SURVEY SOME ATTACKS ON CLIENT SIDE, BROWSER & CLOUD

Pragya singh baghel
Department of Computer science
University of utter Pradesh
Lucknow,Utter Pradesh (India)
Pragya.sb@gmail.com

ABSTRACT
Cloud computing is not a new name in the technology world but there are many new issues arises related with cloud. Every time in consumer mind a fear rotates because he is aware from vulnerabilities related with cloud. Security of customer data is not only responsibility of service provider but consumer should also have concern about this.In this paper I cover some security issues on customer side, on browser and some important issues related with cloud.
KEY WORDS Cloud computing, threat, security issues

1. INTRODUCTION

Cloud computing as defined by NIST "as a model for enabling convenient on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction".

Fig-1 Cloud computing conceptual diagram

Small size business, enterprises and organizations who can not afford the high cost software, hardware and data storage medium to maintain their business as well as to improve it must use cloud services on a pay-per-use basis. Cloud provide many advantages include lower cost, greater business agility, reduced IT administrative overhead, access to best applications.
But one questation about cloud computing is still in its place-**"HOW SECURE IS THE CLOUD".**
End user who wants to access the services of cloud must have browser on their system to access the network. We always talk about attacks on clouds which makes our data insecure on clouds system but there are so many attacks which can also affect our data . when any user login through interface on cloud site then they must take care to perform secure process. I will discuss about those attacks which can take place during login process.

Fig 2: End user login process

2. ATTACKS

Attack on client side

End user access area When client access network for any applications from any public location like restaurant, hotels, offices through Wi-Fi the risk of data theft will be increase.

Malware can affect system Malware is a software designed to damage computer system without the owner's informed content.

Identity theft When wrong person got your identity he may login behalf of you on cloud to get advantages of services. he can also affect your information.

Fake antivirus software Person who creates this kind of software want to access only important information called passive attacker but if attacker modify your work then he is called active attacker.

. Attack on web browser

Web browser works as an interface between consumer and service provider. most popular web browser are Google chrome, internet explorer, opera and safari.

Cross site scripting

Cross site scripting is to insert the malicious code on dynamic web page which can not be detected by client browser interpreter or server.it is also named as xss. once these malicious code get executed on web browser then every time we access the browser it gets private information and deliver to attacks.

Flooding

If Browser gets control by attacker then flooding attack is also possible to consume lot of resources and services as well as to increase the work load on cloud server. When user request of any service then service provider works towards to satisfy their request but when an attack intentionally flood requests to provider then he wants to fulfill the requirement of attacker as he thinks that attacker is a client. As a result cloud system will not be able to satisfy the normal request from user.

Denial of service

Malicious code inject onto browser then attacks execute that code to open window many times.as a result server deny to legitimate user to offer their services.

Plug-ins

We want to open any downloaded file or run any new software then browser asks to install plugins to run this program and we allow to them. This is also a way for attackers to get involve into our system.

Top security concern in cloud computing

Misuse of cloud service

On cloud any one can get register itself as a client to use cloud services for create new technologies to improve their activities**.**

Threat from inside employee

People connect with cloud computations put on their sensitive and confidential information on cloud. Companies which provide services have number of employee who have access to these sensitive data on regular basis and discuss it from out of company. Insider threat is more than just fraud and can also comprise theft of data and intellectual property**.**

Data protection

Everyone wants that their personal data on cloud must be secure.to provide security of data on cloud comprises….

- Where will the data be stored or processed
- Are there are multiple platform involved
- Who is liable for the data or security related issues and natural disasters and data leakage.
- What are legal commercial and reputational risks? Can we move against the cloud vendor to Claim loss of profits?

Identity and access management

In cloud computing technology NIST advices "the need for trusted identities and secure and efficient management of these identities while users privacy is protected is a key element for the successful adoption of any cloud solution**"** the big issue is can the provider segregate and protect individual groups of data within the remote, distributed shared environment.

Identity and access related problems mostly faced by SAAS service provider because they have to manage so many accounts of customers and when user leaves the organization their account remains active increasing risk of data exposure.

Shared technology issues

Cloud customers needs resources dynamically as per requirement. The service provider is able to meet the demand of customer. They use virtualization where virtual machines share the same physical server for multiple customers.

Hypervisor security

On hypervisor (virtual machine manager) many malware ,rootkits and unwanted codes may installing themselves as a hypervisor below the operating system. This can make them difficult to detect because hypervisor based malware could intercept any operations of operating systems. In fig 3 this kind of attack have shown .

Cross virtual machine side channel attacks

Virtual memory shares the physical memory, CPU cycles, network buffers , dram of the physical machine . attacks on virtual machine may takes place in two steps…

- Placement of attacker virtual machine on the same physical machine
- Exploiting the shared resources.

