Overlay Networks for Usage Management

by

Christopher C. Lamb

B.S., Mechanical Engineering, New Mexico State University, 1994
M.S., Computer Science, University of New Mexico, 2002

DISSERTATION

Submitted in Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
Computer Engineering

The University of New Mexico

Albuquerque, New Mexico

July, 2012

Dedication

Dedication.

Acknowledgments

I would like to thank my advisor, Professor Gregory Heileman, for his support.

Overlay Networks for Usage Management

by

Christopher C. Lamb

ABSTRACT OF DISSERTATION

Submitted in Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
Computer Engineering

The University of New Mexico

Albuquerque, New Mexico

July, 2012

Overlay Networks for Usage Management

by

Christopher C. Lamb

B.S., Mechanical Engineering, New Mexico State University, 1994
M.S., Computer Science, University of New Mexico, 2002

Ph.D., Computer Engineering, University of New Mexico, 2012

Abstract

Overlay networks have become a widely used technology with examples ranging from consumer focused distribution systems like BitTorrent to commercial content distribution systems like Akamai. These kinds of systems, with the appropriate policy-centric content management components, can address looming problems in information distribution that both companies and federal agencies are beginning to face with respect to sensitive content. This work addresses the current state of the art in these kinds of cross-domain systems, reviewing current example system architectures from the Unified Cross Domain Management Office (UCDMO), a federal organization specifically tasked with addressing these issues. It then covers other related work, introduces a taxonomy of types of policy-centric usage managed overlay network systems and an associated methodology for evaluating the individual taxonomic elements. It then delves into experimental evaluation of the various defined architectural options and finally presents results of comparing experimental evaluation with anticipated results.

Contents

List of Figures

List of Tables

Glossary

RDFa Resource Description Framework – in – attributes

XDM Extensible Metadata Platform

XML eXtensible Markup Language

Chapter 1

Introduction

1.1 Introduction

Current enterprise computing systems are facing a troubling future. As things stand today, they are too expensive, unreliable, and information dissemination procedures are just too slow. Current approaches to partitioning information in cross-domain scenarios are simply unable to migrate to cloud environments. Additionally, the current approach of controlling information by controlling the underlying physical network is too cost ineffective to continue. This leaves large government and commercial organizations concerned with avoiding the exposure of sensitive data in a very uncomfortable position, where they cannot continue doing what they have done, and cannot migrate to what everyone else is doing.

Generally, such systems still do not use current commercial resources as well as they could and use costly data partitioning schemes. Most of these kinds of systems use some combination of systems managed in house by the enterprise itself rather than exploiting lower cost cloud-enabled services. Furthermore, many of these systems have large maintenance loads imposed on them as a result of internal infrastructural requirements like data and database management or systems administration. In many cases networks

containing sensitive data are separated from other internal networks to enhance data security at the expense of productivity, leading to decreased working efficiencies and increased costs.

These kinds of large distributed systems suffer from a lack of stability and reliability as a direct result of their inflated provisioning and support costs. Simply put, the large cost and effort burden of these systems precludes the ability to implement the appropriate redundancy and fault tolerance in any but the absolutely most critical systems. Justifying the costs associated with standard reliability practices like diverse entry or geographically separated hot spares is more and more difficult to do unless forced by draconian legal policy or similarly dire business conditions.

Finally, the length of time between when a sensitive document or other type of data artifact is requested and when it can be delivered to a requester with acceptable need to view that artifact is prohibitively long. These kinds of sensitive artifacts, usually maintained on partitioned networks or systems, require large amounts of review by specially trained reviewers prior to release to data requesters. In cases where acquisition of this data is under hard time constraints like sudden market shifts or other unexpected conditional changes this long review time can result in consequences ranging from financial losses to loss of life.

Federal, military, and healthcare computer systems are prime examples of these kinds of problematic distributed systems, and demonstrate the difficulty inherent in implementing new technical solutions. They, like other similar systems, need to be re-imagined to take advantage of radical market shifts in computational provisioning.

1.2 Motivation

Current policy-centric systems are being forced to move to cloud environments and incorporate much more open systems. Some of these environments will be private or hybrid

cloud systems, where private clouds are infrastructure that is completely run and operated by a single organization for use and provisioning, while hybrid clouds are combinations of private and public cloud systems. Driven by both cost savings and efficiency requirements, this migration will result in a loss of control of computing resources by involved organizations as they attempt to exploit economies of scale and utility computing.

Robust usage management will become an even more important issue in these environments. Federal organizations poised to benefit from this migration include agencies like the National Security Agency (NSA) and the Department of Defense (DoD), both of whom have large installed bases of compartmentalized and classified data. The DoD realizes the scope of this effort, understanding that such technical change must incorporate effectively sharing needed data with other federal agencies, foreign governments, and international organizations [2]. Likewise, the NSA is focused on using cloud-centric systems to facilitate information dissemination and sharing [8].

Cloud systems certainly exhibit economic incentives for use, providing cost savings and flexibility, but they also have distinct disadvantages as well. Specifically, the are not intrinsically as private as some current systems, generally can be less secure than department-level solutions, and have the kinds of trust issues that the best of therapists cannot adequately address [35].

How to address these issues is an open research question. Organizations ranging from cloud service providers to the military are exploring how to engineer solutions to these problems, and to more clearly understand the trade-offs required between selected system architectures [3]. The problems themselves are wide ranging, appearing in a variety of different systems. Military and other government systems are clearly impacted by these kinds of trust and security issues, and they also have clear information sensitivity problems. This, coupled with the fact that these organizations have been dealing with these issues in one form or another for decades make them very well suited for prototypical implementation and study.

Current federal standards in place to deal with these issues in this environment are managed by the Unified Cross Domain Management Office (UCDMO). UCDMO stakeholders range from the DoD to the NSA. The current standard architectural model in place and governed by the UCDMO to deal with this kinds of issues are *guard-centric cross domain architectures*.

1.2.1 Current Solutions

Current and near-future proposed solutions endorsed by the UCDMO include system architectures assembled by the NSA, Raytheon, and Booz | Allen | Hamilton (BAH). The NSA has been active in this area for decades as a logical extension of their role in signals intelligence collection and processing. Raytheon and BAH have been engaged over the past few years to provide an alternative voice and design approach to these kinds of systems, an effort met with limited success.

These cross-domain solutions are intended to enable sensitive information to easily flow both from a higher sensitivity domain to a lower sensitivity domain, and from lower to higher as well. They generally act over both primary data (say, a document) and metadata over that primary data as well. Note that in these system, in most cases, human intervention is still required to adequately review data prior to passing into lower security domains.

NSA, Filtered

The NSA conducted initial work in this area. Their standard-setting efforts culminated in a reasonable conceptual system architecture, using groups of filters dedicated to specific delineated tasks to process sensitive information [31].

In the scenario portrayed in Figure 1.1, *Domain A* could very well be a private cloud managed by the U.S. Air Force, while *Domain B* is a public operational network of some

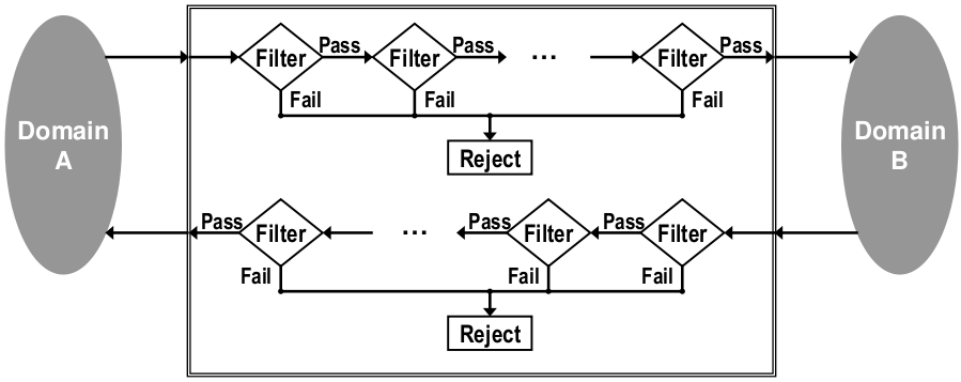

Figure 1.1: NSA Legacy Notional Architecture Model

kind shared by coalition partners in a joint operation.

A system user attempts to send a *data package* consisting of a primary document and associated metadata from *Domain A* to *Domain B*. At some point, that submission reaches a *guard*, which contains at least one *filter chain*. Each filter chain then contains at least one *filter*. Individual filters can execute arbitrary actions over a submitted data package and have access to any number of external resources as required. At any point, a filter can examine the data package and reject it, at which point it will frequently wait for human review. If a filter does not reject a data package, it passes that package onto the next filter or submits it for delivery to Domain B.

NSA, Services

In recent years, the NSA has extended the legacy system architecture for cross-domain information sharing to exploit service-oriented computing styles [31]. Visualized in Figure 1.2, this model incorporates more modern conceptual elements and componentry.

In the view in Figure 1.2, we see on the left the *Global Information Grid*, or *GIG*. On the right, we have the *Distributed Service-oriented Cross Domain Solution*, or *DSCDS*. The GIG is not a truly open system — rather, it is a loosely coupled collection of computational

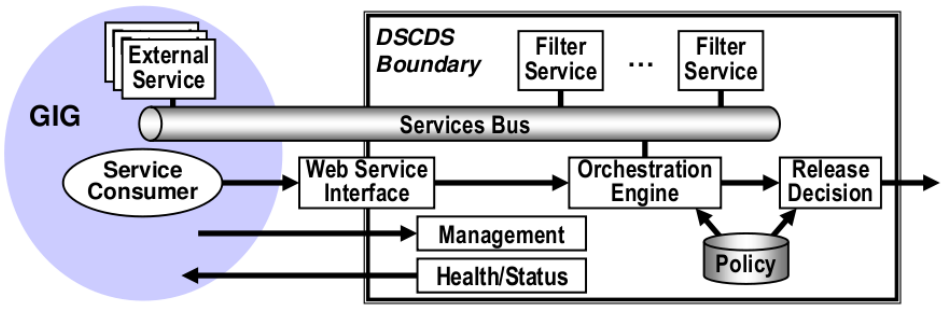

Figure 1.2: NSA Service-Oriented Model

services handing data at a variety of levels of sensitivity, federated to provide stakeholders timely access to relevant information [5]. The DSCDS is essentially the embodiment of the NSA's cross-domain vision applied to service oriented computing. This model fuses various technology choices with previous cross-domain thinking.

