Evaluation of a Security Service Level Agreement

Chen-Yu Lee, Krishna M. Kavi,

Department of Computer Science and Engineering, University of North Texas
1155 Union Cir, Denton, TX 76203, United States
Email: cychrislee@ieee.org, Krishna.Kavi@unt.edu

***Abstract*—Data breaches are the most serious security breaks among all types of cybersecurity threats. While Cloud hosting services provide assurances against data loss, understanding the security service level agreements (SSLAs) and privacy policies offered by the service providers empowers consumers to assess risks and costs associated with migrating their information technology (IT) operations to the Cloud. We have developed ontologies to represent security SLAs so that consumers can understand cybersecurity threats, techniques for mitigating the risks, and their roles and responsibilities and those of the service provider in terms of protecting IT systems. Our ontological representation of security services offered by a provider allows the customer to evaluate the level of compliance with respect to federal regulations such as Health Insurance Portability and Accountability Act (HIPAA). In this paper, we also describe ways to quantitatively assess the strength of compliance and the quality of protections offered by an SSLA. We hope that our approach can lead to negotiated SSLAs.**

Keywords–service level agreement; SLA; security; SSLA; cloud computing.

I. INTRODUCTION

In 2014 and 2015, we have seen numerous and significant data breaches. In September 2014 Home Depot suffered a data breach of 56 million credit card numbers [1] and in October 2014, 1.16 million customer payment cards were stolen from Staples [2]. In February 2015, CareFirst BlueCross BlueShield announced that it was the target of a cyber attack that compromised the information of about 1.1 million current and former consumers [3]. Compromised information included consumer user names for CareFirsts website, as well as names, birth dates, email addresses and subscriber identification numbers. Most recently (June 2015), the US Office of Personnel Management revealed a data breach that lead to a foreign nation having access to millions of US federal employee records [4]. These incidents show that data breaches (or an unauthorized person gaining access to data) are the most prevalent types of security attacks. Some of these attacks involved very sophisticated techniques to circumvent several levels of cybersecurity protections.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that describes a standardized approach to security assessment, authorization, and continuous monitoring of Cloud IT products and services. FedRAMP is the result of close collaborations among cybersecurity and cloud experts from the General Services Administration (GSA), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DOD), the National Security Agency (NSA), the Office of Management and Budget (OMB), and the Federal Chief Information Officers (CIO) Council. The assessment process is based on a standardized set of requirements in accordance with the Federal Information Security Management Act (FISMA). The NIST Special Publication (SP) 800-53 [5] controls security authorizations. NIST is also working on new guidance, SP 800-174, which will address the distribution and placement of security controls for cloud computing environments. The new guidance will list the controls needed for capabilities (or services), and displays how a cloud capability (or service) should be correctly and completely secured. Finally, the NIST Cloud Computing program plans to define security SLAs, security metrics, security intelligence and continuous monitoring based on previous documents SP 500-299 [6], SP 500-307 [7], SP 800-173, and SP 800-174. The Security Service Level Agreement (SSLA) can be used to improve the credibility and verifiability of security and privacy commitments made by cloud providers.

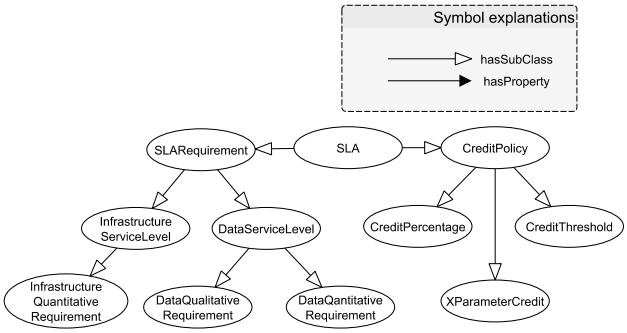


Figure 1. Ontology for SLA

In general, Service Level Agreements (SLAs) written by a Cloud provider are very difficult to understand, and it is even more challenging to quantitatively compare the SLAs of different providers. To capture and present requirements for both providers and consumers, Modica et al. proposed an SLA ontology that captures the definition of a semantic domain of knowledge for the cloud business (see Figure. 1) [8]. Based on the ontology knowledge base, providers can customize their offerings according to their business strategy, and consumers can request the resources and services consistent with their needs. However, this work does not cover security service levels, which led to our development of ontologies specifically for SSLAs.

This paper extends our previous work that proposed ontologies for SSLAs that could be used to understand the security

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-438-1

agreements of a provider and to audit the compliance of service levels with respect to federal regulations, such as HIPAA [9] [10]. We enrich the ontology models and propose an SSLA assessment system to evaluate the strength of agreements in terms of protecting IT assets. Our approach can be used to negotiate desired levels of security. The rest of the paper is organized as follows. Section II discusses research that is closely related to ours. The SSLA ontology framework is introduced in Section III. Our approach for assessing SSLAs is described in Section IV and we illustrate how this approach can be used for negotiating SSLAs in Section V. Section VI includes a discussion of our current research and our plans for extending the framework.

