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 isn't sufficient

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. Phase II builds on phase I via:

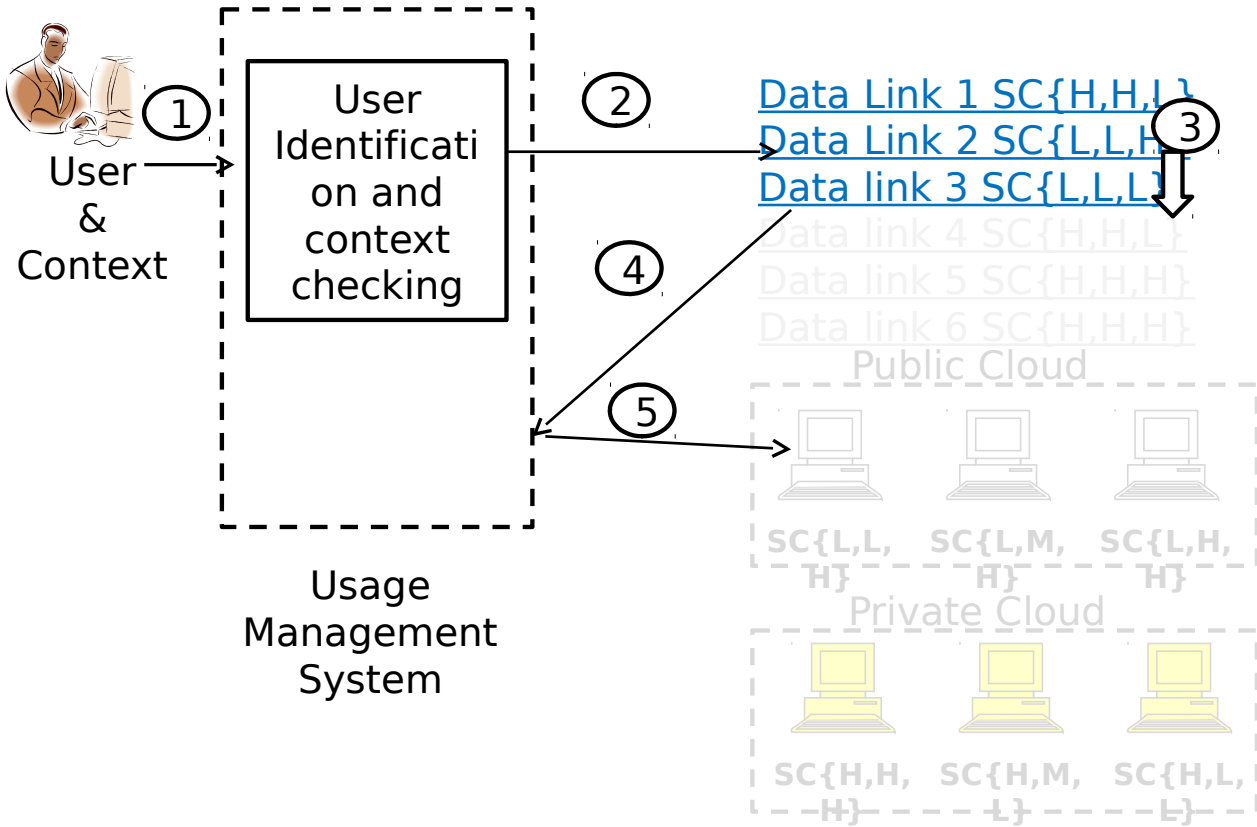
- ***Confidentiality*** — Data object key management, user key management, homomorphic encryption
- ***Integrity*** — Individual and Group signature schemes, integrated integrity verification checking
- ***Availability*** — Hardened instances, redundant images

Other areas of work include robust, graduated logging and auditing.

