Towards a Discipline of Mission-Aware Cloud Computing

Ravi Sandhu
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
ravi.sandhu@utsa.edu

Raj Boppana
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
boppana@cs.utsa.edu

Ram Krishnan
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
ram.krishnan@utsa.edu

Jeff Reich
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
jeff.reich@utsa.edu

Todd Wolff
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
todd.wolff@utsa.edu

Josh Zachry
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
josh.zachry@utsa.edu

ABSTRACT

Even as cloud computing gains rapid traction in the commercial marketplace the twin concerns of availability and security remain paramount to potential customers, especially in the enterprise. Concurrently the vision of what cyber security means is itself changing. The US Department of Defense (henceforth DoD) has recently promulgated a new doctrine of mission assurance in contrast to the earlier approach of information assurance. We argue that this concept of mission assurance is equally applicable to the commercial sector, and has high relevance to the availability and security concerns of cloud computing. While the business community may prefer alternate terms such as "business application assurance," "business function assurance" or "mission effectiveness" we propose to stay with established DoD terminology. Our basic position is that in order to achieve mission assurance in the new paradigm of cloud computing we need to instrument the cloud with hooks and supporting protocols and mechanisms to enable deployment of mission-driven performance, resilience and security policies into the computing and communication infrastructure. The cloud must therefore evolve from its current mission-oblivious state to become mission-aware. This position paper speculates on the research challenges in making this happen.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—Access controls; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—Unauthorized access

General Terms

Security, Reliability

CCSW'10, October 8, 2010, Chicago, Illinois, USA.

Keywords

Cloud Computing, Mission Assurance, Mission Effectiveness, Cyber Security.

1. INTRODUCTION

Cloud computing remains a somewhat amorphous term but one that definitely has gained wide usage. In this paper we will more or less follow the terminology of [14]. In particular the service models of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) have generally become well accepted, as well as the notions of public, private and hybrid clouds. Some authors have suggested a further division of IaaS to include Hardware as a Service (Haas), Data as a Service (DaaS) and Communication as a Service (CaaS) [21]. Others have sought to compare cloud concepts with more traditional grid, utility and distributed computing to emphasize continuity [4, 8].

Our basic premise is that the cloud is here to stay and we are only in the initial stages of where this technology will take us. A major driver is the promised economic benefits of cloud computing [6] to cut costs for existing applications. A significant aspect of the economics is the promise of elasticity on demand. Another major driver is the new set of applications and services that the cloud can enable. Some in the industry see the cloud as the place to develop the full potential of SOA [13] whereby existing applications and services can be easily composed in application frameworks that go beyond the current generation of PaaS. Others propose a notion of application elasticity whereby applications are deployed on resource-constrained end systems, such as mobile devices, and can migrate from device to cloud and back as determined by circumstances and preferences [22]. Looking ahead there is speculation that a layer of cloud broker services will emerge to enable integration between cloud service providers and consumers [9]. From our current vantage point it is impossible to say for sure how these and other anticipated developments will play out in detail. In the big picture we believe it is clear that the cloud will influence not only how existing applications are deployed in the future (in the cloud), but even more so impact how new applications and services are built and assembled in the future (in the cloud).

This brings us to the twin concerns that inevitably arise when adoption of cloud computing is discussed: availability and security. The availability concern relates to reliable and predictable delivery of services from the cloud which at present is not guaranteed. The elasticity of the cloud offers tremendous economic benefit but without some assurance of delivery it is difficult for enterprise users

to commit critical applications to the cloud. The lack of mechanisms to prioritize services further compounds this concern. On the security front, within which we include privacy, it is evident that the cloud like any other new cyber technology brings old security concerns in new clothes and also introduces new challenges. A comprehensive treatment of security concerns in the cloud has been developed by the Cloud Security Alliance [1]. However, as per their own claim this is essentially guidance on security issues that need to be addressed rather than a set of recommended solutions. Significant work remains to be done to arrive at operational guidance towards recommended practices. There is a smattering of academic research literature on security in the cloud. Some of this addresses important but specific point problems in this overall space, such as [5, 10, 11, 16, 17, 19]. Additionally some authors emphasize the intrinsic difficulty of security in the cloud [12, 15], while others emphasize the security benefits potentially offered by the cloud [18].

In this position paper we propose a somewhat different approach to understanding and analyzing the twin problems of availability and security in the cloud. *Our principal point of departure is that concurrent with evolution of cloud technology the nature of cyber security is also undergoing radical change. This change must be factored into discussion of cyber security in the cloud*. We lay out our arguments below.

