FAST-CFP: Finding a Solution To The Cloud Forensic Problem

Special Track running alongside CLOUD COMPUTING 2018, the Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, 18 February 2018 - 22 February 2018, Barcelona, Spain

Bob Duncan
Computing Science
University of Aberdeen, UK
Aberdeen, UK
Email: bobduncan@abdn.ac.uk

***Abstract*—Cloud computing has been a great enabler for a great many companies and individuals in the decade or so since it gained traction. The ability to access new systems rapidly without concern for forward planning, accessing corporate budgets and in particular the ability to scale up (or down) on demand has proved particularly attractive. A great many researchers have been actively involved to ensure that systems are developed in a responsible way to ensure the security and privacy of users. However, there remains a fundamental issue which is of great concern. Namely, that once an attacker successfully breaches a cloud system and becomes an intruder, usually escalating privileges the longer they are in the system, there is nothing then to prevent them from deleting or modifying the forensic trail. This presents a serious challenge, especially in the light of forthcoming regulation from the forthcoming European Union (EU) General Data Protection Regulation (GDPR), which has a regime of penalties which can rise up to the greater of €20 million or 4% of Global Turnover. The other challenging aspect of this legislation is that any security breach must be reported within 72 hours. For cloud users who are breached, particularly where the intruder deletes or modifies the forensic trail, this may become an impossible requirement to comply with, which can also lead to an increase in the fine levied. Solving this problem presents a seriously difficult challenge, but failure to solve this problem can lead to an increase in the level of fines being levied. Looking at the cyber breach reports regularly carried out each year by a number of security organisations, it is very clear that a great many companies are nowhere near being able to comply with this tight reporting requirement, let alone understand which records have been accessed, modified or deleted. Given that the regulation comes into effect on the 25th May 2018, it is clear that many companies are walking blind into a major disaster.**

Keywords–Cloud Forensic Problem; GDPR; Cloud Security and Privacy.

I. INTRODUCTION

All corporate IT systems are under constant attack, from myriad actors with a variety of differing agendas. This is an extremely challenging problem to defend against, but in the case of those who use cloud systems, the problem is significantly more difficult to address, given the complexity of cloud ecosystems, and the challenges faced due to the range of actors with their differing agendas in cloud.

Some take the view that complexity can aid security and privacy, yet the truth is that the greater the complexity, the more of a challenge it is to configure systems securely. Privacy also presents a huge challenge and the forthcoming European Union (EU) General Data Protection Regulation (GDPR) will merely exacerbate this problem.

The main reason for this is what is known as the Cloud Forensic Problem, which arises where an attacker succeeds in breaching a cloud system, thus allowing them to gain, even a small foothold, which allows then to dig in and become an intruder. Once the intruder has leveraged their position to gain greater privileges and can then delete the forensic trail, this removes the possibility of any cloud user from becoming compliant with the requirements of the GDPR [1].

Compliance in the event of a cyber breach requires any company regulated under the GDPR to report the breach within 72 hours of discovery. However, if the forensic trail has been successfully destroyed by the intruder, it is much less likely that the breach will be quickly discovered. This provides the intruder with far more leeway to help themselves to Personally Identifiable Information (PII), thus leading to the possibility of receiving a higher level of fines due to greater theft of PII. Not only must the breach be reported, but it is vital to be able to identify which PII has been affected — a task that is likely to be impossible where the forensic trail has been compromised.

In the six years since 2012, when the global average time between breach and discovery was 6 months [2], thankfully that time has gradually being coming down. Sadly, it is nowhere near the 72 hours that the GDPR would like to see, and is still running in the range of weeks rather than days [3]. Given that the GDPR goes live on 25th May 2018, it is time for all cloud users to take notice.

Last year, Duncan and Whittington [4] warned of the dangers fast approaching. At that time, many cloud users thought they would not be subject to the provisions of the GDPR, however, a late change to the GDPR expands jurisdiction from the EU only to global for any cloud user holding the PII of any EU resident, anywhere in the EU.

These new concerns are what has prompted this special track. We believe that if we can address the Cloud Forensic Problem, we can at the same time mitigate the GDPR compliance problem for cloud users. Thus in the next section, we consider some of the approaches developed by the authors who have submitted to this special track.

II. THE CLOUD FORENSIC PROBLEM AND THE GDPR

We have a total of 14 very different approaches to resolving this problem. Clearly it must be solved, otherwise no cloud

user could ever guarantee being able to achieve security or privacy. Equally, without a solution to the cloud forensic problem, no cloud user will be safe from the massive potential fines that can be levied by the GDPR.

In "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?," Duncan [5] considers the magnitude of the challenge presented by the GDPR for for cloud users, particularly in the light of the as yet unresolved Cloud Forensic Problem.

In "A Study into Smart Grid Consumer-User Profiling for Security Applications," Mwansa et al [6] address user profiling using smart meters, and the concerns which users might consequently dislike.

In "Application of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education: A Higher Education Case Study," Beacham and Duncan [7] follow on from their 2017 paper [8], shifting their focus from mainstream education to Higher Education, and introduce a pilot case study.

In "Providing Tamper-Resistant Audit Trails for Cloud Forensics with Blockchain based Solutions," Neovius et al. [9] demonstrate a Blockchain based approach to providing better security for forensic records and the audit trail. This provides a good technical approach to consider how this could provide a more secure solution.

Since all companies are run by managers, we thought it might be useful to get the view of the people responsible for educating managers in Higher Education. In "A Management View of Security and Cloud Computing," Anomelechi et al [10] address security from a management perspective in order to better understand how management can be better persuaded to ensure a high level of security can be achieved for corporates from here on forward.