Indicative of this more modern system design thinking, we have a variety of services and service consumers attached to a common service bus within the GIG. Within the DSCDS, we have groups of filters implemented as services inspecting transferred data when moved over the bus. Finally, all of this interaction is managed by a management interface and controlled by an orchestration engine accessing a centralized group of policies.

Note that here we have begun to access a common policy repository for various types of security metadata regarding primary data elements.

Raytheon

In the past few years, Raytheon has offered a new model for cross domain use influenced by the NSA service-oriented model [33].

The model in Figure 1.3 is more grounded in the actual technical environment this kind of solution would be embedded within. Here, we have the Non-secure Internet Protocol Router Network (NIPRNet) as one domain, and the Secret Internet Protocol Router Network

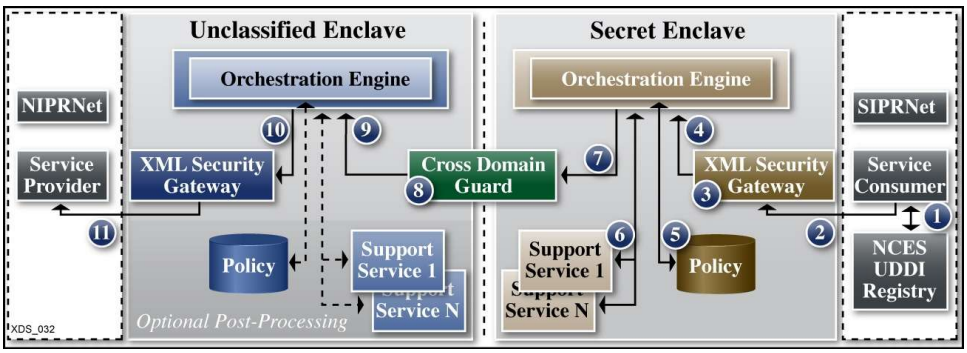

Figure 1.3: Ratheon Model

(SIPRNet) as the other. Here, NIPRNet is the lower security domain (lowside), and SIPRNet the higher security domain (highside). This particular view shows the motion of data from the high side (SIPRNet) to the low side (NIPRNet).

Here, a data request is submitted from SIPRNet first two the *XML Security Gateway* which calls into the *Orchestration Engine* for policy validation. The Orchstration Engine then coordinates calls into a *Policy Repository* as well as to a collection of external *Support Services*. Once rectified against these elements, the request is passed into the *Cross Domain Guard* which routes the request into the *Unclassified Enclave* in NIPRNet. Here, the request is passed directly through the lowside *XML Security Gateway*, without rectification, onto the *Service Provider*. The response from the Service Provider is then passed back to the requester via the inverse path.

This model also begins to use a centralized policy repository, just as the NSA Service Model. It also uses a single cross domain guard to transfer information from both the highside to the lowside, and vice-versa.

Booz | Allen | Hamilton

BAH submitted a competing model, also in 2009 [19]. In fact, both Raytheon and BAH presented their models under competitive contract to the UCDMO at the same conference,

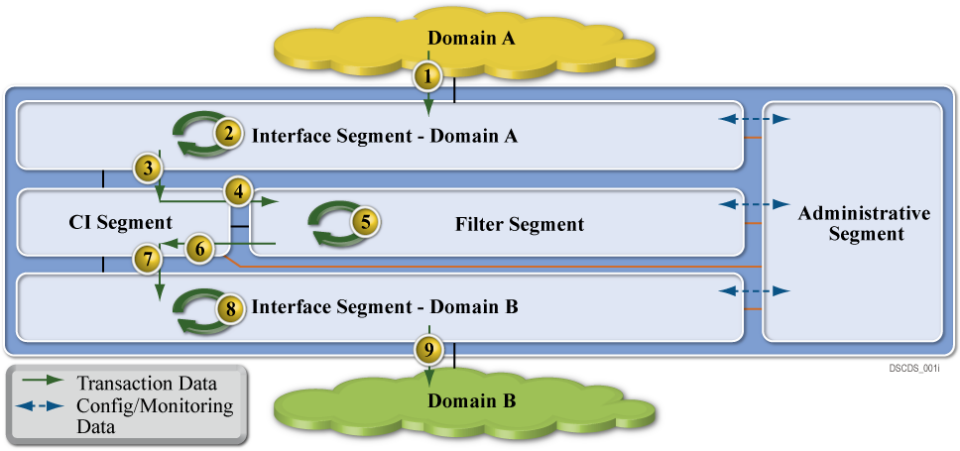

Figure 1.4: Booz | Allen | Hamilton Model

so the domain application is not coincidental.

Figure 1.4 embodies BAH's thinking with respect to cross domain information management. We have a *Domain A* as a high security domain, and *Domain B* as a low security domain. Here, we again have dataflow from the highside to the lowside through the cross domain management system.

While not as detailed as the Raytheon proposal, this does have similar elements. Here, we data first travels from Domain A into the *Interface Segment for Domain A*, similar to the secret enclave used in the Raytheon model. From there, it moves into the *CI Segment*, which in turn submits the transferring data into the *Filter Segment*. From there, the package is moved into the *Interface Segment for Domain B*, and then onto *Domain B*. The *Administrative Segment* provides managment and oversight of the system as a whole.

Note the absence of specific policy-centric elements. This system is reliant on specific policy-agnostic content filters as well.

1.2.2 Cross Domain Solutions

The Unified Cross Domain Management Office (UCDMO) supports efforts to develop other specific solutions that have been presented over the past few years to handle this kind of information management. The National Security Agency set the standard in this area initially. In 2009, at a conference sponsored by the UCDMO, Booz Allen Hamilton (BAH) and Raytheon presented alternative notional architectures contrasting with current NSA-influenced approaches [31, 5, 19, 33].

These kinds of cross-domain solutions still have clear similarities, and in fact have not progressed far beyond the initial notions of how these kinds of systems should work. They still, for example, all use some kind of filter chaining mechanism to evaluate whether a given data item can be moved from a classified to an unclassified network. Both NSA models used filters explicitly, as did the BAH model. They all use a single guard as well, a sole point of security and enforcement, providing perimeter data security, but nothing else. In each of these current system architectures, users are only allowed to exchange one type of information per domain. The physical instantiations of these models are locked by operational policy to a single classification level. Users cannot, for example, have Top Secret material on a network accredited for Secret material. Finally, these models violate end-to-end principles in large service network design, centralizing intelligence rather than pushing that intelligence down to the ends of the system [21].

End-to-end principles are generally considered core to the development of extreme scale, distributed systems. Essentially, one of the key design decisions with respect to the early internet was to move any significant processing to system end nodes, keeping the core of the network fast and simple. Known as the end-to-end principles, this design has served the internet well, allowing it to scale to sizes unconceived when originally built. Current cross domain systems are placed at key routing points between sensitive networks. These locations are core to information transfer between systems and ergo violate the initial

design principles upon which the internet was founded. There does exist some belief that end-to-end principles need to be modified to support future networks, but nevertheless, current cross domain systems still violate the basic ideas behind large, scalable networks [17].

Future systems will generally demonstrate decentralized policy management capabilities, infrastructural reuse, the ability to integrate with cloud systems, and security in depth. Policy management will need to be decentralized and integrated within the fabric of the system. The system is both more secure and resilient as a result, better able to control information and operate under stressful conditions. Multi-tenancy can lower costs and increase reliability and is furthermore a common attribute of cloud systems. An appropriately secured system facilitates integration of computing resources into multi-tenant environments. The ability to handle multi-tenant environments and to reliably secure both data at rest and data in motion leads to computational environments deployable in cloud systems. Finally, systems must operate under *all* conditions, including when they are under attack or compromise [37]. Ergo, they must provide protection to sensitive data in depth.

1.2.3 Other Related Work

This work introduces the notion of usage management embedded in a delivery network itself. It also provides an in-depth analysis of the challenges and principles involved in the design of an open, inter-operable usage management framework that operates over this kind of environment. Besides referencing the material we have covered in depth to portray the current state of the art, the analysis includes application of well-known principles of system design and standards [18, 20, 22], research developments in the areas of usage control [34, 27], policy languages design principles [28], digital rights management (DRM) systems [26], and interoperability [25, 24, 29, 23, 1] towards the development of supporting frameworks.

While a large body of work exists on how overlay networks can use policies for *network* management, very little work has been done on using usage policies for *content* management. The primary contribution in this area focuses on dividing a given system into specific *security domains* which are governed by individual policies [36]. This system fits into our proposed taxonomy as an α-type system as it has domains with single separating guards.

A large body of work currently exists with respect to security in and over overlay networks. These kinds of techniques and this area of study is vital to the production development and delivery of overlay systems, but is outside the scope of this work.

Chapter 2

Proposed Taxonomy

2.1 Taxonomies of Usage Management Overlay

A clear taxonomic organization of potential steps in approaching finer-grained policy based usage management helps in describing the difficulties inherent in developing potential solutions as well as aiding in planning system evolution over time. Here, we have five distinct types of integrated policy-centric usage management systems, as shown in Table 2.1. Of these five, only the first two levels are represented in current system models.

In this taxonomy, it is not required that systems pass through lower levels to reach higher ones. This taxonomy represents a continuum of integration of usage management controls. Systems can very well be designed to fit into higher taxonomic categories without addressing lower categories. That said however, many of the supporting infrastructural services, like identification management or logging and tracing systems, are common between multiple levels.

The taxonomy itself starts with the current state, integrating policy evaluation systems into the network fabric gradually, moving away from filters, then by adding policy evaluation

Name	*Description*
ϕ	The initial level of this taxonomy, ϕ classified systems have a single guard without policy-based control
α	α classified systems have a single guard by have begun to integrate policy-based control
β	Systems that have begun to integrate policy-based control with router elements are in the β category
γ	Systems that have integrated policy-based control with routing and computational elements
δ	Continuous policy-based control with *smart licensed* artifacts

Table 2.1: Proposed Usage Management Taxonomy

into the routing fabric, then the computational nodes, and finally by incorporating evaluation directly into content.

