A compositional Approach of Web Security in Cloud Computing

[1]Sakshi Bhatia,[2]Vikram singh,[3]Deepti Gupta,[4]Ritu Yadav
[1,3,4]Technological Institute of Textile and Sciences,Bhiwani
[2]Chaudhary Devi Lal University,Sirsa

ABSTRACT

Web security has evolved along with the Web itself, and the varying threats and attacks that need to be controlled at any one time. Initially, the biggest threat to people using the Web was one of accidentally viewing inappropriate content. Cloud computing is the provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis. Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. As the cloud computing it self is the composition of different web spaces that are physically distibuted, because of this it require more securiity in terms of their integration.

1. INTRODUCTION

Web security is an ongoing concern of many site developers, browser developers and everyday users. However, the increasing use of Web Services and APIs in various contexts has led to some novel security concerns, as well as the

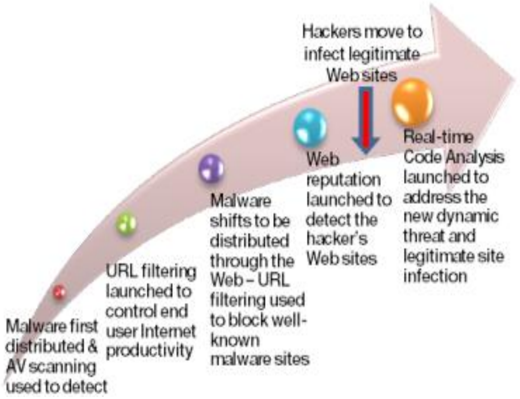

Hackers move to infect legitimate Web sites
Malware first distributed & AV scanning used to detect
URL filtering launched to control end user Internet productivity
Malware shifts to be distributed through the Web – URL filtering used to block well-known malware sites
Web reputation launched to detect the hacker's Web sites
Real-time Code Analysis launched to address the new dynamic threat and legitimate site infection

Figure 1. Web Malware Threats

As can be seen from the figure 1, the actual malware threat only shifted to the Web in the last several years, initially with the bad guys bringing up their own Web sites that were then listed by the URL filtering lists. Today, the reality is very different. Over 84% of all malware-infected Web sites are legitimate Web sites deemed to be safe by URL filtering lists. While many organizations today still consider URL filtering list-based products to be Web security solutions, in reality they are most useful for ensuring productivity. Organizations of all shapes and sizes need to be considering a secure Web gateway solution to provide effective security for Web usage.

The Web security threat has grown dramatically with Web 2.0 and the malware infection of legitimate Web sites. The social networking phenomenon has added rich social dialogue and crowd-based wisdom, but it has also provided a convenient cover to the bad guys by allowing them to capitalize on the lower suspicion level most users have when using the social network of their choice. Hence, more targeted and successful infections occur around Web 2.0 sites and activities. Other malware innovations such as polymorphic viruses have quickly emerged. In this case, the virus keeps changing itself on a regular basis to get around the signature updates.

Another example is the runtime creation of viruses which sees a different virus sample created for each user, again causing the traditional signature-based AV scanner's effectiveness to dramatically drop. In a recent study by M86 Security of 15,000 active live malicious Web sites, the combination of three leading AV scanners only yielded a block rate of 39%...combined.

1.1. Cloud Computing

Cloud computing provides cheap and pay-as-you-go computing resources are rapidly gaining momentum as an alternative to traditional IT Infrastructure. As more and more consumers delegate their tasks to cloud providers, Service Level Agreements (SLA) between consumers and providers emerge as a key aspect. Due to the dynamic nature of the cloud, continuous monitoring on Quality of Service (QoS) attributes is necessary to enforce SLAs. Also numerous other factors such as trust (on the cloud provider) come into consideration, particularly for enterprise customers that may outsource its critical data. With the advancement of the modern human society, basic essential services are commonly provided such that everyone can easily obtain access to them.

Cloud is defined as both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

Software practitioners are facing numerous new challenges toward creating software for millions of consumers to use as a service rather than to run on their individual computers. Over the years, new computing paradigms have been proposed and adopted, with the emergence of technological advances such as multicore processors and networked computing environments, to edge closer toward achieving this grand vision.