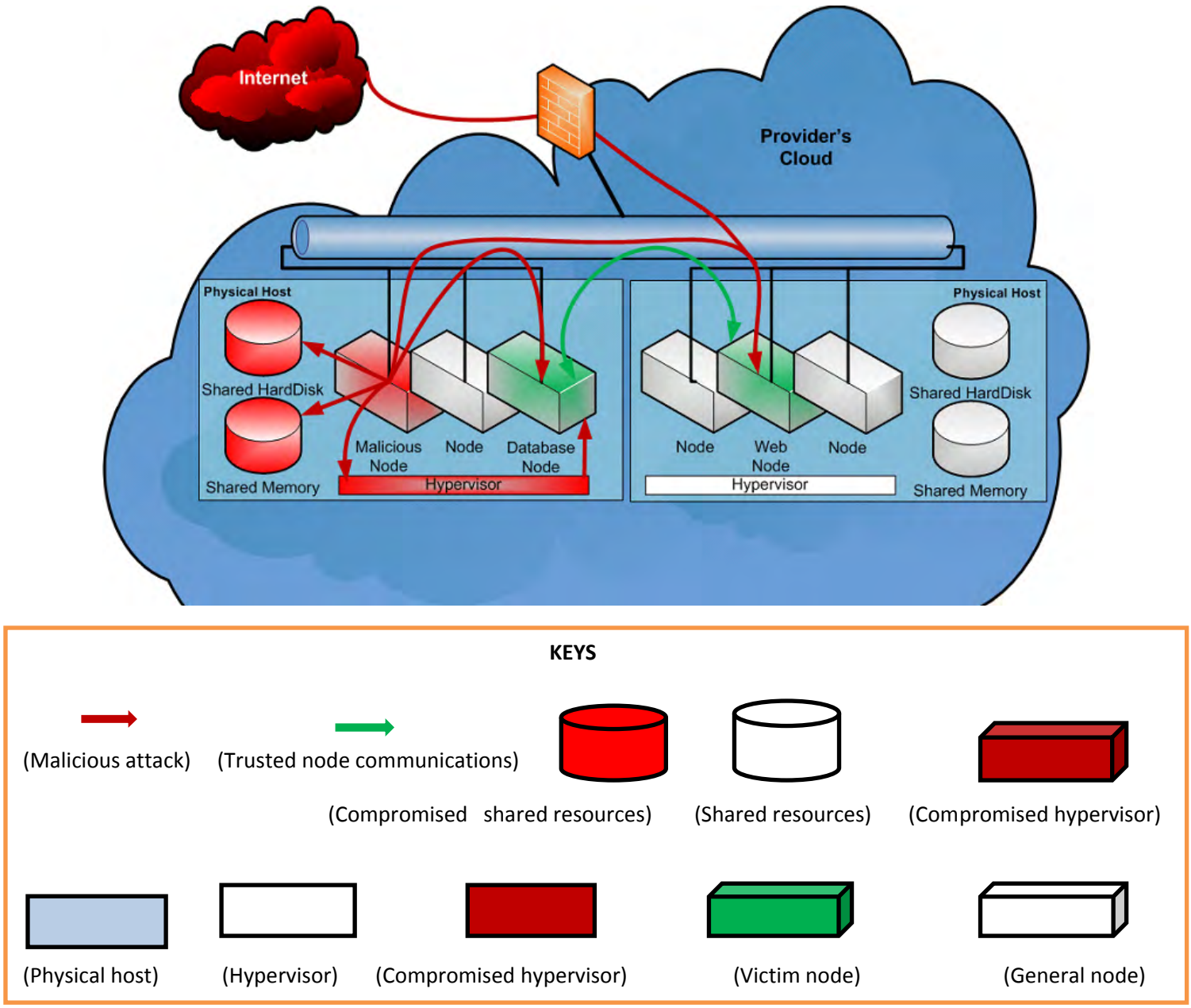

Fig 3 malicious hypervisor attack on hypervisor

Conclusion

Security of cloud computing become more strong if system is secure from client side attacks and web browsers attacks. when both of them is able to persist these attacks then most of security related issues of cloud have not mean .

References

[1] http://www.cloudsecurityalliance.org/topthreads/csathreats.v1.0.pdf
[2] Cloud computing: network/security threats and countermeasures by sara qaisar, kausar fiaz khawaja January 2012 volume 3, number 9
[3] Cloud computing data protection two considerations by Anthony Lin ,advisory board member isc2, Bali ,30-31 march 2012
[4] CSA domain 12: guidance for identity and access management v2.1
[5] Security attacks and solutions in cloud by Kazi zunnurhain and Susanv vrbsky
[6] Virtualization and cloud computing security threats to evolving data centers by trend micro
[7] White paper on security and compliance march 2012, defending against insider threats to reduce your IT risk.