The UCDMO has specific goals, with the ideal end state described as a flat network architecture with usage management injected into the system at the object level. This is exactly the final δ architecture described within this paper [32, 13]. The UCDMO also has specific goals outlined within it's founding charter, including:

- **Optimize Capabilities** — Drive robust and extensible cross domain capabilities to support a secure and integrated information enterprise.
- **Oversee Resources** — Maximize return on cross domain investments, reduce duplication of effort, and increase efficiency of cross domain activities.
- **Mitigate Risk** — Support risk-based decisions by enabling global awareness of cross domain operational connections.
- **Provide Leadership** — Provide leadership across the interagency spectrum to ensure coordinated cross domain governance, oversight and community reciprocity.

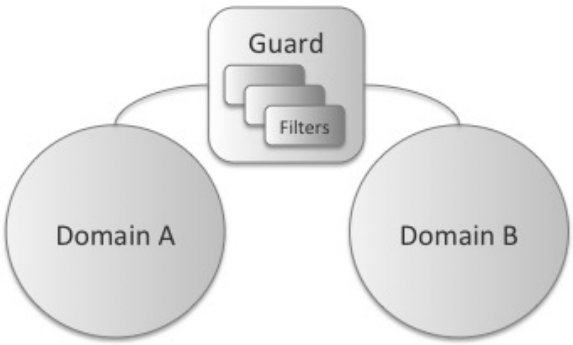

Figure 2.1: Taxonomy (ϕ)

Our work here certainly contributes to these goals, providing robust cross-domain capabilities, helping mitigate risk, and contributing toward advancing the state of the art in this kind of multi-level security environment.

2.1.1 ϕ-level Overlay Systems

The ϕ classification consists of systems like the initial NSA and BAH notional models. These systems consist of two distinct domains, separated by a filter-centric single guard. The initial NSA system model is clearly of this type, separating two domains with a guard using filter chains. The BAH model is also of this type, using a Filter Segment to evaluate data packages transmitted between interface segments attached to specific domains.

Generally one of the domains supports more sensitive information than the other, but that is not always the case. In the models we have examined this has certainly been true, but classified information for example is commonly stored in *compartments* which are separated by clear *need-to-know* policies enforced by access lists and classification guides. These kinds of compartments contain information at similar levels of classification, but contain distinct informational elements that should not be combined.

In these kinds of systems, specific rules regarding information transfer and domain

characterization are tightly bound to individual filter implementations. They are based on *a priori* knowledge of the domains the guard connects, and therefore are tightly coupled those domains. Furthermore, the filter elements are standalone within the system, in this classification, not availing themselves of external resources. Rather, they examining information transiting through the filter based purely on the content of that information.

The set of filters that could be developed and deployed within the guard are unlimited. Developers could easily create a filter that inspects and possibly redacts the sections within the document, rather than passing or not passing the entire document through the guard. Indeed, if we assume even very limited processing capabilities within the guard, that is, turing completeness, then this guard can be made as powerful as any solution we can derive for implementing a cross-domain solution (CDS). Thus the computational power of the guard is not the issue. The real issues are the benefits that can be gained by distributing the capabilities intelligently within the networked environment.

2.1.2 α-level Overlay Systems

The α overlay classification contains systems that have begun to integrate policy-centric usage management. Both policies and contexts are dynamically delivered to the system. The dynamic delivery of context and policies allows these kinds of systems more flexibility with policy evaluation. The α category begins to integrate policy-centric management rather than using strict content filtering.

Here, we again have at least two domains, Domain A and Domain B, though we could potentially have more. ϕ type systems require domain specific information to be tightly coupled to the filter implementations. Separating the permissions, obligations, and other constraints from the filters and incorporating them into a specific separate policy entity frees the guard from this coupling and provides additional flexibility to the system.

The guard can continue to use filters to process data. These filters however are now

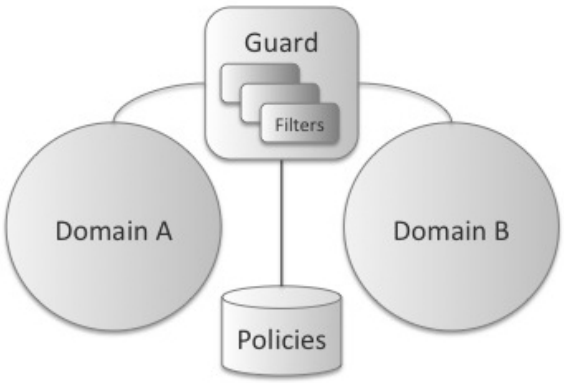

Figure 2.2: Taxonomy (α)

more generic and decoupled from the specific domains the guard manages. The choice of using a specific filtering model rather than some other kind of construct is a design detail level to implementers. That said however, individual filters will be remarkably different and still need to understand the ontologies over which specific licenses are defined rather than specific content semantics.

The policy repository is key to the implementation and differentiation of this taxonomy category. This repository can be implemented as a separate repository keyed into via a data artifact's unique URI, for example. It could also represent a policy sent in tandem with a data artifact in a data package.

The policy repository may be implemented as some kind of external service, and as such, represents the first such external service explicitly used in this taxonomy. Other external services may well exist and be used to adjudicate information transfer decisions as well.

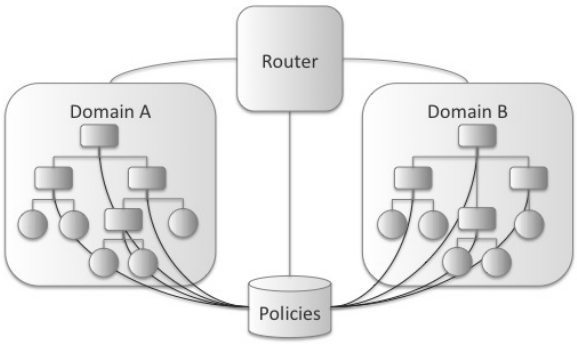

Figure 2.3: Taxonomy (β)

2.1.3 β-level Overlay Systems

The β taxonomic category begins to integrate policy-centric processing with router elements in a given network. While this work is centered on using overlay technology to illustrate and implement these concepts, it is important to note that this kind of distributed policy-centric processing could very well be distributed into the physical routing fabric of a given network as well by extending Software Defined Networking systems like OpenFlow [9].

In this model we can also host multiple domains as a result of flexible policy-based content examination. Each domain hosts a network of some kind, though that hosted network could very well be a degenerate network of a single system. Each network hosted in a domain is hierarchical, with specific computational nodes embodied by workstations, tablet computers or mobile devices, and routing points embodied by routers or switches of some kind.

Policy evaluation in this model has begun to penetrate into the routing elements of the specific domain networks. Here, note that we have started to penetrate into the routing fabric of the network by doing content evaluation at router points. Content-based switching networks have been successful in other domains, and such techniques can be used here to provide policy evaluation capabilities [15].

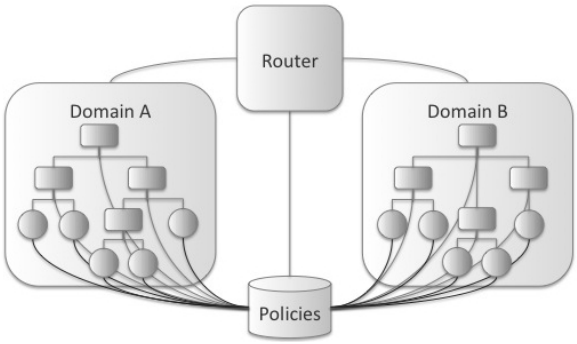

Figure 2.4: Taxonomy (γ)

Certain types of traffic are easier to evaluate than others however. For example, HTTP requests and responses are easier to examine that TCP packets. When examining TCP packets, systems generally require additional context to select an appropriate packet window (e.g. the number of packets cached for examination). HTTP traffic does not usually require this kind of flexibility.

This migration of policy evaluation into the routing fabric provides for enhanced data security and better network management, especially if part of a network is compromised. Now that policy decisions can be made at the router level in a given network, we are starting to have network security in depth rather than simple perimeter protection. This not only provides the ability for additional information protection, but also allows for different compartments holding information at different need-to-know levels to be created ad-hoc under different routing segments. In cases of network compromise, this kind of dynamic policy enforcement can also allow for quick node excision as well.

2.1.4 γ-level Overlay Systems

The γ compartment has integrated policy evaluation with compute and routing nodes. Here, policies can be evaluated against content at all network levels — nodes emitting requests, nodes fielding requests, and all routing elements in between.

We see that the policy repository is supplying services to all computational elements in both domains. This gives us increased granularity with respect to data compartmentalization by integrating information security into each network element. At this point, the network can create compartments of single nodes, while previously in β level systems compartments could only be created under specific routing elements. At this level, we can also provide services revoking data access based on policy evaluation decisions when needed.

Furthermore, individual node exclusion is possible as well. β classified systems could excise network elements under specific routers by dynamic policy application. Now, we can apply the same functionality to individual compute nodes. For example, if a networked device like a smart phone is compromised, that device can be removed from access quickly or used to suoply mis-information.

2.2 Taxonomic Analysis

The various levels of the taxonomy vary primarily with respect to the inclusion of policy-based usage management and overlay structure. ϕ type systems are not structured with overlay use in mind, nor do they use policy-centric management. Conversely, γ type systems are both purely policy oriented and completely overlay structured.

As systems move through the various levels of the taxonomy they gradually move from one side of the spectrum to another. Overlay structures, hierarchical or otherwise, gradually migrate into the network beginning with β systems. Policy orientation is injected into the architectures starting with α systems and moving into the network fabric in parallel with overlay inclusion.

2.2.1 Characteristics of Policy-centricity

In these systems, policy-based management supplies distinct advantages over filter-centric information control. This kind of policy-centric usage management is more content specific than filters, more flexible, and is more expressive than filter-centric systems.

Content Specific

Filters, in filter-based systems, are not coupled to the content passing through the system. Rather, they are usually tied to the characteristics of attached networks. For some filters, that is not problematic. Mal-ware filters, for example, are very general and do not need to have an understanding of filtered content and are not sensitive to that content at all, though they can be very sensitive to specific context. This limitation does however prohibit filters from doing anything content specific. Due to their deployment limitations, in that they are deployed to such a system via a process distinct from processing content, they are unable to use presented content or current dynamic context to influence information processing decisions.