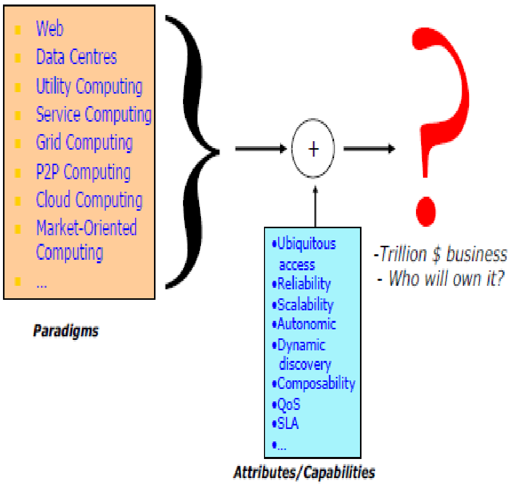


Figure 2.Various paradigms promising to deliver IT as a service.

As shown in Figure 2, these new computing paradigms include cluster computing, Grid computing, P2P computing, service computing, market-oriented computing, and most recently Cloud computing.

2. LITERATURE SURVEY

As previously mentioned, Cloud Computing is an abstraction for a complex on-demand scalable computation grid, that is accessible to users through web-enabled devices. Although the specifics of this paradigm are still being defined and revised, Cloud Computing typically consists of some basic components (e.g. CPUs, storage mediums, network interconnects, etc.) upon which any number of applications can be deployed. A Cloud Computing platform will incorporate some or all of these components, and each component has its own security concerns and issues. In recent months the interest in Cloud Computing has sharply increased, with many of the mainstay computer companies investing money and personal into research and development of both hardware and software systems. For instance, Microsoft recently announced its intention to release a Windows type operating system to run on a Cloud system. [1] Other forerunners of computing and Internet technology such as IBM [2], Google [3] and Amazon [4] are actively pursuing Cloud Computing systems. As this technology becomes more widespread and accessible, the need for proper security becomes ever more evident.

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. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public [1].

The Web Service Level Agreement (WSLA) framework is targeted at defining and
monitoring SLAs for Web Services[2].

The assertions of the service provider are based on a detailed definition of the service parameters including how basic metrics are to be measured in systems and how they are aggregated into composite metrics [3]

What's occurring is that data is being relocated into cloud services, either through database-as-a-services or applications-as-a-service[4]. cloud data storage security, which has always been an important aspect of quality of service[5].

It provides dynamically scalable geographic information technology, spatial data, and spatial applications as a web service [6]. In order to keep your enterprise secure, it is important to understand exactly how the cloud computing infrastructure works[7]

Cloud security issues focus primarily on data confidentiality, data safety and data privacy and discuss mostly organizational means to overcome these issues [8] In a Phishing attack, the attacker lures the victim to a fake Web page (either using spoofed emails or attacks on the DNS), where the victim enters username and password(s)[9].

Naive use of XML Signature may result in signed documents remaining vulnerable to undetected modification by an adversary [10]

.In [11] a method – called inline approach – was introduced to protect some key properties of the message structure and thereby hinder wrapping attacks, but shortly later in [12] it was shown how to perform a wrapping attack anyhow.

Web security has evolved along with the Web itself, and the varying threats and attacks that need to be controlled at any one time [13].

The rapid adoption of these cloud solutions has resulted in more fragmented data and the need to integrate data "in the cloud" with data in on-premise applications and databases [14]

3. SECURITY AND CLOUD COMPUTING

Cloud-based Web security can be divided into two primary architectural categories. Pure cloud Web security solutions run as software completely within Infrastructure-as-a-Service (IaaS) facilities, without any on-premises equipment or software. Pure cloud Web security is managed through browser-based tools and causes all subscriber HTTP/HTTPS traffic to route through the cloud node to deliver services like URL filtering, malware blocking, and content filtering.

