Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

A Secure Cloud Internetwork Model with Economic and Social Incentives (SCIMES)

Alan Rea
Western Michigan University, Kalamazoo, MI, United States., rea@wmich.edu

Xiaojun Cao
Georgia State University, Atlanta, GA, United States., cao@cs.gsu.edu

Aparna Gupta
Rensselaer Polytechnic Institute, Troy, NY, United States., guptaa@rpi.edu

Nirmala Shenoy
Rochester Institute of Technology, Rochester, NY, United States., nxsvks@rit.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
Rea, Alan; Cao, Xiaojun; Gupta, Aparna; and Shenoy, Nirmala, "A Secure Cloud Internetwork Model with Economic and Social Incentives (SCIMES)" (2012). *AMCIS 2012 Proceedings*. 5.
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/5

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Secure Cloud Internetwork Model with Economic and Social Incentives (SCIMES)

Alan Rea
Western Michigan University
rea@wmich.edu

Xiaojun Cao
Georgia State University
cao@cs.gsu.edu

Aparna Gupta
Rensselaer Polytechnic Institute
guptaa@rpi.edu

Nirmala Shenoy
Rochester Institute of Technology
nxsvks@rit.edu

ABSTRACT

The Internet has exponentially expanded to meet the new demands placed on its ever-growing network structure. However, its original data-sharing design cannot address issues, such as malware, Distributed Denial of Service, or the increased need to offer more reliable and trusted connections. With trusted connections come more revenue, reduced risks, and a greater variety of services. However, without incentives to provide better services, infrastructure and service providers have no reason to build a better Internet. The Secure Cloud Internetwork Model with Economic and Social Incentives (SCIMES) provides the framework via a new internetwork model that will support trust ratings, as well as secure social and economic choice mechanisms to promote a more secure Internet. This in turn will result in more revenue for providers and greater benefits for users.

Keywords

Trusted Identity, Secure Computing, Privacy, Social Choice, Social Incentives, Economic Incentives, Cloud Model

INTRODUCTION

Over the last couple of decades, the Internet has morphed from a research endeavor into the backbone of business, communication, entertainment, and social communities (Clark, Wroclawski, Sollins, and Braden, 2005). Organizations use it to grow into strong economic entities; people create and share ideas via e-mail, message boards, and video sites; and focused communities allow individuals to enrich their lives via collaborative knowledge building, formal education, and strong mentoring relationships (Schulzrinne, 1997).

However, with all of the benefits, we have yet to address many challenges (Clark, et al., 2005; Oliveira, Lad, and Zhang, 2009). The original Internet was designed with the mindset of sharing data among a limited number of research institutes. Hence the lack of security and social and economic consideration in the design process has proven to be a critical barrier for Internet growth. For example, connecting into the vast information highway to partake of its potential also allows cybervandals to hijack connections, steal information, or simply fill one's inbox with snake oil cures. Essentially, the Internet must deliver data from one point to another, similar to the Package Delivery (FedEx, etc.) industry. Robustness and growth of the package delivery industry can be largely credited to its increasing reliability, trustworthiness, and service choices. However, in the current Internet model, there is almost no trust among any two entities; there are limited choices due to the Internet's rigid structure; there are more opportunities for one to take advantage of the trust/security "hole" than to behave well; and there are few provider incentives to improve the Internet infrastructure and offer diverse services (MacKie-Mason, 2009).

Despite these shortcomings, ubiquity of this socio-technical network has enabled new kinds of interactions and transactions, which demand new decision mechanisms to provide fairness, revenue maximization, risk management and efficient resource

use (Breslin and Decker, 2007). It is important to look at developing interactions that will allow for increased trustworthiness among infrastructure and service providers, as well as the people and organizations that use them. To enable these features an internetwork model is required that will allow management of the Internet and its traffic through economic and social choice mechanisms, with a goal to achieve better utilization while reducing the nuisance and harm caused by intruders and spammers. These mechanisms can then be used to identify social and economic incentives to mediate the interactions among infrastructure providers, service providers and clients.

The proposed Secure Cloud Internetwork Model with Economic and Social Incentives (SCIMES) combines secure social choice mechanisms to promote both economic and social incentives via a value-added framework that encourages secure computing and privacy protections as a means to increase service selection and economic benefits. SCIMES 1) develops a new internetwork model based on a modular network clouds concept, which 2) embeds security and privacy controls within the clouds, 3) provides economic and social incentivizes to use the clouds and 4) creates robust socio-economic models for infrastructure and service providers within the cloud.