Consider content c impacted by a dynamic context d where d is defined in terms of the content itself, the person or system requesting that content, and the environment in which that request is made. Here, only under certain specific environmental conditions is that requesting agent allowed access to the requested content. Ergo, the decision to pass the content to the requester is based upon characteristics of the content related to dynamic changes within the environment. A filter-centric solution contained within the ϕ level of the taxonomy is unable to change filter rules based on changes like new content or environmental alteration. A policy-based system, on the other hand, is able to express the content specific policy easily for more dynamic evaluation.

For example, if c contains information that can only be accessed for a specific time

period, a static filter simply cannot determine that the information in c is no longer appropriate for dissemination after that time period ends. That kind of evaluation requires meta-data associated with c that specifically describes these time bounds and a dynamic contextual evaluator able to determine when that window of access has closed.

Flexibility

Policy-centric systems are more flexible than filter-based counterparts. In a filter-based solution, the type of content that can be evaluated is tightly coupled to the filters installed. If a given piece of content is new to a given filter-centric solution, that content cannot be appropriately examined and must be submitted for human review. A policy-based system is designed to be more general. Based upon a common ontology [27], the evaluation system can be very general with respect to it's evaluation of a given policy. A general policy engine can handle a great variety of different content as long as the policies associated with that content correspond to known domain ontologies. This generality leads to a greater amount of flexibility with respect to what can be expressed in a specific policy.

A filter is going to have a specific responsibility, like redacting sensitive words from a document, for instance. In order for that filter to redact those sensitive words, it must have access to some kind of list of what those sensitive words are. Remember, ϕ level systems use static filters, so that filter can only be updated when the filter itself is updated. Now a policy-centric system on the other hand can have a policy associating sensitivity with various areas of content in a specific document. In this case, all the system must do is understand the sensitivity described in the policy associated with the content, and can then redact that content if needed. The ontology describing the areas of sensitivity will change more slowly that the possible content itself, leading to a more flexible maintainable system.

This is of course a simple example solvable by creating a dynamic list; the key point of the above example is that the specificity of the filters requires additional complexity in the

filter system itself. The generality of the policy-centric system allows the complexity to be more clearly expressed and contained within the policy file.

Expressiveness

While filters can process content at specific perimeter points, it's lack of reach into a given network fabric limits the power a given filter can actually have over transmitted content. A policy associated with content, when transmitted with content, can reference much more than the semantics of the protected content. That policy can describe specifically, in detail, how that content can be used. Filters simply cannot exercise that level of control.

Assume a distributed system with multiple filter points. In this kind of system, information distribution can be controlled via deployed filters at a relatively fine level of granularity. This kind of distribution control cannot influence the use of protected content however — one that content is distributed, possessors are accorded full access.

Policy-enabled systems are not limited in this way. Policies, when coupled with policy evaluation tools, can exercise control not only over distribution and routing, but also over use of distributed content at endpoints.

These advantages accrue in usage management systems as policy capabilities are propagated through the overlay fabric. Some of these advantages, like expressiveness, appear simply by beginning to use policies instead of filters. The remaining two have more of an impact as additional policy-centric nodes combine to form an overlay system suitable for cloud deployment, increasing their impact as they move from α to δ types of systems.

2.2.2 Overlay Structure

Overlay structure integration exhibits clear advantages over single point perimeter systems as well. Specifically, overlay systems are more partition-able than perimeter solutions,

enable content throttling, provide capabilities for dynamic content control, and allow content to be more traceable.

Characteristics of Partition-ability

Administrators typically deploy filter-based perimeter protection at strategic routing points on secure networks. These kinds of networks are designed with specific regions of enhanced sensitivity separated by cross domain management systems regulating information flows [31, 33, 19]. While sensible from the perspective of each protected region as a secure domain, this design thinking begins to fall apart when exposed to the very real threat of the malicious insider. Boundary-centric information flow control is impossible to realistically achieve when the actual boundaries between malicious actors and system users is constantly in flux. When a malicious actor can be anywhere within a system, boundaries are simply too dynamic to be realistically recognized. In order to surmount this fluid system posture, designers must adopt a security in depth mindset.

Application layer overlay networks enable this kind of defense in depth via the possibility of partitioning. A given overlay system depending on the level of overlay inclusion can partition the user space and by doing so decrease the attack surface available to a malicious insider. ϕ and α level systems based on perimeter filters simply do not present this ability. Systems beginning with β provide the potential to create need-to-know cells of finer granularity up to δ type systems in which cells can be created at the level of specific content. These need-to-know cells serve to help quarantine possible intrusion into the sensitive distribution fabric if that fabric is compromised by helping isolate that system failure within the compromised cell.

For example, assume a hypothetical system with nine nodes connected along a single data plane within a prototypical secure network. With perimeter defenses, if one of those nodes is compromised, a malicious actor can begin to monitor communications traffic

between all network nodes, effectively compromising the entire network. In this same network, if designers partition the system into three overlay cells of three nodes, a similar intrusion in one of those cells will effectively only compromise that cell, leaving the other two cells unaffected. This decrease in possible targets for compromise effectively decreased the network attack surface from any give node by $\frac{2}{3}$, correspondingly increasing the security posture of the system.

Content Throttling

Perimeter located filter systems only have the opportunity to control sensitive traffic at that initial boundary. Information located in repositories behind that boundary is not subject to control if it is retrieved by an agent also ensconced behind that same system boundary. Granted, control can be exerted at the repository level, but in a system with more than one repository, this is of limited impact.

A partitioned cell-oriented system, on the other hand, provides greater opportunity for information monitoring and control. The partitions applied atop the physical infrastructure provides additional potential control points requests must cross in order to access needed information. Furthermore, less random cell design provides the capability to unify repositories, providing tight control of information dissemination.

Our hypothetical nine-node system, for example, provides no control over information dispatched from one of the contained nodes to other contained nodes in its initial design form. There are simply no control points within that nine-node network at which to monitor and control information flow. Partitioning that space into three three-node cells provides at least two potential control points for inter-cell requests at which information flow can be monitored. In cases where a malicious insider is actively collecting and hoarding data for exfiltration, these additional control points give system administrators the ability to automatically throttle the rate at which sensitive material can be accessed by users to

increase the cost of data collection and increase the likelihood of agent discovery.

Dynamic Content Control

Singular perimeter solutions due to their lack of internal control points also forego the ability to provide dynamic content control. Once information has traversed a given perimeter access point, it is no longer under the control of that point and can no longer be retrieved, accessed, monitored, or modified. Overlay solutions with internal control points can provide the ability to continually monitor and control disseminated information.

Within a given overlay system, depending on that system structure, data can be more rigorously controlled. β, γ, and δ systems provide the ability to dynamically change information access via contextual changes at a finer grained level than perimeter solutions can. γ and δ systems can in fact provide the ability to retract information access on a per request basis.

This kind of control is especially useful in situations where external partners may temporarily need access to sensitive information for a specific short period of time, say during some kind of joint exercise or activity. γ and δ systems can provide that access only during the window of operation, and retract that access when that window closes. This kind of use is common in joint military operations with coalition partners, for example.

Traceability

The singular location of perimeter filter solutions also precludes easy information traceability. Data requests within a given network sans internal controls is more difficult to trace than an overlay solution with a partitioned cell structure that is tailored to the specific information requested (say, XML databases or semantic web content). The partitioned overlay requires requests to traverse multiple routing nodes at which request and response

content can be examined and stored for later analysis and visualization. Perimeter solutions without this kind of structure simply cannot monitor flows at this finer-grained level.

The strengths of overlay systems over single perimeter points gradually increase as overlay structures increasingly permeate any given system. Some abilities, like content-centric access repudiation, can only occur with smart licensed artifacts at the δ level. Others, like traceability or throttling, become more effective as a system architecture traverses from lower to higher levels of capability within the proposed taxonomy.

Chapter 3

Metric Selection

3.1 Evaluation Methodology and Model

In order to successfully evaluate the elements of our overlay taxonomy, we must first establish a model against which to measure the presented architectures. The current standard for evaluating software quality is ISO/IEC 25020 and this, along with other related standards from other service delivery organizations has begun to be integrated into both academia and industry as a tractable way to measure system quality [30, 14].

This particular model must address quality attributes specific to the presented architectures rather than the functional domain. The goal of this model is to allow for architectural evaluation of policy evaluating architectures regardless of the specific functional domain. Ergo, injecting a specific functional domain into the evaluation or the evaluating model is unacceptable. Acceptable attributes are those which directly target quality attributes of the architectures in question.

$$E = \{f_e, f_r, f_u, f_p, f_m, f_f, f_s, f_c\} \tag{3.1}$$

$$W = \{w_e, w_r, w_u, w_p, w_m, w_f, w_s, w_c\} \tag{3.2}$$

$$s = \sum_{W,E} w_i f_i \tag{3.3}$$

We are specifically interested in evaluating architectures for policy evaluation functional suitability, reliability, usability, possible performance efficiencies, maintainability, portability, security, and compatibility, specifically neglecting any kind of domain functional suitability. Each area will be associated with an evaluation function. The suitability of a given architectural option will be evaluated by a tuple of these functions, which can then be converted into a weighted sum leading to a single quantitative metric representing suitability under evaluated conditions.

Also important to note, certain attributes may not be able to be evaluated using specific architectural models. For example, conceptual or notional architecture models are intended to convey specific ideas prevalent in a given system architecture rather than ways that architecture will be realized. As such, these kinds of models generally cannot be evaluated for things like portability or performance efficiency, as these qualities usually manifest based on specific standard and technology selections, respectively. In these cases, the evaluation functions representing those attributes will be weighted at zero.

Functional Suitability

Functional suitability in this context is reflects the ability of the system to accurately manage artifacts based on policy and context. As the functional domain is the same for all examined systems, we will neglect this and set $w_e = 0$.

Reliability

Here, we will evaluate reliability via a simple Bayesian Belief Networks and Reliability Theory. The function f_r for a given architecture will be a functional representation of the independent variables required to evaluate the network.

Usability

These are purely notional models, and as a result cannot be evaluated using generally accepted usability metrics like the Systems Usability Scale (SUS) [16]. Ergo, for this analysis we will set the weight $w_u = 0$.

