An Impact of Cloud Computing on Cyber Security in controlling the proliferation of Cyber Crime

*** Prof. Kirti Kakde**

Abstract

Opportunities for the exploitation due to weakness in information security are multiplying because of the exponential growth of internet connections. It is important to know that how the data and the systems on which the data resides or transmitted are kept secured. The best way to predict future computing trends is to look at the recent developments and their motivations. Organizations are moving towards outsourcing their data storage, computations, and even user desktop environments. This trend towards Cloud Computing has a direct impact on Cyber security: rather than securing user machines, preventing malware access and managing removable media, a cloud based security scheme must focus on enabling secure communication with remote systems. Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. Cloud computing advocates promise on-demand delivery of these massive, warehouse-scale computing resources simply and easily through a network browser. This paper presents a review on the Cloud Computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure.

***Keywords**:* Proliferation of Cyber crime, Information Security, Network Connections, Computing trends, Data storage, Remote systems and Cloud Computing.

1. Proliferation of Cyber Crime in Cyber Space:

Technology is a "double-edged sword" and it can be used for both good and bad purpose. Cyberspace is a new strategic domain, but it is unlike the physical territory of which we are used to. It has gradually become the "nervous system" through which society operates. Countries now attach significant importance to the development of cyberspace technologies. Open networks have encouraged information flow and sharing, provided more opportunities for innovations, lowered the costs of innovation, and has helped improve the world's health, wealth and prosperity. Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud. In security breaches, penetration of a wireless network through unauthorized access is termed as wireless cracking. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimum technological skill to crack WLANs. Some of the attacks are Sniffing, Spoofing, Denial of service (DoS), Man-in-the-middle attack, Encryption cracking.It has been seen that organizations are heavily dependent upon a physical security countermeasures such as cables and hardwired locks, laptop safes, motion sensors and alarms, warning labels and stamps. But physical protection of devices is not sufficient. For this purpose Cloud computing is the best solution.

2. Cloud and Pervasive Computing

Cloud computing provides an excellent opportunity to expand prevalent computing. In particular, cloud computing can enable systems consisting of resource constrained devices to

Asst.Prof. MCA Department,Y.M.T. College of Management

perform intense computations. Further, cloud computing enables mobile devices to access a large store of information from nearly anywhere. Rather than developing pervasive systems that attempt to intelligently move or cache important data, these systems can now just store the data in the cloud and rely on it to be available when needed elsewhere.A scenario to demonstrate the relationship between cloud computing and pervasive computing. Consider a typical user, Ken and her interactions with technology for a day. She may begin her day by waking up to her alarm clock and preparing for work. As she walks to her car, she reads the morning's news on her smart phone that was pre-fetched for her and distributed to her phone by her cloud services. If she has not finished her reading when she gets in her car, the cloud can perform a text-to-speech conversion of her news articles and read them to her as she drives. Upon completion of the news, she can stream her music repository to her car. Once at work, Alice can seamlessly move from her office to meeting rooms throughout the day while maintain access to all of her information, applications, and sessions due to her cloud services being accessible from any machine. Even after returning home, she can relax with her favorite computer game through her desktop computer. If hosted by her cloud provider, she will not lose progress in her game even if the power fails; instead, she can continue playing through her smart phone.To enable such a scenario, we must address new challenges in securing the information stored on the cloud and the access to it. The adoption of cloud computing as a part of pervasive systems will affect security in pervasive systems. By using the cloud as a processing and storage powerhouse for pervasive systems, the focus of security in these systems will shift to ensuring that the data and processing controlled by a third party is secure, and the transmission of data between the cloud and the pervasive system is secured. Further, since pervasive systems often enable users to log on from any number of devices, as demonstrated in the example above, authentication mechanisms will also be of high importance.

3. Current Technologies

Cloud computing provides efficiencies for organizations. Rather than attempting to maintain patching, backup and recovery services, and software licensing for hundreds of machines, organizations employing cloud technologies can simply make users' machines into consoles that access network storage or terminals for remote computation.

These cloud- based systems can be instantiated in various approaches:

•**Terminal Services:** Microsoft's Remote Desktop, Virtual Network Computing (VNC), and Citrix's terminal services clients allow users to access an entire desktop environment from a remote server.

•**Web-Based Productivity Tools:** The Docs Web application from Google and the Office Web Apps from Microsoft are two examples of software as a service. These tools provide users with remote data storage and provide software through a Web browser. Google's Chrome operating system is designed to provide only a Web browser, making the computer a terminal to Web-based applications.

•**Window Forwarding:** UNIX and Linux-based systems have long had the ability to forward individual graphical windows to remote systems. This allows a client system to render the window and manage the interface while still executing the application on the server system, possibly in closer proximity to the data.