THE TIERED FLOATING CLOUD INTERNETWORK MODEL

The meshed topological connections in the Internet makes changing service providers and connections tedious from both an administrative and a technical perspective, resulting in a low willingness among users to change their connections and/or current service status. This is a major setback to implement choices both from a social and economic perspective to mold the network operations and services. The Internet's highly meshed structure and the use of logical addresses have made packet forwarding and information routing a very complex process, due to the increased routing table sizes and churn rates that the routers and routing protocols handle. (Valancius, Feamste, Rexford, and Nakao, 2010; Xu and Jain, 2009). This also has adverse impacts on the Internet's service performance and the security and trustworthiness it offers. Logical and geographical hierarchies which introduce structure into the meshed topologies thus making them hybrid topologies attempt to overcome the routing issues. Firewalls and other security measures are erected at the ingress/egress points of networks.

We address the problem through the introduction of tiers into the Internet's meshed topology. We then view the different entities in the Internet such as Internet service providers (ISPs), Autonomous Systems (ASes) and sub-networks amongst others as network clouds, associated to the tiers. To enable the tiered structure and to support structured packet forwarding, we introduce tiered addresses. This Tiered Floating Cloud (TFC) internetwork model is then used to enable greater user services, and infrastructure provider choices, with embedded security, while maintaining privacy. The clouds and the connections amongst them are each assigned a Trust Rating (TR), where higher ratings will be the incentives for higher usage and greater economic benefits for both infrastructure and service providers.

Modularity

In the TFC model, modularity is introduced into a network or sub-network through the concept of network clouds, where a network cloud is an abstracted set of network devices based on the functions or operations performed by the devices. Thus a network cloud can be an ISP cloud, a POP cloud, a stub AS cloud, or a backbone cloud that is made up of backbone routers in a POP, or a border cloud made up of border routers in a stub network. The distinction and association of devices to different clouds also allows for functional isolation and partial autonomy (Shenoy, Yuksel, Gupta, Kar, Perotti, and Karir, 2010).

Connection Flexibility

Connection flexibility between service providers, customers and peer networks, is introduced by the tiered structure and addresses. To facilitate easy connection of network clouds to the tiers, the network clouds are assigned tiered addresses. Network clouds can thus move (float) across tiers and establish connections at any tier.

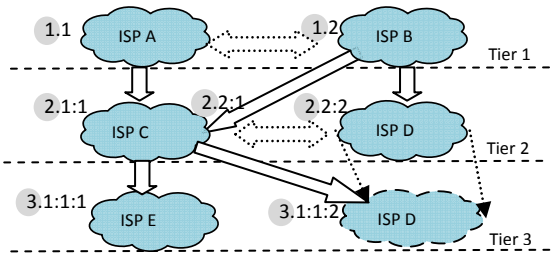

Figure 1: An Example of Tiered Floating Clouds (TFC)

Figure 1 shows an example of applying the TFC model to network clouds at the ISP level, where each ISP has a tiered address (CloudAddr). The CloudAddr has a tier value indicating the tier level of the cloud. It also has an identifier for the cloud (MyCloudID). The CloudAddr for the top tier clouds starts with a tier value 1, followed by a MyCloudID. Since ISP A is the first cloud in tier 1, it is assigned a CloudAddr as 1.1 in the format of TierValue.MyCloudID. Similarly, ISP B has a CloudAddr as 1.2. More generally the identifier for a cloud inherits from its parent clouds. Thus the CloudAddr of a cloud is a function of its tier and the parent cloud, and follows the format: TierValue.ParentCloudID:MyCloudID, where the second field identifies the parent's CloudAddr (without the TierValue). In this case the TierValue depends on the tier level at which a network cloud connects to a parent's CloudAddr and will be one greater than the TierValue of its parent. Thus, ISP C at tier 2, through its connection to ISP A acquires a CloudAddr 2.1:1. At the same time, through its connection to ISP B, ISP C also acquires the CloudAddr 2.2:1. ISP D, which is connected to ISP B via CloudAddr 2.2:2, may decide to change its service provider to ISP C by moving to tier 3, or remain simultaneously connected to ISPs B and C, by using two CloudAddrs at different tiers. Clearly, CloudAddrs should allow for easy movement across tiers provided the internal operation and structure of a cloud is not tied to the CloudAddr.

Structured Packet Forwarding

The TierValue, which is the first field in a CloudAddr, is used to decide the direction of packet forwarding, which depends on the relative positions of the source (SRC) and destination (DST) clouds in the tier structure and the links between sibling clouds in a tier. For example in Figure 1, if the SRC cloud is *3.1:1:1* and the DST cloud is *2.2:2* at the source a comparison is made between the two addresses to determine the tier of a common parent (or grandparent) cloud for the SRC and DST. In this case, it will be a tier '1' cloud as there are no address components after the TierValue common in the SRC and DST CloudAddrs. The remaining fields in the DST address (after the common part) are then appended to the TierValue to provide the forwarding address. In this case the forwarding address will be *1.2:2* (Tuncer, Nozaki, and Shenoy, 2012).

