Information Protection in Content-centric Networks

Christopher C. Lamb

Department of Electrical and Computer Engineering
University of New Mexico

November 6, 2012

THE UNIVERSITY of NEW MEXICO

Outline

Definitions

There are a few different definintions of **Assured Information Sharing**:

- The DoD's vision for AIS is to *"deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment"*
- Daniel Wolfe (formerly of the NSA) defined assured information sharing (AIS) as a framework that *"provides the ability to dynamically and securely share information at multiple classification levels among U.S., allied and coalition forces."*
- For the scope of Nublu: *A modern computer system capable of dynamically and securely managing delivery and use of open and sensitive information to U.S., Allied, and Coalition partners when and where the partners need it, in a form they can use, to provide an asymmetric operational advantage to U.S. affiliated forces.*

Definitions

So what does this mean?

- **Modern computer system** — cloud based; we'll use openstack as it is what MilCloud is based on and we want to integrate with this to have a chance for Phase III.
- **dynamically and securely managing delivery and use** — providing the ability to *autonomously* provide and retract access to information based on *changing properties* of that information, the environment, and system users. The information must be delivered respecting defined *confidentiality*, *integrity*, *availability*, *urgency*, and *importance* requirements.

CIA doesn't cut it!

CIA is not enough; need some idea of information importance and urgency too.

Phase I Goals

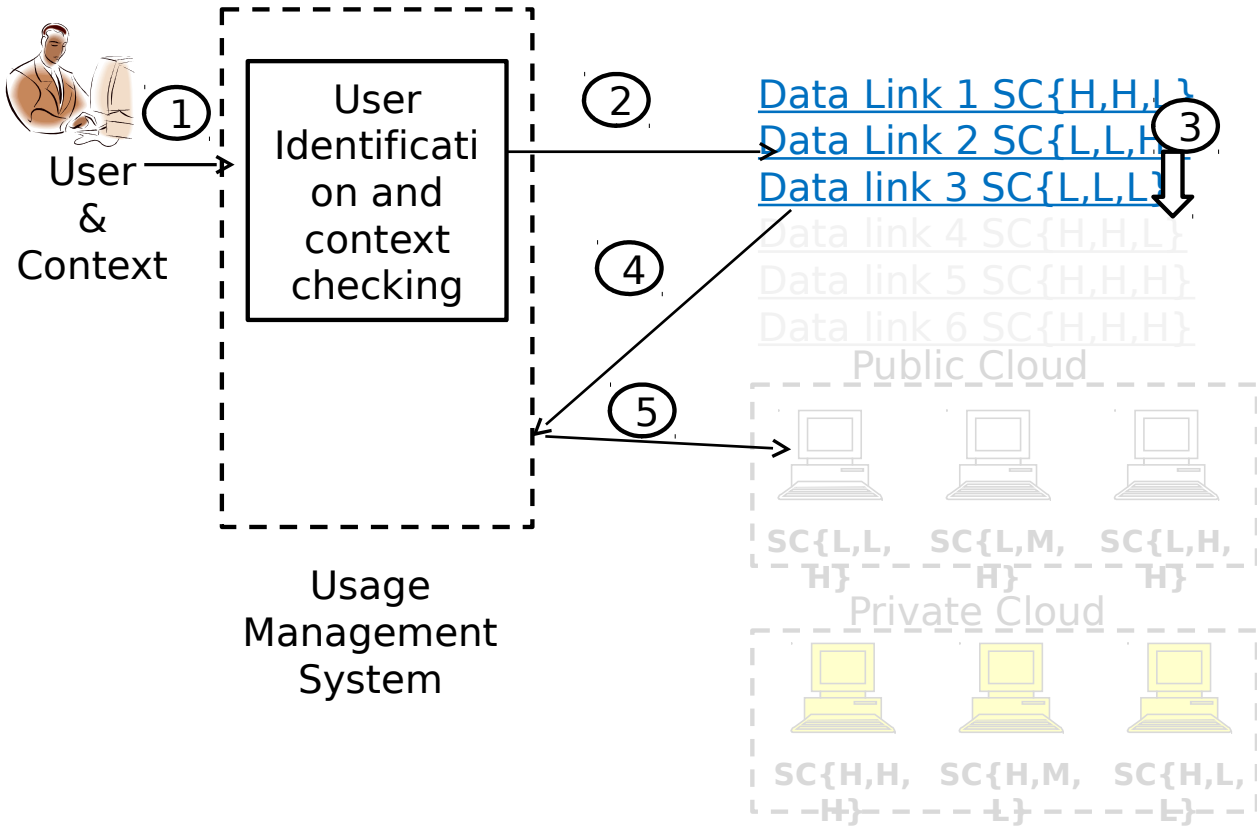
Original Concept of Operations — resource access and virtual machine instantiation is a function of user authorization, operating context, resource attributes, and usage policies.

