Demystifying the myths of public cloud computing

Authors
Christopher John Hodson, MSc (Royal Holloway, 2017)
Geraint Price, ISG, Royal Holloway

Abstract

Cloud computing is a growing trend in all industry verticals. Multi-tenant solutions often provide cost savings whilst supporting digital transformation initiatives; but what about the security considerations? Are cloud architectures inherently less secure than systems we build within our own datacenters? Does cloud introduce a new set of threats and vulnerabilities? In his thesis, Chris Hodson looks into the constituent components of public cloud ecosystems and assesses the service models, deployment options, threats and good practice considerations.[a]

[a]This article is published online by Computer Weekly as part of the 2018 Royal Holloway information security thesis series `http://www.computerweekly.com/ehandbook/Demystifying-the-myths-of-public-cloud-computing`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

My motivations:

Most of us in the security business are familiar with the conversation: our CIO or CTO politely informs us that we are "going to the cloud". We overcome the instinct to, somewhat philosophically, assert that (with digital transformation being the pervasive beast that it is) cloud is "coming to us" and respond with some questions such as:

- For which applications?
- When?
- IaaS, PaaS, SaaS?
- What about our legacy estate?
- Have you considered our compliance and regulatory obligations?

We get the impression that our executive isn't sure that these points are relevant; others are using cloud services and there must be business benefits to be gleaned, otherwise why would it be so popular? "I've been told there are some risks with going to the cloud and I need you to make it secure" is how the conversation generally continues.

Many internal members of the IT community might be against such a comprehensive shift of IT strategy. The veteran sysadmin sensing that jobs could be following servers out of the organisational datacenter. "Risks of cloud" being applied as a euphemism for "don't take my job, I like it here".

Your security colleagues may also be reticent to embrace cloud services: "the cloud is insecure, I saw at Blackhat a VM Escape attack which leveraged a vulnerability in Layer -1 and resulted in data theft so long as the moons are aligned, and the day of the week had a 'z' in it".

So, the top down message is that cloud is the way to go, the bottom up sentiment suggests that cloud could be more trouble that it is worth. Generally, CISOs run with the following:

- Remind your exec that the nebulous definition of “cloud” is no more useful than “mode of transportation” which could be a car, a bike, walking or a spaceship.
- In parallel, you explain to your colleagues that context is important with any security vulnerability - how likely is it that the vulnerability will be successfully exploited?

The motivation for my study was simple: I’d engaged in this conversation with educated, brilliant people in organisations across most industry verticals. If they were confused by the opaque, esoteric jargon of cloud, what hope did the rest of us have? I therefore opted to include “option 3”, namely:

Write a thesis on the perceived “risks” of public cloud in an attempt to educate and enlighten a broader set of stakeholders in a considered, academic fashion with as little bias and opinion as possible.

Failing to plan is planning to fail.

Having worked in the InfoSec world for many years, I was at an advantage in many areas of thesis preparation although one distinct downside was the risk of “boiling the ocean”. I worked very closely (and candidly) with my tutor to ensure that my subject matter was carefully ring-fenced whilst still offering me the opportunity to produce an interesting dissertation.

Enclosed within the RHUL guidance is a statement which suggests “writing about something you’re passionate about”. When I was considering my subject matter, I gave this due attention. At first, I was sure I would write about the evolution of exploit kit obfuscation/evasion techniques, the ethics of ransomware payment or something around DevSecOps. All eminently interesting areas of study. Whilst whiteboarding (yes, sadly I have a whiteboard at home) these ideas, I could not escape the fact that in my day job, I am repeatedly presented with arguments not to adopt public cloud solutions for nebulous reasons. I thought that if I spent the time to consider, through a structured risk management process, all the reasons that I could think of for not adopting cloud, I’d be a better CISO as a result AND my findings could be used for others in the industry.

What did I do?