II. Related Works

A. Service Level Agreement

A SLA is a documented legal agreement between a service provider and a consumer and identifies services and levels of service targets based on the ISO 2000 standard for service management systems [11]. A Cloud Service level agreement is a document that states the services offered, performance levels and promises made by the cloud provider.

B. Security Service Level Agreement

The Security Service Level Agreement (SSLA) for specifying the security service requirements of an enterprise was first proposed by Henning [12]. Monahan et al. considered the issues of meaningful security SLAs and discussed how a security SLA embodies certain legal and contractual elements to satisfy two basic requirements: separation and compartmentalization [13]. In 2013, the terms SSLA and security service-oriented agreement were proposed by Takahashi et al. [14]. The authors proposed a non-repudiatable security service-oriented agreement mechanism that describes security requirements for users and capabilities of service providers. Rong et al. described some cloud security challenges including resource location, the multi-tenancy, authentication and trust of acquired information, system monitoring, and cloud standards [15]. Hale et al. built an XML-based compliance vocabulary compatible with the WSLA schema [16]. However, there are no prior attempts to describe SSLAs formally. Currently SSLAs are described informally in English, and it is very hard to evaluate or negotiate the strength of such informal descriptions. Previously we proposed an ontology for SSLA that covers the security issues required to meet most security regulations [9] [10]. This paper expands our previous ontology and proposes to evaluate the strength of an SSLA.

III. Ontology For SSLA

As an alternative to the traditional SLAs, written in natural languages, an XML-based SLA is more useful for automated processing. Previously we defined several different ontologies including ontologies for vulnerabilities, attacks and Security SLAs ([9] [10] [17]). Our ontology for Security Service Level Agreements (or SSLAs) are based on the design concepts of a trustworthiness ontology proposed in [18] and also extends Hale's work [16]. To increase the coverage of our SSLA ontology, we take into account the challenges in covering all control domains specified by the Cloud security alliance (CSA) Cloud Control Matrix (CCM) v3 [19] and the properties of some security frameworks, such as HITRUST [20].

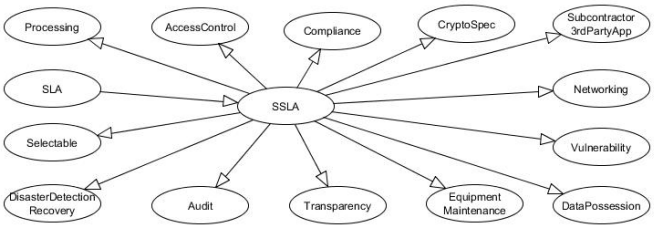


Figure 2. All classes in SSLA

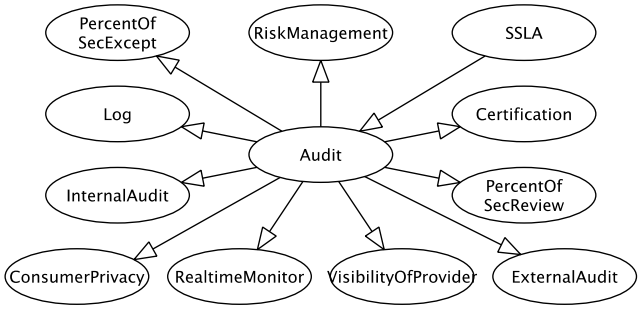


Figure 3. Audit class in SSLA

In this paper we extend our previous SSLA ontology so that SSLAs can be evaluated for their strengths. Our SSLA ontology facilitates an understanding of security concerns in service level agreements and allows one to match the security requirements of a customer with the SSLAs offered by service providers. Summarizing, our SSLAs offer these benefits.

- SLA agreements are easier to understand, particularly those related to security.
- During negotiations, consumers can compare the SLAs offered by different providers and choose the one that best fits their needs.
- It will be easier to monitor (or audit) the compliance of securities levels offerred by service providers with security requirements of federal regulations.

For completeness sake we introduce our SSLA ontology first. Without loss of generality, here we represent fourteen classes in our SSLA ontology, including `Networking`, `Vulnerability`, `Transparency`, `DisasterDetectionRecovery`, `DataPossession`, `CryptoSpec`, `AccessControl`, `Processing`, `Compliance`, `Audit`, `Selectable`, `Subcontractor3rdPartyApp`, and `Equipment Maintenance` as shown in Figure 2. Each class is described below. The ontology can be modified by removing or adding additional classes.

- Networking: This class organizes the agreements about the networking environment such as traffic isolation (`TrafficIsolation` subclass); IP and bandwidth monitoring (`BandwidthMonitoring` and `IPMonitoring` subclasses). These subclasses can be used to define functions such as allocating bandwidth and blacklisting (or whitelisting) IP addresses.

