www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 3 Issue 5, May 2014, Page No. 5848-5865

Mitigation of co residence profiling from malicious user through MUSSEL BEHAVIOR framework

A.P.Leela Vinodhini .M.E A.Justine Jerald M.Tech

ABSTRACT

This work focused on how a malignant user could attack customers which share physical resources and operate coresidence profiling and public-to-private IP mapping to target. Malicious user's attack: resource placement (VM) on the target's physical machine and extraction from the target's physical machine. The proposed work depends on user account and workload clustering to reduce co residence profiling by mussel self-organization. Similar user behavior and workload types are belonged to same cluster. In order to unclear the public-to-private IP map, each cluster is supervised and used by an account proxy. In this work, each proxy uses one public IP address, which is used by all clustered users when accessing their instances, and maintains the mapping to private IP addresses. This work explained set of abilities and attack paths in which an attacker needs to launch attack for targeted co residence. It shows how our approach disturbs the critical steps in the attack path for most cases and then performs a risk

assessment to determine the probability an individual user will be victimized, given that a successful non directed exploit has occurred.

Introduction

Cloud computing

cloud computing, or something being in the cloud, is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user—arguably, rather like a cloud.

Advantages of Cloud computing

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically re-allocated per demand. This can work for allocating resources to users. For example, a cloud computer facility, which serves European users during European business hours with a specific application (e.g. email) while the same resources are getting reallocated and serve North American users during North America's business hours with another application (e.g. web server). This approach should maximize the use of computing powers thus reducing environmental damage as well since less power, air conditioning, rackspace, etc. is required for a variety of functions.

The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as you use it).

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

Security and Privacy

The integrity, availability, and maintenance of appropriate confidentiality of institutional data is critical to U-M's reputation and to minimizing institutional exposure to legal and compliance risks. Much of the challenge in deciding whether cloud computing is desirable and appropriate for an institution like U-M is determining whether a prospective cloud computing vendor has adequate physical, technical, and administrative safeguards as good as or better than the local on-campus systems.

While cloud computing services have numerous potential benefits, there are also potentially significant privacy and security considerations that should be accounted for before collecting, processing, sharing, or storing institutional or personal data in the cloud. Consequently, institutions should conduct careful risk assessment prior to adoption of any cloud computing service.

Specific risks and challenges to consider include:

- Vendor transparency and inadequate or unclear service level agreement
- Privacy and confidentiality of personal, sensitive, or regulated data and information
- Legal and regulatory compliance
- Cyber security and support for incident forensics
- Records preservation, access, and management
- Service availability and reliability

Security issues associated with the cloud

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Proxy Server Cloud

- Send up to 600 Queries Per Minute to your target websites - without being detected or blocked
- Each GET Request sent on randomly rotating IP addresses, C Classes and locations from across the United States
- Every request is completely anonymous
- Compatible with most Software

Perform mass Web Scraping and Data Extraction, while completely hiding your identity and not tipping off your target sites that they're even being scraped. Every one of your Internet requests is randomly distributed across our Proxy Server network of thousands of Private Proxy Servers designed for this purpose.

You can connect your software to Trusted Proxies' Proxy Server Cloud service, and send your queries at up to 600QPM. So not only can you extract the business intelligence data you need without getting blocked, you can do it really fast too!

CloudProxy is a new service NOT included in the regular Sucuri plans (extra monthly charge). It is a powerful web application firewall (WAF) that functions as a filter between your website and all your visitors.

It is considered an intrusion prevention system (IPS) for websites and serves as a virtual patching and hardening mechanism for those unable to update their websites. This product is ideal for anyone that values the reputation of their website and cannot afford to get hacked or compromised.

Features

The number one focus of this product is Website Security. There are some other good side effects that you will be able to take advantage of right off the bat. They include improved performance and better uptime. Our cloud proxy includes:

- Traffic filtering (blocking malicious requests)
- Virtual patching
- Virtual hardening
- WAF (Web application firewall) - To prevent SQL injections, XSS, RFI, etc)
- IDS/IPS (Intrusion prevention system)
- Extended access control (white listing of IPs allowed to go to the admin pages)
- OSSEC HIDS (Full log analysis and traffic monitoring)
- Improved performance and caching
- Fully managed.