Performance Efficiency

Performance efficiency is generally a characteristic of logical and physical system architectures. Specific logical architectures can certainly decrease the performance of a given system through poor design, insufficient caching, badly considered state management, or inferior scalability. Physical architectures clearly impact performance if processing power, storage, communication bandwidth, or other attributes are insufficient to process apparent loads. We will therefore set $w_p = 0$ in this analysis.

Maintainability

Maintainability can be measured via examination of a given system with an eye toward areas prone to change. Loosely coupled components directly contribute to the ability to change a specific system component. With this in mind, we can measure develop a simple ratio to indicate the maintainability of a given system — the total number of components

with high change impact to the number of components with high change impact that have been decoupled from the system via an interface

$$f_m = c_i / c_\delta \tag{3.4}$$

Portability

One way to evaluate system portability is via standard compliance [30]. Proposed architectures herein will not be evaluated to the level at which proposed standards have an impact. Therefore, in this analysis, $w_f = 0$.

Security

We will evaluate security using Reliability Theory and Bayesian Belief Networks as well. In that network we will evaluate confidentiality, integrity, and availability failure modes. We will define f_s as we did f_r previously.

Compatibility

Compatibility with existing systems requires either accepted system standards or other systems with which to be compatible. In this analysis, we have neither accepted standards or other systems, so we will set $w_c = 0$.

Any weights not explicitly set to zero previously will be set to one, giving us:

$$W = \{0,1,0,0,1,0,1,0\} \tag{3.5}$$

or, in essence:

$$s = f_r + f_m + f_s \tag{3.6}$$

As Pearson and Benameur [35] show, cloud technology is not currently as private as some organizations would like:

- *User Data Control* — In virtually any given Software-as-a-Service (SaaS) scenario, user data controls are sadly lacking. Once data has been committed to a specific provider, that data is completely out of the original data owners control. Furthermore, as we will see below, that data my not even be solely owned by the original owner anymore either.
- *Secondary Use* — Most consumer facing social systems extensively mine user provided data for additional business advantages. This is a common and well known secondary use for supplied data. SaaS providers again have strong incentives to examine user provided information.
- *Offshore Development* — Service users have no real control over who actually develops the systems a given service deploys. Organizations have attempted to contractually limit development and support functions companies pursue to, say, the continental United States but have had very poor results with these kinds of unsupportable arrangements.
- *Data Routing* — Both system providers and system users in fact have little control over routing issues. Prohibiting data routing through sensitive countries is a difficult task for a single organization.
- *Secondary Storage* — Most large-scale systems expect to use Content Delivery Networks (CDNs) to help manage content, and that expectation is heavily reflected

in their physical system architectures. They simply cannot divorce use of CDNs from their systems for a single organization.

- *Bankruptcy and Data Ownership* — Ownership and obligation to maintain expected data arrangements for a given company is not established under bankruptcy [4, 10, 6].

Security issues also emerge from utility computing infrastructures:

- *Data Access* — System users have very little control over who, in the system provider's organization, is able to access their data and systems.

- *Data Deletion* — Most savvy organizations have procedures in place to sanitize old storage elements like disk drives or backup tapes. System users have very little control over if and how this is done when computing services are treated as a utility.

- *Backup Data Storage* — Backup media is very difficult to encrypt, and most system providers still use tape systems as preferred media solutions for backup and storage needs. These tapes, or copies of them, are generally stored offsite to support disaster recovery scenarios. Security of these types of systems has been spotty to date [12, 7, 11].

- *Intercloud Standardization* — Cloud computing systems do not have any standardized way to transfer computational units or data between systems. Any protocols used for this kind of thing must be developed by customers themselves. Due to the desire of providers to lock-in customers, this will likely not change as any standard development is strongly counter-incentiveized.

- *Multi-tenancy and Side-Channels* — Multi-tenant architectures in which multiple customers simultaneously use the same systems open those customers to covert side-channel attacks.

- *Logging and Auditing* — Logging and auditing structures, especially for inter-cloud systems, are non-existent.

Finally, such systems suffer from internal and external trust issues:

- *Trust Relationships* — Trust is difficult to establish between individual cloud providers long-term.
- *Consumer Trust* — Service users are still not entirely trusting of cloud system providers.

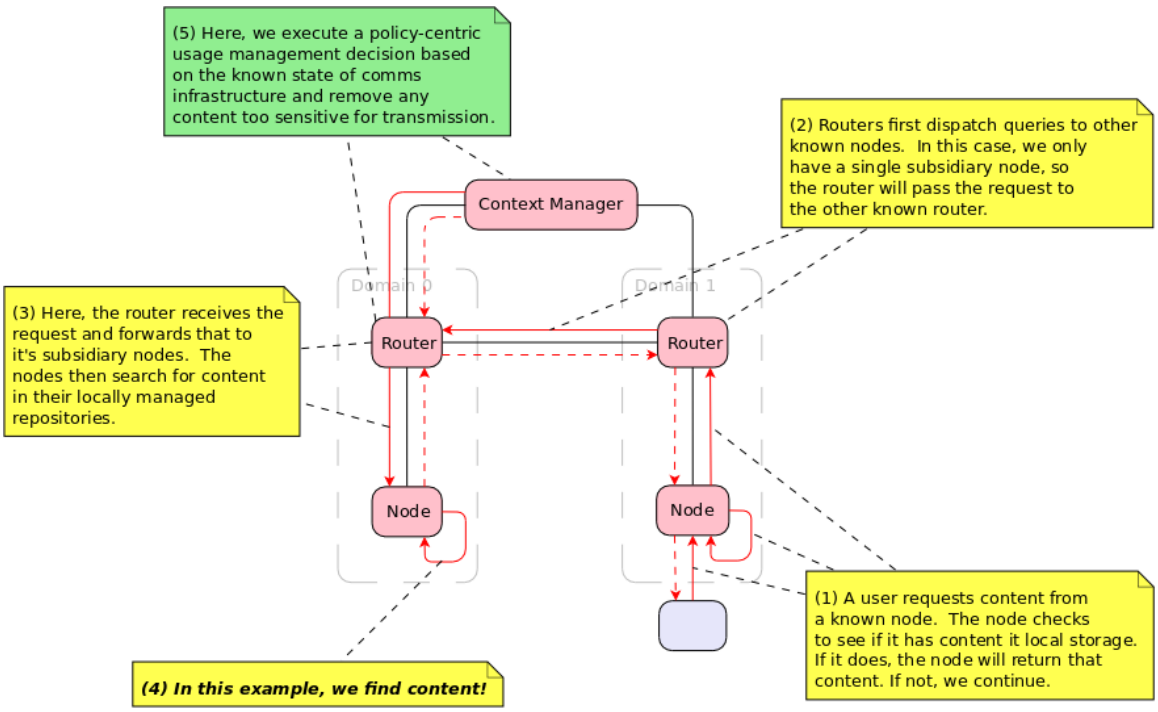

Figure 4.1: Simulation Logical Configuration

Chapter 4

Experimental Configuration

4.1 Overlay Implementation Concerns

A key concept in our current work is the separation of content management from physical communication networks. In the past, content was controlled via partitioning and physical network access management. Physical networks were tightly controlled as a way to manage access to sensitive content. Classified networks in common use today are canonical examples of this kind of approach to content management. Access to these networks is tightly controlled by classification authorities and the ability to transfer content from these networks to more open systems is rigorously managed. Corporate systems have also commonly used this kind of approach, though not usually with so much regulation or rigor.

This kind of approach is not scalable however. It imposes huge costs and infrastructural requirements that are becoming too large to effectively manage. Furthermore, future systems containing sensitive information require similar security features, and simply cannot be developed without custom controlled infrastructure. Health care systems, for example, have huge security needs and a more finely grained level of application than even deployed government systems. These systems will contain exabytes of data, all of which

needs to be explicitly controlled, managed, and reviewed by those associated with specific managed records.

Separating content networks from physical networks enables network infrastructure virtualization and multi-tenancy. Use the popular file-sharing system BitTorrent as an example. BitTorrent is a content network optimized for download efficiency. It run over traditional TCP/IP networks, but manages traffic according to specialized algorithms unique to BitTorrent. These algorithms take advantage of the asymmetry between upload and download speeds of typical home-use Internet systems in which upload speeds are regularly an order of magnitude slower than download speeds. By partitioning content into distinct sections and downloading them from multiple clients, a downloading node can effectively use all available download bandwidth and is no longer necessarily constrained by the upload bandwidth of a serving peer system. We use a similar approach, in that our hypothesized systems also overlay TCP/IP traffic, but rather than optimizing download speeds we focus on content usage management.

Just as systems like BitTorrent runs over current established protocols, usage management overlay systems could as well. They support multi-tenant cloud computing systems by providing secure compartmentalized access to managed information. They also support the ability to create and use integrated overlay systems between multiple cloud providers, supporting running of overlay components in systems hosted at Amazon while accessing nodes executing on Rackspace infrastructure.

Content networks must deal with situations analogous to those encountered in previous physical systems. Specific examples include cross-domain monitoring and content mashing. Both problems are currently areas of active research within physical networks and need extensive examination in overlay systems as well.

To begin with, in content-specific overlay networks, cross-domain routing can become an even more pervasive issue. Currently, cross-domain data processing guards are installed

on the perimeter of sensitive networks where they can monitor and manage outgoing and incoming traffic. In content networks, these kinds of systems can begin to multiply within the information transmission fabric. In physical networks, the network topology is fixed and is established when the network is installed. After installation, changes in the essential network topology are cost-prohibitive and correspondingly rare. Overlay systems do not suffer from this high cost of change, and can easily morph from one topology to another. As additional content enclaves appear within a given overlay topology, the need for content usage management between those enclaves increases.

Mashup scenarios become similarly common. As additional sources of accessible data appear, opportunities for inappropriate data combinations increase at best geometrically. Data combinations need to be likewise managed to prevent inappropriate data combinations.

4.2 Initial Prototype Implementation

Our first completed prototype shows that overlay routers can in fact use licenses bundled alongside content to modify transmitted content based on dynamic network conditions. Running on a single host over HTTP, it simulates two content domains and communication between them. The communication link has uncertain security state and changes over time. Note that this prototype currently runs on a single host with varying ports, but it could easily run on multiple hosts as well. The current single host configuration is simply to simplify system startup and shutdown.