- Vulnerability: This class defines assurances in terms of detecting and patching known vulnerabilities. `PatchPolicyComplianceRate` and `ScanFrequency` subclasses can be used for specifying policies on how often the system is scanned for malware, and how soon a known patch is applied to remove vulnerabilities.
- Transparency: This class regulates the transparency of the information related to the security management processes used by the provider. The SSLA should record the responsible office that will provide the information regarding all security breaches and actions taken when requested.
- Disaster detection and recovery: This class describes the contingency plans and the security incident procedures, and details disaster detection and the recovery steps in the event of a breach. It may also define data backup functions because data is usually the most valuable asset for consumers.
- Data possession: This class controls data storage procedures and verification methods, and how often they are applied to ensure data authenticity. This class can be used to specify the ownership and the location of the storage.
- Audit: This class describes the processes for internal and external audits of the architecture, management, and services of providers, and the certificates obtained (listed in Certification) to build consumer trust in the providers as shown in Figure 3. `InternalAudit` and `ExternalAudit` subclasses also define the respective audit plans. `Log` is the most important evidence of behaviors of attackers, consumers, and providers. To protect the security of the log, the `Log` subclass regulates the secure storage and retention of the logs. The `RiskManagement` subclass describes the risk management and data risk assessment programs. The system administrators of the providers' systems have the highest level of privilege. They can perform any action on any object. Thus, the `ViabilityOfProvider` subclass defines what level of consumer data security is appropriate for a specific person and under what conditions. In addition, the class outlines the real time monitoring mechanisms, the acceptable percentage and types of security exceptions, security reviews, and the protection of consumer privacy in `RealtimeMonitor`, `PercentOfSecExcept`, `PercentOfSecReview` and `ConsumerPrivacy` subclasses.
- Subcontractor and third party application: This class clarifies the rights and duties with respect to security of the subcontractor and the third party application providers.
- Cryptography specification: Some providers offer encryption services. It is useful to optimize consumer data encryption while also reducing the associated computational complexity. Thus the level or type of encryption technique can be specified here.
- Access control: Access control of the instance control panel directly impacts the security of the instance. This class defines the access authentication, authorization, accounting schemes, including access using mobile devices. This class also can be used to specifiy the responsibility of the consumer in terms of permitting accesses within their user groups.
- Processing: This class covers the security demands for building a secure run time environment for virtual machine migration, queue service capability, virtual firewalls, isolation, portability and integrity of applications. Systems relying on hardware trusted platform modules may be viewed as providing higher levels of trust and this can be indicated in this class.
- Compliance: Some specific services must be certified as compliant with security and privacy standards, and practices as required by law. For example, user services that involve warehousing or mining of electronic Protected Health Information (ePHI), electronic Personally Identifiable Information (ePII), or Health Insurance Portability and Accountability Act (HIPAA) data must comply with all associated federal and local standards [21]. There are many subclasses defined in Compliance as shown in Figure 4. An SSLA can indicate the subclasses (or specific rules of the law) for which the provider is compliant.
- Equipment Maintenance: Keeping equipment maintained and upgraded may lead to fewer exploitable weaknesses. This class of our SSLA ontology defines the state of equipment, software versions and all upgrades since the installation.

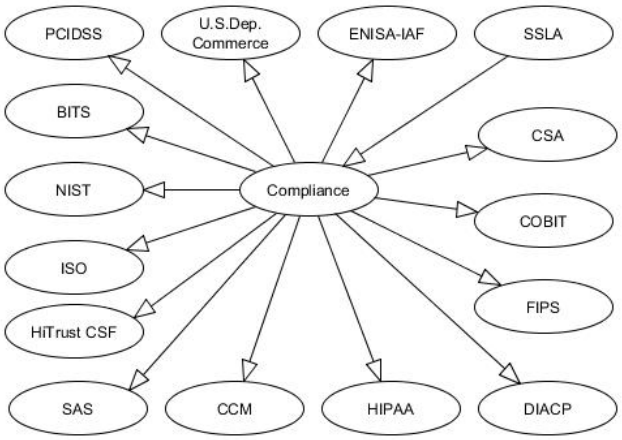


Figure 4. Compliance class in SSLA

IV. SSLA Assessment System

During the process of purchasing cloud services, a review of the service level agreement is the necessary phase where customers agree to a binding contract in term of the services received and payments made. At present, the agreement lists service guarantees and responsibilities of the provider. Often they are biased in favor of the provider; in many cases the customer is not afforded a chance to negotiate service levels. This is particularly the case when it comes to security levels offered by the provider. There is very little opportunity for the customer to explore whether the security is sufficient, or

if a lower or higher level security option is available. More importantly, the customer cannot evaluate the security levels using meaningful and quantitative measures.

Our SSLA ontology described in Section III contains fourteen classes and several subclasses that cover most of the security issues of interest. We feel that this allows one to map a SSLA contract to our ontology and evaluate the strength of security provided by the SSLA. In this section, we outline some potential ways for quantitatively assessing the strength of SSLAs.

A. Regulation Compliant

In general, a regulation describes rules, such as specifications, policies, standards, or law, especially the public regulations that apply in particular fields. Some examples of regulations include PCI-DSS [22], HIPAA and others shown in Fig.4. Each regulation defines different rules, but many rules in the regulations are similar. Therefore, an SSLA is stronger if it complies with more regulations.