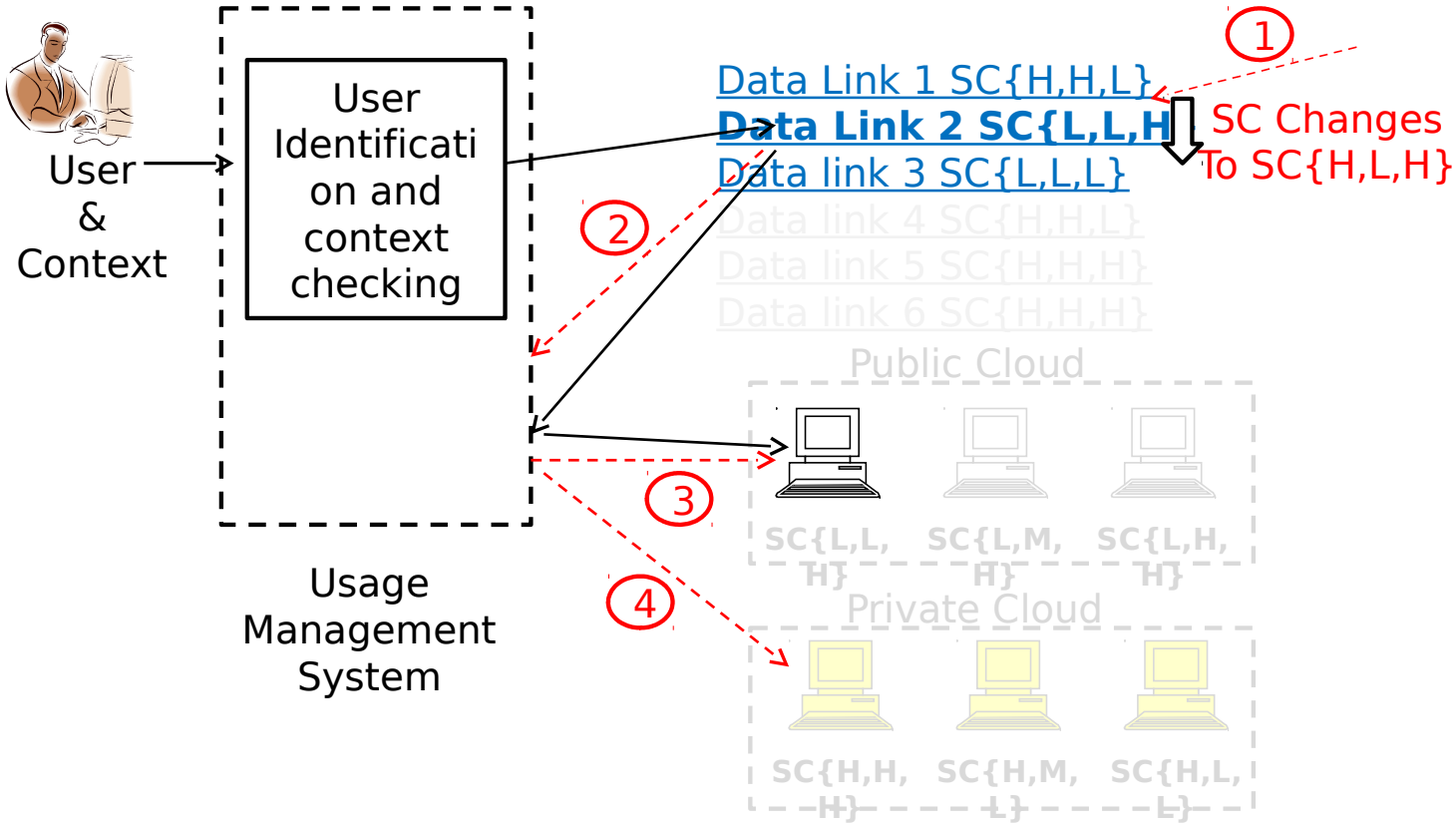
Usage Management System

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.