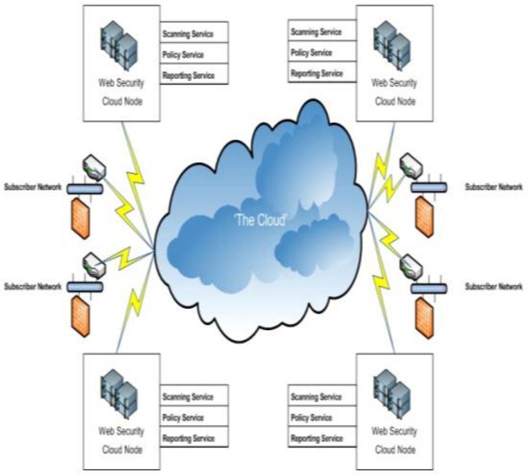


Figure 3. Pure Cloud

Figure 3. shows the concept of Pure Cloud. Software-as-a-Service delivered through rented cloud computing

infrastructure (or Infrastructure-as-a-Service) is a proven cost reduction method for enterprise information technology consumption, made even more popular by the recent world-wide recession and slow recovery. Ownership costs for on-premises security solutions consist not only of standard licensing, support, and subscription charges, but also ongoing on-site information technology labor for systems management and maintenance. So called Total Cost of Ownership, or TCO, is an advantage for pure cloud solutions, because initial startup costs are lower without licensed software or hardware. Pure cloud TCO also benefits from the ongoing management of the service in the SaaS.

4. PROPOSED SYSTEM

In this paper we are proposing the concept of composition of security at different level and form a new system for the Cloud Architecture. In case of we use the Pure Cloud we face number of problems such as

4.1 Data Location Non-compliance

Pure cloud IaaS providers vary in their world-wide data center location coverage. SaaS vendors typically operate either from major IaaS facility providers such as Rack Space and Amazon Web Services, or have built up their own managed facilities. In either case, facilities are not located in every country, and certain countries mandate storage of logs and reports within their geographic boundaries.

4.2 Latency and Performance

Routing all inbound and outbound Web traffic through another network hop to the Web security cloud node has the potential to introduce response time delay for end users. The primary factors determining whether a performance impact is occurring include the end-to-end network throughput per user, and the load on the
scanning service in the Web security cloud node.

Proposed cloud Web security solutions run a combination of on-premises hardware/software and cloud-based software. The hybrid approach is often designed to meet specific requirements of existing on-premises appliance installations, such as adding support for mobile users or meeting requirements for logging and reporting data storage.

Proposed Web Security is now offering an option for the Secure Web Gateway which combines on-premises appliance technology with cloud-based Web security services. Known as Secure Web Service System, this option creates a unified Web security administrative process and system for security officers who must manage end user Web security across corporate on network, mobile and remote branch office-use cases. The proposed system also logs and reports all block cases to a single logging and reporting system which stores security data on-premises. Branch office and remote users route all Web traffic by either direct IP or proxy through the Web security cloud node services provided.

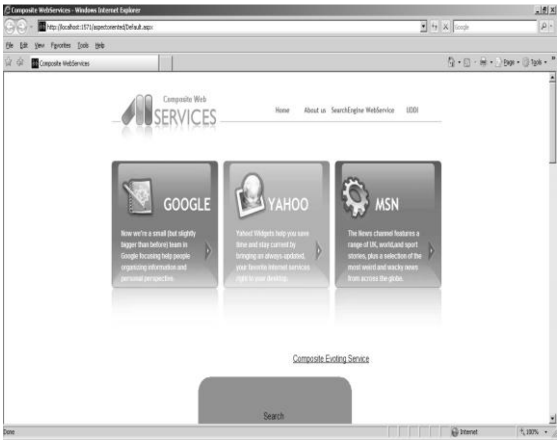
For customers with existing Secure Web Gateway investments, or for customers with requirements that include mobile user and branch office support, unified logging and reporting, unified user administration, unified policy management, and report/log data location compliance, SWSH offers the best of both on-premises and cloud-computing worlds.

We are approaching the concept of open cloud to integrate different web services under one unit. The basic principle of model Many clouds will continue to be different in a number of important ways, providing unique value for organizations. It is not our intention to dine standards for every capability in the cloud and create a single homogeneous cloud environment. Rather, as cloud computing matures, there are several key principles that must be followed to ensure the cloud is open and delivers the choice, flexibility and agility organizations demand:

1. Cloud providers must work together to ensure that the challenges to cloud adoption (security, integration, portability, interoperability, governance/management, metering/ monitoring) are addressed through open collaboration and the appropriate use of standards
2. Cloud providers must not use their market position to lock customers into their particular platforms and limit their choice of providers.
3. Cloud providers must use and adopt existing standards wherever appropriate. The IT industry has invested heavily in existing standards and standards organizations; there is no need to duplicate or reinvent them.
4. When new standards (or adjustments to existing standards) are needed

5. RESULTS

We have defined complete concept of cloud computing with interaction of web services. To implement this we use the ASP.net as the implementation Platform. We designed a GUI to perform different Web service call from different web servers. We have taken the example of Goggle, MSN and Yahoo Web Services to represent our concept.