B. Types of metrics

To evaluate an SLA, each individual (or a subclass) in our ontology has to be examined. Each entity should be quantified and we offer three different types of measurements for this purpose.

- Boolean measures (α): This type of quantification allows us to assess if a specific requirement (such as a specific HIPAA regulation or rule) is satisfied or not. Service providers will be fined if the provider fails to show that specific federal requirements are met. Note that different regulations (e.g., HIPAA, ENISA [23], PCI) may define different security requirements, and this translates to different subclasses (or individuals) in our ontology for meeting the requirements.
- Level measures (β): It should be possible to assess the strength of an agreement using qualitative measures as High, Medium, Low (or some other such levels). For example, in terms of the strength of encryption offered, one can say that using encryption algorithm Triple DES [24] is classified as low, but if one uses AES-128 [25] then the level may be viewed as medium, and the level is considered High if AES-192 or AES-256 are used for encryption. These are subjective assessments and we hope a consensus on the measurement can be reached through standards committees.
- Range measures (γ): These types of assessments can be used to define minimum threshold guarantees. For example, a user requires that the Cloud provider scan the systems for malware at least once every 12 hours. Any scanning rate below that can be viewed as less than satisfactory, and a value (say a percentage) may be assigned as a qualitative strength for the individual (or subclass).

C. Estimation of the security strength

We propose a quantitative analysis approach to estimate the security strength of each service level agreement. The process can follow the following outline.

Step 1: Prepare an ontology graph for the SSLA. Normally the ontology data can be stored in OWL or RDF format. The first step is to parse the ontology file as a graph for further query, e.g., RDFLib [26] in Python.

Step 2: Traverse all the individuals using SPARQL query. To examine each rule in the SSLA ontology, the approach traverses each individual with a recursive SPARQL query from the root through a class to each instance. SPARQL is a semantic query language for databases. It is used to retrieve and manipulate data stored in Resource Description Framework (RDF) format.

Step 2a: When visiting an individual (or a subclass), a score is assigned using the three types of measurement stated above.

$$P(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is satisfied} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

$$P(\beta) = \begin{cases} score_{high} & \text{if } \beta \text{ is given a } \texttt{HIGH} \\ score_{medium} & \text{if } \beta \text{ is given a } \texttt{MEDIUM} \\ score_{low} & \text{if } \beta \text{ is given a } \texttt{LOW} \end{cases} \quad (2)$$

$$P(\gamma) = \{score_{range} \quad \text{if } \gamma \text{ is given } score_{range} \quad (3)$$

where $0 \leq score_{range}, score_{high}, score_{medium}, score_{low} \leq 1$ and the mapping scores from `HIGH`, `MEDIUM`, and `LOW` grades can be defined by the security committee.

Step 2b: The total score of a given SLA is $Score_{total}$.

$$Score_{total} = \sum_{i=1}^{n} class_i \quad (4)$$

$$class_i = \sum_{j=1}^{n} (P_j(\alpha) + P_j(\beta) + P_j(\gamma)) w_{i,j} \quad (5)$$

where $w_{i,j}$ is the weight of the j^{th} measurement of the i^{th} class and it can also be defined by security committee based on the emphasis level. The default value of $w_{i,j}$ is 1. Weights can be used to customize the measurements for individual needs. We describe the customization in the next section.

V. Customized Agreement

With our assessment system it is possible to compare SSLAs during the negotiation phase. An SSLA that scores highest is the optimal SSLA. This also means that the provider is held to very high levels of responsibility and liabilities, and this in turn can translate into higher cost to the customer. A customer should be able to understand the trade-offs between cost and the strength of an SSLA.

Figure 5 shows a comparison of two different types of companies. Figure 5(a) is a medical service provider that emphasizes compliance, access control, and audit classes of our ontology since these aspects of an SSLA are most important to their business. Other classes, such as networking or

encryption level are not as significant to their business (and does not interfere in demonstrating compliance with HIPAA regulations). On the other hand, Figure 5(b) is a company that offers online or downloadable games. Such a company is more interested in the security with on-line transactions (including payment transactions) and must be compliant with PCI DSS regulations. The company would also have significant interest in the access control, networking and infrastructure security. These examples are for illustration purposes only and the classes of companies used here are generic examples. More detailed analysis of each users requirements is needed to customize SSLA measurements. These two examples show that different types of companies may pay attention to the different classes of security needs. When negotiating SSLA, which part should be strengthened can be determined through the evaluation methods we describe in this paper. We assume that consumers will negotiate their customized SSLAs, instead of a generic SSLA offered by the provider. A generic SSLA may not be optimal in terms of cost and the level of security offerred. However, the generic SSLA may suffice for most customers.