All intermediate clouds between *3.1:1:1* and the tier 1 cloud, will forward the packet upwards, using only the tier value until it reaches cloud *1.2*. Cloud 1.2 then identifies the destination to be at tier 2 because of the two address fields after the TierValue replaces the TierValue with *2* and forwards the packet down to the DST cloud. However if a trunk link (dotted double arrows in Figure 1) existed between ISP C and ISP D, the border routers will have entries of their peer network clouds and can forward the packet directly to ISP D. Tier-based inter-cloud routing requires routing knowledge that is linearly proportional to the number of directly connected clouds. In other words, large routing tables can be eliminated in the TFC model. However, a large number of tiers can result in long CloudAddrs. Nesting described below provides better and granular cloud and CloudAddr management and contain unwieldy address lengths.

Cloud Nesting

Assume that ISP 1 with CloudAddr 1.1 Fig. 1 shows a representative AT&T network. This network which is considered tier 1 from a global perspective, can internally house several 3-tier structure for each of its POPs.

In Figure 2, the 3-tier structure in the Seattle POP is shown with the backbone (BB) clouds at tier 1, the distribution (DB) clouds at tier 2 and the access (AC) clouds at tier 3. Clouds can be nested within a cloud. The internal tiers and CloudAddr have a local scope within the AT&T network. Packet forwarding between the notional POPs can follow a process similar to that outlined earlier for ISP network clouds. However, when packets are to be forwarded outside of the AT&T network, the ISP's CloudAddr has to be pre-pended to identify the originating ISP network to facilitate forwarding across ISP clouds. For example a packet from AC cloud 3.1:1:1 that leaves the AT&T ISP network would have an address 1.1{3.1:1:1}, where the

curly brace is a notation for nesting of tiered addresses. The nested address is directly accessible from outside of the AT&T cloud, which makes the proposed nesting concept different from and more powerful than Network Address Translation (NAT).

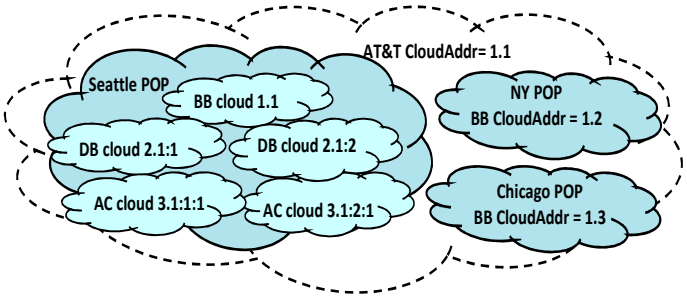

Figure 2: Nested Clouds and Addresses

EMBEDDED SECURITY AND PRIVACY CONTROLS IN THE CLOUD

Nesting clouds can be used to implement a set of built-in security and privacy controls, as well as factor in a trust rating that will enable our interaction paradigm to create a more dynamic and protected Internet relationship among entities.

Security and Breach Isolation

Security breach or fault isolation is highly complex in the current Internet due, in part, to the intricate logical addressing, which makes the detection and location of malusage difficult. Monitoring capabilities are currently difficult to implement with the current internetwork model (i.e., a highly meshed structure), as it lacks a sense of traffic flow. However, with the TFC model, as can be noticed in the data forwarding example illustrated in Figure 1, the structured connections between the network clouds through the tiered addresses will allow for identifying the traffic flow as arriving from a particular network cloud, due to path information inherent in the tiered address. The structured tiered addresses enable each network cloud to trace-back the origin of the misbehavior, if the proper monitoring mechanism is in place.

Moreover, in the TFC model, the security or breach isolation can be made more powerful through the Cloud Sizing concept. The granularity and modularity in the network cloud can allow for appropriate monitoring and disciplining at every network cloud suited to its operation and functions. For example, within a stub network the distribution clouds can monitor the traffic and behavior of access clouds and the border network clouds.

Privacy with Nesting

We must balance the TFC model security monitoring component with the need for privacy for successful model adoption. An Internet user may wish to be identified to make online credit card purchases in order to verify the transaction while being able to anonymously surf the web for news. However, with today's internetwork model, the IP address assigned to each user is many times used as the user's identification, which is bound with the user's physical location or organization.

With the TFC model, the built-in address nesting features provides inherent privacy protections. Figure 3, which extends the tiered addresses and nesting property to stub networks connected to ISP A and ISP C (Figure 1), demonstrates how a user can control his or her individual identity through nesting.

