FAST-CCS: Finding a Solution to Cloud Cyber Security

Special Track running alongside CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

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

***Abstract*—Cloud computing has been with us for over a decade now. Cloud based systems present a multiplicity of attack vectors. Cloud users frequently fail to grasp the complexity of cloud ecosystems, and fail to monitor properly what is going on within their cloud ecosystem. Due to the failure to monitor properly, and the frequent time lag between penetration and discovery, cloud forensic trails have usually long been destroyed, leaving no real evidence with which to analyse the event to understand what has gone wrong. Understanding which data records have been accessed, modified or deleted becomes an exceptionally difficult task, which is likely to result in failure to comply with new data governance rules. In addition, cloud simulators are often used to teach students about the dangers of using cloud, yet these very tools have their own vulnerabilities. The aim of this special track is to try to identify some novel approaches to address a number of these problems, with a view to providing a much more robust approach to cloud cyber security. We present some 6 papers which provide some novel ideas for addressing these very real problems in a highly effective way.**

***Index Terms*—Cloud security and privacy; immutable database; forensic trail.**

I. Introduction

Cyber security is a challenging proposition for companies. When cloud is involved, this challenge can increase exponentially. The make up of a cloud ecosystem has become considerably more complex since it first evolved, leading to ever more complexity. Complexity can be seen as the enemy of security, due to the extreme difficulty in writing software in a secure way to run on cloud systems. This is particularly true where software from systems developed to run securely on conventional distributed networks is transferred over to run on the cloud, with the expectation that everything will run smoothly. While the software often continues to function well in terms of providing continuing functionality of operation, unfortunately this rarely extends to running securely on a cloud environment.

We have seen a great many technical solutions proposed and implemented over the intervening years, yet we continue to see systems being breached year after year, often using the same attack techniques. This situation is often perpetuated by management reluctance to take security sufficiently seriously to take even basic steps to safeguard their systems. Another issue, arguably of greater concern, is that company employees are contributing to this problem, through making errors, failing to update systems properly, or failing to follow security policies properly [1].

Some five years ago in 2012, Trustwave [2], were reporting an average time taken by enterprises of 6 months between breach and discovery. Discovery was often made by third parties external to the enterprise, rather than by the enterprise themselves. This time lag between breach and discovery has been significantly reduced since then, but nevertheless, remains a great concern, particularly in the light of forthcoming legislation, such as the EU General Data Protection Regulation (GDPR), coming into force in May 2018. Looking at the latest security breach reports, it is clear that many enterprises will be unable to comply with the requirement to report any breach within 72 hours.

While improvements have been forthcoming year on year, it is rather disappointing to discover that in the Trustwave 2016 report [3], we find that discovery time is now increased to an average of 200 days. In their 2015 cyber breach report, PWC [1], rather worryingly confirm these findings. It is obvious that companies are failing on a number of fronts, allowing much more serious breaches to continue to take place. This would suggest that many firms are not monitoring their systems properly, do not maintain proper audit trails, thus leading to inadequacy in retaining a proper forensic trail to understand exactly what information has been accessed, modified or deleted. Penalties for non-compliance can reach up to 4% of global turnover, an eye-watering sum for any company.

There are many other contributing factors which have helped to allow this worrying trend to continue. The costs to companies can be astronomical [1], with cyber breaches now estimated to be costing from £1.46m - £3.14m for large corporates, and £75k - £311k for small to medium sized enterprises (SME)s. Non-compliance fines will be extra, as will the costs, and lost business time, of recovering from such major incidents.

Duncan and Whittington [4] have written about the dangers surrounding failure to monitor cloud systems properly, and [5] have also written about the difficulties surrounding proper

audit of cloud based systems. They have talked about the need for enterprises to maintain a proper audit trail in their systems, and about the weaknesses arising as a result of poor configuration of database systems, particularly in the context of cloud systems [6]. They have proposed addressing this problem through the use of an immutable database for the purpose of secure audit trail and system logging for cloud applications [7].

The concerns surrounding these various issues are what have prompted this special track, which aims to try to resolve a number of these issues, particularly in the light of poor motivation by companies to protect themselves.

II. Why Conventional Technical Approaches Fail

The business architecture of a company comprises a combination of people, process and technology [8]. Yet, for years, many researchers have tried to solve these issues using technical solutions alone. Of the components of business architecture, technical systems are often well set up, but a great many are not. Company processes are usually well documented, especially the larger the company, although even much smaller companies are beginning to realise the benefits to be had from compliance with various standards, such as quality assurance, risk, security and privacy. The largest problem comes from the people in the organisation.