Workload

Workload is an abstraction of the actual work that your instance or a set of instances are going to perform. Running a web server or a web server farm, or being a Hadoop data node - these are all valid workloads.

Workloads by themselves may have properties or attributes that could dictate where workload can or can't run. This justifies existence of a workload as a separate entity - it is in theory possible to construct a workload for which no deployment can exist in any of the clouds available today.

There are many examples what kind of attributes a workload may possess. A workload may have a compliance attribute, which says that this workload must run in an environment with a certain certification. Another attribute may be a geo location requirement, whereas it must run within a certain geographic region for a legal reason.

A workload may be time-bound ("runs for 5 hours") or time-unbound. A workload may have a specific start time or flexible start time, in which case it may have a hard stop time (for example, must finish by a certain time in the future). It can be interruptable or must run without interruptions.

A workload may have a certain lower limit of resources that it needs, expressed in work-

independent form. For example, serving Wordpress blog for 1 visitor a day as opposed to 100 visitors an hour are two very distinct workloads.

Workload may have a budget associated with it, it may have redundancy requirements. It may require a certain OS or distribution. It may require a certain feature (for example, persistent disk or non-private IP address directly attached to eth0). It may require a certain minimal access speed to some data source (for example, if my data are in S3 on the East coast, I may want my workload to run somewhere near). Each requirement is a restriction - the more requirements a workload has, the fewer clouds can potentially run it.

REVIEW OF LITERATURE

1. Cloud Computing Security Issues and Challenges

When a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power.

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted.

From one point of view, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers.

This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system. The following section highlights a brief review of literature on security issues in

cloud computing and the remaining sections are organized as follows. Section 3.0 discusses security issues in cloud computing laying emphasis on SaaS, PaaS and IaaS; and cloud computing deployment methods. Section 4.0 deliberates on associated cloud computing challenges; and Section 5.0 presents the conclusion.

DISADAVANTAGES

- Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing;
- It extends Information Technology's (IT) existing capabilities
- In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry.
- Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers.

2. Cooperative problem solving in a social carnivore

Numerous field researchers have described cooperative hunting in social carnivores, but experimental evidence of cooperative problem solving typically derives from laboratory studies of nonhuman primates. We present the first experimental evidence of cooperation in a social carnivore, the spotted hyena, Crouton crocus. Eight captive hyenas, paired in 13 combinations, coordinated their behavior temporally and spatially to solve cooperation tasks that modeled group-hunting strategies. Unlike many primates that cooperate infrequently or require extensive shaping, spotted hyenas' displayed a natural aptitude for teamwork: all teams achieved success rapidly, repeatedly, and without specific training.

Social influences on cooperative performance included an audience effect that could influence party formation and hunting success in the wild. Performance also varied across dyads, notably with rank related aggression between partners impairing performance. Efficiency improved as partners increasingly attended to one another and coordinated their actions. Lastly, experienced cooperators modified their behavior to accommodate a naı¨ve companion, using visual monitoring and tracking to promote coordination. We suggest that social carnivores should be considered relevant models for the study of cooperative problem solving, as their abilities provide a comparative framework for testing theories about the mechanisms of social learning and the evolution of intelligence.

Animal cooperation has held significant interest to evolutionary biologists and comparative psychologists, particularly with regard to understanding the cognitive implications of cooperation in our own species. In experimental

studies of cooperative problem solving, at least two animals must jointly perform similar or complementary actions to obtain a food reward.

For animals to be considered 'cooperators' within this paradigm, partners must pursue their common goal while taking account of each other's behavior The level of behavioral organization between participants can vary, increasing in temporal and spatial complexity from mere similarity of action, to synchrony (similar acts performed in unison), then coordination (similar acts performed at the same time and place), and finally collaboration.

For over seven Decades, such studies have focused almost exclusively on nonhuman primates reflecting a general premise that higher-order cognitive functioning in large-brained or highly encephalized animals should enable organized teamwork. Curiously, however, primates are often inefficient at solving cooperation problems in the laboratory, potentially reflecting a weak tendency to cooperate for food in nature.