2. EVOLUTION OF CYBER SECURITY

We use the term cyber security to define the security discipline in the large, as an amorphous evolving term whose interpretation will change over time. The term cyber security has come into usage only recently but has caught on rapidly. For instance, the US White House under President Obama has created the position of a cyber security coordinator (popularly, the cyber security czar) after considerable pressure from security professionals. So we use the term cyber security to refer to the discipline including applying it to the past. We give an impressionistic history of the cyber security discipline leading up to the notion of mission assurance (admittedly strongly influenced by the DoD viewpoint).

Looking at the past decades since the late 1960's when multi-user computers appeared on the scene the cyber security discipline has evolved in the following phases. In the first phase where there were no networks or computer-to-computer communication, cyber security was equated to computer security (CompuSec). This phase culminated in the so-called Orange Book [7] (although by then national-scale computer networks did exist and were simply ignored in this standard). In the CompuSec phase the concept of communications security (CommSec) was more or less considered as a separate discipline and in the DoD was essentially classified and primarily unrelated to computers.

Although DES and public-key cryptography had appeared in the public domain in the late 1970's the disciplines of Computer Security and Communications Security did not get unified until the early 1990's when the doctrine of Information Security (InfoSec) was introduced along with emphasis on the familiar triad of confidentiality, integrity and availability. This led to the modern notion that Information needs to be protected at rest (in storage), in motion (on the network) and in use (in computation or display).

In the next phase the term Information Assurance was promulgated by DoD. At first it appeared that the term was more or less used to broaden the perceived implicit implication that Information Security was mainly about confidentiality, so Information Assurance more expansively equally emphasized integrity and availability. A subsequent DoD directive [3] gives the following definition for Information Assurance, "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

More recently in Wikipedia we have [20], "Information assurance is closely related to information security and the terms are sometimes used interchangeably. However, IA's broader connotation also includes reliability and emphasizes strategic risk management over tools and tactics. In addition to defending against malicious hackers and code (e.g., viruses), IA includes other corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery. Further, while information security draws primarily from computer science, IA is interdisciplinary and draws from multiple fields, including accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to computer science. Therefore, IA is best thought of as a superset of information security." This reflects an explicit broadening of the cyber security discipline from its narrow roots in computer science.

The most recent evolution is the latest transition to Mission Assurance discussed next.

3. MISSION ASSURANCE

The motivation to move to Mission Assurance from Information Assurance is twofold. Information Assurance is intrinsically security-focused with priority on protection of data and systems. This attitude often conflicts with the Mission Assurance attitude of getting the job done. An emphasis on Mission Assurance thereby explicitly recognizes that security is a secondary objective. This aspect is familiar to most security professionals (although often not practised effectively in our systems). The second motivation is the growing realization that completely eliminating malicious presence in a cyber system is practically impossible. Setting a somewhat arbitrary date of 2008, it has become clear that even the best managed systems have been breached with the system operators often oblivious to long running persistent penetrations. Hence the recognition that the mission needs to be accomplished even if some of the information and system has been compromised.

A recent DoD directive [2] defines Mission Assurance as follows, "A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations."

This does seem rather forbidding and of little relevance to most enterprises. However if one removes a few high end phrases such as "force protection; antiterrorism; critical infrastructure protection;" and "chemical, biological, radiological, nuclear, and high explosive defense;" and substitutes Enterprise for Department of Defense and National Military, the end result is something that most businesses will find appropriate. With these removals and substitutions, we can define Mission Assurance for businesses as follows, "A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities

and all supporting infrastructures are available to the Enterprise to carry out its Strategy. It links numerous risk management program activities and security-related functions, such as IA; continuity of operations; readiness; and installation preparedness to create the synergy required for the Enterprise to mobilize, deploy, support, and sustain its operations throughout the continuum of operations."

Now this seems pretty innocuous and worthy of support in any enterprise. Indeed a well managed enterprise already does this in a systematic way, with cyber security dealing with the cyber aspects of this goal. Cyber security then becomes a piece of the larger goal of Mission Assurance. By itself it becomes a secondary goal that should not prevent the mission from being accomplished. Conversely there should be compensating mechanisms so that failure of cyber security does not result in failure of the mission. The mantra of cyber security is then that it exists in support of the bigger goal of mission assurance for the enterprise.

4. MISSION-AWARE CLOUD

By definition a cyber infrastructure such as a cloud cannot directly achieve mission assurance. Mission assurance is a bigger goal of which the cyber piece is only one component. We therefore believe that terms such as Mission-Assured Cloud are meaningless. The cloud, or any other cyber infrastructure, by itself cannot guarantee mission assurance. Mission assurance requires non-cyber components including human beings and other supporting enterprises to act in a proper way to achieve mission assurance. What cyber infrastructure can be engineered to do is to provide appropriate hooks and supporting protocols and mechanisms to ensure that the cyber component functions in support of mission assurance. Any cyber infrastructure that provides such hooks can be said to be mission-aware. Hence the concept of a mission-aware cloud.