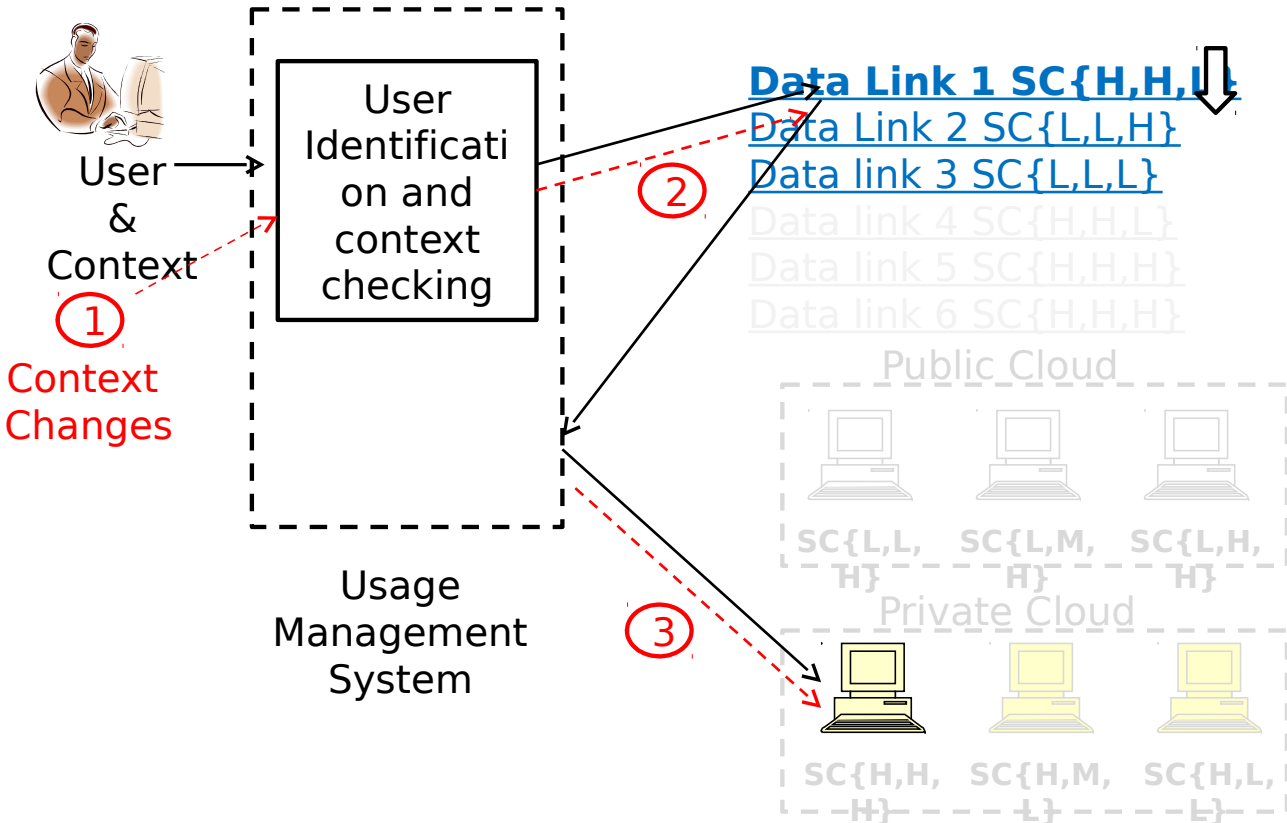
Operation — Initial Configuration



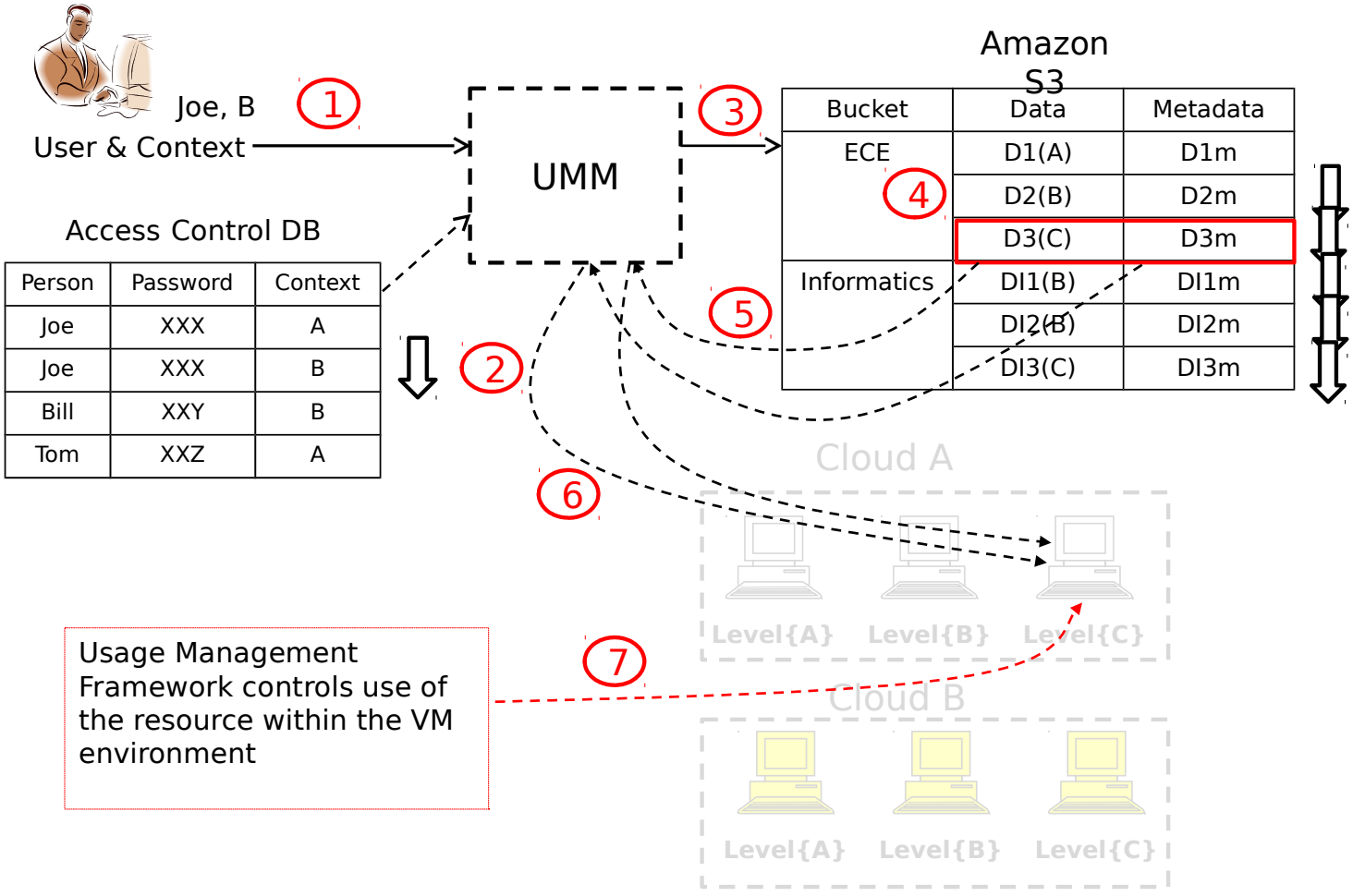
Operation — Dynamic Re-configuration 1



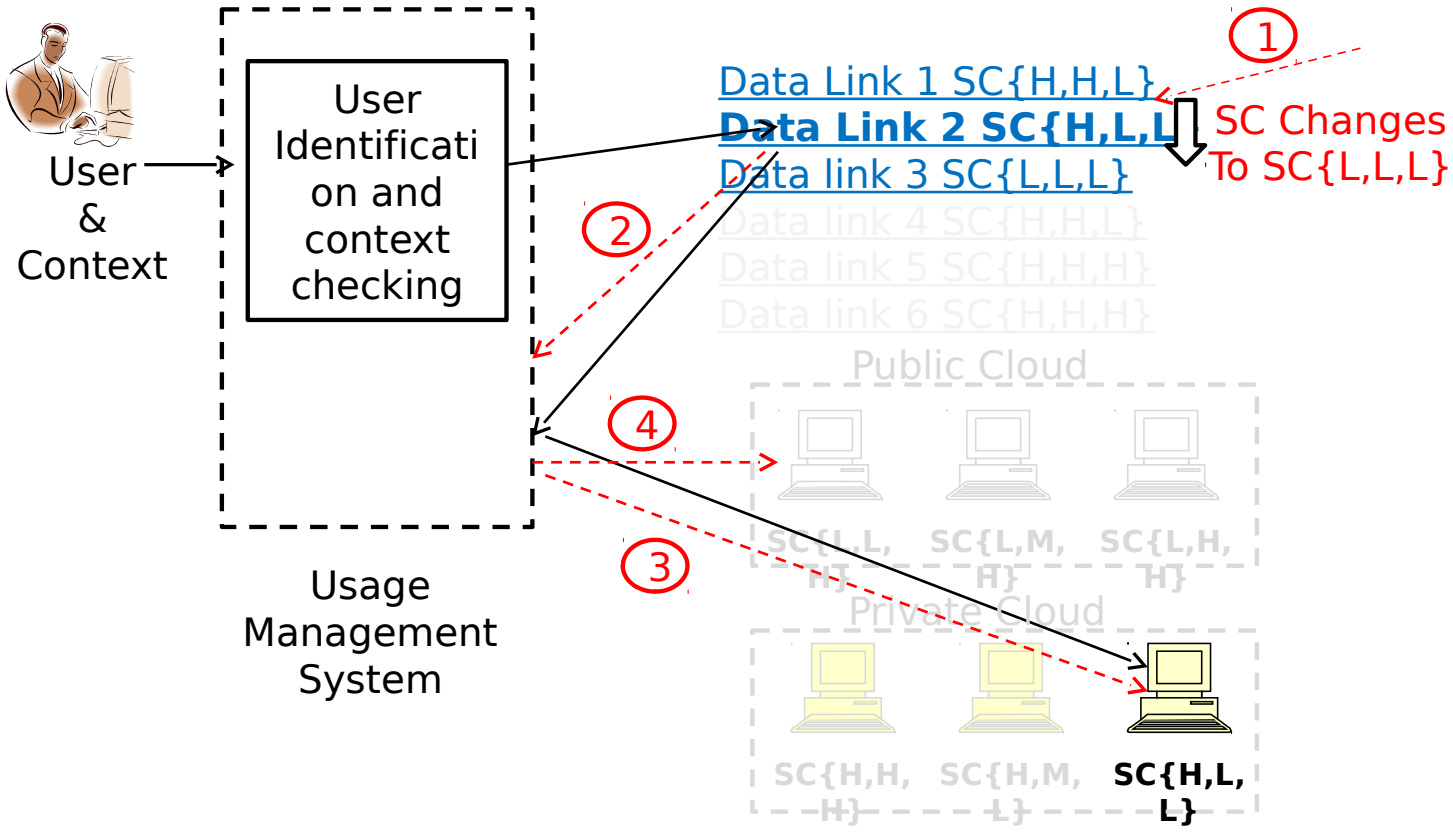
Operation — Dynamic Re-configuration 2



Operation — Usage Management

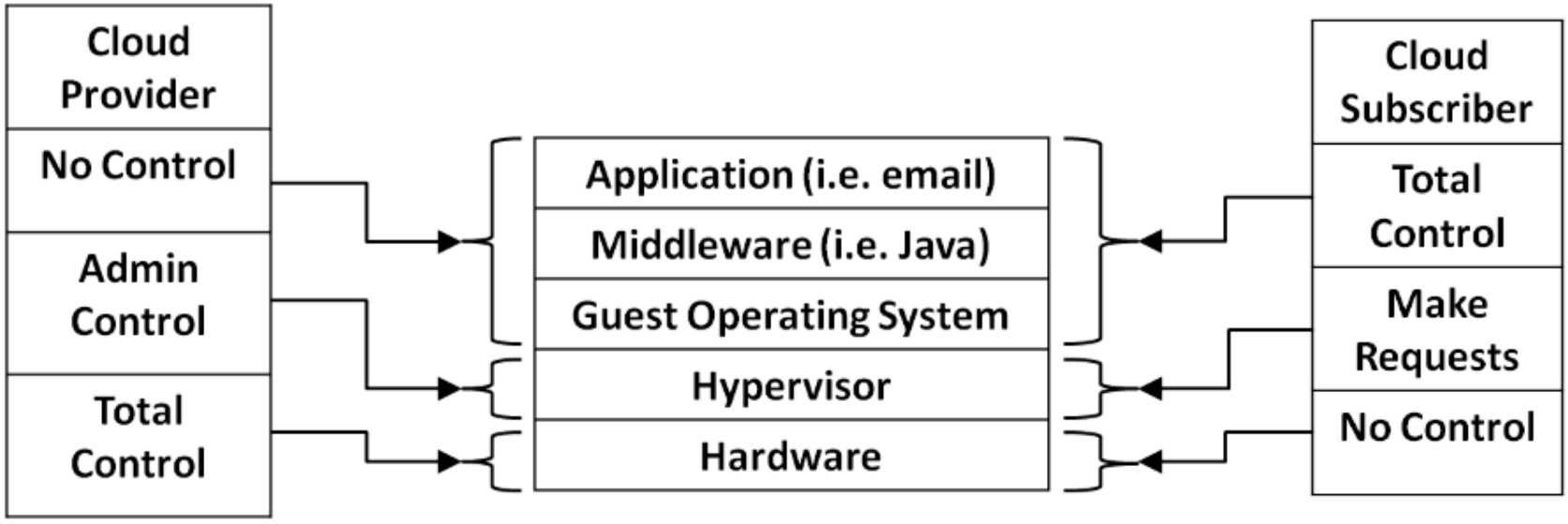


Operation — Dynamic Re-configuration 3

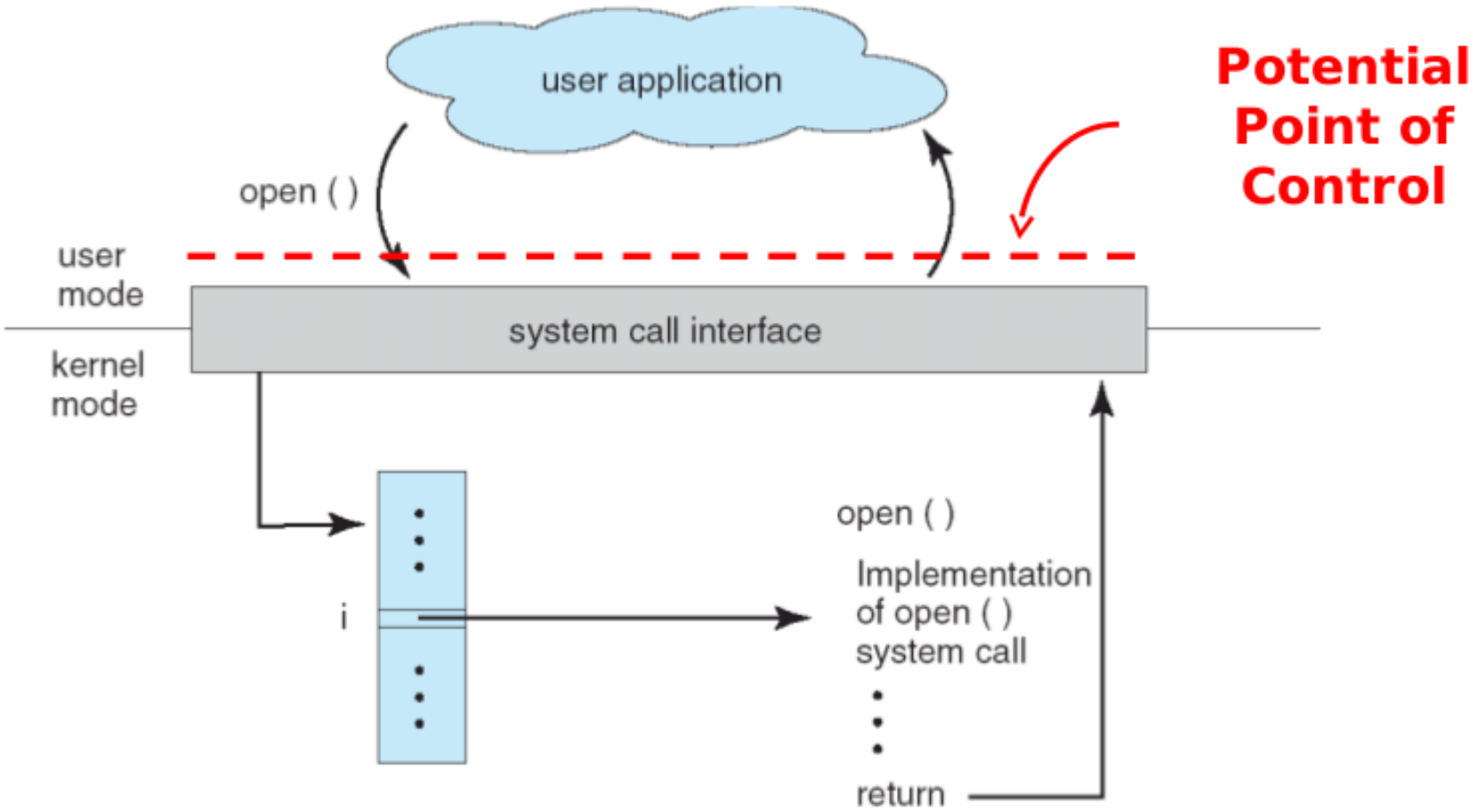


Building on Phase I

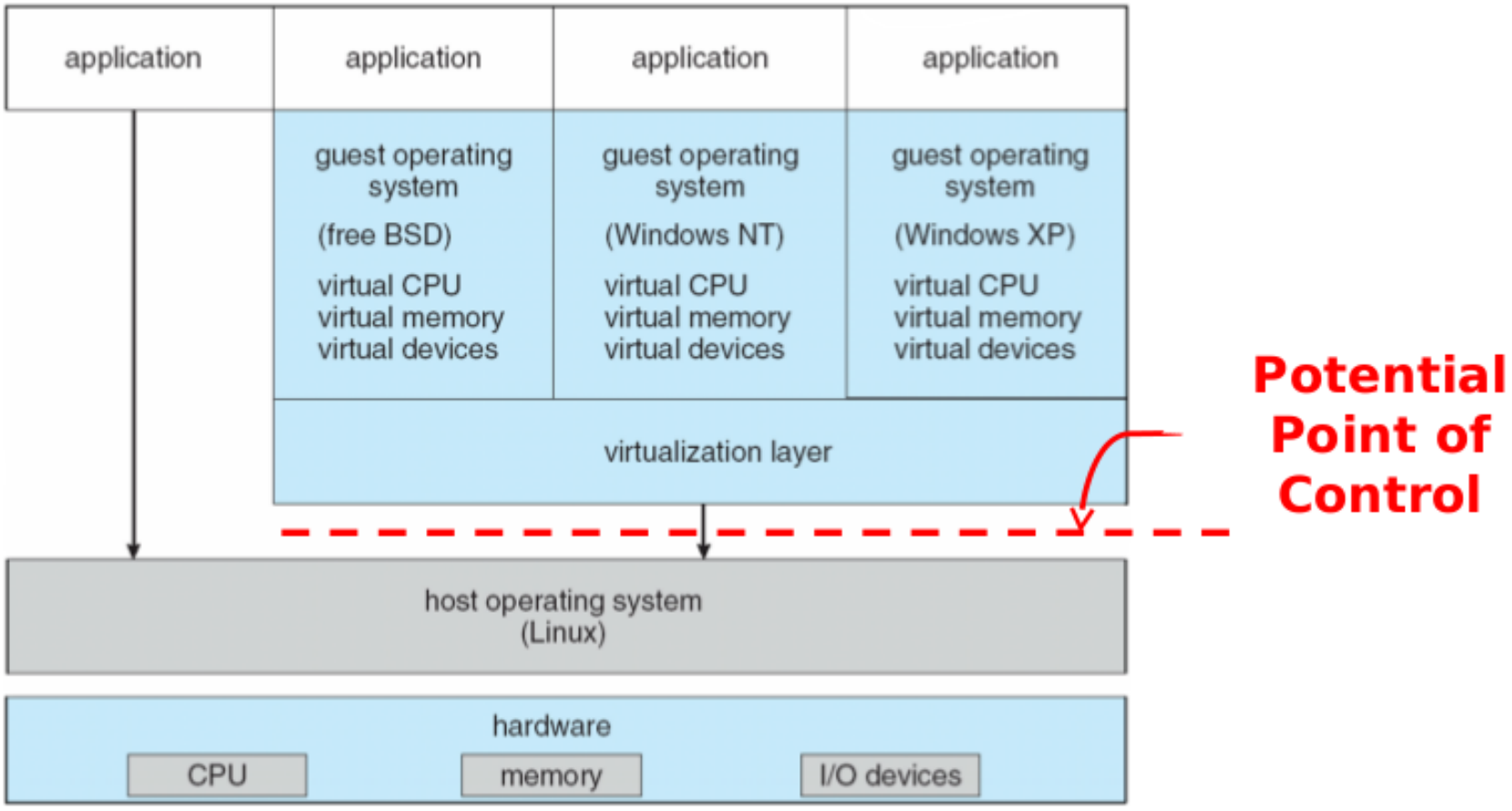
Span of Control — IaaS



Application Software and OS



Layering with VMWare



Key Considerations

- The interfaces between the application and operating system, and between the operating system and the hardware, lend themselves to the introduction of control functions.
- It is highly undesirable to modify the operating system itself because of the size and complexity.
- It is also undesirable to modify application software.