We therefore asked whether species that cooperate for food more routinely in the wild, such as social carnivores, might better meet the criteria of cooperative problem solving in the laboratory. In three successive experiments, we tested captive spotted hyenas', Crouton crocuses, for evidence of synchrony and coordination during cooperative problem solving, social modulation of cooperative performance and behavioural adjustment between cooperating partners.

DISADVANTAGES:

- We present the first experimental evidence of cooperation in a social carnivore, the spotted hyena, Crouton crocus.
- Unlike many primates that cooperate infrequently or require extensive shaping, spotted hyenas' displayed a natural aptitude for teamwork: all teams achieved success rapidly, repeatedly, and without specific training.

- Social influences on cooperative performance included an audience effect that could influence party formation and hunting success in the wild.

- Curiously, however, primates are often inefficient at solving cooperation problems in the laboratory, potentially reflecting a weak tendency to cooperate for food in nature.

- the cognitive implications of cooperation in our own species. In experimental studies of cooperative problem solving, at least two animals must jointly perform similar or

complementary actions to obtain a food reward.

3. Crowds: Anonymity for Web Transactions

The lack of privacy for transactions on the world-wide-web, or the Internet in general, is a well-documented fact While encrypting com- medication to and from web servers (e.g., using SSL can hide the content of the transaction from an eavesdropper (e.g., an Internet service provider, or a local system administrator), the eavesdropper can still learn the IP addresses of the client and server computers, the length of the data being exchanged, and the time and frequency of exchanges. Encryption also does little to protect the privacy of the client from the server. A web server can record the Internet addresses at which its clients reside, the servers that referred the clients to it, and the times and frequencies of accesses by its clients.

With additional effort, this information can be combined with other data to invade the privacy of client seven further. For example, by automatically fingering the client computer shortly after an access and comparing the idle time for each user of the client computer with the server access time, the server administrator can often deduce the exact user with high likelihood. Some consequences of such privacy abuses are described

The anonymity provided by Crowds is subject to some caveats. For example, Crowds obviously cannot protect a user's anonymity if the content of her web Trans- actions reveals her identity to the web server (e.g., if the user submits her name and credit card number in a web form). More subtly, Crowds can be undermined by executable web content that, if downloaded into the user's browser, can open net- work connections directly from the browser to web servers, thus bypassing Crowds altogether and exposing the user to the end server.

In today's browsers, such ex- excitable content takes the form of Java applets and ActiveX controls. Therefore, when using Crowds, it is recommended that Java and ActiveX be disabled in the browser, which can typically be done via a simple preferences menu in the browser. The rest of this paper is structured as follows. Roundworm to compare our approach to other approaches to anonymity in We describe the basic Crowds mechanism in analyze its security in We describe the performance and scalability of our system in respectively.

DISADVANTGES

- A web server can record the Internet addresses at which its clients reside, the servers that referred the clients to it, and the times and frequencies of accesses by its clients.
- Encryption also does little to protect the privacy of the client from the server
- The server administrator can often deduce the exact user

with high likelihood. Some consequences of such privacy abuses are described

- Crowds can be undermined by executable web content that, if downloaded into the user's browser, can open net- work connections directly from the browser to web servers, thus bypassing Crowds altogether and exposing the user to the end server.

4. Searching for SNPs with cloud computing

Improvements in DNA sequencing have made sequencing an increasingly valuable tool for the study of human variation and disease. Technologies from Illumines (San Diego, CA, USA), Applied Biosystems and 454 Life Sciences (Branford, CT, USA) have been used to detect Genomic variations among humans to profile methylation patterns to map DNA-protein interactions and to identify differentially expressed genes and novel splice junctions meanwhile, technical improvements have greatly decreased the cost and increased the size of sequencing datasets.

A single Illumined instrument was capable of generating 15 to 20 billion bases of sequencing data per run. Illumine has projected that its Instrument will generate 90 to 95 billion bases per run by the end of 2009, quintupling its throughput in one year. Another study shows the per-subject cost for whole-human re-sequencing.