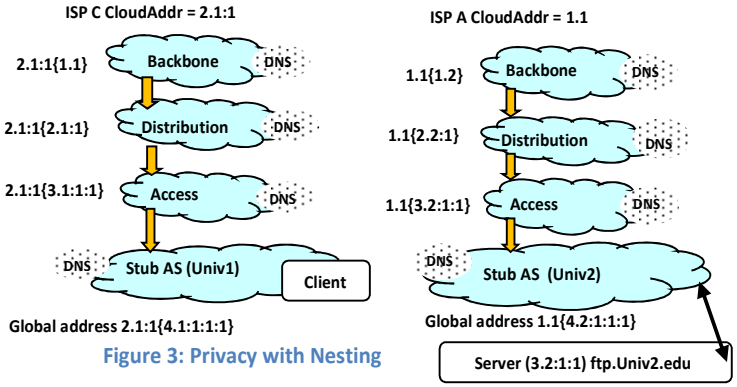

Figure 3: Privacy with Nesting

In Figure 3, the Server at Univ2 is known by its global name ftp.Univ2.edu. A client in Univ1 would like to access ftp.Univ2.edu. However this name has to be resolved. The query can be directed upwards till one of the DNS servers is able to resolve the name. As per the proposed nesting properties, we allow DNS servers to provide partial name resolution. For example, the DNS at Backbone cloud 2.1:1{1.1} is able to resolve only up to Univ2.edu. It will then return a response to the query as 1.1{4.2:1:1:1{ftp}}, where the name is still carried as part of the server address. This is made possible by the nested addresses, as there is no restriction on the type of identity (or name) used in the address as long as it is scoped. The client can then send its service request using this partially resolved address, which will eventually be resolved at the DNS at stub AS Univ2. The server may then decide to reveal its address based on the authenticity of the client. A similar process may be extended to all devices in a stub AS, lending all users privacy. Determining authenticity is factored in part from the entity's Trust Rating (TR).

CLOUD TRUST RATING

We propose a Trust Rating (TR) model that measures and assigns a score to each user, ISP, web service provider, or a network agent. The TR model indicates a particular entity's ability to enter into an interaction with another entity. The TR score is established via three (3) components: privacy, security, and social input. Any entity wishing to establish a relationship with another can use individual components to set baselines and rely on overall TR to facilitate continued transactions. In this paper we discuss the Trust Rating model. Subsequent research involves creating the mechanisms to facilitate assisted, as well as automated rating techniques.

Determining TR Component Score

In order to assign a measureable score to each of the TR components, we must first look at the criteria used to measure each component. Many of these evaluation criteria overlap our constituencies of user, service provider, and infrastructure provider; however, items such as privacy policies and practices, are distinctly in the realm of providers though they may be expressed in different forms (e.g., data sharing versus data shaping). These criteria are evaluated using a set of heuristics shown in Table 1 that will be embedded in a software agent or a reporting mechanism to be developed at a later date.

Privacy

The user privacy criteria centers on protecting individual data whereas service and infrastructure providers center on protecting all data. It should be noted that service providers are only responsible for their particular data sets and transmissions, whereas the data protection scope is much larger for infrastructure providers.

Privacy in interconnected networks continually balances between adequate information sharing and protection of data. Researchers have focused on the security within network interaction (Chang, Wu, and Tan, 2011; Parris and Henderson, 2012) as well as the complications and challenges involved when social connections and data sharing are major transactions (Moscaritolo, 2010; Van Eecke and Truyens, 2010). As such, privacy must be considered as one of the main criteria in determining a trust rating whether it is between ISP/ISP, ISP/user, or user/user interactions.

Security

Protecting system integrity and data is a major focus of security. These criteria are more prescriptive for the user than the service and infrastructure provider only because we provide more of a baseline for users, expressed via planned configuration rules in their software agents. On the provider level we examine Security Policies and Plans and, subsequently, their procedures for handling incident and disaster scenarios.

There is an abundance of research focusing on networking security. What interests us most is data sharing and communication among the various entities. In order to make sure that transactional security is in place, we look to research that focuses on the intersection of entities and the negotiation between them within the negotiated trust interaction (Ahn, Shehab, and Squicciarini, 2011; Strassmann, 2010).

Social Input

Although a relatively new component in evaluation frameworks, our social input measurement harnesses collected data on trust relationships expressed through social contracts, as well as various interaction evaluations collected via planned software agent reporting to determine how well an entity performs with other entities. Think of these as user ranked, as well as automated, recommendation systems such as the Facebook "like", Google+ or Reddit recommendation.