•**Remote Storage:** Amazon's Simple Storage Service and Mozy's online backup services allow a user to store data in remote systems. These services provide redundancy, allowing users to have greater reliability in case of disk or system failures. The benefits and lower costs of these cloud services enable systems and organizations to offload responsibilities that were previously handled internally. Many of these services scale well, allowing providers to leverage economies of scale to reduce costs while developing specialized services.

4. Emerging Technologies

Recent technological advances can offer greater support to cloud computing. Developers of modern Web browsers have optimized their JavaScript engines, including just-in-time compilation and hardware acceleration, to expedite processing for clients. These optimizations allow Web sites to use more complicated client-side functionality without degrading client -side performance. Web browsers now natively support standards such as HTML5, allowing the integration of video and animated content without requiring third-party plug-ins, allowing sites to have rich interactions with the user.

Web browsers also have begun implementing isolation to prevent actions in one Web browser window from affecting other windows. This isolation allows the browser to continue functioning, even if one window malfunctions.
Combined, these Web browser optimizations allow Web sites to provide clients with code that will execute in an independent, isolated environment. This provides flexibility to Web-based applications without endangering the client.

5. Likely Progression

With the national focus on high-speed Internet deployment, increasingly complex cloud services will extend toward many new users and platforms. With evolutionary optimizations in Web browser technology, the continued adoption of rich, Web-based applications is likely. Accordingly, users will have decreased need to install or maintain host-based applications. The Google Chrome OS is an example of an operating system that has been greatly simplified, largely operating to support a Web browser.

With greater network availability, client devices are more likely to resemble terminals to remote resources. This approach will allow pervasive system interfaces to become smaller and lighter without sacrificing functionality. As an example, a recent demonstration showed a smart phone running a notoriously graphically/compute intensive game. In the demonstration, a computation system simply pushed the rendered pixels for the smart phone to display, reducing the smart phone into a simple input/output device. With the pervasive computing researchers working on mechanisms to determine which computation to perform on the client and which to perform remotely, we are likely to see seamless execution across heterogeneous devices.

6. System focus: Components and services

Cloud computing providers can offer services at different layers of the resource stack, simulating the functions performed by applications, operating systems, or physical hardware. The term services in cloud computing is the concept of being able to use reusable, fine-grained components across a vendor's network. This is widely known as "as a service".

- **Software as a Service (SaaS):** offers finished applications that end users can access through a thin client. SaaS is the model in which an application is hosted as a service to

customers who access it via the Internet. SaaS include Gmail, Google Docs, and Salesforce.com. The end user does not exercise any control over the design of the application, servers, networking, and storage infrastructure.

- **Platform as a Service (PaaS):** offers an operating system as well as suites of programming languages and software development tools that customers can use to develop their own applications. Prominent examples include Microsoft Windows Azure and Google App Engine. PaaS gives end users control over application design, but does not give them control over the physical infrastructure.
- **Infrastructure as a Service (IaaS)** offers end users direct access to processing, storage, and other computing resources, allowing them to configure those resources and run operating systems and software on them as they see fit. Examples of IaaS include Amazon Elastic Compute Cloud (EC2) and IBM Blue cloud.The Figure illustrates hierarchical arrangement based on which a cloud is perceived in the form of IaaS, PaaS and SaaS from any cloud end-user's viewpoint.

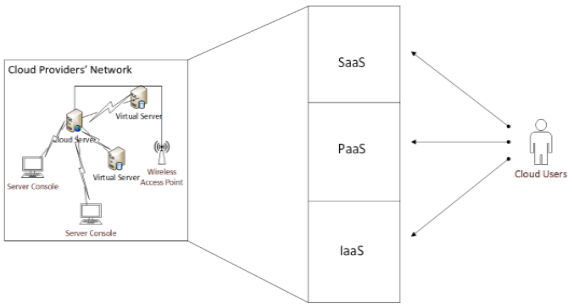

Figure 2: Cloud Service Hierarchy

7. Security threats originating from the host (hypervisor)

- **Monitoring virtual machines from host**

Monitoring the VM from the hypervisor software is an important part of managing and controlling the VMs. Hypervisor is the software that controls the layer between the hardware and the operating systems. The system administrator or other authorized user can make changes to the components of one or more virtual machines (VMs), generating a security risk.

- **Virtual machine modification**

Hypervisor represents the next lower layer of software under the customer's operating system, applications and data. Attacks on the hypervisor layer are attractive to hackers because of the scope of control they can gain if they can install and execute their malicious software on this layer of the VM software

Compromising the hypervisor means that an attacker can take control of that layer and all of the hosted virtual machines that are hosted on that machine.