My work had four core objectives. In the interests of brevity, I’ve addressed these below at a macro level. Please refer to my thesis for more detail:

1 Understand cloud: A common lexicon for cloud, why everyone is adopting, the benefits, etc..

2 Security risks: Actors, events and vulnerabilities - what do we mean by “risk”?

3 Analysis of public cloud vulnerabilities: Security equivalence with PC tools - pragmatic on other risks.

4 Can established risk management methodologies cater for public cloud?

Clouds are like roads:

If we are to establish the risks, benefits and suitability of cloud, we need to better define the various cloud deployment, operational and service models in use today and in the future. A recent analogy I used in a speaking engagement was that clouds are like roads; they facilitate getting to your destination. Be that destination a network location, an application or a development environment. No one would enforce a single, rigid set of rules and regulations for all roads - many factors come into play: volume of traffic, the likelihood of an accident, safety measures, requirements for cameras. If all roads carried a 30 mile an hour limit, you might reduce fatal collisions, but freeways and motorways would cease to be efficient. Equally, if you applied a 70 mile an hour limit to a pedestrian precinct,

unnecessary risks would be introduced. Context is very important, imperative in fact. The same goes for cloud computing. If I was to present an academic study regarding the risks of cloud, it was vital that we defined what "cloud" meant.

Cloud adoption continues to grow, and as it does, such an explicit delineation of cloud and on-premise will not be necessary. Is the world of commodity computing displacing traditional datacentre models to such an extent that soon all computing will be elastic, distributed and based on virtualisation? On the whole, my research supported this assertion. Organisations may have specific legacy, regulatory or performance requirements for retaining certain applications closer-to-home but these will become the exception, not the rule. Public cloud services are democratising carrier-grade infrastructure and security services - who wouldn't want to consume these? As consumers and businesses, we continue to benefit from the convenience and cost savings associated with multi-tenant, cloud-based services. Service-based, shared solutions are pervasive in all industry verticals and the "cloud"/"non-cloud" delineation is not a suitable method of performing risk assessment.

The benefits of cloud.

Early on in my study, I looked at the benefits of cloud computing. I soon discovered that this is a well-trodden metaphorical path. In fact, most books, websites and interviews I reviewed espoused the virtues of a public cloud model for cost saving, flexibility/elasticity and even the green effect. I was surprised to discover that there was very little documentation which covered the security benefits of cloud.

The security benefits of cloud, whilst lesser known in the mainstream, are plentiful. In fact, most cloud providers have adopted a "paranoia by default" approach to information security: a single breach could put them out of business; this isn't the case in an end-user organisation. Public cloud providers also benefit from economies of scale which small and medium (SME) organisations simply couldn't take advantage of. Public cloud security services have put carrier grade security capabilities in the hands of companies of any size.

So, what is risk and does cloud introduce new risks?

From a personal perspective, my optimal explanation of risk came from the International Organisation for Standardisation (ISO):

> *"the effect of uncertainty on objectives."*

Does cloud introduce new forms of risk which didn't exist in previous computing ecosystems? It is important that we understand how many of these are unique to cloud and a result of the intrinsic nature of cloud architecture. Risk is inherent in our daily lives. As human beings, we take both conscious and unconscious risks every day. A lot of research has been undertaken around the human appetite for risk and the contributing factors that make one risk palatable while others are considered "too risky".

I was interested to understand if research existed which covered the ethological or sociological aspects of risk perception. My studies led me to research by Gerd Gigerenzer, a German psychologist who asserts that people tend to fear what he calls "dread risks": low-probability, high-consequence but with a primitive, overt impact. In 2004, his study entitled "Dread Risk, September 11, and Fatal Traffic Accidents" pulled figures from the months and years before 9/11 and those immediately afterwards. Gigerenzer proves beyond reasonable doubt that the events of 9/11 caused more people to travel across the United States (US) via automobile rather than take a flight. This increase in road

Dread risks

- low probability
- high consequence
- overt impact

travel resulted in an increased number of cars on the road and consequentially road traffic accidents which resulted in fatalities. Whilst Gigerenzer proved through statistics that flying was considerably safer than getting in a car, people feel safer in cars. This myopic approach to risk management has parallels in the world of cloud; we seem to feel safer with our servers in our datacentre but would we be better served to leave security to those with cyber security as their core business?