5. OUTLINE OF A RESEARCH AGENDA

In this section we speculate on some elements of a research agenda to realize the goal of a mission-aware cloud. The list of topics given here is not intended to be complete. To some degree it is a strawman for discussion. In many of the individual topics there is considerable prior work to build upon, but it is typically scattered and fragmented. Thus the need for systems level integrated theoretical and experimental treatment in context of the cloud remains.

1. *Develop a heterogeneous experimental cloud computing infrastructure (denoted as the cloud henceforth) spanning multiple locations, security and assurance levels*. This experimental cloud infrastructure should be able to simulate multiple architectures, geography and security and assurance levels. This will provide capability to simulate real-world environments and creation of controls to support assured interactions with environments that have varying security and assurance levels.

2. *Experimentally explore, develop, and implement extensive instrumentation to monitor, measure and gather statistical data regarding activities in the cloud*. Conduct extensive experiments on heterogeneous clouds in disparate locations to establish baseline performance and operating conditions in local and global environments. The instrumentation should enable monitoring of the cloud at local and global levels with metrics including processors loads, bus speeds, VM utilization, network latency and incoming/outgoing messages to detect anomalous behavior and malicious activity. Conduct experiments to evaluate impact of innovative techniques, e.g., memory cloaking, network communication concealment, evasion methods and predictive network and application isolation.

3. *Analyze gathered data to estimate underlying network performance and threat vulnerability using regression, analysis of variance, and other generalized linear statistical model*s. Develop advanced statistical inference and estimation methods to determine various network performance metrics under normal, congestion and attack situations. Use regression models to predict certain types of performance measures as well as to validate experiments. Employ factorial designs to determine the impact of various heuristics and protocol features in normal operation and to identify the most likely mode of attack when the cloud is potentially unstable. Employ Poisson regression models to analyze computing and communication throughputs that are impacted by multiple covariates such as attacks, network load levels and available routes. Employ logistic regression models to estimate false positives/negatives in intrusion detection and identification of malicious insiders.

4. *Develop new protocols that cope with denial of service (DoS) and insider attacks and ensure predictable delivery of mission critical data*. Develop new protocols that cope with denial of service (DoS) and insider attacks and ensure predictable delivery of mission critical data, messages and information. Insider attacks are launched from previously trusted nodes that are compromised by malware, while DoS attacks may be launched from external sites as well as by malicious insiders. Data and communication among VMs participating in mission-critical computations are compromised by these attacks. Efficient new routing protocols that use memory cloaking, anonymous and multipath communication techniques should be developed. To cope with DoS attacks from external malicious nodes, additional security protocols that incorporate VM redundancy and migration as well as peer-to-peer communication techniques to hide mission-critical data and VMs should be designed. The impact of VM migration on communication can be mitigated using efficient on-demand route discovery techniques. Implement, validate and tune the proposed security protocols using experiments and analysis of gathered statistical data.

5. *Develop integrated efficient security enforcement and implementation mechanisms that do not hinder mission assurance*. The traditional overhead of security enforcement is increasingly untenable in high performance and heterogeneous environments where many of the end devices have constrained bandwidth and computational power. Protocols designed for a best-effort wired infrastructure do not scale to the reality of the emerging highly dynamic, high performance, adaptable and contested cyberspace. Research on lightweight security protocols that leverage existing connections and contexts for continued persistent operations and experiments to quantify their resilience and performance should be conducted.

6. *Develop new or enhance existing virtual machines (VMs) that enable efficient implementation of access control and trust policies to facilitate mission assurance*. The multi-tenancy aspect of cloud computing presents a unique challenge in regards to information assurance and security. The risk posed to a VM by adjacent VMs, although more pronounced within the context of a public cloud, represents a significant threat to privately hosted clouds as well. Substantive research is

required which strives to improve current state-of-the-art in terms of hypervisor and virtual machine design such that exploitation of one VM does not compromise the security of adjacent VMs. Areas of research include memory cloaking, multi-shadowing and techniques which facilitate the association of security policy with VM identities to prevent the mixing of VMs from different trust levels within the context of a single physical server.

7. *Develop models, methodologies and architectures for decentralized dynamic management of security and assurance policies*. A critical component of a mission-aware cloud is the decentralized and dynamic management infrastructure required to inject, maintain and adapt mission-driven performance, resilience and security policies in the cloud. Research on novel models and supporting architectures and the resulting assurance and security of the management mission should be conducted, both theoretically and experimentally. Effective analysis of safety, liveness and assurance of the management infrastructure and specific management policies is essential to success of a mission-aware cloud. Undecidability and high complexity results in this arena abound, but careful design can achieve these goals.

