1 Introduction

Currently, the security of networked infrastructures tends to be managed statically. That is, security requirements are developed and implemented within the networking environment, and all of the information that traverses the network will have these hard-coded security policies applied to it. Thus, the security policies applied to all information is ?one-size-fits-all,? and can typically only be modified by network administrators. The result is that if there is a mismatch between mission requirements and network security, the network resources simply cannot be used to service the mission.

The ability to quickly, securely, and reliably share information across security domains is a capability that must be developed in order to ensure mission success in Department of Defence (DoD)cloud-based network-centric environments. We propose the continued development of an assured information-sharing framework for cloud-based systems that leverages our ongoing work in the areas of policy-based usage management and semantic interoperability. The development of this framework involves research related to the creation of a novel approach to information sharing that treats security as a commodity that can be dynamically provisioned within the cloud, along with other cloud resources.

Policy Tools. First, we must develop the technologies that allow administrators to easily generate policies that leverage cloud computing-specific capabilities. That is, additional research is needed to develop a set of cloud computing-specific security policies that can be encoded into the extensible markup language (XML) policy format we currently use. This work will include extending our existing policy generator capabilities to address these cloud specific policies.

Dynamic Evaluation. In addition, the usage management framework must be extended to include the ability to formally interpret and enforce cloud-specific policies. These capabilities must include the ability to dynamically monitor the policies associated with resources in use in order to immediately react to changes. We envision this research including the development of a satellite usage management capability that operates in each VM. This approach will also require the development of capabilities that allow the global usage management mechanism to communicate in an assured manner with the usage management mechanisms executing in the individual VMs, providing comprehensive usage control across a distributed cloud environments.

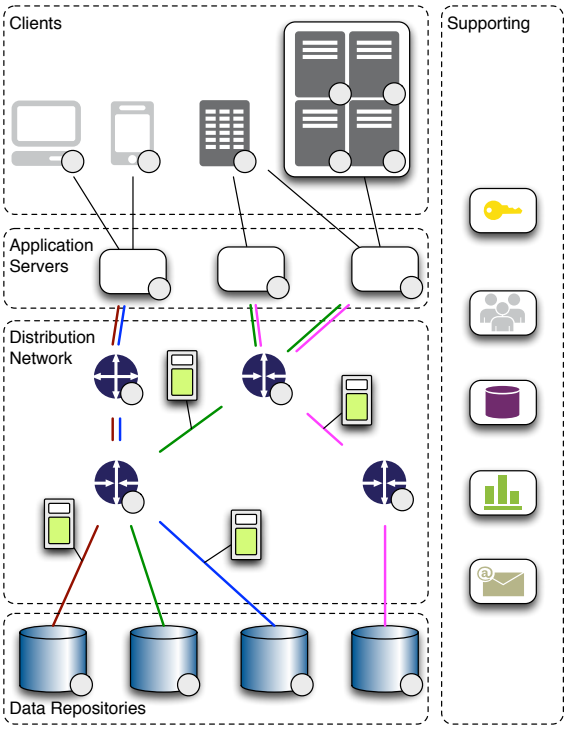

Figure 1: A notional view of the Nublu system, showing various required and provided services in an end-to-end perspective.

Enforcement. Finally, policy enforcement mechanisms are needed at all levels of the cloud hierarchy to control how data and services are used. For example, if a data item is specified at a certain level of sensitivity, the usage management mechanisms must ensure that this item is not stored or routed through the cloud infrastructure in a way that would violate the policies associated with its sensitivity level. In order to accomplish this, our approach maintains clean

separations between policy specification, interpretation and enforcement. This allows the framework to leverage security capabilities that are currently available or in development by other information security research groups.

Security Primitives and Control. In general, a DoD cloud computing infrastructure may be highly heterogeneous and used by multiple parties that may be involved in multiple missions, leading to highly complex usage patterns and security requirements. Thus, our Phase II research will continue to investigate the use of control theory in order to ensure that multiple missions can be simultaneously satisfied within a given infrastructure. Our next steps in this area involve investigating VM performance control capabilities that enable monitoring of central processing unit utilization and the development of appropriate control algorithms that automatically add or remove VMs to meet performance requirements within a given security posture.

Additional security issues associated with cloud computing that will be considered as a part of this usage management/control-theoretic framework include joint tenancy of a not trusted user's VM on the same server hardware, data remnants in cloud storage repositories and VMs, and the trust associated with cloud provider?s administrators (who have complete access to user data and VMs). Some of these concerns could potentially be addressed with usage policies; however, further research is needed to explore how the proposed usage management framework, in conjunction with

2 Operational Scenarios and Requirements

Nublu is intended to provide assured information sharing capabilities over private and public infrastructures. To do this, we will provide a secure virtualized system protected by integrated policy-based usage management integrated with key encryption technologies. Virtualization will span the entire system, from data repositories to communication networks to application servers to clients, when possible.

