A summary of the Summer School on Cloud Computing

report for "IMT6003 - COINS Summer School - 2015" @ Metochi

by PhD Candidate Andrii Shalaginov
andrii.shalaginov@hig.no
Høgskolen i Gjøvik, Norway

September 21, 2015

Abstract

This report reflects a content of a COINS summer school that happen in August 2015 with s special focus on Cloud Computing. In this work author also provides a parallel line with the research in Digital Forensics and its applications. Below the summery of every day is given together with a defined questions related to the presentations.

Keywords: Cloud Computing, Network Security, Forensics, SDN, Virtualization

1 Friday 21/8 - ENISA visit

European Union Agency for Network and Information Security (ENISA)[1]. During this meeting students learned about the largest non-profit security-oriented organization that provides a consultancy and advisory services across Europe. ENISA is not a Computer emergency response teams (CERT), yet has a mission to exchange best practices in Information Security, to bridge different communities and to provide expertise on demand. Among the areas of interest there were mentioned three main: *development of regulations*, *policy implementation* and *cooperation between parties.* Moreover, ENISA offers cybersecurity exercises and trainings for governmental organizations as well as for SME. Variety of training resources are available on the ENISA resources website[2], which includes digital artefact analysis, mobile threats,

[1] https://www.enisa.europa.eu/

[2] https://www.enisa.europa.eu/activities/cert/training

digital forensics, advanced persistent threats, honeypots, etc. Some of these resources are available absolutely free of charge to general public and some of the courses are provided upon request.

Along with information about ENISA the Eropean Cyber Security Challenge[3] has been presented as an initiative to gather specialists in the area and find out most talented ones based on the competition results. Additionally, the European Cyber Security Month[4] was described as an advocacy campaign that take place in October and supported by ENISA. Main goal of the Security Month is to enhance the awareness of the employee on the working places about the cyber security threats and culture in addition to better understanding of Cloud solutions.

2 Sunday 23/8 Teaching

On the first day of the summer school there was initial Information meeting devoted to Metochi study center and 1^{st} COINS Summer School. Then, *Sandra Scott-Hayward* from CSIT (Belfast, UK) gave morning and afternoon sessions on SDN security. SDN states for Software-defined networking, where the software abstraction was included for better flexibility and broader functionality. One of the main applications of the SDN is a basis for IaaS, where SDN together with the VM resources may provide very flexible distributed solutions to the customers. Though the programmability of such hybrid architecture might be in opposite dependency with respect to the provided bandwidth. The architecture typically includes *Infrastructure*, *Controller* and *Applications*. One of the nice examples of the protocols between that makes a transit between the *Infrastructure* and *Controller* is OpenFlow used to control forwarding behaviour of Ethernet switches, which however has a lot of security concerns, like man-in-the middle attacks, etc. Number of attacks against SDN were mentioned: Unauthorized Access, Data leakage, DOS, Compromised applications that affect all three layers of the architecture. With respect to this, SDNsecurity.org[5] was established to address and resolve security problems related to SDN. Moreover, Sandra showed some possible ways of protections against different attacks scenarios like Policy chaining and permissions categorization.

Question 1: Can we consider NSaaS (Network Security as a Service) as the one applicable only for IaaS or it can be considered also within SaaS and PaaS scopes.

[3] `http://www.europeancybersecuritychallenge.eu/`

[4] `https://cybersecuritymonth.eu/`

[5] `http://sdnsecurity.org/`

Response: Sandra said that it can be any kind of infrastructure where the SDN security is applicable as a Network Security service, including physical or virtual environment.

Finally, a PhD student *Vivek Agrawal* presented his work on "Secure migration to the cloud", which was also published as a book chapter. The topic is related to the problems that arise with the security policies and SLA agreements when a company wants to migrate to or from Cloud.