Researchers are just beginning to examine this rich interaction among connected entities. Most research looks to previous studies on e-commerce and Web site trust rankings via feedback mechanisms such as the Web of trust (Kim and Phalak, 2012; Zhang, Cohen, Zhang, and Cohen, 2007). Others have applied these input mechanisms to social networks in order to measure trust relationships (Kim and Song, 2011; Lesani, Montazeri, Lesani, and Montazeri, 2009; Yuan, Guan, Lee, and Lee, 2010). Whatever the case, we must look at the social interaction ranking as a means to establish the trust relationship.

Privacy Component Evaluation Criteria		
User	**Service Provider**	**Infrastructure Provider**
• Strict Identity Policies • Robust Identity Procedures • Strong Identity Management Practices • Low-to-No Peer Identity Leakage Incidents	• Transparent Privacy Policies • Well-defined Privacy Procedures • Strict Personal Data Practices • No Personal Data Leakage Incidents	• Device-Readable Transparent Privacy Policies • Well-defined Privacy Procedures • Strict Data Practices • No Data Leakage Incidents
Security Component Evaluation Criteria		
• Current Security Software Patches Installed • Anti-Virus Software Installed with Updated Definitions • Anti-Malware Software Installed with Updated Definitions • Software Firewall Installed • No Rogue Ports Open	• Comprehensive Security Policies and Plans • Secure Data Transmission Procedures • Secure Data Storage Procedures • Gateway Scanners to Detect Malware Intrusion • Firewall to Thwart Malware Intrusion • SPAM Filtering (for mail service providers) • Web Malware Scans	• Comprehensive Security Policies and Plans • Gateway Scanners to Detect Malware Intrusion • Stateful Packet Inspection to Guard against Network Floods
Social Input Component Evaluation Criteria		
• Number of Social Contracts Entered and Maintained • Peer-reported Evaluations of Interactions • Service-reported Evaluations of Interactions • Infrastructure-reported Evaluations of Interactions	• Number of Social Contracts Entered and Maintained User-reported Evaluations of Interactions • Peer-reported Evaluations of Interactions • Infrastructure-reported Evaluations of Interactions	• Number of Social Contracts Entered and Maintained • User-reported Evaluations of Interactions • Service-reported Evaluations of Interactions • Peer-reported Evaluations of Interactions • Internal Cloud Evaluations of Interactions

TABLE I: TR Components

An Example of Calculating the TR

In order to calculate the TR, each of the above components is assigned a value between 0.00 - 5.00. From these values, an average score is calculated to present an overall TR. However, all agents that provide TR scoring must also track each individual component. Otherwise, a TR can be misleading. Let's look at two examples to illustrate this point:

Service Provider A has a checkered record in its past. Although operating for a period of years with a good security baseline, it has divulged some user information to other entities. Users are not pleased and reduce the social component score for this breach of trust, and user information leakage also damages the Service Provider's privacy score resulting in a low TR: [**Privacy: 2.00 x Security: 3.00 x Social Input: 2.00 = 2.33**]

A new service provider--Service Provider B--publishes transparent privacy policies and makes its policies readable via the P3P schema. This effort earns the provider a 4.00 on the privacy component. The service provider also offers high-level encryption for transactions and data storage thereby earning a 4.00 on the security component. However, since this service provider is new to the market, its social input rating is low. This results in a TR that, on first examination, only appear marginally better than Service Provider A: [**Privacy: 4.00 x Security: 4.00 x Social Input: 0.00 = Trust Rating: 2.67**]

A user would not readily see the difference between doing business with these two entities by simply viewing the TR. Therefore, users wishing to try this new provider need to benefit in some manner. As a result of a user entering into a social contract with Service Provider B, she will earn a bit more on her social input scale than she would with an established provider. Entities, such as users, will be able to set their risk aversion tolerances within their individual software agents to assist with these decisions. To avoid confusion, software agents factor each component score and weigh them accordingly.

TFC Trustworthiness Applied

The TFC model can essentially resolve well-known threats such as SPAM and distributed denial of service (DDOS). For example, to resolve the SPAM issue, the TFC model can force the lower rated mail senders to deliver email using the pull technique while allowing higher rating ones push emails to a receiver's inbox. In other words, for a lower rating sender, say LS, the cloud will only deliver a short and limited notification to the intended receivers and the email bodies LS send out will stay in LS's mail outbox. Unless the interested receivers pull the email explicitly, the email body will not flow across the clouds. Certainly the pulling process can help raise or degrade the rating of LS, which in turn serves as an implicit incentive for LS to reduce SPAM. Similarly, the aforementioned cloud monitoring and isolation can be used for quick identification and recovery from such attacks.