Composite WebServices - Windows Internet Explorer
http://localhost:1571/aspectoriented/Default.aspx
Google
File Edit View Favorites Tools Help
Composite WebServices
Page Tools
Composite Web SERVICES
Home
About us
SearchEngine WebService
UDDI
GOOGLE
YAHOO
MSN
Composite Evoting Service
Search
Done
Internet
100%

Now we're a small (but slightly bigger than before) team in Google focusing help people organizing information and personal perspective.

Yahoo! Widgets help you save time and stay current by bringing an always-updated, your favorite internet services right to your desktop.

The News channel features a range of UK, world,and sport stories, plus a selection of the most weird and wacky news from across the globe.

Figure 4: Web service Integration

Figure 4 represents the actual GUI created by us in ASP.net. This GUI will accept the request and distribute it to different web servers that are integrated using concept of cloud computing and derive the best service for user.

6. CONCLUSION

While some features of Cloud Computing are more secure, some are more vulnerable to exploitation and attack, these aspects can be categorized into two groups: general security weaknesses and specific security weaknesses. A typical Cloud Computing platform has various layers and we wish to address the issues in the platform and applications layers. We aim to develop a lightweight easily deployable security application that addresses most if not all of the aforementioned concerns.

7. REFRENCES

[1] Armbrust, M., Fox, A., Gri_th, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee,

[2] G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A

[3] berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS

[4] Department, University of California, Berkeley (Feb 2009)

[5] Keller, A., Ludwig, H.: The wsla framework: Specifying and monitoring service

[6] level agreements for web services. J. Netw. Syst. Manage. 11(1) (2003) 57{81

[7] Ludwig, H., Keller, A., Dan, A., King, R., Franck, R.: Web service level agreement

[8] (WSLA) language speci_cation. IBM Corporation (2003)

[9] Theimportance of data integration in the era of cloud compuing bhttp://www.ebizq.net/blogs/linthicum/2009/01/the_importance_of_data_integra.php

[10] Tribhuwan, M.R. ; Bhuyar, V.A. ; Pirzade, S..: Ensuring Data Storage Security in Cloud Computing service

[11] . In: 2010 IEEE International Conference on Advances in recent tech in comm. and computing.

[12] Xiaolin Lu, "Service and cloud computing oriented web GIS for labor and social security applications " 20102nd international conference on information science and engg.

[13] SearchCloudSecurity.com http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-model-overview-Network-infrastructure-issues

[14] J. Heiser and M. Nicolett, "Assessing the security risks

[15] of cloud computing," Gartner Report, 2009. [Online]. Available:http://www.gartner.com/DisplayDocument?id=685308.

[16] R. Dhamija, J. D. Tygar, and M. A. Hearst, "Why phishing works," in Proceedings of the 2006 Conference on Human Factors in Computing Systems (CHI), Montr´eal, Qu´ebec, Canada. ACM, 2006, pp. 581–590.

[17] M. McIntosh and P. Austel, "XML signature element wrapping attacks and countermeasures," in SWS '05: Proceedings of the 2005 workshop on Secure web services. ACM Press, 2005, pp. 20–27.

[18] S. Gajek, L. Liao, and J. Schwenk, "Breaking and fixing the inline approach," in SWS '07: Proceedings of the 2007 ACM workshop on Secure web services. New York, NY, USA: ACM, 2007, pp. 37–43.

[19] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," in ICWS '09: Proceedings of the IEEE International Conference on Web Services. Los Angeles, USA: IEEE, 2009.

[20] .M86 White paper http://www.m86security.com/documents/pdfs/white_papers/business/WP_Hybrid_Web_Security.pdf

[21] Informatica , data integration company http://www.informatica.com/solutions/on_demand/Pages/index.aspx