- Hardware components like the TPM can provide extremely useful capabilities in private cloud environments.
- Encryption is a key element in information security.Partially homomorphic encryption can be useful in some applications, but is not a universal solution.
- Isolation methods using nested virtualization are very useful.
- Key management procedures and certificates will be essential.

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.

Attributes of Use Cases

Use cases embody:

- **Who** — U.S., Allied, Coalition, computerized agents
- **What** — managing sensitive and open information (giving, limiting, or denying access), impact of environmental attributes, bursting based on performance, differential security control application, storage, processing, information display, dynamic information control (distribution, retraction)
- **When** — time bounds on information delivery, time boxed information
- **Where** — Geographic bounds on information dissemination, geographic bounds on information sources
- **Why** — N/A
- **How** — Dynamic policy and security postures, other

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?

Information Objects

Start with an *Information Object*.

This is a resource that contains valuable, managed data.

Protected it via encryption, and digitally sign the encrypted information object.

Now, the *information object* has become a *protected information object*. This package can then be stored in any number of object or document-centric storage schemes common in cloud environments.

Policies are associated with protected information objects, forming *protected information packages*. Policies are not encrypted. *Integrate open and closed source encryption algorithms.*

Virtual Networking

The protected information package moves through securely provisioned *virtual networks*. These networks are configured with strong encryption, and