The TFC model, in conjunction with novel rating schemes, also enables us to rate the clouds, providers and users. For instance, if the misbehavior of the stub AS was unnoticed by the AC cloud, it may still be caught by the DB cloud. In this case, the DB cloud would degrade the rating of the AC cloud, thus imposing a penalty on a cloud for missing the detection of a security breach. This recursive monitoring can be used to enforce discipline in network clouds, thus forcing them to monitor and discipline their child clouds. The incentive to monitor child clouds derives from the fact that based on the POP's behavior it could be rated by its neighbor clouds or peers. Top tier clouds can influence clouds in tiers below them by imposing a penalty for failure of service and malpractice to enforce cloud rating.

INCENTIVIZING THE CLOUD

In order to encourage innovation and growth of the Internet, we empower the TFC model with social and economic incentives for users and service providers. Users must want their devices to meet baseline specifications (e.g., updated anti-virus) and service providers must want to implement secure options and transparent privacy policies. If users are rewarded for taking security precautions, as well as managing their privacy options via software agents, they will be rewarded via increased service offerings as well as economic incentives from providers. Social contracts that help build trust relationships between user and provider need to be monitored and rewarded. Through TR mechanics, we increase security and economic benefits via social contracts while simultaneously discouraging rogue behavior.

Clouds not only have choices to various paths to route data but also to types of data they choose to relay according to the TR among providers. With the TR in place, users can choose to form social contracts with various ISPs and Web services. Moreover, we can extend the social choice interactions among users as well via Secure Social Choice Mechanisms (SSCM).

Secure Social Choice Mechanisms (SSCM) for Choices and Incentives

We should strive to allow a user the maximum choice in flexibility as long as data and transactions are not put at risk. However, we must also balance the reliability and trustworthiness of the interactions among participants, as well as the network connections within our overall TFC model against the security requirements whether they be user requested (e.g., identity obfuscation) or set via transaction negotiation (e.g., high assurance).

However, the balance does not need to be one of binaries. A user should not need to choose privacy over security thereby removing her from desired connections or services. For example, she should not need to provide more personal identifiable information to an unknown service without knowing 1) why the personal information is needed, 2) what privacy protections

are in place, and 3) how secure the service's operations are in terms of protecting her information initially and over time.

We solve this dilemma by implementing a means to allow for more transparent social negotiations between two entities. As with all relationships, there needs to be a set of baseline security, privacy, and interaction assurances that meet users' expectations, but going beyond these baseline assurances will take place as trust relationships are formed and mature. We can accomplish this initial assurance with a Trust Rating factored with a set of parameters within SSCM to implement fine-grained decisions.

Social Engineering to Incentivize Trust

Without benefits, users would have no reason to move into new social contracts and entities would have no reason to improve. Motivating individuals to negotiate and form relationships for increasingly complex interactions must be accomplished by providing each person the incentive to want to keep security levels far above baseline requirements, as well as complete more assured social contracts for value-added interactions. Moreover, providers must be enticed to invest resources (time and funds) to create increasingly secure paths, as well as complete and transparent privacy policies.

The TR accomplishes this in many ways. With a higher rating an individual can access more services with a decreased economic cost over time. Providers also benefit with a higher TR as each provider moves to the "top" of both other providers' as well as users' "lists" with a higher rating. Moreover, providers will benefit from increased interaction with users with higher TRs as well.

CREATING SOCIAL ECONOMIC MODELS FOR THE CLOUD

The TFC model combined with the Trust Rating system yields new levers to providers that can be used to improve management of risks underlying security, privacy and trust issues for their domains. An improved approach to management of these risks will help reduce the social cost from the externalities created by these risks for users and providers alike. The TR systems can be used to build a monetary incentive and disincentive structure for the information highways, much akin to traffic police penalizing reckless and dangerous driving. Finally, formal service guarantees designed for security and privacy features make cooperation between providers possible to facilitate end-to-end security and privacy for users. Therefore, the TFC and SSCM help agents design robust security solutions, and make economically sound, responsible, and responsive decisions for their and other's security and privacy.

Effectiveness of proposed Trust Rating for Assessment of ISP Internal Risks

The TFC model and SSCM provide many valuable degrees of freedom and channels of information for enhancing security and privacy risk assessment, as making a clear and reliable assessment of risks, their sources and their impact on an enterprise is fundamental for enterprise risk management. A network service provider would be able to observe and monitor the TR of its customer base, as well as that of its peering network service providers. The deteriorating TRs are a signal of enhanced risk, therefore the ISP would benefit from the evolving TR profile of its environment. Similar to the notion of Credit Rating and Credit Scoring System in banking, TRs can assign probabilistic measures for realized threat events and episodes. As in the Credit Migration Methodology, the evolution of a provider's TR profile can assess the changing profile of vulnerabilities and implication on probabilistic measure of realized threat events and episodes. Good predictive capability of the TR system makes the system a valuable tool to support risk management.