Declining rapidly over the past year which will fuel further adoption. Growth in throughput and adoption are vastly outpacing mprovements in computer speed, demanding a level of computational power achievable only via large-scale parallelization. Two recent projects have leveraged parallelism for whole genome assembly with short reads. Simpson et al. Use Abyss to assemble the genome of a human from 42-fold overage of short reads using a cluster of 168 cores (21 computers), in about 3 days of wall clock time. Jackson and colleagues assembled a Drosophila melanogaster genome from simulated short reads on a 512-node Blue Gene/ L supercomputer in less than 4 hours of total elapsed time. Though these efforts demonstrate the promise of parallelization, they are not widely applicable because they require access to a specific type of hardware resource. No two clusters are exactly alike, so scripts and software designed to run well on one cluster may run poorly or fail entirely on another cluster.

Software written for large supercomputers like Blue- Gene/L is less reusable still, since only select researchers have access to such machines. Lack of reusability also makes it difficult for peers to recreate scientific results obtained using such systems.

An increasingly popular alternative for large-scale computations is cloud computing. Instead of owning and maintaining dedicated hardware, cloud computing offers a 'utility computing' model, that is, and the ability to rent and perform computation on standard, commodity computer hardware over the Internet. These rented

computers run in a virtualized environment where the user is free to customize the operating system and software installed.

Cloud computing also offers a parallel computing framework called Map Reduce which was designed by Google to efficiently scale computation to many hundreds or thousands of commodity computers. Hardtop is an open source implementation of Map Reduce that is widely used to process very large datasets, including at companies such as Google, Yahoo, Microsoft, IBM, and Amazon. Adopt programs can run on any cluster where the portable, Java-based Hardtop framework is installed.

This may be a local or institutional cluster to which the user has free access, or it may be a cluster rented over the Internet through a utility computing service. In addition to high scalability, the use of both standard software (Hardtop) and standard hardware (utility computing) affords reusability and reproducibility.

DISADVANTAGES:

- Though these efforts demonstrate the promise of parallelization, they are not widely applicable because they require access to a specific type of hardware resource
- The ability to rent and perform computation on standard, commodity computer hardware over the Internet
- Adopt programs can run on any cluster where the portable, Java-based Hardtop framework is installed.
- Cloud computing also offers a parallel computing framework called Map Reduce which was designed by Google to efficiently scale computation to many hundreds or thousands of commodity computers
- Lack of reusability also makes it difficult for peers to recreate scientific results obtained using such systems.

5. Security and Privacy Issues in Cloud Computing

As per the definition provided by the National Institute for Standards and Technology (NIST) "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It represents a paradigm shift in information technology many of us are likely to see in our lifetime. While the customers are excited by the opportunities to reduce the capital costs, and the chance to divest themselves of infrastructure

management and focus on core competencies, and above all the agility offered by the on-demand provisioning of computing, there are issues and challenges which need to be addressed before a ubiquitous adoption may happen.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. There are four basic cloud delivery models, as outlined by NIST, based on who provides the cloud services. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services.

These four delivery models are:

(i) Private cloud in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.

(ii) Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service.

(iii) Community cloud in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

These services may be managed by the organizations or a third party and may exist offsite. A special case of community cloud is the Government or G-Cloud. This type of cloud computing is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role).

(iv) Hybrid cloud which is a composition of different cloud computing infrastructure (public, private or community). An example for hybrid cloud is the data stored in private cloud of a travel agency that is manipulated by a program running in the public cloud.

From the perspective of service delivery, NIST has identified three basic types of cloud service Offerings. These models are:

(i) Software as a service (Sais) which offers renting application Functionality from a service provider rather than buying, installing and running software by the user.

(ii) Platform as a service (Peas) which provides a platform in the cloud, upon which applications can be developed and executed.

(iii) Infrastructure as a service (Iasi) in which the vendors offer computing power and storage space on demand.

From a hardware point of view, three aspects are new in the paradigm of cloud computing these aspects of cloud computing are:

(i) The illusion of infinite computing resources available on demand, thereby eliminating the need for cloud computing users to plan far ahead for provisioning.

(ii) The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.

(iii) The ability to pay for use of computing resources on a short-term basis as needed and release them when the resources are not needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

In a nutshell, cloud computing has enabled operations of large-scale data centers which has led to significant decrease in operational costs of those data centers. On the consumer side, there are some obvious benefits provided by cloud computing. A painful reality of running IT services is the fact that in most of the times, peak demand is significantly higher than the average demand.