VI. Discussion

This paper expands the SSLA ontology to cover more security regulations and security frameworks including HITRUST Cyber Security Framework (CSF). Therefore, in the next subsections, we first describe the implementation issue for the evaluation system for an SSLA based on the SSLA ontology. The system provides a quantitative result for the assessment that can be used to SSLA comparison and negotiation. Also, the coverage of HITRUST CSF is explained in subsection VI-B

A. Implementation

We implemented an SSLA assessment system to compute scores of the given agreement based on the approaches introduced in Section IV. Figure 6 is a snapshot of estimating HIPAA compliance in our assessment system. The program first shows each rule of the law for the consumer so that the consumer can understand the requirement. The quantitative scoring of the SSLA is based on the answers provided by the consumer. Current SSLAs are described in a natural language (i.e., English) and may be difficult to map onto our ontology. We require some input from the customer and service provider to interpret the SSLAs and map them to our ontologies. We hope future SSLAs will rely on more formal ontological definitions.

B. HITRUST Cyber Security Framework

The HITRUST Cyber Security Framework (CSF) is based on the Cyber Security Framework released by the National Institute of Standards and Technology (NIST) in February 2014. HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to demonstrate regulatory compliance and risk management. Although HITRUST CSF is not a regulation, it provides for more security and privacy than HIPAA compliance. Figure 7 shows the fact that the HITRUSgrT properties subsume HIPAA rules related to access authorization. Thus if a provider satisfies the HITRUST CSF framework, the provider is also compliant with HIPAA regulations, as far as the access authorization class of our ontology is concerned. Likewise one can map the compliance with respect to other classes of the SSLA ontology.

C. Scoring system

The assessment system evaluates the SSLA quantitatively. In general, each mapped individual in our model is assigned one point; thus an SSLA with more points is assumed to be better as it satisfies more classes of our ontology. The weight valuable $w_{i,j}$ can be used to allow one to ignore some classes and place more emphasis on other classes.

D. Benfits of our Scoringe system

- For Cloud infrastructure provider: Since an ontology is a useful means for describing knowledge, a Cloud provider can employ our SSLA ontology to present the security levels guaranteed. Additionally, the SSLA ontology provides for negotiated agreements. With respect to HIPAA, the Cloud infrastructure provider must make sure that the Cloud environment is secure enough at least for known vulnerabilities and can resist known attacks. Moreover, the provider can use some vulnerability evaluation systems (like OKB [17]) to evaluate the security risks of its resources to define the most appropriate security guarantees, or price different levels of negotiated security agreements.
- For Cloud infrastructure users (primarily service providers): When service providers employ a Cloud environment, they can utilize our SSLA ontology framework to negotiate better levels of security guarantees from the infrastructure provider. Additionally, the service provider can use our framework to understand compliance issues about the services they offer.

VII. Conclusion

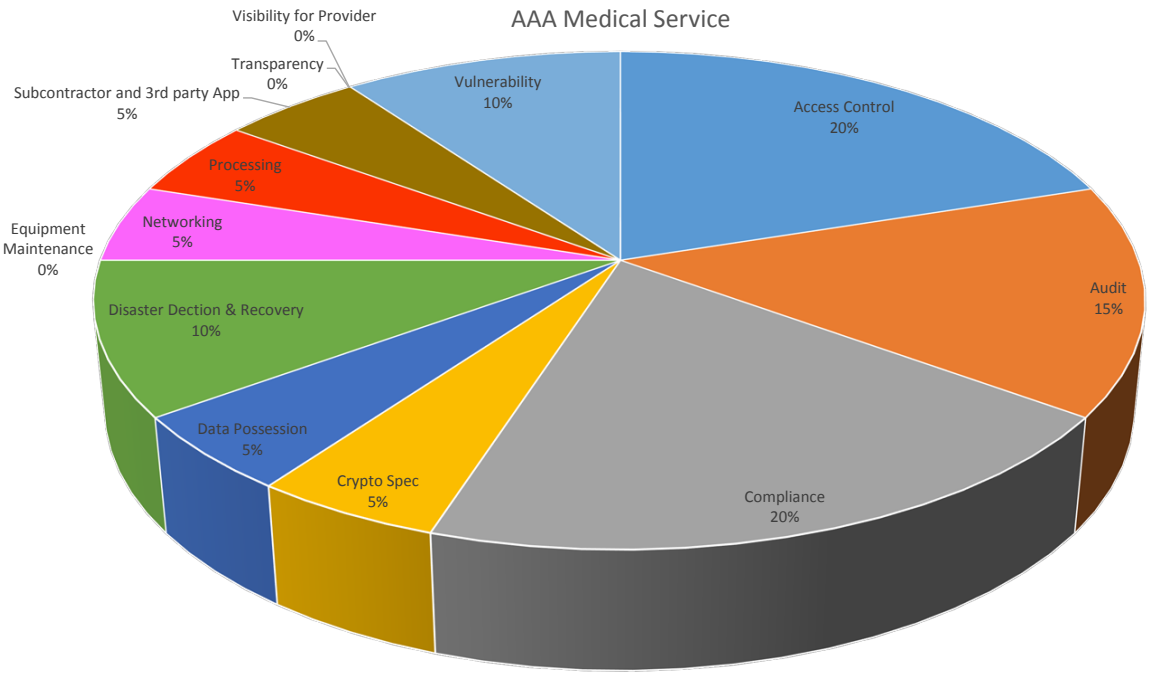
In this paper, we have developed an SSLA ontology framework that can be used to understand the security agreements of a provider and to audit the compliance of a provider with respect to federal regulations. The SSLA assessment system can be used to quantitatively measure the security strength of an SSLA, and can be used in the negotiation phase. In this paper, we are limited by the lack of accessible SSLAs of cloud providers such as Google, Amazon or Microsoft. We were only able to outline how HITRUST and HIPAA regulations translate into security requirements of individual IT systems and policies. It is our hope that the new federal guidelines and standards will force service providers to disclose details of their security SLAs. We will then be able to evaluate actual SSLAs of providers.