3 Monday 24/8 Teaching

On the second day, *Zhiqiang Lin* presented during morning and afternoon sessions a survey and extensive study of Virtual Machine Introspection (VMI) as a hypervisor-based monitoring in the host virtualization environment. Generally one can distinguish Virtualization with hypervisors of the following types: *Type-1* that run directly on the hardware and *Type-2* that use operation system on host. The first type provides better performance, while the second type gives a bit better scalability. The general development of computer architecture went from multi-tasking to multi-OS in 1974. The VMI is a techniques similar to exception of the system in real-time mode to ensure that there are no viruses or malicious activity happen. The most important thing is that it can happen in read-only mode and does not necessarily inform a guest VM or require it consent. Such anti-malware technique is launched on the host machine to monitor the guest machine even in case when the malware is smart enough to disable the anti-malware protection inside the guest machine. The VMI was described by Garfinkel et al. [6] for network security. This is applicable for network forensics and logs preservation for better evidences extraction when malicious and illegal activity happened inside the guest VM. This is relevant to the forensics in terms that the states of the guest OS can be gathered at any moment in read-only moment for further analysis and inspection by different forensics methodologies.

Question 2: Is it possible to apply VMI techniques for monitoring malware that could possibly run on the Graphics processing unit (GPU), which can be considered as a shared resource as in case of Xen.

Response: It is possible since the resources are used within a guest machine and corresponding Vm kernel hooks on the side of host may be utilized. For example, in case of Xen the GPU is a specific resource that can be assigned to any of the virtual machine during the boot time. Moreover, there can be an array of GPU on a single physical machine. So, there might

[6] `http://suif.stanford.edu/papers/vmi-ndss03.pdf`

not be that trivial task to detect malicious code that is executed, yet still it is not a trivial task and requires knowledge for analysis of GPU's code.

After dinner: *Sachin Shetty*: Moving Target Defence (MTD)[7] is a new concept that appears recently and whose main idea is to evaluate threats and to increase uncertainty in the system in order to improve the defensiveness. The main problem in static systems is the inability to protect them when the behaviour of the system is deterministic or predictable. There exist different techniques like instruction set or address space randomization.

4 Tuesday 25/8 Teaching

On the third day *Sachin Shetty* gave a lecture on the End-to-End Defence against Kernel Rootkits in a Cloud Environment. Rootkits are one of the most dangerous malicious software that can execute different actions such that decrypting SSH or PGP in the memory. Sachin described how an attacker can execute different codes including hijacking of system calls, changing the system calls table, etc. Rootkits pose especial danger for Cloud Computing because of many different applications operate variety of data in the same virtualized environment including IaaS, PaaS and SaaS. The most harm can be done from rootkits that are designed intentionally to operate on IaaS since they can gain an access over not only guest VM, yet over all physical host system. Sachin also mentioned several possible properties of defending the kernel rootkits in the Cloud Environment: (i) *End-to-End defence* intends to manually analyse a target system and prevent from further modifications, (ii) *Scalable defence* defines the overhead, scalability and add-on protection costs that have to be as linear as possible, (iii) *Adoptable defence* presents compatibility with modern frameworks and platforms. Most of the existing commercial anti-virus solutions offers protection, yet in a Cloud environment it becomes useless due to enormous overhead,. One of the practical examples of the End-to-End defence is a system called RootkitDet[8], which can effectively detect kernel rootkits with overall overhead of 1%. In our opinion such system helps forensics analysis to analyse how the system becomes vulnerable to a specific attacks and what are the possible vulnerabilities. Furthermore, reversing a rootkit may lead to a physical attacker or at least to understand likely involved parties.

Question 3 was related to whether the black and white lists may facilitate detection of kernel rootkits in the Cloud Environment and what are the limitations.

[7] `http://www.dhs.gov/science-and-technology/csd-mtd`

[8] `http://link.springer.com/chapter/10.1007%2F978-3-319-11212-1_27`

Response was that it is possible to do on the kernel memory strictures, yet requires additional resources since the memory structures are dynamic trees of different resources allocated. Moreover, it might facilitate fast detection, yet the number of possible combination may vary from version of kernel, installed software and used data. Sachin mentioned that RootkitDet can address it by registration of the LKM (Loadable Kernel Module).