2.1 Abstract Requirements

2.2 Selected Scenarios

We have specific scenarios that embody information sharing that we can use to highlight the kind of functionality the system needs to produce in order to provide assured cloud-based information sharing. These scenarios have distributed communication requirements, use encryption, have multiple parties of various trust levels and need to know, and use both human and machine agents.

Streaming Data From Drone. This is a data ingestion scenario. Data from some kind of drone, manned or unmanned, is pulled into a cloud-centric distribution system for storage and processing.

Streaming Data Consumption by Coalition Partner. In this scenario, a coalition partner is streaming video from a data source to some type of client. The video itself is not classified, but it is sensitive, and is accompanied by specific usage and routing policies.

Block Data Transfer within Datacenter. Datacenters in cloud environments usually host block storage for cloud clients on systems that are distinct from the computational systems themselves. Here, filesystem blocks are transferred from a block store to a client. The blocks themselves are categorized as sensitive, and have associated usage and management policies.

Automated Information Consumption by Remote System Agent. Here, a system agent on a remote system acquires data from a variety of cloud services for analysis. The agent itself is authenticated and authorized to access information, and the secondary data resulting from the analysis is saved and protected by usage policies that provide provenance information pointing to the original data used.

U.S. Operator Information Creation. In this scenario, a remote operator in the field creates some kind of data record. This record can be either an audio, video, or document-centric record. The information is saved with a default policy based on information gathered automatically from the creation location and user authentication information as well as a small amount of information entered by the user.

3 Solution Overview

We will use a simple model to begin development. We have three distinct layers — *application*, *logical*, and *physical* layers. This application layer consists of *data repositories*, *communication networks*, *application servers*, and *clients*. The logical layer contains *images* and *instances* running in *containers*, while the physical layer contains all physical hardware and software required to enable the logical layer.

These can be combined into common *patterns*, including:

- Intra-datacenter
- Inter-datacenter
- Datacenter to cache
- Datacenter to application server
- Datacenter to Client
- Cache to application server
- Cache to client

All these communication patterns have distinct *trust profiles*.

3.1 Major Features

The major system features differentiating this approach from other information sharing approaches is the scale of the system, the system's flexibility, and integrated content usage management.

System Scale. Unlike other information environments like SIPRNet or JWICS, this system will prototype the ability to store information from a single system at a variety of classification and sensitivity levels via integrated encryption. Furthermore, this system will operate as a cloud computing environment with the scalability that implies [1].

System Flexibility. The system will allow policies to be evaluated within a dynamic context. For example, under cases of duress, the system may elect to transmit sensitive information to users that would generally not be allowed access to that information. This information would be shared in such a way that it could be retracted at a later date, and the system would create traceable records outlining which users received the information. In addition to this information management flexibility, the system will also support the kind of operational flexibility expected of cloud systems [1].

Content Usage Management. Nublu will enable management of information content throughout the system and information life-cycle.

---

[1] P. Mell and T. Grance, "Nist sp 800-145: The nist definition of cloud computing," 9 2011.

4 Threat Model

In order to understand the security controls needed for Nublu infrastructure, we first need to understand the threat landscape. Today, the Cloud Security Alliance [2] maintains an up-to-date list of the most active security threats to cloud systems. The most recent version, for 2013, outlines the nine most common security threats that exist today as well as security controls that can help alleviate the risk imposed by those threats [3]. Out threat model is based on this list of current cloud threats.

Figure 1 shows a notional representation of our proposed Nublu system. This shows the primary catagories of services we will provision, as well as supporting services. To begin with, at the bottom of the figure, we have a collection of *Data Repositories*. These repositories can be of a variety of types, ranging from graph databases(like Neo4j [4]) to document databases (like MongoDB [5]) to data structure databases (like Redis [6]) to relational databases. These data repositories exchange information via a *Distribution Network*. This distribution network transfers information at a variety of security and quality-of-service (QoS) levels, based on the content traversing the network. This figure shows *Secure Data Objects* traversing the distribution network over links provisioned at varying security and QoS levels. The individual network links are managed and connected by control nodes, similar to switches or routers, that manage the flow of information and data transmission performance through the distribution network. The system delivers information to *Application Servers* that deliver information to *Clients*. All elements have embedded information usage and distribution management components, and depend on common services to provide and enforce security controls. Specific common services from top to bottom include key management and public key infrastructure (PKI), identity and access control (ICAM), directory, monitoring and management, and messaging. Within this view, the Nublu system is responsible for the technical performance of services within the Repository, Distribution Network, and Application Server layers.