The resultant massive over-provisioning that the companies usually do is extremely capital-intensive and wasteful. Cloud computing has allowed and will allow even more seamless scaling of resources as the demand changes.

DISADVANTAGES

- Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service
- It represents a paradigm shift in information technology many of us are likely to see in our lifetime.
- The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.
- Platform as a service (Peas) which provides a platform in the cloud, upon which applications can be developed and executed.
- Private cloud in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.

6. Cloud Computing Security Issues in Infrastructure as a Service

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. It's a pay-per-use model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guarantees typically exploiting a pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. From one perspective, cloud computing is nothing new because it uses approaches, concepts, and best practices that have already been established. From

another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

- Security
- Privacy
- Reliability

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed it's sometimes referred to as utility computing. Infrastructure as a Service is sometimes referred to as Hardware as a Service.

Disadvantages

- The service delivery model allows the customer to rent virtualized servers.
- Associated services for running existing applications or developing and testing is risk one.
- Multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems.
- Cloud computing environment was proposed in by delegating SLA monitoring and enforcement tasks to a third party.

7. Guidelines on Security and Privacy in Public Cloud Computing

In cloud computing has rapidly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Security and privacy, however, are a concern for agencies and organizations considering migrating applications to public cloud computing environments, and form the impetus behind this document.

Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [Mel09]. Cloud computing can be considered a new computing paradigm insofar as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. Because of the implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention lately. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other practicable efficiencies. However, cloud computing is an emerging forming of distributed computing that is still in its infancy. The term itself is often used today with a range of meanings and interpretations [Fow09]. Much of what has been written about cloud computing is definitional, aimed at identifying important paradigms of use and providing a general taxonomy for conceptualizing important facets of service. Public cloud computing is one of several deployment models that have been defined. A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization. At the other end of the spectrum are private clouds. A private cloud is one in which the computing environment is operated exclusively for an organization. It may be managed either by the organization or a third party, and may be hosted within the organization's data center or outside of it. A private cloud gives the organization greater control over the infrastructure and computational resources than does a public cloud.

Disadvantages

- While not unique to cloud computing
- Logical separation is a non-trivial problem that is exacerbated by the scale of cloud computing.
- Access to organizational data and resources could inadvertently be exposed to other subscribers through a configuration or software error.

System analysis

Existing system

In existing approach can also introduce new vulnerabilities. Using the Amazon EC2 service as a case study, it is possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target.

Placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine.

Draw backs:

- Security
- Privacy

Proposed system

Similar user behavior and workload types are belonged to same cluster. In order to unclear the public-to-private IP map, each cluster is supervised and used by an account proxy. In this work, each proxy uses one public IP address, which is used by all clustered users when accessing their instances, and maintains the mapping to private IP addresses.

Advantage

- To remove the usefulness of public to private IP map
- Mitigate coresidence profiling
- Avoid malicious user from exploiting honest user which share resources.

Module description

The proposed work contains four modules.

1. Mussels behavior
2. Range density
3. Self organization approach
4. Risk assessment

1. Mussels behavior

Use the individual-based model to create a computer model which captures the clustering essence of mussel behavior. An individual mussel decides to move when its chance of movement is greater than a random value drawn from a uniform distribution. Otherwise, it maintains its current position. In the event a mussel decides to move, it takes a LW.

2. Range Density

This module is used to identify the mussel density. There are two types of range density used in mussel bed clustering model.

1. Short range density

- Euclidean distance of peers used to determine short-range density

2. Long range density

3. Self organization approach

This module is used for cloud providers to reduce the risk. The technical analysis of the mussel inspired self-organization approach towards reducing the risks. Cloud providers should obfuscate the internal structure of their services and placement policies in order complicate the adversary's attempts.

4. Risk assessment

Bayes' Theorem used to identify the likely hood of the user in Risk assessment. A risk assessment is to determine the likelihood of the event, considering that the impact of nondirected exploits is workload and user dependent. The risk assessment that suggests reduced per-individual chance of being randomly victimized given a nondirected attack.

Conclusion

This proposed work depends on mussel-inspired user account, workload clustering, and account proxies to unclear the public to private IP map and then presented arguments how our strategy increases the effort required for an opponent to carry out a directed attack against a target set. It also gave results from a risk assessment that suggests a reduced per-individual chance of being randomly victimized given a non-directed attack.