Cloud computing is mostly enabled by web serves, thus we look to the Open Web Application Security Project (OWASP), who carry out a survey every 3 years in which they collate the number of web vulnerabilities with the greatest impact on companies. In TABLE I we can see the top ten list from 2013, 2010 and 2007:

2013	2010	2007	Threat
1	1	2	Injection Attacks
2	3	7	Broken Authentication and Session Management
3	2	1	Cross Site Scripting (XSS)
4	4	4	Insecure Direct Object References
5	6	-	Security Misconfiguration
6	-	-	Sensitive Data Exposure
7	-	-	Missing Function Level Access Control
8	5	5	Cross Site Request Forgery (CSRF)
9	-	-	Using Components with Known Vulnerabilities
10	-	-	Unvalidated Redirects and Forwards

TABLE I. OWASP Top Ten Web Vulnerabilities — 2013 - 2007 [9]

OWASP provide simple but effective mitigation strategies to defend against such attacks. It is clear that this approach is doomed to failure due to the failure of the people within companies to actually carry out such simple mitigation and monitoring year, after year, just one example of the problems caused by people.

III. A Possible Alternative Solution

In a special track entitled "Finding a Solution to Cloud Cyber Security", running in Cloud Computing 2017, six papers are presented as part of a new approach to trying to resolve these known security problems. The first three consider how to deal with attacks on the cloud system. Duncan and Whittington [10], warn of the dangers of failing to monitor systems properly. It is clear from reviewing security breach reports that far from learning lessons in this regard, cloud users are taking longer and longer to realise that a breach has occurred.

In "Anomaly Detection in Cloud Based Application using System Calls", Aranitasi and Neovius [11] present a novel approach to anomaly detection, which is used to detect anomalous behaviour within cloud systems. Without such a system in place, it is virtually impossible to monitor what is happening within a cloud ecosystem.

In "Strategies for Intrusion Monitoring in Cloud Services", Weir and Aßmuth [12] adopt another novel approach to cloud forensics to highlight and report on intrusions before they become problematic. Too often, by the time a breach is discovered, the attacker has taken steps to eradicate all trace of the incursion, leading to extreme difficulty in carrying out a proper forensic examination of the breach.

Duncan and Whittington in [13] "Creating an Immutable Database for Secure Cloud Audit Trail and System Logging", suggest how the use of immutable databases for logging audit trail and system log data allows users to retain a forensic trail which can be used to properly analyse what happened in the case of a breach, allowing for the possibility of identifying all data affected and using it for proper forensic analysis.

Hurst et al. [14] in "Advancing the Micro-CI Testbed for IoT Cyber-Security Research and Education", consider how to provide improved training capabilities for students which are more realistic than those currently offered through simulation software. Reliance on simulation systems can cause cloud users to develop a false sense of security, due to the weaknesses inherent in such systems.

Beacham and Duncan [15], in "Development of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education", are working on a very interesting use case for cloud security. Providing a secure learning environment for children presents particular challenges, due to the potential dangers from certain unwelcome attackers, leading to great concerns, particularly from parents.

In "Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?", Duncan, Zhao and Whittington [16], consider how failure to understand cloud security risks properly can cause major issues for corporate cloud users. Many corporate cloud users have a poor understanding of all the cloud cyber risks they face, and frequently underestimate the impact of such breaches taking place, both in regards to cost impact, and the disruptive impact to the company.

References

[1] PWC, "Price Waterhouse Coopers," 2015. [Online]. Available: http://www.pwc.co.uk/ Last Accessed: Jan 2017

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

[3] Trustwave, "2016 Trustwave Global Security Report," Chicago, Tech. Rep., 2016.

[4] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement," in *14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. (IEEE Trust.*, Helsinki, Finland, 2015, pp. 1088–1093.

[5] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Cloud Audit Problem," in *Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization*. Rome: IEEE, 2016, pp. 119–124.
[6] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in *Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization*. Rome: IEEE, 2016, pp. 125–130.
[7] B. Duncan and M. Whittington, "Cloud Cyber-Security: Empowering the Audit Trail," *Forthcom. Int. J. Adv. Secur.*, vol. v9, no. 3&4, p. 15, 2016.
[8] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.comwww.bis.gov.uk Last Accessed: Jan 2017
[9] OWASP, "OWASP Top Ten Vulnerabilities 2013," 2013. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project Last Accessed: Jan 2017
[10] B. Duncan and M. Whittington, "The Importance of Proper Measurement for a Cloud Security Assurance Model," in *2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci.*, Vancouver, 2015, pp. 1–6.
[11] M. Aranitasi and M. Neovius, "Anomaly Detection in Cloud Based Application using System Calls," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–5.
[12] G. Weir and A. Aßmuth, "Strategies for Intrusion Monitoring in Cloud Services," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–5.
[13] B. Duncan and M. Whittington, "Creating an Immutable Database for Secure Cloud Audit Trail and System Logging," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–6.
[14] W. Hurst, N. Shone, A. E. Rhalibi, A. Happe, B. Kotze, and B. Duncan, "Advancing the Micro-CI Testbed for IoT Cyber-Security Research and Education," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–6.
[15] N. Beacham and B. Duncan, "Development of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–4.
[16] B. Duncan, Y. Zhao, and M. Whittington, "Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?" in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–6.