I wanted to support the following hypothesis:

Cloud computing is no more or less secure than on-premise technical architecture per se. There are entire application ecosystems running in public cloud which have a defence-in-depth set of security capabilities. Equally, there are a plethora of solutions which are deployed with default configurations and patch management issues. I assert that an indistinguishable situation exists when applications and infrastructure is deployed into a customer location. How could I prove this? Or at least provide supporting evidence for my argument?

I thought that the best approach for this was to critically analyse preeminent literature which covered perceived “risks of cloud”. I wanted to review content from leading vendors, research organisations and academia. I discovered that an assortment of cloud risk papers existed pertaining to cloud risks; although the European Union Agency for Network and Information Security (ENISA) provided the most comprehensive and well-constructed decomposition of what it considered the most appropriate vulnerabilities with cloud usage. If I could understand the vulnerabilities purportedly inherent in cloud models, I would have a much easier time understanding the associated risks.

ENISA breaks cloud vulnerabilities into three areas, included in the table below:

Risk Category	**Description**
Policy and organisational	Vendor lock-in | Gevernance | Compliance | Reputation | Service termination | acquisition | Supply chain failure
Technical	Resource exhaustion | Isolation failure | Malicious insider | Interface compromise | Data interception | Data leakage | Insecure data deletion | Denial of service (DDoS) - Distributed/Economic | Loss of encryption keys | Malicious probes | Compromised service engine | Hardening conflicts
Legal	Subpoena and e-discovery | Changes of Jurisdiction | Data protection risks | Licensing risks

I took each of these classifications, and the sub-categories therein, and provided a breakdown of which vulnerabilities are truly a result of cloud architecture:

Vulnerability Category	**Instances**
Unique to cloud	4 (two legal, two resource sharing)
Exacerbated by cloud	13
General	14

What my findings highlight is that over half of the vulnerabilities would be present in any contemporary technology environment. The most interesting and insightful information I took away from this analysis was the number of exacerbated vulnerabilities that are a result of a need for process change as opposed to any technical vulnerability. Based on these findings, I can assert that organisations would be wise to focus on operational process change when dealing with public cloud adoption.

So, the cloud introduces new vulnerabilities?

At this point in my study, I had established some fairly key points:

- Cloud causes confusion due to the myriad service and deployment models available.
- Risks are often, incorrectly, explained as threats or vulnerabilities.
- Cloud can provide an improved security posture.

Having identified that understanding the concepts of risk is a key first step, I explored threats, vulnerabilities and controls as separate (although intrinsically linked) sections. The detail of this is in the thesis but I came to the following conclusions:

1 The threat actors in an on premise and public cloud ecosystem are broadly similar. An additional "accidental actor" exists at a cloud service provider: the admin who could "bring down the cloud" as we saw in Amazon's infamous S3 outage.

2 Cloud threat events mirror those of their on premise counterparts

3 Multitenant cloud environments carry the potential to exacerbate the impact of a threat event due to the aggregation of services and data from multiple clients.

Multitenancy is a trade-off; organisations benefit from the elasticity, cost and performance benefits of a shared service although the impact of a breach of CIA in one tenant could impact other tenants. It is therefore imperative that organisations understand the feasibility (and likelihood) of such a threat event being (successfully) initiated.

I continued my analysis and challenged myself with four key questions regarding multitenancy for public cloud:

1 What is multitenancy and more specifically: Is this coarse-grained definition appropriate for all public cloud implementation?

2 Is multitenancy the exclusive reserve of public cloud?

3 Are the vulnerabilities associated with resource sharing exploitable with a reasonable degree of likelihood by a range of threat actors with varying levels of skill and persistence?

4 Are the vulnerabilities of multitenancy appropriately contextualised? Do other attack paths exist which are more likely exploitable by all/any of the threat actors used in this study?

In an effort to understand the root cause of multitenancy concern, I took literature from both ENISA and the Open Web Application Security Project (OWASP) and constructed a multitenancy mind map (Figure 1). My findings were very interesting; almost all technical vulnerabilities associated with multitenancy emanated from resource isolation. Great! If I could understand the likelihood of a threat actor exploiting one of these vulnerabilities, I'd be able to qualify my assertion that cloud environments do not materially introduce fresh risks for an organisation!

