Information Protection in Content-centric Networks

Christopher C. Lamb

Department of Electrical and Computer Engineering
University of New Mexico

November 6, 2012

THE UNIVERSITY *of*
NEW MEXICO

Outline

THE UNIVERSITY *of*
NEW MEXICO

Contribution of Work

The contribution of this work is a quantitative analysis of policy-centric overlay network options, associated taxonomies of use, and prototypical technology proofs-of-concept.

- *Network Control Options* — This includes various types networks and associated strengths and weaknesses addressing centralized and decentralized models.

- *Taxonomies of Use* — Depending on the specific usage management requirements and context, different overlays have different applicability; this work will provide guidance on suitability; it will eventually lead to how to manage data flow within SDN-capable infrastructure.

- *Prototypical Technologies* — Examples and proofs-of-concept will be required to appropriately analyze various architectural alternatives.

THE UNIVERSITY of
NEW MEXICO

Meeting the Goals

Network Control Options

I have developed and analysed multiple types of overlay systems, both centralized (hierarchical) and non-centralized (non-hierarchical), with differing topologies and integrated content-centric control.

Taxonomies of Use

I have established an verified a taxonomy of usage management and applied that within the network providing mechanisms extendable to SDN use.

Prototypical Technologies

Prototype information-centric networks are running between the Rackspace and Amazon clouds.

Impact and Originality

- Information-centric architectures common in future internet designs
- Significant work with respect to name/object binding, overall topologies, approaches
- No significant work yet on exploiting information-centricity for enhanced security
- They have significant new capabilities inherent in approach that allow for better information security

Additional Contributions

This work, as well as providing alternatives analysis with respect to information-centric security with respect to architectures and approaches, also demonstrates the first implementation of granular context-sensitive security functionality embedded in an information-centric network.

Results Overview

Overall evaluation of impact against strategy:

- Encryption most likely to be used...
- ...Rerouting likely the best compromise (but expensive)
- Hierarchical and non-hierarchical networks had similar performance
- No clear leading strategy under all conditions

Property	Redaction	Rerouting	Encryption
Confidentiality	3	2	1
Integrity	0	1	3
Availability	0	1	2

Strategy Impact by Attribute

What does this mean? How did we get it?

THE UNIVERSITY of NEW MEXICO

Methodology

Confidentiality, Integrity characteristics based on approach.

- **Redaction**, by removing information, by definition destroys integrity while guaranteeing confidentiality; unavailable information that is cannot be leaked

- **Rerouting** removes information from a context damaging integrity that can possibly be repaired later, potentially increasing confidentiality by rendering that information unavailable

- **Encryption** minimizes integrity impacts be keeping ciphered data with original context at the expense of possible interception and cryptanalysis exposure

Availability is based on performance.

- **Performance** is measured via end-to-end time of transmittal

Redaction: Removing content that is not approved for transmission over a given link or consumption by a given agent from a larger context of suitable content.

- Strongest confidentiality
- Destroys integrity
- Mixed impact on availability

Fast and easy to implement

Property	Redaction	Rerouting	Encryption
Confidentiality	3	2	1
Integrity	0	1	3
Availability	1	1	2

THE UNIVERSITY *of*
NEW MEXICO

Rerouting

Rerouting: Removing content that is not approved for transmission over a given link and rerouting that content to its destination through secondary means (e.g. SMTP).
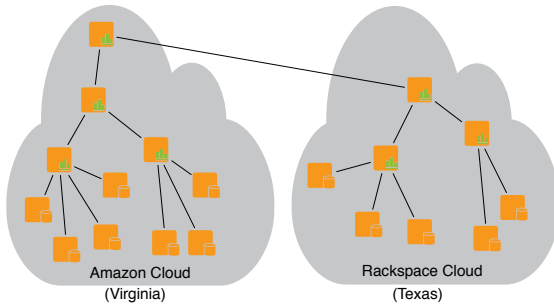
- Confidentiality dependent on secondary links
- Integrity compromised temporarily and perhaps permanently
- Availability dependent on secondary links

Undependable, expensive, good information control

Property	Redaction	Rerouting	Encryption
Confidentiality	3	2	1
Integrity	0	1	3
Availability	0	1	2

THE UNIVERSITY of
NEW MEXICO

Encryption: Enciphering content within larger documents, deciphering enciphered sections when suitable by defined policy and when content needs to be re-evaluated.

