted Network Operating Systems and Network Hypervisors
  - Sophisticated AAA