I am a techie at heart and this section of my study allowed me to think like an attacker. I performed a series of threat models in an attempt to understand all the weird-and-wonderful ways that a nefariously inclined individual could compromise the confidentiality, integrity and/or availability of services in the public cloud. I combined my output with analysis conducted by other researches and academics.

My thesis defines the threat events associated with public cloud into four areas. Each of these areas is technical in nature and required extensive analysis (included within my thesis):

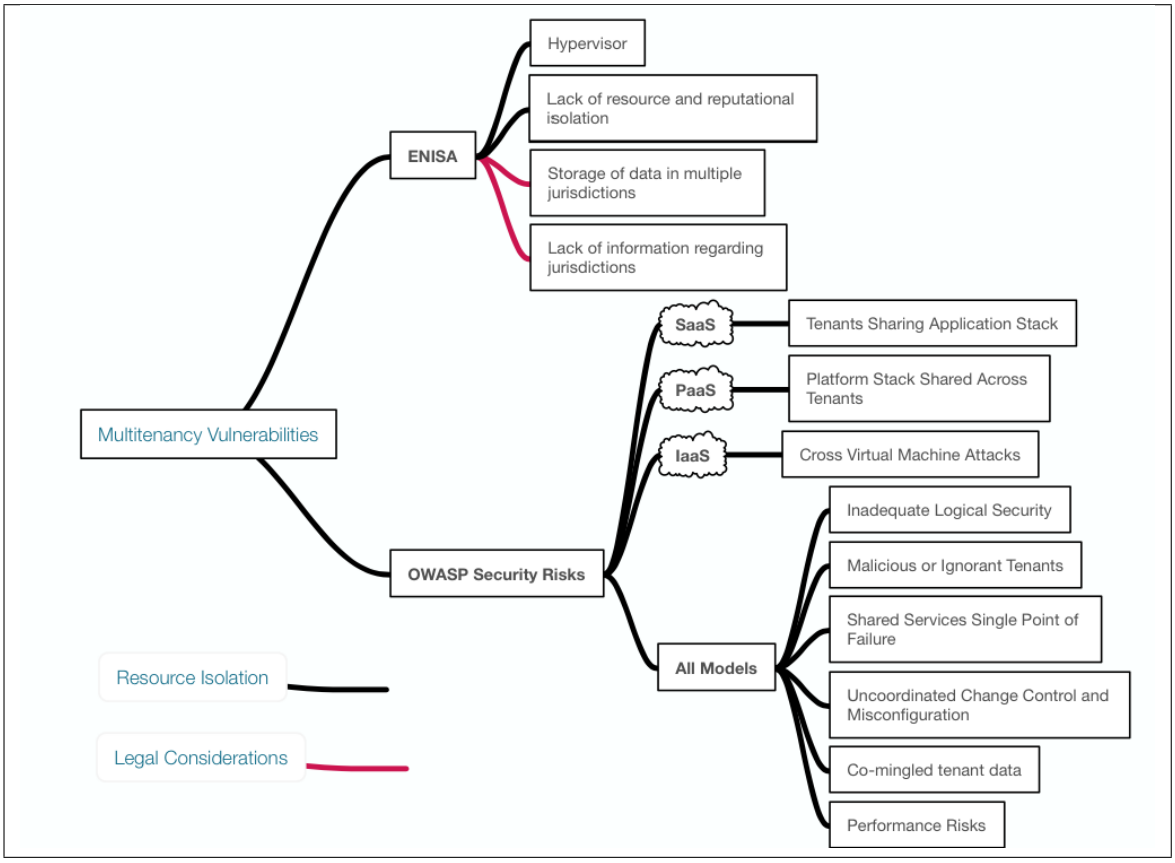

Figure 1: Cloud multitenancy vulnerabities

- VM Escape Attacks
- Rouge Hypervisors
- Inter-VM Attacks
- Distributed Denial of Service