For future work, we plan to design SSLA templates for different types of industries with various levels of budgets based on the evaluation of collected agreements. These templates can be used to negotiate SSLAs with providers.

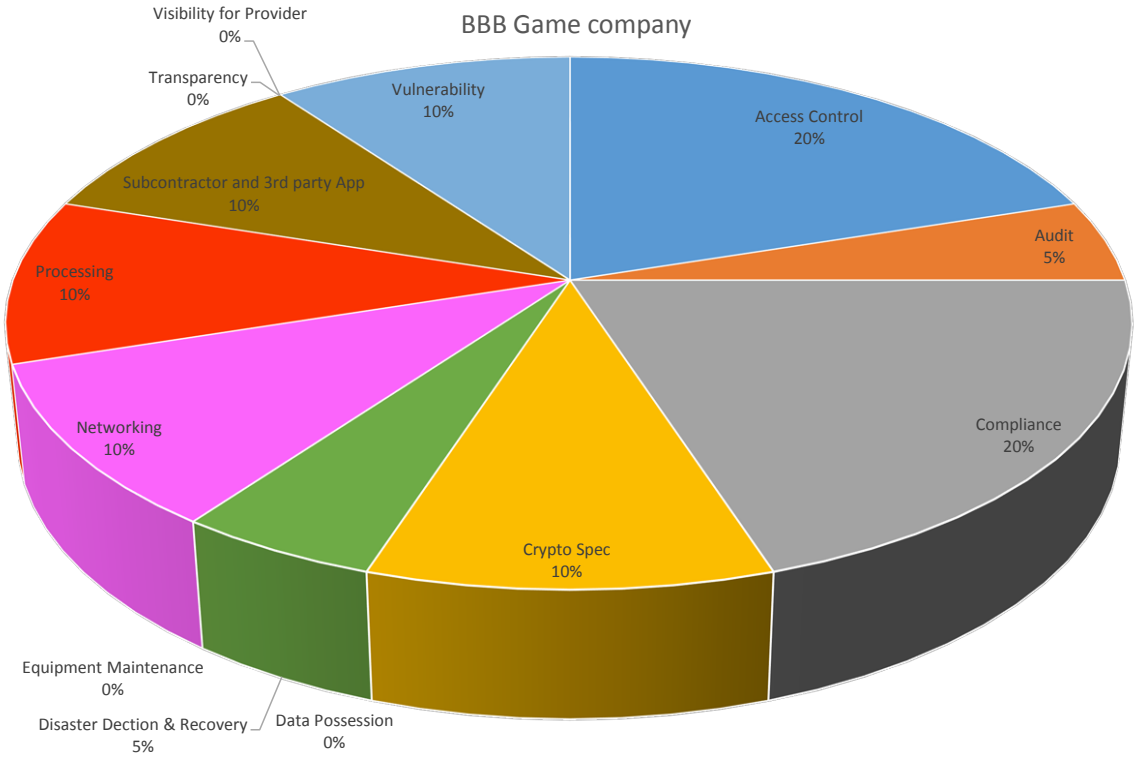
Acknowledgment

This research is supported in part by the NSF Net-centric and Cloud Software and Systems Industry/University Cooperative Research Center and NSF award 1128344. The authors want to thank David Struble for his editorial contributions to this paper.