License bundles are hosted on the filesystem, though they could be hosted in any other data store. These artifacts are currently XML. They are stored in a directory, and the license file has a LIC extention while the content file has an XML extension. Both the content and the license files have the name of the directory in which they reside (for example, if the directory is named test, the license file is named test.lic and the content file test.xml). In

this context, the directory is the content bundle. The license and content files are simply documents and port to document-centric storage systems like MongoDB easily. They can certainly be stored in traditional relational databases as well.

The system itself has two domains, Domain 0 and Domain 1. Each domain consists of a client node and a content router node. Requests are initially served to client nodes. If client nodes do not contain the requested content, they the forward that request to their affiliated content router. The content router will send that request to all the content routers of which it is aware. Those other routers will then query associated client nodes for content. If the requested content is in fact found, it will be returned to the original requesting router and then to the requesting node. If the content is not found, HTTP status 404 codes are returned to requesting routers and nodes.

All router-to-router content traffic is modified based on security conditions. A Context Manager maintains metadata regarding network paths. If a given network path is only cleared for data of a certain sensitivity level, a transmitting router will remove all license information and content that is associated with higher sensitivities, and then transmit only information at an appropriate sensitivity level over the link.

Figure 4.1 shows the prototypical workflow through the system across the domains, and Figure 4.2 shows the current system configuration of the simulation, with the cross-domain link highlighted in red. The system is current configured to use ports 4567 through 4571.

All content requests are via HTTP GET. Link status can be changed via HTTP POST and we use the CURL command to exercise the network.

This proof-of-concept does implement a simple overlay network for usage managed content over HTTP, easily extensible to HTTPS. Changes in the context of the network dynamically change the format of transmitted content. All source code for this simulation is publically available on GitHub, at https://github.com/cclamb/overlay-network, with documentation on how to run the simulation.

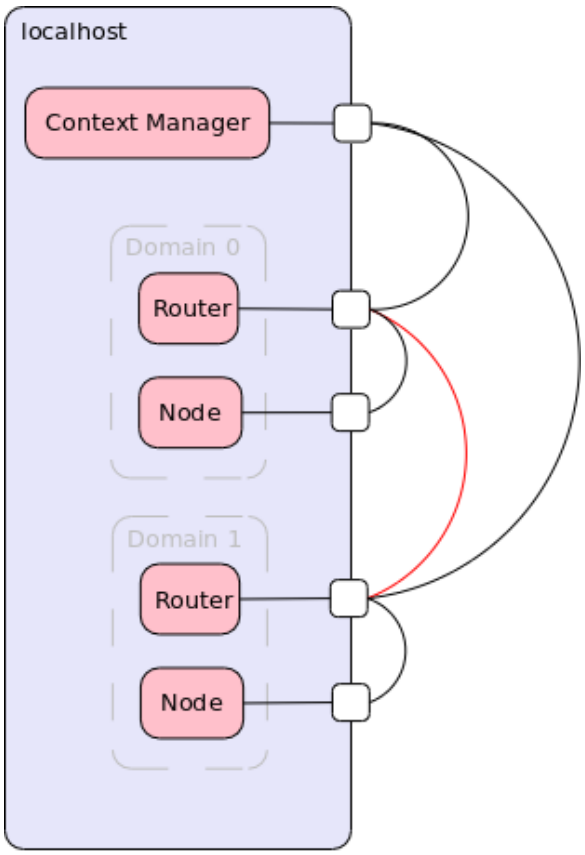

Figure 4.2: Physical Simulation Configuration

4.3 Initial Prototype Results

Policy and content delivery over HTTP possible

Ruby/Sinatra will support HTTP overlay development, CURL for usage

Information Filtering Expectations

Extension into larger distributed system feasible

4.4 Inter-Provider Cloud Configuration

At this point, I have created and deployed baseline system images in both Amazon's Elastic Compute Cloud (EC2) and Rackspace Servers infrastructures. I have also created and exercised our deployment, configuration, and logging systems to enable distributed monitoring and centralized reporting. Overall, we currently have 20 nodes running with two distinct providers geographically dispersed across the continental United States. This leads to a distinct requirement for a centralized system with distributed access for both initial configuration information as well as logging and auditing. We have implemented this required infrastructure using Amazon's Simple Storage Service (S3), accessible from both Rackspace and Amazon hosted virtual machines.

The specific technical components are Amazon EC2, Amazon S2, Rackspace Servers, and GitHub. Both EC2 and Rackspace nodes are Ubuntu virtual machines, albeit at different versions, as we run Ubuntu version 11.04 in Rackspace and Ubuntu Version 12.04 in Amazon's infrastructures. These systems are provisioned with Git, Ruby, the Ruby Version Manager (RVM), and supporting libraries. They all run as micro-intances or equivalent, and are bootstrapped with the appopriate project information to begin to participate as an overlay network node. While EC2 and Rackspace Server infrastructures are infrastructure-as-a-cloud (IaaS) offerings supporting virtual machine instances of various types, Amazon S3 is a simple key-value store. Running with REST sematics over HTTP, S3 stores arbitrary documents associated with specific keys in buckets. These documents can be downloaded by any authorized participant, where authoriztion state is proven by possention of a secret key. In this way, we can store the global configuration of a specific overlay network in a single location from which every node can access informationm with respect to their pending role and needed configuraiton information. Likewise, all overlay network state can also be saved to centralized buckets for later analysis. Finally, Github is a centralized source code repository used to share code between all participating nodes. Prior to each content network instantiation, each node checks the repository for updates,

Category	*Components*
Infrastructure	Amazon S3, Amazon EC2, Rackspace Servers
OperatingSystems	Ubuntu 11.04, Ubuntu 12.04
Technologies	Ruby (Sinatra, Capistrano, YAML)
SupportingSystems	Git, Github

Table 4.1: Supporting Components

and downloads them if they exist.

All data saved within S3 is serialized in a text-based data serialization language known as YAML. YAML is a widely supported hierarchical data representation language with support within the Ruby core platform. This enables us easily serialize Ruby-native data structures to text-based representations for storage within S3. More importantly, it simplifies post-experimental data analysis as any information logged to the centralized logging system during a given experimental run can be easily read and analyzed after the fact.

In order to manage and initialize all overlay nodes, we use Capistrano. Capistrano is a distributed deployment system initially used to manage large clusters of Ruby-on-Rails systems. It has since expanded into a general-purpose distributed deployment toolchain, tightly integratd with Git. This allows us to bootstrap different configurations of networks from a single command-and-control node simply and efficiently.

All these infrastructural elements, protocols, and technology components have been successfully tested, allowing for unified control and configuration of large, distributed overlay systems. We have successfully tested our logging systems, and integrated them with the Ruby runtime for ease of access. We have also passed configuration information to both Rackspace and Amazon EC2 systems and verified access from all participating nodes. Finally, we have successfully exercised the ability to dynamically update all participating nodes from Github as well as the capability to manage the system via Capistrano.

4.5 Inter-Cloud Architecture

At this point the system is a distributed content network distributed across multiple nodes and domains providing cross-domain managed data access. This network consists of clients accessing information through a user interface subsystem that accesses data from external sources and a distributed cross-domain information network. Queries are submitted through a client, to an application server, then to external services and information nodes.

The unique strength of this system is enabling dynamic distributed content control. This includes information retraction, redaction, protection, and secure routing. Information retraction involves quickly removing a user's access to sensitive data. Redaction addresses simple data removal, while protection would operationally involve applying encryption layers of increasing strength based on operational demands. Finally, secure routing would provide the ability to send data over a more secure link if such a link is available and required.

In this system information retraction involves changing the execution context such that access for a given user, perhaps even on a specific device, is removed. This context then propagates through the information network and attached clients. This is useful when a given user, say a coalition partner, is suddenly considered compromised and can no longer be allowed access to sensitive information. Likewise, a specific user's system may likewise be compromised and be forbidden access to specific information.

Information redaction is generally used when a user simply does not have authorization for a specific section of content, generally within a larger document. In these cases, that information and related policy metadata are simply removed from any query responses. Likewise, information protection also addresses specific subsections of information in a larger document, but unlike redaction, a user is in these cases authorized to access information, but one of the links over which the information must travel is not authorized to transmit specific sensitive information. In these cases that information can be encrypted

with appropriately strong encryption to allow for more secure information transmission.

Finally, secure routing use directly addresses the ability to select communication links based on information content. In these situations, a network has more than one path over which to return content. Furthermore, these multiple paths have different characteristics providing different levels of service. The system, based on rules contained in a policy and the current context can then select communication links of different security levels when returning content.Likewise, the content network must:

- Support and distribute queries for available content based on submitted constraints including artifact key and hop count.
- Support and distribute queries for specific content based on key.
- Evaluate returned content for suitability for transmission to a requesting node at each transmission step.
- Support partitioning into multiple domains.
- Allow for dynamic information distribution at network start.
- Collect experimental metrics for evaluation.
- Be distributed across multiple nodes.

Overall, the system consists of an HTML 5 based user interface subsystem, external data sources, and a content network, as shown in Figure 1. The user interface layer displays maps and associated metadata to users based on submitted geolocation information and supports two different mobile profiles (tablet and telephone) and a single workstation profile. We use HTML 5 media queries for end device detection, allowing us to format information differently for our three profiles facilitating usability. External data sources could be any data programming interface offered by a third party over which we have no

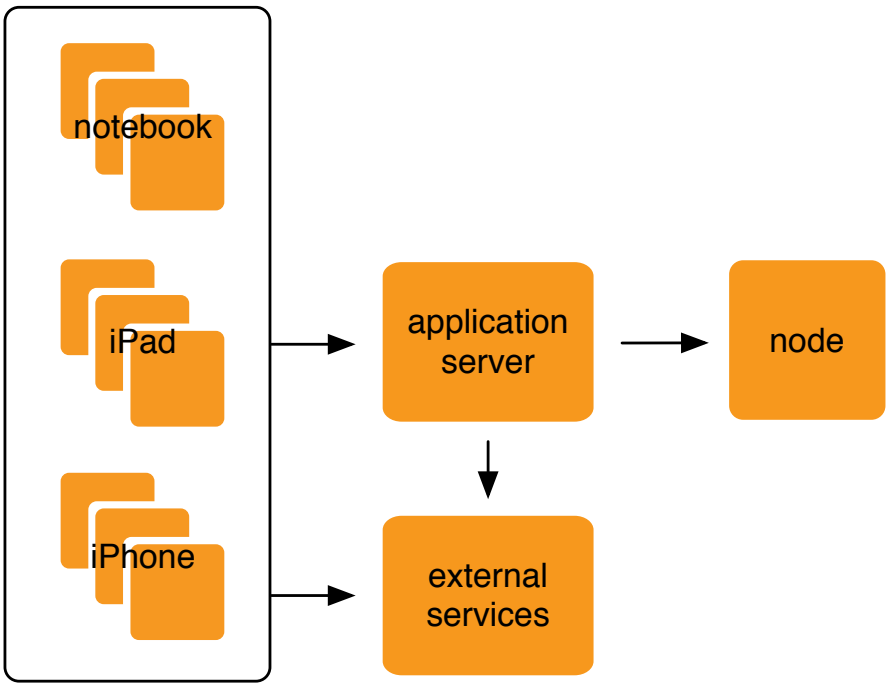

Figure 4.3: Overall System Architecture

direct control. In this system, we use Google Maps to define, download, display, and format maps. Finally, we have a content network configurable either as a hierarchical network or a non-hierarchical network containing geo-tagged information at various sensitivity levels. This content network can be configured arbitrarily, enabling us to create a virtually unlimited number of different information domains.