- ***Confidentiality*** — Proof-of-concept in Phase I, extended in Phase II
- ***Integrity*** — To be addressed in Phase II
- ***Availability*** — Out of scope for Nublu

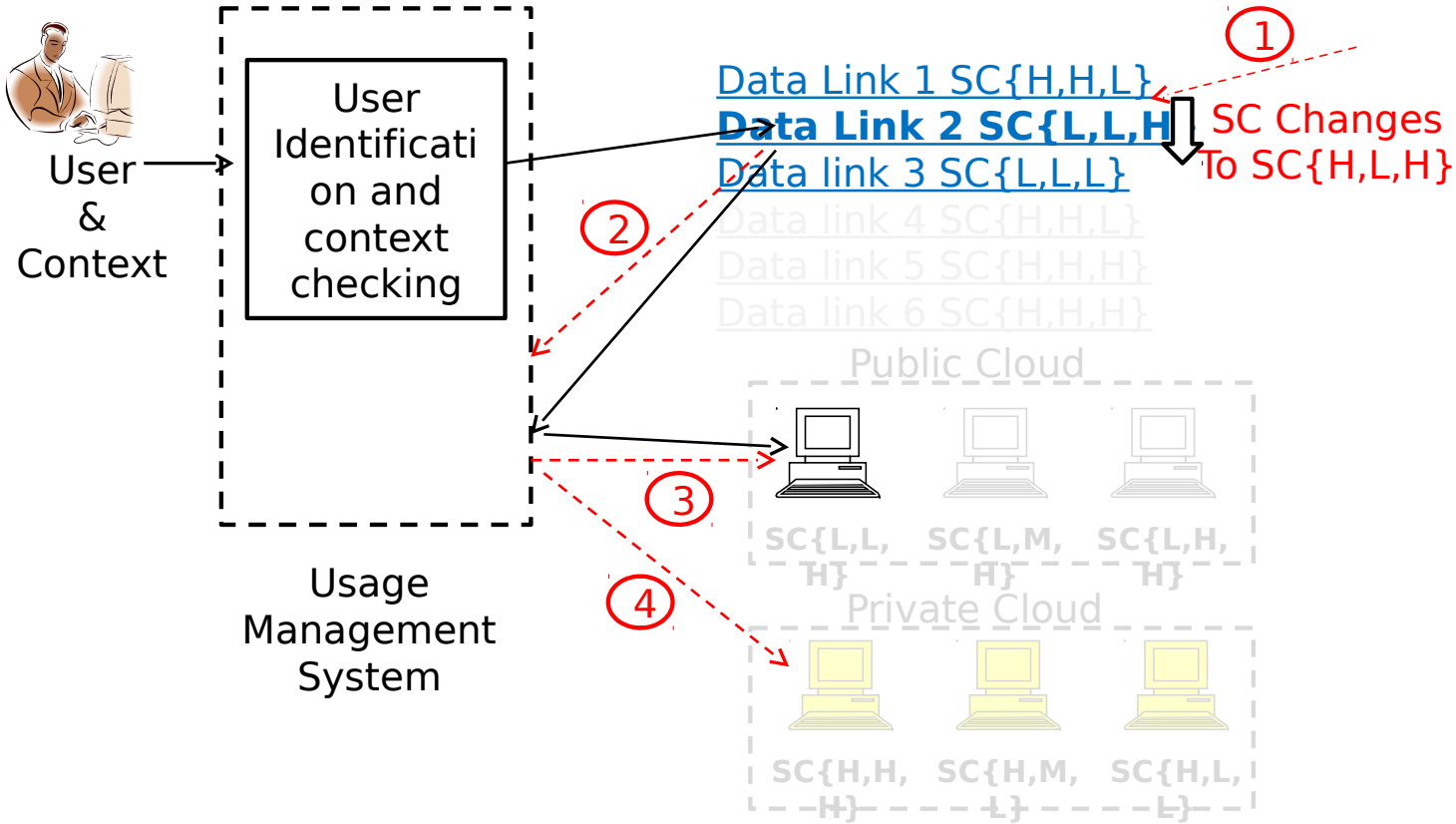
Usage Management System

Controls the initial resource access and cloud computing system provisioning. Monitors the resource security parameters, cloud computing resource security characteristics, and operator context to provide continuous control.

