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

THE UNIVERSITY *of*
NEW MEXICO

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.*

THE UNIVERSITY of
NEW MEXICO

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.

THE UNIVERSITY *of*
NEW MEXICO

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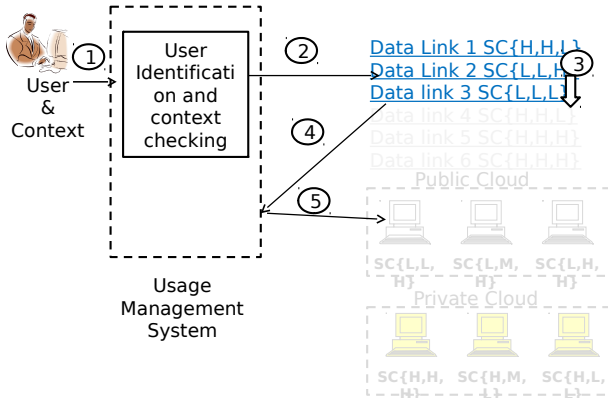
- *Confidentiality* — Data object key management, user key management, homomorphic encryption
- *Integrity* — Individual and Group signature schemes, integrated integrity verification checking
- *Availability* — Hardened instances, redundant images

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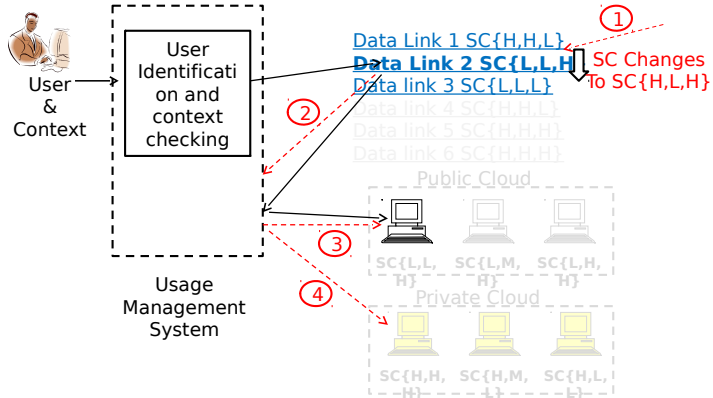
Usage Management System

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.

THE UNIVERSITY of NEW MEXICO

Operation — Initial Configuration

User
&
Context

①

User
Identificati
on and
context
checking

②

Data Link 1 SC{H,H,L}
Data Link 2 SC{L,L,H}
Data link 3 SC{L,L,L}
Data link 4 SC{H,H,L}
Data link 5 SC{H,H,H}
Data link 6 SC{H,H,H}

③

④

Public Cloud

SC{L,L,H} SC{L,M,H} SC{L,H,H}

⑤

Private Cloud

SC{H,H,H} SC{H,M,L} SC{H,L,L}

Usage
Management
System

Operation — Dynamic Re-configuration 1

User & Context

User Identification and context checking

Usage Management System

Data Link 1 SC{H,H,L}
Data Link 2 SC{L,L,H}
Data link 3 SC{L,L,L}
Data link 4 SC{H,H,L}
Data link 5 SC{H,H,H}
Data link 6 SC{H,H,H}

① SC Changes To SC{H,L,H}

②

③

④

Public Cloud

SC{L,L,H}   SC{L,M,H}   SC{L,H,H}

Private Cloud

SC{H,H,H}   SC{H,M,L}   SC{H,L,L}

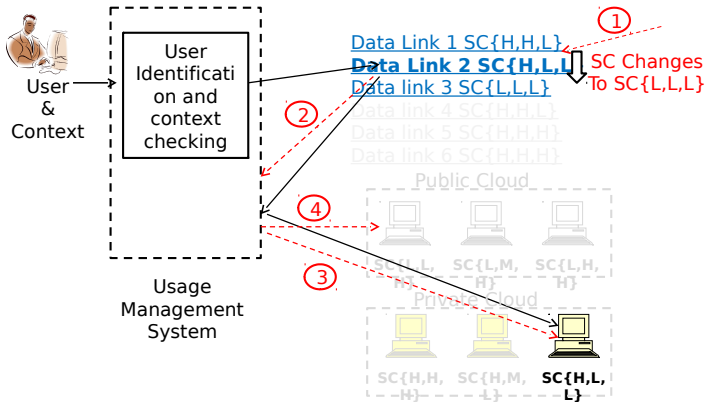# Operation — Dynamic Re-configuration 2

Operation — Usage Management

Operation — Dynamic Re-configuration 3

User & Context

User Identification and context checking

Usage Management System

Data Link 1 SC{H,H,L}
Data Link 2 SC{H,L,L}
Data link 3 SC{L,L,L}
Data link 4 SC{H,H,L}
Data link 5 SC{H,H,H}
Data link 6 SC{H,H,H}

① SC Changes To SC{L,L,L}

②

④

③

Public Cloud

SC{L,L, L} SC{L,M, H} SC{L,H, H}

Private Cloud

SC{H,H, H} SC{H,M, L} **SC{H,L, L}**

THE UNIVERSITY of
NEW MEXICO

THE UNIVERSITY of
NEW MEXICO

Span of Control — IaaS

Cloud Provider			Cloud Subscriber
No Control	Application (i.e. email)	Total Control	
	Middleware (i.e. Java)		
Admin Control	Guest Operating System	Make Requests	
Total Control	Hypervisor	No Control	
	Hardware		

Application Software and OS

Layering with VMWare

application	application	application	application
	guest operating system (free BSD) virtual CPU virtual memory virtual devices	guest operating system (Windows NT) virtual CPU virtual memory virtual devices	guest operating system (Windows XP) virtual CPU virtual memory virtual devices
	virtualization layer		

host operating system (Linux)

hardware

CPU   memory   I/O devices

Potential Point of Control

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.

THE UNIVERSITY *of*
NEW MEXICO

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.

THE UNIVERSITY *of*
NEW MEXICO

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?

AIS in the Cloud

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 an *information package*.
This package can then be stored in any number of object or
document-centric storage schemes common in cloud environments.

The 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.

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 resign any content en-route to a specified destination.

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