In this work, the client systems layer will be replaced with a command-line interface and external services will not be accessed, but a typical deployment operationally would have these elements.

The user interface subsystem processes requests and returns information from both Google Maps and the content network based on those requests. Technically, it is based on the latest version of Ruby on Rails (RoR) using standard RoR configuration conventions

running on top of Ruby 1.9.*. We use Rake for deployment, and Gem for component installation. We use Bundler to maintain consistent application dependency state and RVM to manage Ruby virtual machine versions. HTML 5 interface elements are defined using SASS and HAML.

Operationally, typical system use involves query submission, usage management rectification, and result display. We have two distinct types of queries - an initial query for a map of a specific location, generally triggered by entering some kind of geolocation parameters (though potentially using device-generated location information, allowing automatic map alignment with a user's current location) and a query for specific sensitive information. Initial queries have two distinct subqueries, one of map information directed at the Google Maps API, and another of the content network to see what data is available. All content is usage managed to ensure that mashed information is consistent from a data sensitivity perspective prior to display to the user. Currently, no information is cached within the interface subsystem.

The content network can be configured to run as an HTTP overlay system using HTTP routers and nodes or in a peer-to-peer configuration. In either case, queries can be submitted to the network from any one of the constituent nodes - note that routers do not store data; rather, they focus soley on routing queries through a hierarchical network. After initial submission, queries propagate throughout the network based on user-submitted search parameters. The content network physically runs on nodes provisioned from Rackspace Cloud and Amazon Elastic Compute Cloud (EC2). It is built using Sinatra for HTTP processing and uses Capistrano for distributed system deployment and control. We store distributed data in Amazon Simple Storage Service (S3) buckets. We use RVM, Gem, and Bundler in this system as we do with the user interface subsystem.

In both configurations, the common functional flow is built around responding to content queries with information of appropriate sensitivity for a given query context, as shown in Figures 4.4 and 4.5. In general, systems are designed with a layered perspective, with an

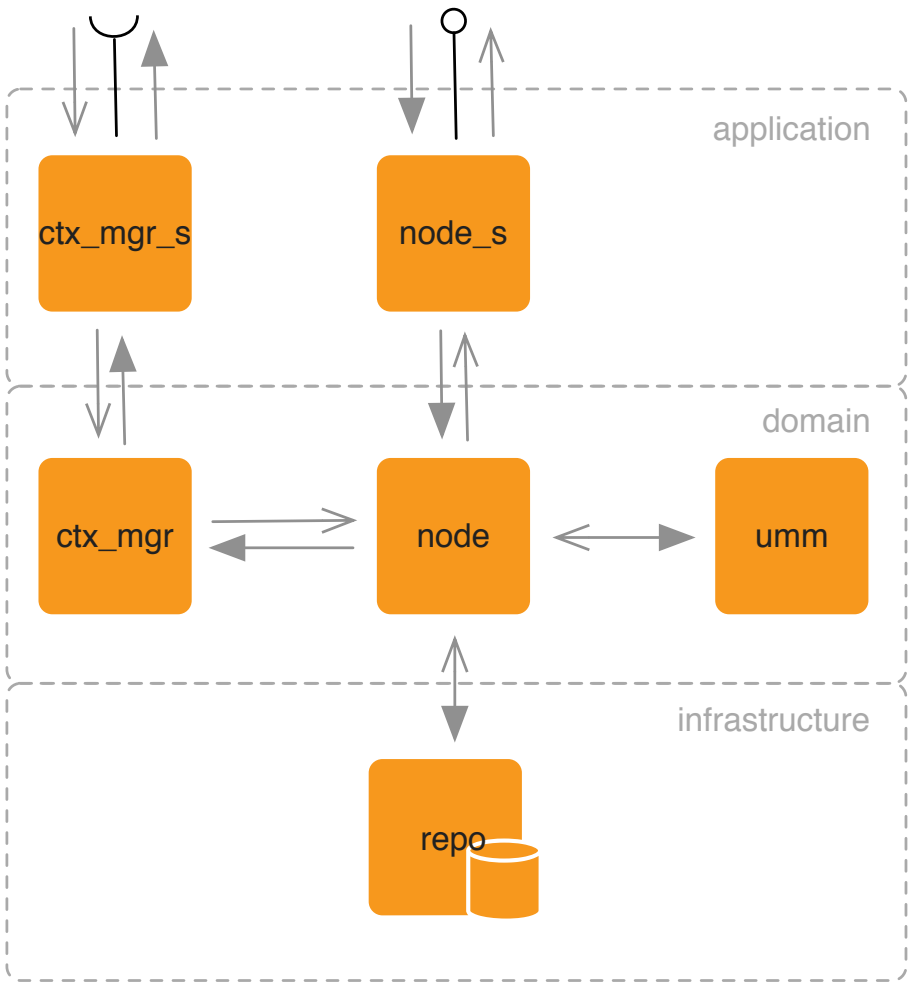

Figure 4.4: Node Architecture

application layer fielding initial requests, a protocol-agnostic domain layer that manages query responses, and an infrastructure layer that contains specific required libraries and other technical artifacts. In these systems, the application layer handles HTTP protocol issues, translating requests from the lingua franca of HTTP into the domain language reflected in the domain layer. The infrastructure layer consists of various data management technologies called upon by the domain layer when needed.

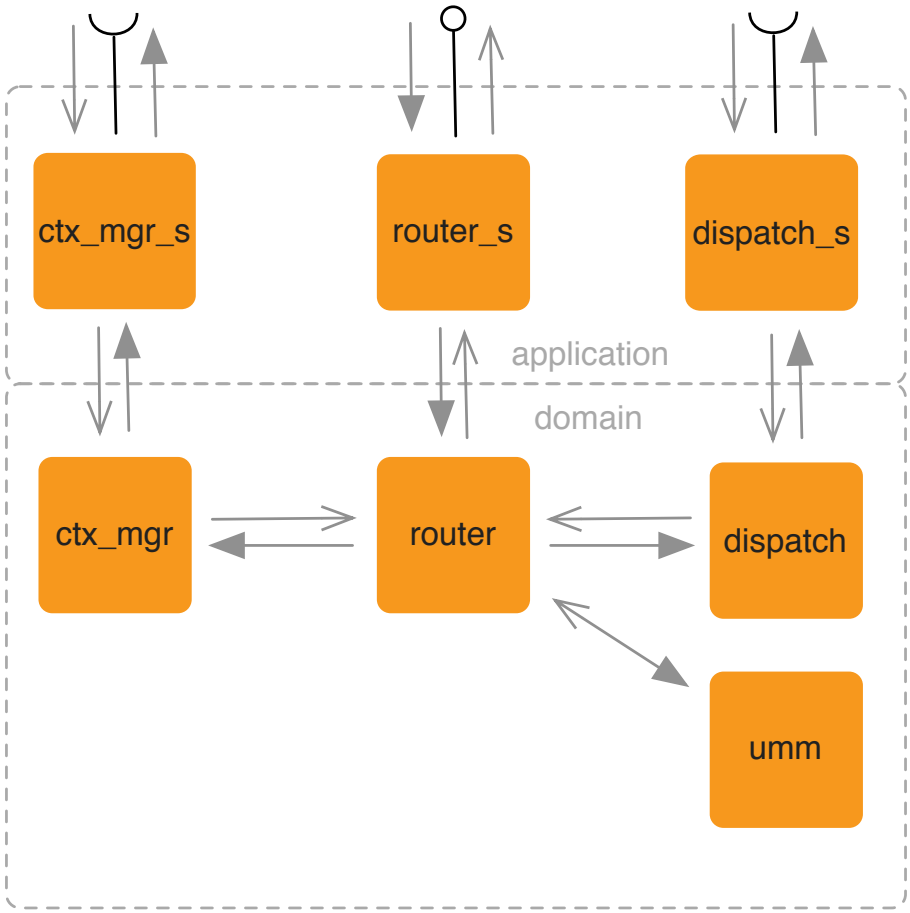

Figure 4.5: Router Architecture

Figures 4.4 and 4.5 highlights communication ordering within components in a hierarchical content network and also shows the functional components within the system. From a communication perspective, requests come in through the application layer and are then handed off for processing to the domain layer. The domain layer retrieves the current context and is responsible for query dispatch (in the case of a router) or data reponses (in the case of a node) that are managed according to the current environmental context.

The primary components in the router and node systems' application layer are small adapters intended to translate between HTTP protocols and domain components. They are:

- **Context Manager Client Service (ctx_mgr_s)** — This is an adapter between the domain context manager and the external context service.
- **Node Service (node_s)** — The node service provides a RESTful interface to external clients. All content requests are initially sent to a known node service. This is essentially the external interface to a given content network. A content network generally contains many distinct nodes as well.
- **Router Service (router_s)** — The router service is essentially a customized HTTP router that dispatches content requests and responses through a hierarchical content network in accordance with established policies and the current environmental context.
- **Dispatch Service (dispatch_s)** — This service dispatches information requests to known nodes based on known policies and context.