This system will provision infrastructure on demand at various levels of service and security via software defined infrastructure and network management. These levels can then dynamically change based on the environment, increasing performance or security based on external events and risk.

Data Breaches Data breaches are the most common issue facing cloud deployed information today. Misconfigured databases or multi-tenant virtualization platforms can expose sensitive data to theft. Recent research highlights these issues, demonstrating how attackers can exploit side-channel weaknesses to steal sensitive information [7]. Other recent breaches demonstrate how poor governance and data retention practices can lead to the leak of large swaths of sensitive information as well [8]. Data breaches differ from data loss as breaches imply a leakage of data to unauthorized personnel, while data loss implies permanent loss of information. Ergo, breaches impact all levels of concern within the Nublu system, ranging from repositories through the distribution network to application servers.

Data Loss Data loss is tied to the permanent loss of information via deletion, hardware destruction, or other permanent means. This threat applies to individuals storing information in various cloud services as well as organizations and information stored in systems owned and on premises or managed by third parties. In either case, the data loss can be the result of malicious actors or natural events. Whatever the cause organizations must be prepared to reconstitute lost information. In our system, data loss threats primarily

[2] "The cloud security alliance." `https://cloudsecurityalliance.org/`. Accessed: 2013-10-26.

[3] C. C. Alliance, "The notorious nine: Cloud computing top threats in 2013." `https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/`, 2013. Accessed: 2013-10-22.

[4] "Neo4j - the World's Leading Graph Database." `http://www.neo4j.org/`. Accessed: 2013-10-26.

[5] "MongoDB." `http://www.mongodb.org/`. Accessed: 2013-10-26.

[6] "Redis." `http://redis.io/`. Accessed: 2013-10-26.

[7] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-vm side channels and their use to extract private keys," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 305–316, ACM, 2012.

[8] M. DeCarlo, "Td bank misplaced the unencrypted data of 267,000 customers." `http://www.techspot.com/news/50514-td-bank-misplaced-the-unencrypted-data-of-267000-customers.html`, 10 2012. Accessed: 2013-10-26.

impact the data repository layer. Any data stored in any repositories must support efficient, effective, and secure backup to avoid this threat.

Hijacking Service and account hijacking are still relevant threats, and such credentials are, by definition, the primary target of phishing attempts. As such, they need to be actively protected, not shared, and two-factor identification should be utilized whenever possible. Though specific ICAM services are outside the scope of this work, developed system must support interfaces to such systems. Furthermore, PKI and other key management systems must be strongly secured to protect against unauthorized key leakage and associated system damage. Overall, this threat has wide impact on Nublu. It affects each layer, and all system agents. System agents must be authenticated and be authorized to act within the system. Usage management components are extensions of the ICAM system and make decisions regarding data distribution and must also be secured and authenticated. All credentials associated with these components must be protected from exfiltration or unauthorized access, and must be able to be quickly suspended in case of compromise.

Interfaces Interfaces to cloud systems must also be secured. Not only can malicious actors gain access to cloud-stored information and services via service hijacking, they can also compromise these services via exploing insecure programming interfaces (APIs). All major commercial cloud service providers support programmatic access to their platforms [9,10], and Nublu will be no exception from that trend. In fact, the integration of security controls into the cloud framework and extensive use of software defined infrastructure and networks will increase Nublu's susceptibility to this particular threat. This threat impacts all service layers and supporting services, as they are all software systems consuming and providing interfaces for external access.

Denial of Service Denial of service attacks are common and expected within large scale, visible systems. Government and military systems must be designed to handle large scale denial of service attacks as they are guaranteed when engaged with a hostile power in any way. In fact, denial of service attacks are commonplace today and typically used by extra-national political organizations and criminal gangs toward a variety of ends, ranging from extortion to simple bragging rights. Though all components of Nublu are susceptible to Denial of Service attacks, some specific parts of Nublu are more vulnerable than others. Specific common services, for example, like monitoring and management can be exploited to bring the system down. ICAM and PKI systems can be used to bring down the system as well if not appropriately hardened.

Insider Threat Insider threat issues are notoriously difficult for organizations to protect themselves from. Generally, staff vetting and background checks are primary methods through which organizations try to address insider threat, with some success, though there have been well publicized failures over the past few years with this approach. Monitoring and usage data collection, as well as observing the principle of least privilege, are common contributors to lessening the risk of insider threat. Specific insider threat protections are outside of the scope of Nublu, but some of the associated monitoring and management systems can very well be used to contribute to insider threat detection. Supporting robust authentication and authorization capabilities is also paramount.