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-438-1



(a) The proportion of the classes in a medical service's SSLA



(b) The proportion of the classes in a game company's SSLA

Figure 5. The proportion of the classes in SSLA

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-438-1

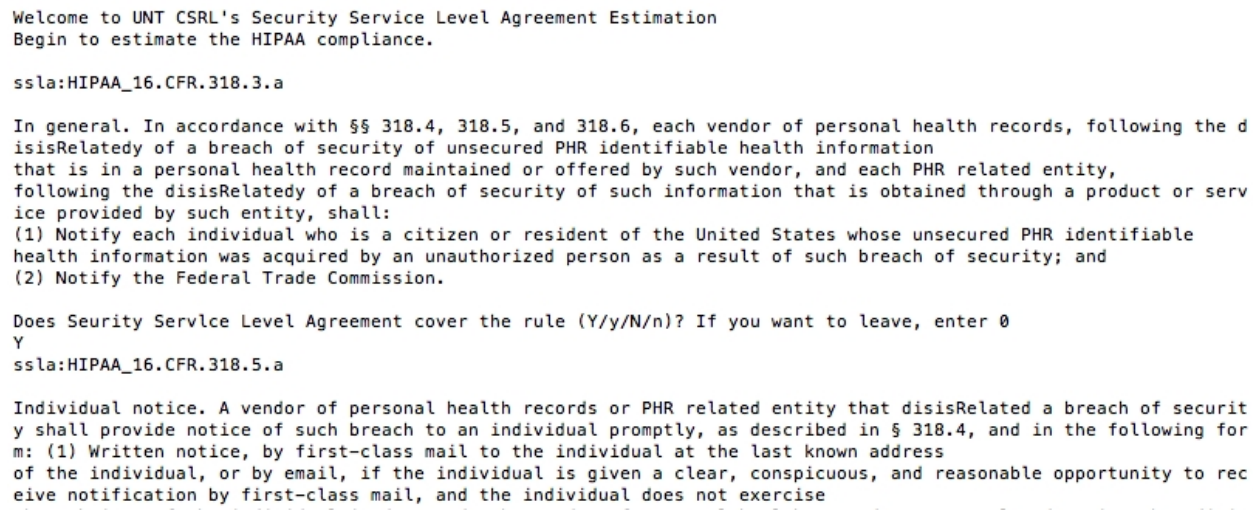


Figure 6. Snapshot of our SSLA assessment system. For estimating HIPAA compliance, the system first shows the rule of law, and the estimation is based on the administrators answer.

REFERENCES

[1] M. Backman, "Home depot: 56 million cards exposed in breach," Sep 2014, URL: http://money.cnn.com/2014/09/18/technology/security/home-depot-hack [accessed: 2015-09-15].

[2] J. Tom Huddleston, "Staples: Breach may have affected 1.16 million customers' cards," Dec 2014, URL: http://fortune.com/2014/12/19/staples-cards-affected-breach/ [accessed: 2015-09-15].

[3] D. Bowman, "Hack attack on carefirst compromises info for 1.1 million consumers," May 2015, URL: http://www.fiercehealthit.com/story/hack-attack-carefirst-compromises-info-11-million-consumers/2015-05-20 [accessed: 2015-09-15].

[4] "Office of personnel management data breach," June 2015, URL: http://www.c-span.org/video/?326593-1/hearing-office-personnel-management-data-breach [accessed: 2015-09-15].

[5] Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, NIST, U.S. Department of Commerce Std., Rev. 4, Apr. 2013, URL: http://dx.doi.org/10.6028/NIST.SP.800-53r4 [accessed: 2015-09-15].

[6] NIST Cloud Computing Security Reference Architecture, SP 500-299 Draft, NIST, U.S. Department of Commerce Std., May 2013.

[7] Cloud Computing Service Metrics Description, SP 500-307 Draft, NIST, U.S. Department of Commerce Std., 2015, URL: http://dx.doi.org/10.6028/NIST.SP.307 [accessed: 2015-09-15].

[8] G. D. Modica, G. Petralia, and O. Tomarchio, "A business ontology to enable semantic matchmaking in open cloud markets," in Proc. SKG2012, Beijing, China, Oct. 2012, pp. 96–103.

[9] C. Y. Lee, P. Kamongi, K. M. Kavi, and M. Gomathisankaran, "Optimus: Framework of vulnerabilities, attacks, defenses and sla ontologies," International Journal of Next-Generation Computing, 2015.

[10] C. Y. Lee, K. M. Kavi, R. A. Paul, and M. Gomathisankaran, "Ontology of secure service level agreement," in Proc. HASE 2015, Jan 2015, pp. 166–172.

[11] Information technology. Service management. Service management system requirements, ISO/IEC 20000-1:2011, Std., 2011.

[12] R. R. Henning, "Security service level agreements: quantifiable security for the enterprise?" in Proc. NSPW 1999, Ontario, Canada, Sep. 1999, pp. 54–60.

[13] B. Monahan and M. Yearworth, "Meaningful security slas," HP Laboratories, Tech. Rep. HPL-2005-218R1, 2008.

[14] T. Takahashi and et al., "Tailored security: Building nonrepudiable security service-level agreements," IEEE VT Mag., vol. 8, no. 3, Sep. 2013, pp. 54–62.

[15] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Comput. Electr. Eng., vol. 39, no. 1, 2013, pp. 47–54.

[16] M. Hale and R. Gamble, "Building a compliance vocabulary to embed security controls in cloud slas," in Proc. SERVICES 2013, Jun. 2013, pp. 118–125.

[17] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "Vulcan: Vulnerability assessment framework for cloud computing," in Proc. SERE 2013, 2013, pp. 218–226.

[18] R. Paul and et. al., "An ontology-based integrated assessment framework for high-assurance systems," in Proc. ICSC 2008, Aug 2008, pp. 386–393.

[19] "Cloud controls matrix version 3.0," Cloud Security Alliance.

[20] HITRUST Cyber Security Framework, URL: https://hitrustalliance.net/ [accessed: 2015-09-15].