In "About an Immune System Understanding for Cloud-native Applications — Biology Inspired Thoughts to Immunize the Cloud Forensic Trail," Kratzke [11] takes a biology inspired view to harden the audit trail. We cannot rely on technical solutions alone, and any additional mechanisms that might help are well worth the exploring.

In "Could Block Chain Technology Help Resolve the Cloud Forensic Problem?," Zhao and Duncan [12] take a risk based approach to evaluating the risks inherent in Blockchain technology and various crypto-currencies to consider whether there would be any merit in trying this approach for secure logging or forensic and audit trail data.

In "Managing Forensic Recovery in the Cloud," Weir and Assmuth [13], consider a tighter approach to managing forensic recovery in the cloud and propose companies include a state of 'forensic readiness' as part of their forensic armoury.

In "Dark Clouds on the Horizon. The Challenge of Cloud Forensics," Renaud, Ferguson and Irons [14] provide an interesting background of the challenges and provide a fruitful take on serious discussion on how forensic approaches should look to the future.

In "Intruder Detection through Pattern Matching and Provenance Driven Data Recovery," Chapman [15] presents a novel method of dealing with lost or missing data, in order to attempt to identify when an intrusion has taken place.

In "Data Analysis Techniques to Visualise Accesses to Patient Records in Healthcare Infrastructures," Boddy et al. [16] use data analysis techniques to aid healthcare infrastructure security.

In "Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance," Duncan et al., [17] look at the use of a unikernel based approach to monitor live systems for cyber attack and to drive defence against the attackers. This promises the prospect of both a powerful deterrent, while also providing an efficient and lightweight mechanism.

In "Securing 3rd Party App Integration in Docker-based Cloud Software Ecosystems," Binkowski and Assmuth [18] consider the use of Docker-based cloud software ecosystems, and propose a novel means of ensuring a secure integration of applications within cloud ecosystems using Docker based components, in order to retain a much higher level of cloud forensic data.

In "Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming EU General Data Protection Regulation?," Duncan and Whittington [19] extend their previous work in this area and suggest there will now be a need to develop a new breed of forensic cloud audit specialists to deal with the Cloud Forensic Problem, and compliance with other legislation and regulation. These new specialists will be cross discipline, and will need to have an extensive understanding in audit techniques, forensics, legislation, regulation, cloud technicalities

III. Conclusion and Future Work

It is rather unfortunate that it has taken until now to focus minds on what is a very serious issue. Many have tried, and swiftly moved on to other things after discovering just how big a challenge it is. The arrival of the GDPR has certainly helped to focus our collective minds on what needs to be done, with a matter of some urgency. The authors you will meet presenting these works have all recognised the serious challenge this situation presents, and have not run away. Instead, they have focussed their minds on how to deal with such a serious challenge, resulting in all these different approaches to solving this problem. You should give them a great deal of credit for their perseverance.

A number of pilot studies have already started on a number of these solutions, and it may be that some of these solutions might be combined to provide an even more powerful solution. Make no mistake, this is a problem that will never go away. Attackers and intruders have had it far too easy up until now. It is time we woke them up, made them smell the coffee and make life so difficult for them that they are forced to move on to other pastures.

References

[1] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/

[2] Trustwave, "2012 Global Security Report," Tech. Rep., 2012.

[3] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016.

[4] B. Duncan and M. Whittington, "Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging," International Journal On Advances in Security, vol. 10, no. 3&4, 2017, pp. 155–166.

[5] B. Duncan, "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?" in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[6] M. Mwansa, W. Hurst, C. Chalmers, S. Yuanyuan, and A. Boddy, "A Study into Smart Grid Consumer-User Profiling for Security Applications," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[7] N. Beacham and B. Duncan, "Application of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education: A Higher Education Case Study," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[8] ——, "Development of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education," in Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Athens, 2017, pp. 1–4.

[9] M. Neovius, M. Westerlund, J. Karlsson, and G. Pulkkis, "Providing Tamper-Resistant Audit Trails for Cloud Forensics with Blockchain based Solutions," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[10] N. Anomelechi, W. Cooper, B. Duncan, and J. Lamb, "A Management View of Security and Cloud Computing," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[11] N. Kratzke, "About an Immune System Understanding for Cloud-native Applications — Biology Inspired Thoughts to Immunize the Cloud Forensic Trail," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[12] Y. Zhao and B. Duncan, "Could Block Chain Technology Help Resolve the Cloud Forensic Problem?" in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[13] G. Weir, A. Assmuth, and N. Jaeger, "Managing Forensic Recovery in the Cloud," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[14] K. Renaud, I. Ferguson, and A. Irons, "Dark Clouds on the Horizon. The Challenge of Cloud Forensics," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[15] A. Chapman, "Intruder Detection through Pattern Matching and Provenance Driven Data Recovery," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[16] A. Boddy, W. Hurst, M. Mackay, A. El Rhalibi, and M. Mwansa, "Data Analysis Techniques to Visualise Accesses to Patient Records in Healthcare Infrastructures," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[17] B. Duncan, A. Happe, and A. Bratterud, "Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[18] C. Binkowski, S. Appel, and A. Assmuth, "Securing 3rd Party App Integration in Docker-based Cloud Software Ecosystems," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.

[19] B. Duncan and M. Whittington, "Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming EU General Data Protection Regulation?" in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization. Barcelona, Spain: IARIA, 2018.