Evening sessions concluded *Daniel Hedin*, who presented a view on the Cloud application security, First, a broad description of different aspects of Cloud Computing were given such that properties of Cloud apps like Simplicity, Availability, Collaboration. One of the nice examples of such app was Vivino[9] that aggregates an access to multiple services such that Google+ or Facebook. Such applications also represent a great interest since they can be investigated under the Cloud Forensics, which is currently promoted by ENISA (European Union Agency for Network and Information Security)[10]. However, many cloud applications can be consdired as a web-applications and therefore are affected by XSS and other types of attacks according to OWAS Top 10[11]

After dinner *Andrei Costin*, who works with embedded devices security, gave a speech on his experience in doing a Ph.D.

5 Thursday 27/8 Teaching

During the morning session *Andrei Costin* presented a work on Security of Network Monitoring Systems (NMS) for Cloud and HPC. One of the way of observing the behaviour of the system is so-called Network Monitoring Systems (NMS) that are deployed over the High-Performance Computing (HPC) architecture. Some of such systems are Ganglia, Nagios, Zabbix, Cacti/SNMP, etc. Andrei focused in particular on the Ganglia and how it can be compromised. During the first stage of Attack life-cycle leaked information is collected. On the second stage, an initial compromise is performed by means of exploiting web-applications such that XSS or remote code execution. Further, such attacks as buffer overflow, CVE exploits, process mimicry can be executed to escalate the privileges and to maintain the presence in the system respectively. After theoretical parts, Andrei demonstrated the lifecycle of attacks on Gagnlia in Norway. In particular through Google dorsk -

[9] https://www.vivino.com/

[10] https://www.enisa.europa.eu/

[11] https://www.owasp.org/index.php/Top_10_2013-Top_10

Google Hacking Database (GHDB)[12] and search engine Shodan[13] there have been found 364 Gangllia installation. Moreover, about 40k nodes were publicly exposed to the network or also called information leakage through the web. In overall after data analysis there have been found that almost all of the 35 available versions of Ganglia affected by vulnerabilities. Also Andrei provided virtual machine images for exercises on the testing the flows and developing simple exploits as well as securing the MNS by password protection and decreasing the privilege of user.

Question 4: Can we consider available installations of NMS as a threat to Operations Security of organization.

Response: Undoubtedly, revealing the monitoring and corresponding entire architecture information may results in worse system compromise. However, static analysis of the systems may reveal such unnoticed vulnerabilities and reduce the risk of information leakage.

In the evening session *Kaniz Fatema* gave a talk on the Privacy in cloud environment. There was an interesting survey revealing that people tend to give up sensitive information to unknown parties more often than necessary. At this point, no way to ensure the privacy and that the information is stored properly. At the end of the session Kaniz made a survey and we found that many people consider the habits information and music tastes as somewhat sensitive.

6 Friday 28/8 Teaching

During the morning session *Kaniz Fatema* followed the Privacy in cloud environment lecture. There can be found number of Laws and Privacy and data security across the world. In total 109 countries have implemented data privacy laws. Kaniz gave a comparative study on different laws with respect to accountability, use limitations, security, breach notification, etc. There was also presented an nice view on Security vs Privacy with respect to Confidentiality, Integrity and Availability. An examples on the privacy breach by other persons followed up with the possible dangers as identity theft, harm, loss of business, etc. In overall, we can defined following *data life-cycle in Cloud*: Generation, Transfer, Use, Share, Storage, Archival and Destruction. Kaniz showed that customer privacy in the Cloud is affected by legal compliance, location control as well as Authentication and Authorisation. Finally, it was concluded that Cloud service providers have to work hard to ensure

[12] `https://www.exploit-db.com/google-hacking-database/`

[13] `http://www.shodanhq.com/`

that the private data are stored and handled properly and customer's right on privacy is preserved.

Evening session by *Daniel Hedin* on Cloud application security was a conclusive talk for the COINS Summer School. In particular, we focused on Information Control Flow (IFC) exercises. We refer to the challenge posted at Chalmers[14]. The main idea is to leak information on every step, which will give a pass-phrase leading to the next stage of the challenge.

Question 5 was about whether the IFC can be the only tool in this scenario when new information is necessary for a successful attack.

Response was that this is the most optimal tool for dealing with attacks where the information required for further performing an attacks becomes available on each step of the compromise.

[14] `http://ifc-challenge.appspot.com/steps/start`