The domain layer components include:

- **Context Manager (ctx_mgr)** — The context manager client service calls into the context manager service to retrieve the most current contextual information with respect to the content network, attached clients, users, and devices.
- **Node (node)** — The node component contains all logic needed to process and respond to information requests. Nodes manage requests, responses, context evaluation, and usage management mechanism application.
- **Usage Management Mechanism (umm)** — The usage management mechanism will apply rules grouped into policies against a known context to determine the acceptability of an intended action. It will indicate whether or not that action can proceed. It can also make changes to a proposed action so that the alternative action can be executed.

- **Router (router)** — Router domain components manage the distribution of information requests and responses, applying managing information dispersal throughout a content network in accordance with context and policy.
- **Dispatcher (dispatch)** — Dispatchers send requests to known routers or nodes in the larger context network.

Finally, the sole infrastructure component:

- **Information and Policy Repository (repo)** — Unique to nodes, information and policy repositories contain specific network content, organized by key, and associated policies.

We use the same components to assemble non-hierarchical networks, in which nodes have both content and policy storage as well as request response and dispatching responsibilities. Also note that context management and usage management components are shared between all types of content networks as well as all types of component systems within those networks. Non-hierarchical nodes and hierarchical routers and nodes all need these kinds of services.

4.6 Primary Interfaces and Mappings

Each of the defined components have an associated interface defined over domain datatypes. These interfaces are implemented using Representational State Transfer (REST) semantics over Hypertext Transfer Protocol (HTTP), and the datatypes are represented in Extensible Markup Language (XML).

Listing 4.1: Key Artifact Dataypes

```
1 typedef Policy string;
```

```
2 typedef Artifact string;
3
4 struct ArtifactDescriptor {
5   Policy policy;
6   Artifact artifact;
7 };
8
9 typedef sequence<ArtifactDescriptor> ArtifactDescriptorList;
```

As shown in Listing **??**, we deal primarily with two key datatypes, *Artifacts* and *Policies*. For the purpose of networked data transfer, both of these datatypes are formatted strings of XML data. An *ArtifactDescriptor* combines an Artifact with its associated policy. An *ArtifactDescriptorList* is an unlimited sequence of ArtifactDescriptors.

Listing 4.2: Key Status Dataypes

```
1 enum Status { unsecured, confidential, secret, topSecret };
2
3 struct Status {
4   string edgeName;
5   Status status;
6 };
7
8 typedef sequence<Status> StatusList;
9
10 struct Context {
11   date date;
12   StatusList networkStatus;
13 };
```

Network status information is contained in *Status* elements and grouped into a *Context* structure, as shown in Listing 4.2. A *StatusList* is essentially a dictionary of network connection statuses organized by edgename, where an edge is named by concatinating the edge nodes in any order. These nodenames are concatenated and separated by a pipe symbol, so that the edge between *NodeA* and *NodeB* is named *NodeA*|*NodeB* or *NodeB*|*NodeA*. This makes searching less efficient in exchange for easier and more terse data exchange.

Listing 4.3: Key Error Dataypes

```
1 exception NetworkError {
2   string code;
3 };
```

Finally, shown in Listing 4.3, the *NetworkError* exception is represented by standard HTTP error codes and responses operationally, and is used extensively throughout system interface operations.

The node interface described in Listing 4.4. The Node interface is mapped to a REST style request over HTTP where the argument ordering is preserved when building the URL for accessing artifact content. For example, when accessing a specific artifact, the artifact operation called with a username of 'truchas', on an iphone, for artfact X1234 would map to the URL http://host/artifact/truchas/iphone/X1234. Likewise, a similar operation call on the artifacts operation would use the URL http://host/artifacts/truchas/iphone.

Listing 4.4: The Node Interface

```
1 interface Node {
2   ArtifactDescriptor artifact(in string uname, in string device, in string id) raises
        (NetworkError);
3   ArtifactDescriptorList artifacts(in string uname, in string device) raises (
        NetworkError);
4 };
```

This type of calling convention is used throught the system. The specific ordering of the URL elements stems from corresponding artifact set relationships. Specifically, the set of all artifacts a user has access to is the same as or larger than the set of all artifacts that a user on a specific device can access and the same size or smaller that the set of all available artifacts.

Listing 4.5: The Context Manager Interface

```
1 interface ContextManager {
```

```
2   Context context() raises (NetworkError);
3 }
```

The *ContextManager* interface defined in Listing 4.5 describes how the nework context monitor exposes network state information to requestors. Note, in this case, the defined interface maps to the URL http://host/context.

References

[1] Marlin architecture overview. Technical report, 2006. http://www.marlin-community.com.

[2] DoD Information Sharing Strategy. http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf, May 2007.

[3] Assured Information Sharing in Clouds. http://www.zyn.com/sbir/sbres/sttr/dod/af/af11-bt30.htm, August 2011.

[4] Barnes and Noble pays for Borders customer data, sparking ethics debate. http://www.infusioncrm.com/barnes-and-noble-pays-for-borders-customer-data-sparking-ethics-debate, October 2011.

[5] Department of Defense Global Information Grid Architectural Vision. http://cio-nii.defense.gov/docs/GIGArchVision.pdf, 2011.

[6] Important Information Regarding the Right of Borders Customers to Opt Out of Transfer of Personal Information to Barnes and Noble. http://www.ftc.gov/opa/2011/10/bordersbarnes.shtm, October 2011.

[7] Military Health Plan Data Breach Threatens 4.9 Million. http://www.informationweek.com/news/healthcare/security-privacy/231700161, October 2011.

[8] NSA Pursues Intelligence-Sharing Architecture. http://www.informationweek.com/news/government/cloud-saas/229401646, April 2011.

[9] Openflow - Enabling Innovation in Your Network. http://www.openflow.org, November 2011.

[10] Privacy Alert: Barnes and Noble buys Borders customer list. http://www.broadbandexpert.com/blog/privacy/privacy-alert-barnes-and-noble-buys-borders-customer-list/, October 2011.

[11] TRICARE discloses SAIC breach: backup tapes held data on 4.9 million. http://www.phiprivacy.net/?p=7854, October 2011.

[12] TRICARE discloses SAIC breach: stolen backup tapes held data on 4.9 million (updated). http://www.databreaches.net/?p=20816, October 2011.

[13] About the UCDMO. http://www.ucdmo.gov/about.html, January 2012.

[14] ISO/IEC 25020:2007. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnum January 2012.

[15] JBoss ESB. http://www.jboss.org/jbossesb, January 2012.

[16] Measuring Usability with the System Usability Scale (SUS). http://www.measuringusability.com/sus.php, January 2012.

[17] Marjory S. Blumenthal and David D. Clark. Rethinking the design of the internet: the end-to-end arguments vs. the brave new world. *ACM Trans. Internet Technol.*, 1:70–109, August 2001.

[18] Marjory S. Blumenthal and David D. Clark. Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world. *ACM Transactions on Internet Technology*, 1(1):70–109, Aug. 2001.

[19] Booz, Allen, and Hamilton. Distributed service oriented architecture (soa) compatible cross domain service (dscds). Presented at the Unified Cross Domain Management Office Conference, 2009.

[20] David D. Clark. The design philosophy of the DARPA internet protocols. In *ACM SIGCOMM*, pages 106–114, Stanford, CA, Aug. 1988.

[21] David D. Clark. The design philosophy of the darpa internet protocols. *SIGCOMM Comput. Commun. Rev.*, 25:102–111, January 1995.

[22] David D. Clark, John Wroclawski, Karen R. Sollins, and Robert Braden. Tussle in cyberspace: Defining tomorrow's internet. In *SIGCOMM*, pages 347–356, Pittsburg, Pennsylvania, USA, Aug. 2002.

[23] Coral consortium whitepaper. Technical report, Feb. 2006. `www.coral-interop.org/main/news/Coral.whitepaper.pdf`.

[24] Gregory L. Heileman and Pramod A. Jamkhedkar. DRM interoperability analysis from the perspective of a layered framework. In *Proceedings of the Fifth ACM Workshop on Digital Rights Management*, pages 17–26, Alexandria, VA, Nov. 2005.

[25] Pramod A. Jamkhedkar and Gregory L. Heileman. DRM as a layered system. In *Proceedings of the Fourth ACM Workshop on Digital Rights Management*, pages 11–21, Washington, DC, Oct. 2004.

[26] Pramod A. Jamkhedkar and Gregory L. Heileman. Digital rights management architectures. *Computers Electrical Engineering*, 35(2):376–394, 2009.

[27] Pramod A. Jamkhedkar, Gregory L. Heileman, and Chris Lamb. An Interoperable Usage Management Framework. In *Proceedings of the Tenth ACM Workshop on Digital Rights Management*, Chicago, Oct. 2010.

[28] Pramod A. Jamkhedkar, Gregory L. Heileman, and Ivan Martinez-Ortiz. The problem with rights expression languages. In *Proceedings of the Sixth ACM Workshop on Digital Rights Management*, pages 59–67, Alexandria, VA, Nov. 2006.

[29] Rob H. Koenen, Jack Lacy, Michael MacKay, and Steve Mitchell. The long march to interoperable digital rights management. *Proceedings of the IEEE*, 92(6):883–897, 2004.

[30] M. Lepmets, E. Ras, and A. Renault. A quality measurement framework for it services. In *SRII Global Conference (SRII), 2011 Annual*, pages 767 –774, 29 2011-april 2 2011.

[31] NSA. Distributed service oriented architecture (soa)- compatible cross domain service (dscds) dscds overview. Presented at the Unified Cross Domain Management Office Conference, 2009.

[32] Unified Cross Domain Management Office. Cd101. Presented at the Unified Cross Domain Management Office Conference, 2009.

[33] Jason Ostermann. Raytheon dscds intro. Presented at the Unified Cross Domain Management Office Conference, 2009.

[34] Jaehong Park and Ravi Sandhu. The UCON$_{ABC}$ usage control model. *ACM Trans. Inf. Syst. Secur.*, 7(1):128–174, 2004.

[35] S. Pearson and A. Benameur. Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, pages 693 –702, 30 2010-dec. 3 2010.

[36] G.M. Perez, F.J.G. Clemente, and A.F.G. Skarmeta. Building and managing policy-based secure overlay networks. In *Parallel, Distributed and Network-Based Processing, 2008. PDP 2008. 16th Euromicro Conference on*, pages 597 –603, feb. 2008.

[37] Ron Ross. Next generation risk management. Presented at the Unified Cross Domain Management Office Conference, 2009.