Service Abuse Cloud systems can be compromised and used toward unauthorized ends. For example, virtual machines (VMs) running within a cloud environment can be used by malicious actors to store malware, stolen digital property, or to attack stolen encrypted information [7]. Nublu is vulnerable to this kind of abuse in all three service layers. Data storage can be abused to save illicit information, just as virtualized

---

[9] "API documentation." `http://docs.rackspace.com/`. Accessed: 2013-10-26.

[10] "AWS SDKs & tools." `http://aws.amazon.com/tools/`. Accessed: 2013-10-26.

[7] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-vm side channels and their use to extract private keys," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 305–316, ACM, 2012.

application servers can be compromised for computational horsepower or as pivot points for distributed denial of service attacks. Likewise, networks can be compromised to transfer stolen digital goods or to hide unauthorized communication.

Due Diligence Due diligence addresses the need for organizations to adopt cloud computing systems with a clear understanding of the implications of this kind of technology. Organizations will frequently migrate operations into cloud environments without organizational expertise in the technology or management issues that will arise, leading to mistakes that could have been avoided. This is primarily a management issue with little impact on Nublu.

Shared Technology Multi-tenant systems introduce new vulnerabilities into distributed computing systems. Whether the vulnerabilities enable tenant-to-tenant attacks or tenant-to-infrastructure attacks, Nublu is very vulnerable to thse kinds of threats. Nublu is heavily virtualized — hosts are virtualized, networks are virtualized, and data repositories are virtualized to maximize flexibility and efficiency.

Impact on Nublu The majority of these threats impact Nublu work and need to be handled by security controls designed into the system rather than controls injected into Nublu as an afterthought. The only control that does not apply to the Nublu system is *Due Diligence*, in the context of the definition supplied by the CSA [3]. We will then categorize other threats by actual risk, as opposed to perceived risk, and then by alleviating security controls, deliberately not addressing threats that have controls that are outside of the scope of Nublu.

This cursory analysis trims the list of critical threats from eight to four. First, both *Data Loss* and *Service Abuse* are rectified via controls that are outside toe scope of Nublu. Potential data loss is alleviated via data retention and risk policies, environment assessments, and equipment location, all of which are tied to specific production environments the analysis of which are outside of the scope of Nublu work. Service abuse controls include legal preparation and acceptable use policies, again areas outside of Nublu scope. Lower priority items, threats with lower actual risk, include *Insider Threat* and *Shared Technology*. These will be lower priority threats for the team to address.

This leaves a group of four priority threats we must address within Nublu, including *Data Breaches*, *Hijacking*, *Interfaces*, and *Denial of Service*. Looking over these threats, we have a list of baseline controls defined by the CSA [11] that apply to Nublu:

- **CCM DG-04:** *Data Governance — Retention Policy*
- **CCM DG-05:** *Data Governance — Secure Disposal*
- **CCM DG-06:** *Data Governance — Non-Production Data*
- **CCM DG-07:** *Data Governance — Information Leakage*
- **CCM DG-08:** *Data Governance — Risk Assessments*
- **CCM IS-04:** *Information Security — Baseline Requirements*
- **CCM IS-07:** *Information Security — User Access Policy*
- **CCM IS-08:** *Information Security — User Access Restriction/Authorization*
- **CCM IS-09:** *Information Security — User Access Revocation*

---

[3] C. C. Alliance, "The notorious nine: Cloud computing top threats in 2013." `https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/`, 2013. Accessed: 2013-10-22.

[11] C. C. Alliance, "Cloud controls matrix v.3." `https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/`, 2013. Accessed: 2013-11-01.

- **CCM IS-10:** *Information Security — User Access Reviews*
- **CCM IS-18:** *Information Security — Encryption*
- **CCM IS-19:** *Information Security — Encryption Key Management*
- **CCM IS-22:** *Information Security — Incident Management*
- **CCM OP-03:** *Operations Management — Capacity/Resource Planning*
- **CCM RS-07:** *Resiliency — Equipment Power Failures*
- **CCM SA-02:** *Security Architecture — User ID Credentials*
- **CCM SA-03:** *Security Architecture — Data Security/Integrity*
- **CCM SA-04:** *Security Architecture — Application Security*
- **CCM SA-06:** *Security Architecture — Production/Non-Production Environments*
- **CCM SA-07:** *Security Architecture — Remote User Multi-Factor Authentication*
- **CCM SA-14:** *Security Architecture — Audit Logging / Intrusion Detection*

Note that this is not a list of all controls and approaches that must be used to provide assured information sharing. Rather, this is a list of controls that must be in place or supported to provide a competent security baseline from which we can begin Nublu development. Note, not all controls in this list are within the scope of Nublu work. While that may be the case, the Nublu system must identify the interfaces and support those external controls require, and implement those interfaces and whatever support is needed to facilitate external control integration. Controls that are within Nublu scope must be implemented at a technology readiness level commensurate with the Nublu project as a whole.