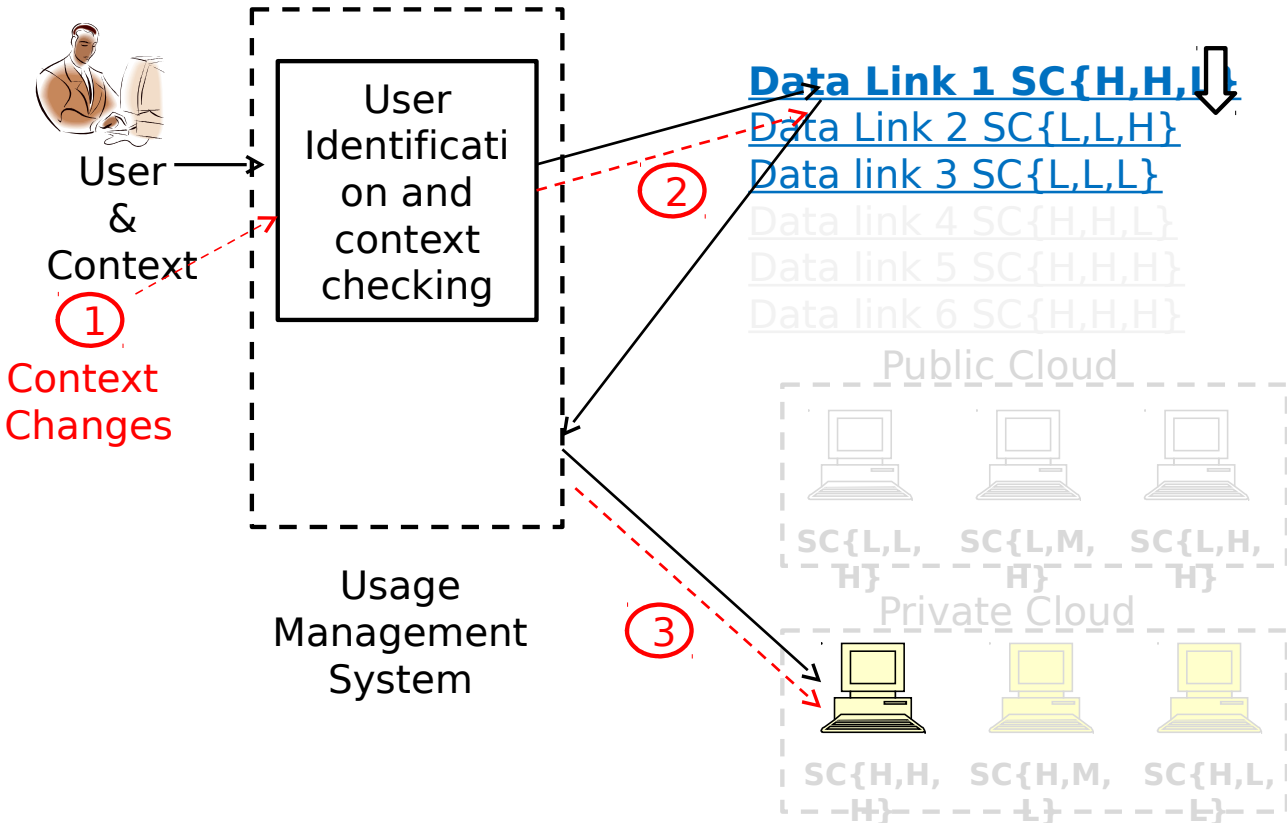
Operation — Initial Configuration



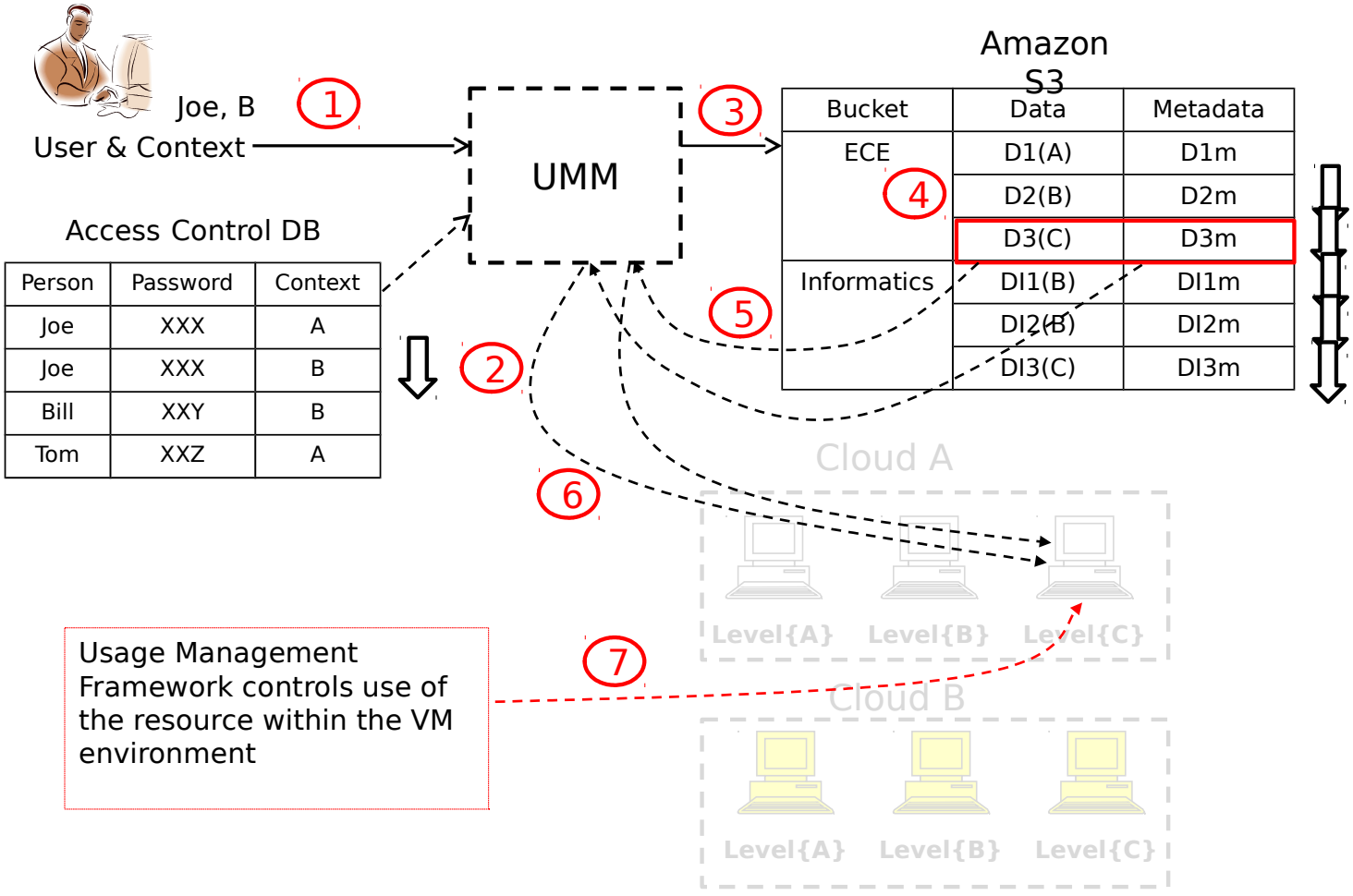
Operation — Dynamic Re-configuration 1



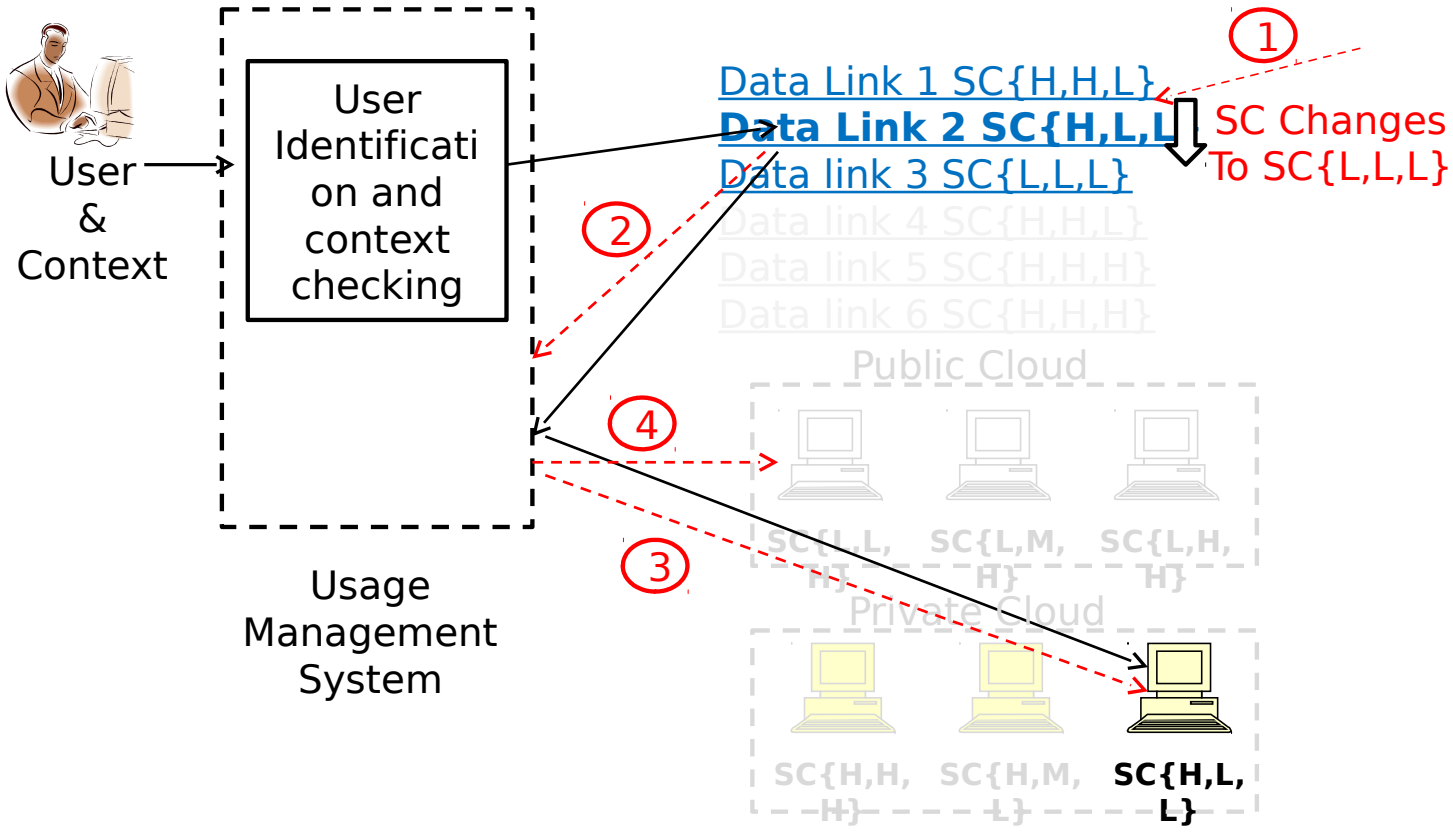
Operation — Dynamic Re-configuration 2



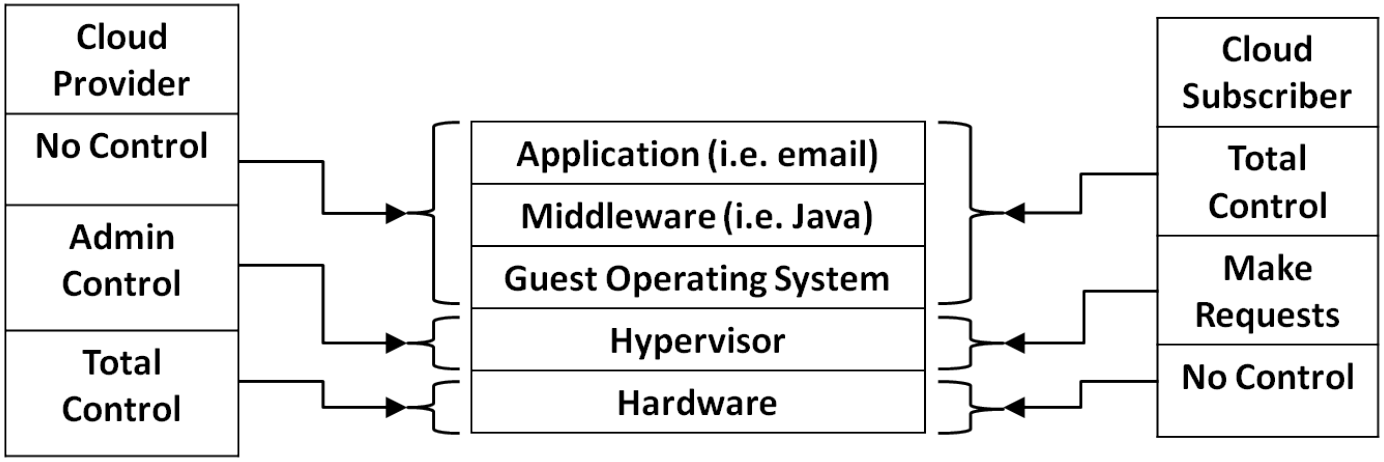
Operation — Usage Management



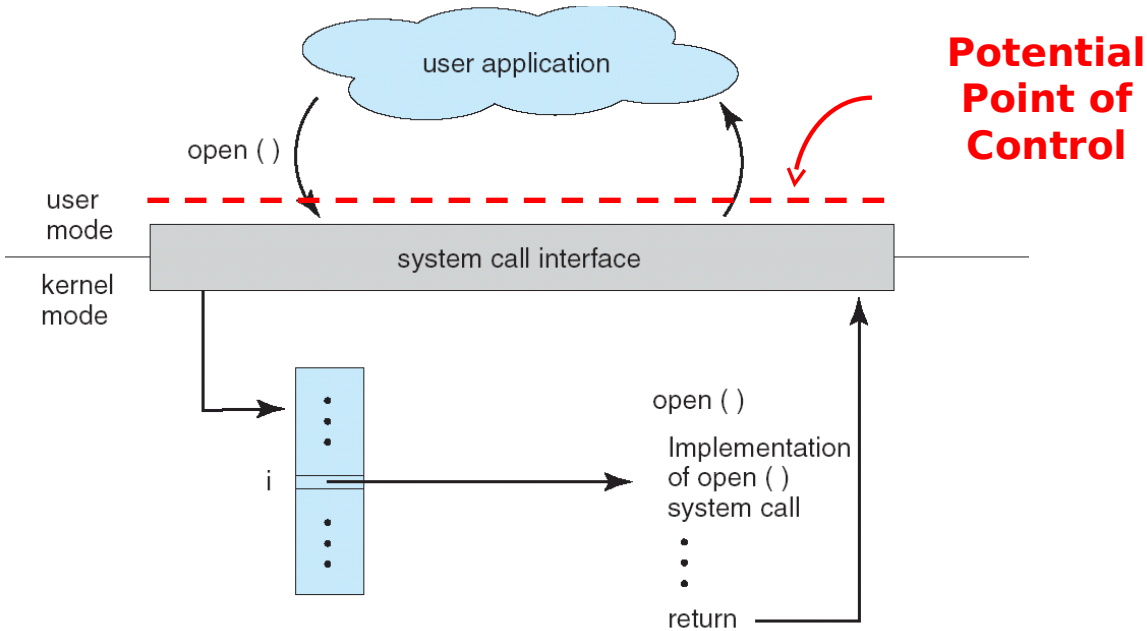
Operation — Dynamic Re-configuration 3



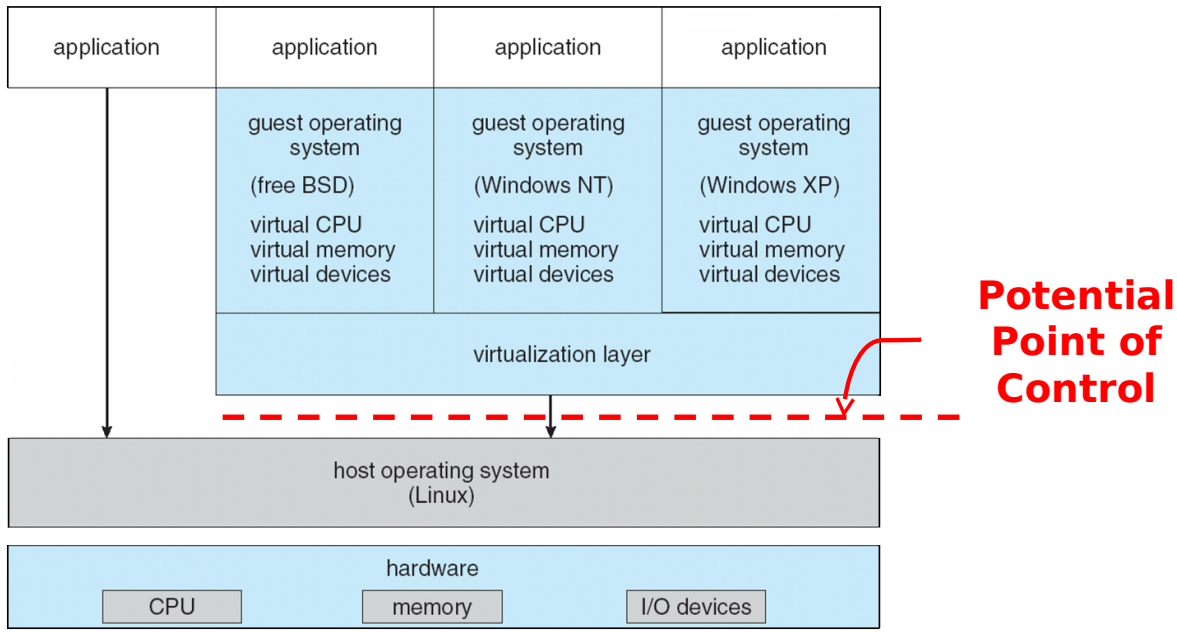
Span of Control — IaaS



Application Software and OS



Layering with VMWare



What else will we not do?