- **Threats on communications between virtual machines and host:**

In a cloud computing system, all communications must pass through the hypervisor to all of the hosted VMs, and at this point, an attacker can inject malicious software in an attempt to eavesdrop or gain control over any or all of the systems. However, the worst case occurs when the hypervisor is compromised by malware, since this puts all the VMs that are being hosted on that machine at risk for security breaches

- **Placement of malicious VM images on physical systems :**

The attack known as cloud malware injection involves creating a malicious virtual machine image and then places that image into the hypervisor so that it is treated like a legitimate system in a collection of virtual machines. If this is successful, then the malicious virtual machine image is allowed to run the adversary's Code.

8. Client Authentication

With so much remote execution, cloud computing requires robust credential management that enable secure logins to multiple cloud services from multiple devices in a seamless manner. The password schemes currently employed are a burden on users and have practically forced users into poor practices. Generally, users can remember a small number of passwords, yet each Web resource generally requires users to develop a unique set of credentials. Services such as OpenID, which allow users to have a single set of credentials for multiple sites, are powerful, but may be inappropriate for sensitive institutions such as banks or government sites. Users may instead be able to use one-time-password devices, but they would need to have a unique device for each remote site to prevent one site from being able to use the credentials to authenticate to another

Opportunities: Rather than use passwords, users can instead leverage mobile devices. If properly isolated from the devices's general computing and communication hardware, a secure dedicated circuit could be created to manage hash chains for multiple sites. To further increase security of the approach, the hash chain could be manually seeded by the mobile device and a visual depiction of the seed value transmitted to the remote site via a camera capture of the mobile device's screen. In Figure 1, we provide a visual depiction of the authentication process. To authenticate, the user could then select the appropriate Web resource and then present the mobile device's screen to the computer's camera, allowing the Web site to obtain the device's hash value from the visual depiction and compare it with the locally derived hash, authenticating the user. This approach allows greater key sizes and entropy than passwords, making exhaustive enumeration attacks challenging while still making the technology usable for people.

Fortunately, the technology for this kind of authentication already exists. Software for reading QR-codes is common on many modern smart phones. Likewise, these devices are able to display barcodes that can be read by simple barcode readers. Accordingly, the transmission of hash values from a mobile device to a computer's camera proves little barrier to adoption. The construction of hash chains and rendering them into visual depiction is likewise straight-forward. Adding this component to a mobile device in a secure way may require some separate hashing hardware and storage for initial hash values; however, device manufacturers may be able to reuse the device's screen and input hardware to reduce costs.

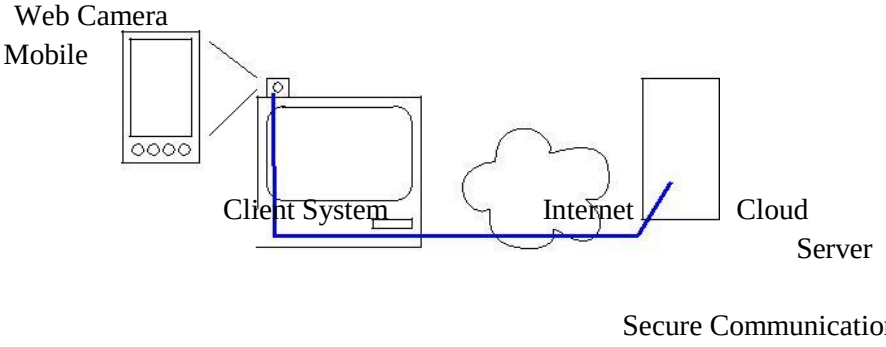

Fig. 1. Mobile device for remote authentication

While hardware-based hashing operations may significantly improve the security and usability of remote authentication, there are important questions that must be addressed. For example, what happens if the device is lost or stolen? How would the credentials be revoked and how would a user be able to reestablish their identity and control? Research in addressing authentication management techniques is critical to cyber security.

Conclusion

The continued movement towards cloud computing will have a direct impact on cyber security research. Since pervasive computing has generally focused more on improving functionality and reliability, a transition to using a cloud computing backbone in pervasive systems as an op-portunity to bring stronger security to pervasive systems. Advancements in virtual machine isolation, homomorphic encryption, client authentication, resource management, and secure opportunistic computing will facilitate the adoption of cloud computing while ensuring greater security and privacy for users.

References

- *Cyber Security-Understanding Cyber crimes, Computer Forensics and Legal Perspectives, by Nina Godbole*
- *M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing,"*
- *X. Jiang and J. A. Landay, "Modeling privacy control in context-aware systems," IEEE Pervasive Computing, vol. 1, pp. 59–63, July 2002.*
- *C. Gentry and S. Halevi, "A working implementation of fully homo-morphic encryption," in EUROCRYPT, 2010.*
- *Cloud Security Alliance, ''Top Threats to Cloud Computing V 1.0'', 2010. <https://cloudsecurityalliance.org/topthreats>.*
- *Cyber Security &Global Information Assurance, Kennetch J. Knapp, Information Science Publishing.*
- *Security And Cloud Computing - ISACA.org, www.isaca.org/*