Risk Management of Service Providers' Internal Security and Privacy Risks

Classic risk management methodologies, built on the 'avoid, mitigate, transfer, keep' paradigm, have established solid conceptual framework and rich guidelines for security risk management of a general enterprise. But an ISP is a unique enterprise at the very core of provisioning information security and privacy, being the backbone for computing, information and communications infrastructure. Availability of metrics and levers under the TFC and the SSCM by which to assess and manage security and privacy risks strongly facilitates an ISP's risk management process. Benefits of the risk management process improve the enterprise's bottom line and provide insight into the value of investment for security and privacy.

ISP's internal risk analysis also provides an understanding of the effectiveness of our TR system in assessing security and privacy risk exposure of the provider. The features of the TFC, namely modularity and granularity in definition of clouds, flexibility in cloud connection, ability to nest and decouple for inter- and intra-cloud operations, breach isolation, nested addressing for privacy, are each very beneficial for the avoid-mitigate-transfer-keep decisions underlying risk management. Interfacing the TR driven SSCM with the features of the TFC, promotes the development of risk management strategies for an ISP to mitigate and control its security and privacy risk exposures. These strategies can involve actions like, cloud rating resetting, cloud promotion/demotion in the tier-structure, cloud isolation, routing modifications, and internal penalties.

Assessment of Social Cost Reduction under the SSCM

Security, Privacy and Trust in the information and communication systems domain from any entity's perspective is ridden with externalities. Network insecurity is like air pollution or congestion, where people who connect insecure machines to the Internet expose others to the consequences of their actions (Anderson and Moore, 2007). Conversely, if an entity takes some protective measures, it can create positive externalities for others that can discourage them from making the necessary investments for safe choices. However, the TR-supported SSCM addresses this moral hazard issue by responding to the actions in the form of penalties and rewards in terms of deterioration or improvement in the TR. Thus, actions of an entity that affect its security, privacy and social input ratings, result in consequences giving a reason to all entities to become more accountable for their actions and decisions.

ISP's investments towards risk management based on the TFC-supported SSCM would create positive externalities from which all stakeholders will benefit. Significant overall benefit and social cost reduction will be realized from ISPs and other service providers adopting more risk-aware and risk-responsive business practices.

Monetary Incentives, Penalties and Guarantees under the SSCM

The risk management objectives of the ISPs and other providers are motivated by improving their own bottom line, which is a solid incentive. While these investments may result in positive externalities for other users and providers, they may not by themselves motivate them to adopt more risk-aware and risk-responsive choices towards each other. Explicit mechanisms to promote good behavior and reduce negative externalities on the information highways can be implemented by a reward and penalty structure for users, individual and institutional, for their choices and actions on the information internetworks. Rather than a reactive response plan that responds to the threats a posteriori after an encounter with an unfavorable event, the goal is to create an incentive structure that instills responsible behavior in all stakeholders so that the unfavorable events are entirely eliminated or minimized. The ideas behind cap and trade mechanisms for carbon dioxide and other greenhouse gases (Camp and Wolfram, 2004) can be applied in the security and privacy threats domain. A combination of severity of threat and level of TR of an entity will determine the 'security' tax or credit to be levied. The 'security' tax or credit models can guide the security and privacy guarantee terms in the contracts designed for provider cooperation for end-to-end services.

CONCLUSION

The SCIMES model provides the necessary framework, components, and interaction mechanisms to transform the Internet into a more secure, robust, reliable and value-added endeavor for infrastructure and service providers, as well as users. The modularity and flexibility in the SCIMES cloud and tiered concept supports better security and privacy options. Trust ratings enabled by this new model will provide the Internet community with a means to measure each other's security, privacy, and social input (reflected by community ratings) to decide with whom they most want to interact and build and foster trust relationships. These social interactions based on the TR negotiation will be encouraged through increased services and economic incentives available to users with high TR score. Moreover, the SCIMES model encourages innovation and healthy competition among providers while still requiring stronger security and privacy controls that will benefit, rather than hamper economic strides.