We are to provide a cloud-based system integrable with MilCloud that supports these goals. We will not:

- Provide last-mile data consumption
- Develop sensor networks

Still...

We need to be able to take data from sensor networks and deliver information to mobile consumers. This implies some kind of *very simple* mobile client emulated sensor input.

Building Blocks and Strategy

Strategy: Use functional partitioning to simplify overall architecture and issue traceability. Some examples:

- **Enclaves** — Dedicated environments providing processing, networking, or storage services.
- **Processing** — Processing nodes of various sizes and configurations, hosted in various enclaves.
- **Networking** — Networks connecting nodes using overlays and differential routing supplying different protection schemes.
- **Storage** — Storage using different approaches and security profiles. Includes primary (repositories) and secondary (caches) storage.
- **Information** — Meaningful data of different types (e.g. streaming, structured, document-based.
- **Policies** — Policies describing use of information.

Attributes? Internal and external structures? Security Models?

Possible Research Topics

- In VM usage management, or dedicated VM instances?
- Cross Domain Communication Surfaces and Design
- Controllable Bursting System Design (inter- and intra- cloud)
- Provisionable, dynamic network security
- Data Management Standards: Rest, Motion, Use
- Cloud Confidentiality, Integrity, Availability Strategies and Costs
- SEIM Cloud Solutions and Architectures: How to build?
- Implications of the Last Mile: Delivering Sensitive Info to Mobile Devices
- System and Data Security Models and Implications

Attributes of Use Cases

Use cases embody:

- **Who** — U.S., Allied, Coalition
- **What** — managing sensitive and open information (giving, limiting, or denying access), impact of environmental attributes, bursting based on performance, differential security control application
- **When** — time bounds on information delivery
- **Where** — Geographic bounds on information dissemination
- **Why** — N/A
- **How** — Dynamically and Securely, other