- Confidentiality questionable over time
- Integrity compromised temporarily and perhaps permanently
- Availability dependent on secondary links
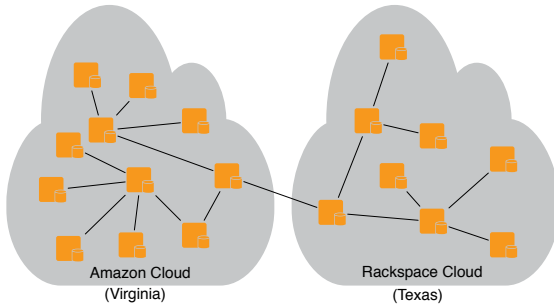
Reasonably secure, simple and performant

Property	Redaction	Rerouting	Encryption
Confidentiality	3	2	1
Integrity	0	1	3
Availability	0	1	2

THE UNIVERSITY *of* NEW MEXICO

Physical Topology

Hierarchical Topology

Amazon Cloud
(Virginia)

Rackspace Cloud
(Texas)

THE UNIVERSITY *of*
NEW MEXICO

Non-Hierarchical Topology

Amazon Cloud
(Virginia)

Rackspace Cloud
(Texas)

Hierarchical Effects
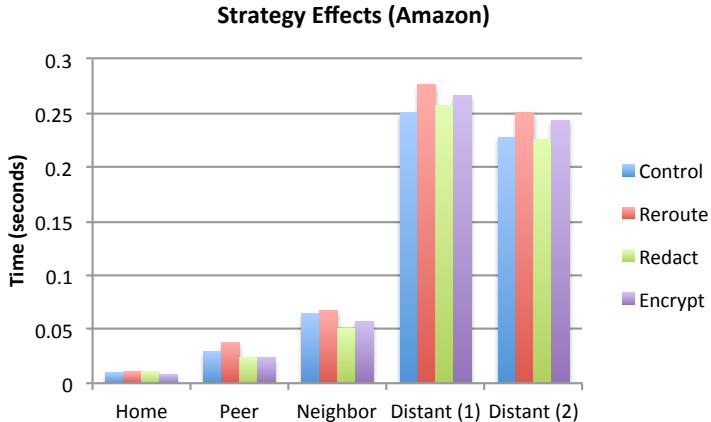
Figure: Hierarchical Results from Amazon

Hierarchical Effects
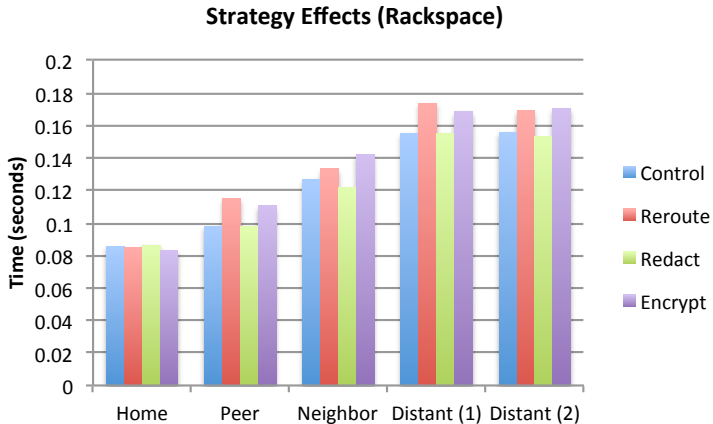
Strategy Effects (Rackspace)

Figure: Hierarchical Results from Rackspace

THE UNIVERSITY of NEW MEXICO
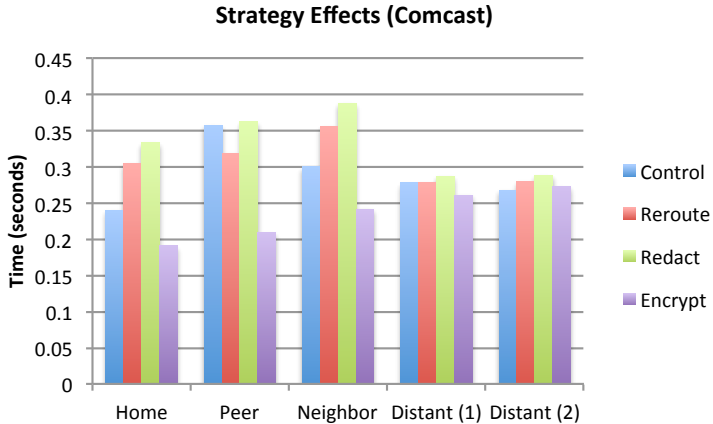
Hierarchical Effects