8. *Design automated systems that analyze the tradeoffs between security and availability versus performance and scalability and take corrective action before threats or bottlenecks compromise mission assurance*. Resilient, fault tolerant networks which are capable of performing under adverse conditions and which are able to fight through attacks in support of the war fighter's mission, will require the ability to assess, in near real-time, the efficacy of various tradeoffs in terms of availability and security versus performance and scalability. Research should be performed using advanced statistical techniques leading to development of technologies which provide the ability to quantify the effects associated with these tradeoffs and which will facilitate the implementation of corrective actions to recover from events which negatively impact mission assurance. The research should design suitable self-healing and self-correcting methods that take this analysis and proactively determine suitable VM redundancy and VM migration to bypass debilitating DoS attacks on the underlying network, and activation of security techniques such as memory cloaking and anonymous communication among VMs.

We hope this position paper will encourage development of a vibrant research community working on system level issues in the cloud, integrating both cyber security and performance and resilience synergistically to achieve the vision of a mission-aware cloud infrastructure.

6. CONCLUSION

In this position paper we have argued that the twin issues of availability and security in the cloud can be adequately addressed only within a framework that recognizes the ongoing evolution of cyber security to the notion of mission assurance in lieu of information assurance. Although the mission assurance concept has been developed by the DoD, we have argued that it applies equally in the commercial sector. We have argued that to enable mission assurance we must transition from current mission-oblivious clouds to mission-aware clouds. We have speculated on some of the research issues involved in making this happen.

Acknowledgment

This work is partially supported by a grant from the State of Texas Emerging Technology Fund.

7. REFERENCES

[1] Security guidance for critical areas of focus in cloud computing, version 2.1. *Cloud Security Alliance*, December 2009.

[2] *DoD Directive 3020.40*, January 14, 2010.

[3] *DoD Directive 8500.01*, October 24, 2002.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[5] D. Banks, J. S. Erickson, and M. Rhodes. Toward cloud-based collaboration services. In *HotCloud'09: Usenix Workshop on Hot Topics in Cloud Computing*, 2009.

[6] R. Buyya. Market-oriented cloud computing: Vision, hype, and reality of delivering computing as the 5th utility. *IEEE International Symposium on Cluster Computing and the Grid*, 2009.

[7] DoD National Computer Security Center (DoD 5200.28-STD). *Trusted Computer System Evaluation Criteria*, December 1985.

[8] I. Foster, Y. Zhao, I. Raicu, and S. Lu. Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08*.

[9] Gartner Press Release. Gartner says cloud consumers need brokerages to unlock the potential of cloud services. July 9, 2009.

[10] R. Geambasu, S. D. Gribble, and H. M. Levy. Cloudviews: Communal data sharing in public clouds. In *HotCloud'09: Usenix Workshop on Hot Topics in Cloud Computing*, 2009.

[11] C. Hewitt. ORGs for scalable, robust, privacy-friendly client cloud computing. *IEEE Internet Computing*, 12(5):96–99, 2008.

[12] T. Jaeger and J. Schiffman. Outlook: Cloudy with a chance of security challenges and improvements. *Security & Privacy, IEEE*, 8(1):77–80, Jan.-Feb. 2010.

[13] P. Krill. The cloud-SOA connection. *InfoWorld*, Feb 10, 2009.

[14] P. Mell and T. Grance. The NIST definition of cloud computing: version 15. *National Institute of Standards and Technology*, Oct 7, 2009.

[15] D. Owens. Securing elasticity in the cloud. *Commun. ACM*, 53(6):46–51, 2010.

[16] 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 *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 199–212, New York, NY, USA, 2009. ACM.

[17] N. Santos, K. Gummadi, and R. Rodrigues. Towards trusted cloud computing. *HotCloud'09: Proc. of USENIX Workshop on Hot Topics in Cloud Computing*, 2009.

[18] J. Viega. Cloud computing and the common man. *IEEE Computer*, 42(8):106–108, 2009.

[19] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning. Managing security of virtual machine images in a cloud environment. In *CCSW '09: Proceedings of the 2009 ACM*

workshop on Cloud computing security, pages 91–96, New York, NY, USA, 2009. ACM.

[20] Wikipedia. Information assurance — wikipedia, the free encyclopedia, 2010. [Online; accessed 7-July-2010].

[21] L. Youseff, M. Butrico, and D. Da Silva. Toward a unified ontology of cloud computing. In *Grid Computing Environments Workshop, 2008. GCE'08*.

[22] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong. Securing elastic applications on mobile devices for cloud computing. In *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 127–134, New York, NY, USA, 2009. ACM.