[21] HIPAA Administrative Simplification, U.S. Department of Health and Human Services Office for Civil Rights Std., Mar. 2013, URL: http://www.hhs.gov/ocr/privacy/hipaa/administrative/ [accessed: 2015-09-15].

[22] Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures, PCI Security Standards Council Std., Rev. 3.0, Nov. 2013, URL: https://www.pcisecuritystandards.org/security_standards/ [accessed: 2015-09-15].

[23] Procure Secure: A guide to monitoring of security service levels in cloud contracts, European Union Agency for Network and Information Security (ENISA) Std.

[24] FIPS PUB 46-3 Data Encryption Standard (DES), National Institute of Standards and Technology Std.

[25] FIPS PUB 197 Advanced Encryption Standard (AES), National Institute of Standards and Technology Std.

[26] RDFLib Python library, URL: https://github.com/RDFLib/rdflib [accessed: 2015-09-15].

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-438-1

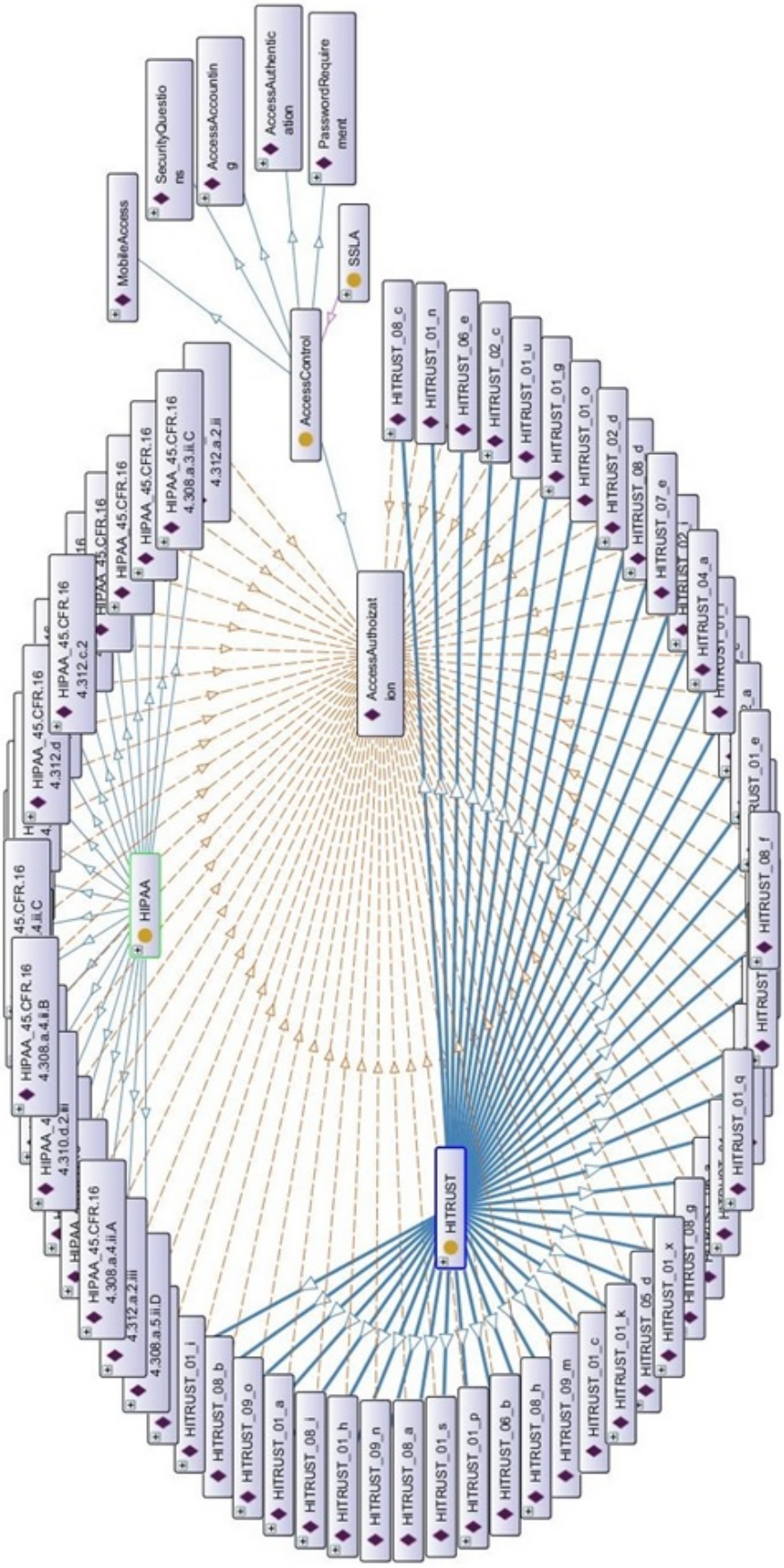


Figure 7. Individuals for both HIPAA and HiTrust in the `AccessAuthorization` class. The left side is for HiTrust and the right side is for HIPAA.