Figure: Hierarchical Results from Comcast

Non-Hierarchical Effects
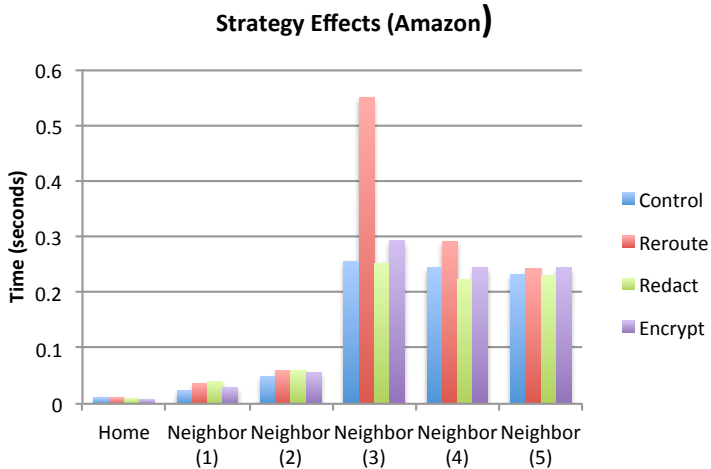
Figure: Non-Hierarchical Results from Amazon

Non-Hierarchical Effects

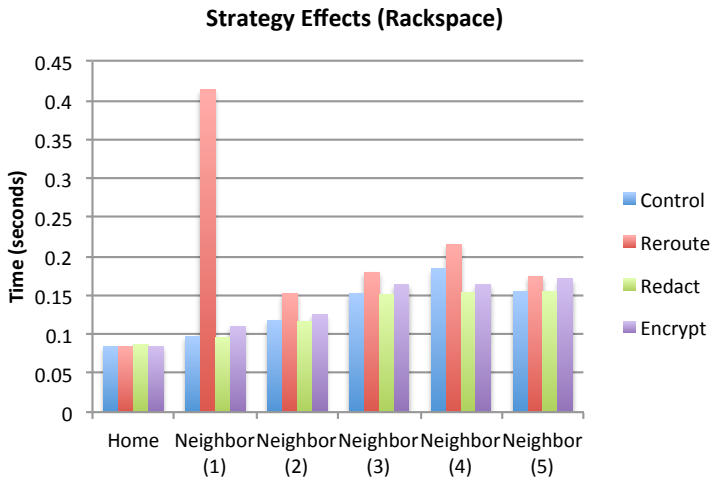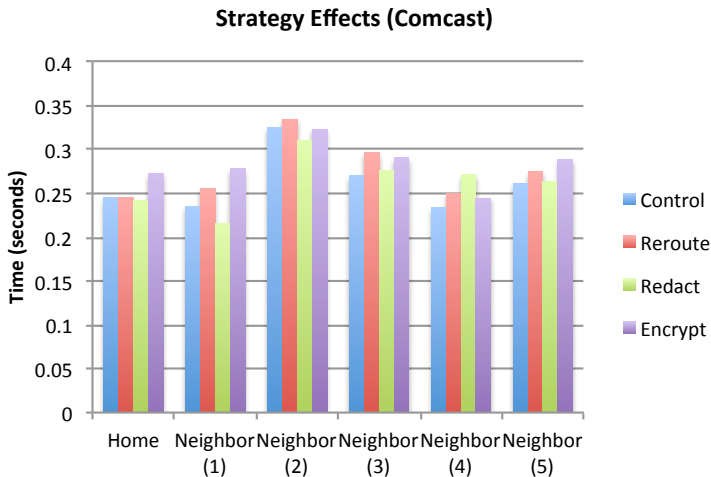Figure: Non-Hierarchical Results from Rackspace

THE UNIVERSITY of NEW MEXICO

Non-Hierarchical Effects

Figure: Non-Hierarchical Results from Comcast

Network-Free Evaluation

Cumulative Processing Time, 1000 Requests
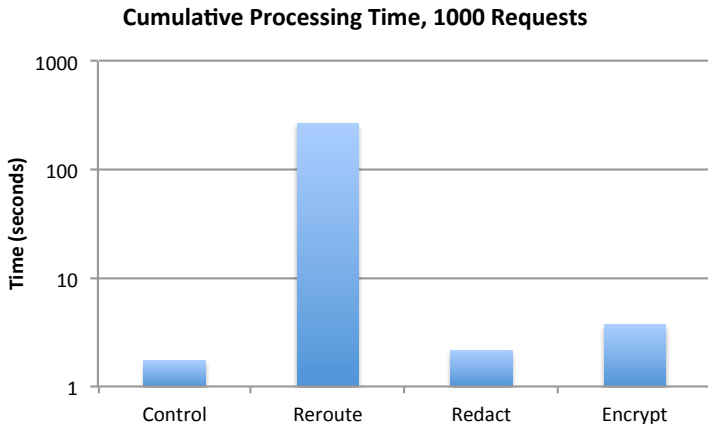
Figure: Results from Requests to a Singe Node

Questions? Comments?