REFERENCES

1. Ahn, G.-J., Shehab, M., and Squicciarini, A. (2011). Security and Privacy in Social Networks. *Internet Computing, IEEE*, *15*(3), 10 –12. doi:10.1109/MIC.2011.66
2. Anderson, R. and Moore, T. (2007). "The Economics of Information Security: A Survey and Open Questions," in Fourth Bi-annual Conference on the Economics of the Software and Internet Industries, Toulouse, France, January 19-20.
3. Breslin. J. and Decker, S. (2007). "The Future of Social Networks on the Internet: The Need for Semantics," IEEE Internet Computing, vol. 11, no. 6, pp. 86-90.
4. Camp, L.J. and Wolfram, C.D. (2004). "Pricing Security: Vulnerabilities as Externalities," Economics of Information Security, vol. 12, 2004. [Online]. http://ssrn.com/abstract=894966
5. Chang, W., Wu, J., and Tan, C. C. (2011). Enhancing Mobile Social Network Privacy. *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* (pp. 1 –5). doi:10.1109/GLOCOM.2011.6133610
6. Clark, D., Wroclawski, J., Sollins, K.R., and Braden, R. (2005). "Tussle in cyberspace: defining tomorrow's Internet," IEEE/ACM Transactions on Networking, vol. 13, no. 3, pp. 462-475.
7. Hasan Tuncer, Yoshihiro Nozaki, Nirmala Shenoy, "Virtual Mobility Domains – A Mobility Architecture for the Future Internet," Symposium on Next Generation Networks, IEEE International Conference on Communications, June 10-15 Ottawa Canada, 2012
8. Kim, Y. A., and Phalak, R. (2012). A trust prediction framework in rating-based experience sharing social networks without a Web of Trust. *Information Sciences*, *191*, 128–145. doi:10.1016/j.ins.2011.12.021
9. Kim, Y. A., and Song, H. S. (2011). Strategies for predicting local trust based on trust propagation in social networks. *Knowledge-Based Systems*, *24*(8), 1360–1371. doi:10.1016/j.knosys.2011.06.009
10. Lesani, M., Montazeri, N., Lesani, M., and Montazeri, N. (2009). FUZZY TRUST AGGREGATION AND PERSONALIZED TRUST INFERENCE IN VIRTUAL SOCIAL NETWORKS, FUZZY TRUST AGGREGATION AND PERSONALIZED TRUST INFERENCE IN VIRTUAL SOCIAL NETWORKS. *Computational Intelligence, Computational Intelligence*, *25, 25*(2, 2), 51, 51–83, 83. doi:10.1111/j.1467-8640.2009.00334.x, 10.1111/j.1467-8640.2009.00334.x
11. MacKie-Mason, J. (2009). "Incentive-Centered Design for Security," IEEE Security and Privacy, vol. 7, pp. 80-83.
12. Oliveira, R., Lad, M., and Zhang, L. (2009). "Understanding the Challenges in Securing Internet Routing," in the Ninth Annual International Symposium on Applications and the Internet, 2009, pp. 145-148.
13. Moscaritolo, A. (2010). Privacy and the Social Network. *SC Magazine*, *21*(4), 16.
14. Parris, I., and Henderson, T. (2012). Privacy-enhanced social-network routing. *Computer Communications*, *35*(1), 62–74. doi:10.1016/j.comcom.2010.11.003
15. Schulzrinne, H. (1997). "Internet Technology Series," IEEE Communications Magazine, vol. 35, no. 6, pp. 158-158, 1997.
16. Shenoy, N., Yuksel, M., Gupta, A., Kar, K., Perotti, V., and Karir, M. (2010). "RAIDER: Responsive Architecture for Inter Domain Economics and Routing," in FutureNET II workshop, Globecom , 2010.
17. Strassmann, P. A. (2010). Social (Network) Security. *Signal*, *64*(5), 49,51,53.
18. Valancius, V., Feamste, N., Rexford, J., and Nakao, A. (2010). "Wide-Area Route Control for Distributed Services," in USENIX Annual Technical Conference, 2010.
19. Van Eecke, P., and Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, *26*(5), 535–546. doi:10.1016/j.clsr.2010.07.006
20. Xu, X. and Jain, R. (2009). Routing Architecture for the Next Generation Internet (RANGI). [Online]. http://tools.ietf.org/id/draft-xu-rangi
21. Yuan, W., Guan, D., Lee, Y.-K., and Lee, S. (2010). The small-world trust network. *Applied Intelligence*, *35*(3), 399–410. doi:10.1007/s10489-010-0230-7
22. Zhang, J., Cohen, R., Zhang, J., and Cohen, R. (2007). A COMPREHENSIVE APPROACH FOR SHARING SEMANTIC WEB TRUST RATINGS, A COMPREHENSIVE APPROACH FOR SHARING SEMANTIC WEB TRUST RATINGS. *Computational Intelligence, Computational Intelligence*, *23, 23*(3, 3), 302, 302–319, 319. doi:10.1111/j.1467-8640.2007.00307.x, 10.1111/j.1467-8640.2007.00307.x