An organisation is idiomatically only as strong as its weakest link. Whilst it is prudent to acknowledge the threats and vulnerabilities associated with public cloud computing, there are a myriad of risks to the confidentiality, integrity and availability which exist across enterprise environments and through my risk analysis, I assert that these are significantly more easily exploited. Such as:

- Poor credential management
- Unpatched system and application vulnerabilities

I used the Information Security Forum (ISF) Information Security Risk Assessment Methodology (IRAM2) to assess the likelihood of a threat event successfully exploiting a vulnerability in a public cloud environment. The benefits of IRAM are plentiful but, for me, the most beneficial is IRAM's semi-quantitative measurements. Through using IRAM, I was able to contextualise the likelihood of an event succeeding having taken into account the controls and safeguards which exist across leading Cloud Service Providers (CSPs).

Public cloud is not a technology problem.

I concluded my paper with a series of reusable architectural artefacts. I drafted a "Cloud Risk Metamodel" which details the key components of a cloud risk discussion. I subsequently defined a breakdown of responsibilities between a customer and a CSP when assessing operational responsibility for cloud services which was based on Amazon's Shared Responsibility Model.

My final action was to summarise my research into a "top ten considerations for public cloud". These are succinct enough to be beneficial for anyone embarking on a cloud deployment/migration:

1. Information risk deals with the compromise of the confidentiality, integrity and/or availability of data. Cloud introduces new vulnerabilities which are exploited by existing threat actors and variations of existing threat events.
2. Technical security controls exist across mature CSPs to provide "Security Conservation".
3. Public cloud computing offers organisations a comprehensive suite of logical and physical security controls for the protection of sensitive enterprise data.
4. The technical vulnerabilities associated with public cloud are difficult to exploit.
5. Preeminent regulatory guidelines support the use of, and provide guidance around, the use of public cloud.
6. In 2017, most cyber-attacks are focused at the user or application level - a network-centric defence strategy, focusing solely on network vulnerabilities, is doomed to fail in a cloud-first world.
7. In many situations, public cloud adoption can improve an organisation's security posture.
8. Sensitive information is increasingly being stored in public cloud.
9. Public cloud consumption is growing rapidly, securing public cloud is a discipline the security team needs to become comfortable with.
10. Business processes inside and outside of IT are altered because of public cloud. We are not dealing with a technology problem.

If I was doing this again/If I had more time:

For me, the dissertation was, by far, the most interesting and rewarding aspect of my MSc. I was able to answer several pertinent questions regarding the security of public cloud providers and the direction that technology services are taking to support enterprise digital transformation.

As with all technology trends, nothing stands still. If I had more time, I would have included in my analysis other forms of software virtualization such as containerisation and microservices architecture.

I found the study of the psychological aspects of cloud very interesting. Given more time, I would have further researched dread risks and their applicability to public cloud scenarios.

Biographies

Christopher John Hodson has an IT background that has spanned engineering, design, architecture, and management. Today, he is the EMEA CISO for Zscaler: the world's largest security-as-a-service cloud provider. As CISO, he is a trusted advisor to executives, board members and other stakeholders, helping them define well-balanced strategies for managing risk and improving business outcomes. Chris enrolled on Royal Holloway's MSc Cyber Program to achieve academic recognition of his industry experience. Christopher is a director of the not-for-profit IISP (Institute of Information Security Professionals) and is a member of CompTIA's Cyber Security Committee.

Geraint Price BSc (London), PhD (Cantab) obtained his B.Sc. in Computer Science from Royal Holloway University of London in 1994 and his Ph.D. from University of Cambridge in 1999. His Ph.D.

dissertation analysed the interaction between Computer Security and Fault Tolerance. Since then he has worked on various projects including Denial of Service attacks in networks and the future of Public Key Infrastructures, funded by academia and industry. Geraint is a Senior Lecturer in the Information Security Group, and has a strong interest in the practice of information security. He leads the ISG's external engagement activities with business and government. Geraint is a regular attendee, panellist and speaker at a number of industrial fora, including I-4 and the ISF.

Series editor: S.- L. Ng