Threat Model In order to understand the security controls needed for Nublu infrastructure, we first need to understand the threat landscape. Today, the Cloud Security Alliance [3] maintains an up-to-date list of the most active security threats to cloud systems. The most recent version, for 2013, outlines the nine most common security threats that exist today as well as security controls that can help alleviate the risk imposed by those threats [1]. Out threat model is based on this list of current cloud threats.

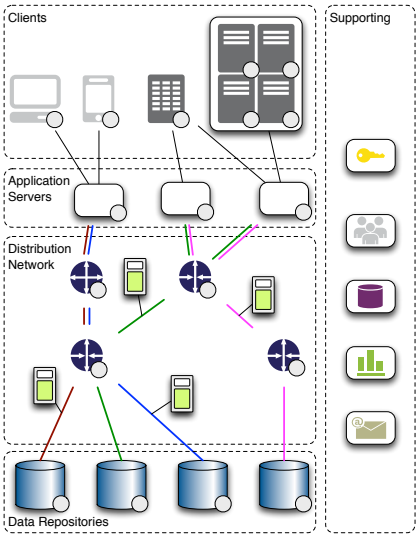

Figure 1: A notional view of the Nublu system, showing various required and provided services in an end-to-end perspective.

Figure 1 shows a notional representation of our proposed Nublu system. This shows the primary catagories of services we will provision, as well as supporting services. To begin with, at the bottom of the figure, we have a collection of *Data Repositories*. These repositories can be of a variety of types, ranging from graph databases(like Neo4j [6]) to document databases (like MongoDB [5]) to data structure databases (like Redis [8]) to relational databases. These data repositories exchange information via a *Distribution Network*. This distribution network transfers information at a variety of security and quality-of-service (QoS) levels, based on the content traversing the network. This figure shows *Secure Data Objects* traversing the distribution network over links provisioned at varying security and QoS levels. The individual network links are managed and connected by control nodes, similar to switches or routers, that manage the flow of information and data transmission performance through the distribution network. The system delivers information to *Application Servers* that deliver information to *Clients*. All elements have embedded information usage and distribution management components, and depend on common services to provide and enforce security controls. Specific common services from top to bottom include key management and public key infrastructure (PKI),

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

[1] Cloud Computing Alliance. The notorious nine: Cloud computing top threats in 2013. `http://www.internet2.edu`, 2013. Accessed: 2013-10-22.

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

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

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

identity and access control (ICAM), directory, monitoring and management, and messaging. Within this view, the Nublu system is responsible for the technical performance of services within the Repository, Distribution Network, and Application Server layers.

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

Data Breaches Data breaches are the most common issue facing cloud deployed information today. Misconfigured databases or multi-tenant virtualization platforms can expose sensitive data to theft. Recent research highlights these issues, demonstrating how attackers can exploit side-channel weaknesses to steal sensitive information [9]. Other recent breaches demonstrate how poor governance and data retention practices can lead to the leak of large swaths of sensitive information as well [4]. Data breaches differ from data loss as breaches imply a leakage of data to unauthorized personnel, while data loss implies permanent loss of information. Ergo, breaches impact all levels of concern within the Nublu system, ranging from repositories through the distribution network to application servers.

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

Hijacking Service and account hijacking are still relevant threats, and such credentials are, by definition, the primary target of phishing attempts. As such, they need to be actively protected, not shared, and two-factor identification should be utilized whenever possible. Though specific ICAM services are outside the scope of this work, developed system must support interfaces to such systems. Furthermore, PKI and other key management systems must be strongly secured to protect against unauthorized key leakage and associated system damage. Overall, this threat has wide impact on Nublu. It affects each layer, and

---

[9] Yinqian Zhang, Ari Juels, Michael K Reiter, and Thomas Ristenpart. Cross-vm side channels and their use to extract private keys. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 305–316. ACM, 2012.

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

all system agents. System agents must be authenticated and be authorized to act within the system. Usage management components are extensions of the ICAM system and make decisions regarding data distribution and must also be secured and authenticated. All credentials associated with these components must be protected from exfiltration or unauthorized access, and must be able to be quickly suspended in case of compromise.

Interfaces Interfaces to cloud systems must also be secured. Not only can malicious actors gain access to cloud-stored information and services via service hijacking, they can also compromise these services via exploing insecure programming interfaces (APIs). All major commercial cloud service providers support programmatic access to their platforms [7,2], and Nublu will be no exception from that trend. In fact, the integration of security controls into the cloud framework and extensive use of software defined infrastructure and networks will increase Nublu's susceptibility to this particular threat. This threat impacts all service layers and supporting services, as they are all software systems consuming and providing interfaces for external access.

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

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

Service Abuse Cloud systems can be compromised and used toward unauthorized ends. For example, virtual machines (VMs) running within a cloud

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

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

environment can be used by malicious actors to store malware, stolen digital property, or to attack stolen encrypted information [9]. Nublu is vulnerable to this kind of abuse in all three service layers. Data storage can be abused to save illicit information, just as virtualized application servers can be compromised for computational horsepower or as pivot points for distributed denial of service attacks. Likewise, networks can be compromised to transfer stolen digital goods or to hide unauthorized communication.

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

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

[9] Yinqian Zhang, Ari Juels, Michael K Reiter, and Thomas Ristenpart. Cross-vm side channels and their use to extract private keys. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 305–316. ACM, 2012.