Future work

Instead of using Euclidean distance, calculate dijkstra distance for short range density

Drawback

- It can't determine the correlation between user profiles that have similar trends in tastes, but different ratings for some of the same items.
- Accuracy
- Fast

REFERENCES:

[1] M. C. Schatz, "Cloudburst: Highly sensitive read mapping with mapreduce," *Bioinform.*, vol. 25, no. 11, pp. 1363–1369, 2009.

[2] B. Langmead, M. Schatz, J. Lin, M. Pop, and S. Salzberg, "Searching for SNPs with cloud computing," *Genome Biol.*, vol. 10, no. 11, p. R134+, Nov. 2009 [Online]. Available: http://dx.doi.org/10.1186/gb-2009-10-11-r134

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph,R.Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010 [Online]. Available: http://doi.acm.org/10.1145/1721654.1721672

[4] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, vol. 8, no. 6, pp. 24–31,Nov. 2010 [Online].Available: http://dx.doi.org/10.1109/MSP.2010.186

[5] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security Privacy*, vol. 9, no. 2, pp. 50–57, Mar./Apr. 2011.

[6] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," *Computer*, no. 3, pp. 344–349, 2010 [Online]. Available: http://ieeexplore.ieee.org/xpls/absall.jsp?arnumber=5533317

[7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conf. Computer and Commun. Security (CCS '09)*, New York, NY, USA, Nov. 2009, pp. 199–212 [Online].

Available:
http://dx.doi.org/10.1145/1653662.1653687
[8] A. Colorni, M. Dorigo, and V. Maniezzo, *Distributed Optimization by Ant Colonies*. Amsterdam, The Netherlands: Elsevier, 1991, vol. 142, pp. 134–142 [Online]. Available:
http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:
Distributed+Optimization+by+Ant+Colonies#0
[9] A. E. Hirsh and D. M. Gordon, "Distributed problem solving
in social insects," *Annals Math. Artif. Intell.*, vol. 31, no. 1, pp.
199–221, 2001 [Online]. Available:
//www.springerlink.com/index/
T648V87668512N27.pdf
[10] C. M. Drea and A. N. Carter, "Cooperative problem solving
in a social carnivore," *Animal Behaviour*, vol. 78, no. 4, pp.
967–977, 2009 [Online]. Available:
http://linkinghub.elsevier.com/retrieve/
pii/S000334720900339X
[11] E. Jelnikar and I. M. Cote, "Predator-induced clumping behaviour in
mussels (mytilus edulis linnaeus)," *J. ExperimentalMarine Biol. Ecol.*,
vol. 235, no. 2, pp. 201–211, 1999 [Online].
Available: http://linkinghub.
elsevier.com/retrieve/pii/S0022098198001555
[12] M. M. Casey and D. Chattopadhyay, "Clumping behavior as a strategy
against drilling predation: Implications for the fossil record," *J. Experimental
Marine Biol. Ecol.*, vol. 367, no. 2, pp. 174–179, 2008 [Online].
Available:
http://www.sciencedirect.com/science/article/B6T8F-
4TW9WHW-
1/2/00a8aaa5177c0ceea5863d60b0591330
[13] J. Kobak, T. Kakareko, and M. Poznanska, "Changes in attachment
strength and aggregation of zebra mussel, dreissena polymorpha in the
presence of potential fish predators of various species and size," *Hydrobiologia*,
vol. 644, no. 1, pp. 195–206, 2010 [Online].
Available: http://dx.doi.org/10.1007/s10750-010-0113-2
[14] C. Shields and B. N. Levine, "A protocol for anonymous communication
over the Internet," in *Proc. 7th ACM Conf. Computer and Communications
Security (CC5'00)*, New York, NY, USA, 2000, pp. 33–42
[Online]. Available:
http://doi.acm.org/10.1145/352600.352607
[15] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions,"
ACM Trans. Inform. Syst. Security, vol. 1, no. 1, pp. 66–92,
1998 [Online]. Available:
http://citeseerx.ist.psu.edu/viewdoc/summary?
doi=10.1.1.42.2499