involve only those parties that need access to the distributed information. They are configured dynamically, when needed. They are multiplexed over shared physical infrastructure.

SDN and pop-up VLANS?

Policy Enforcement

Distribution and policy enforcement is handled by a *usage management mechanism*. This usage management mechanism acts as both a policy decision point and a policy enforcement point.

This component can filter and modify content based on dynamic subject, environment, and resource centric policies. It furthermore is closely coupled to any PKI systems, and can extract, repackage, and re-sign any content en-route to a specified destination.

We have policy enforcement throughout the system.

Can we maintain secret inputs here too? How to manage keys and encryption algorithms? Every UMM must have access to content to do content modification. How many keys does a UMM need to manage? How do we secure key management subsystem? Multi-party computation is maturing; applicable?.

Processing

Processing nodes receive data and are able to commence processing. These nodes are virtualized, and all keys are pinned in memory when used.

Nodes may either control computation via internal usage management, or be configured to handle information at a specific sensitivity level, or both.

bursting? Can we use an encryption scheme that supports usage management? e.g. portion marked fields are encrypted with different keys, and access becomes a key distribution issue rather than a content editing problem?

Delivery and Consumption

Thick clients, web, mobile clients, need to support multiple technologies, though we don't need to develop professional clients. Proof on concept clients are acceptable. Can we decrypt in Javascript, or do we need to write our own library (this may be out of scope)?

Do clients subscribe to feeds that deliver secure information packages? how do we retract content a user has been given access to? We must control the endpoints to make this happen; think Kindle when your CC doesn't process.

SIEM

Logly, others? Opensource SIEM projects we can leverage?

This is important but starts to become a bit out of scope; we need to limit the work here, yet show possible forensic capability.

Tie to OpenStack

OpenStack and by extension MilCould has specific functional components that provide the services we'll use to provide the functions we've outlined.

Tie the functional view into these specific OpenStack components to show how we will build what we propose. Show specific functions used in these functional components, highlight what may be missing today.

Discuss OpenStack relationship to MilCloud.

Other Concerns

system and data security models? Show how the supported system supports known security models (Bell-LaPadula, Brewer Nash, etc.)