REFLECTION REPORT FOR ESORICS 2017

Coins has funded my participation for both Secure Cloud Services and Storage Workshop 2017 as well as the ESORICS conference

I. About the Secure Cloud Services and Storage Workshop 2017

The Norwegian Research Council, through the Cryptographic Tools for Cloud Security project, has funded the cloud services and storage workshop, which was held on Oslo.

With a panel of speakers from both academia and industry, the workshop was an excellent opportunity to become aware and discuss the latest security advancements with regards to providing security guarantees to cloud and storage services.

The rest of this report will present some of the main takeaways of the workshop.

1. Selected Security and Privacy Schemes for Cloud Computing

Dr. Refik Molva first presents the main motivation behind outsourcing computation and storage to cloud services. These can be summarised in: high availability, no maintenance, decreased costs, elasticity & flexibility. Such a model does not come at no cost, as it introduces several security risks to the end user adopting it.

This new computational model has introduced new security requirements in order to gain back trust that the data and computation and being performed by the cloud provider following the security requirement of the end user.

For instance, one solution to provide the end user with integrity guarantees over its stored data are Proof of Retrievability schemes. The main challenge here is to provide such a proof to the end user without having to do any computation at the client side, as well as avoiding any bulk data transfer over the network.

One solution which has been proposed by Dr. Molva is the StealthGuard presented previously at ESORICS 2014. This is a probabilistic scheme that draws upon the idea of tagging blocks then randomly verifying them. Furthermore, this scheme allows for an unlimited number of verification queries.

The speaker also pointed out that securing cloud storage, is sometimes in conflict with the business model of cloud providers. For the latter, being able to duplicate data is essential for them, since it allows them to store the same duplicated data of different users only once.

2. Securing Cloud-Assisted Services

Dr. Asokan discussed in this scheme how cryptography can be combined with some recent system architecture advancements in order to provide solutions for the new ways in which people are starting to use cloud services.

One specific example the talk focused on is cloud based malware scanning, which would require to know the apps running on user' platform in order to check whether it is malicious or not, at the same time the user would want to preserve his/her privacy while using this service.Naïve encryption solution don't solve this as they leak meta data about the user through which the service provider can infer and have access to security sensitive data about the user.

The two main attack vectors for the service provider when data is encrypted is through measuring the dictionary's processing time and measuring query-response time.

To protect against this attacks, the scheme should spend equal time processing each dictionary entry and only respond after one full carousel.

II. About ESORICS

The European Symposium on Research in Computer Security (ESORICS) was held in Oslo during its 2017 edition. It is a well-established security conference which draws high quality research papers in different fields.

In the rest of this report, I will present the main takeaways of the talks that were most relevant to me.

3. Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android

Given the ubiquous use of mobile phones as well as their increasing acceptance within enterprises, malware writers are turning their attention and focus towards them. Indeed, mobile phone have access to valuable data such as location, photos and messages. The presentation discussed how sandboxing and running applications within this sandbox is used in android in order to detect malware. However, these sandboxes are usually emulators that an intelligent malware can detect, and only trigger its malicious payload when it is running outside of the emulator. This allows the malware to evade detection and continue into running undetected within the user's platform.

The speaker presented his new solution, mirage, which can be extensible against softwar and can dynamically detect malware which tried to evade detection within the sandbox.

4. Securing Data Analytics on SGX with Randomization

Outsourcing computation to remote cloud providers presents a number of advantages to enterprises and individuals alike. However, the security risks that such a model introduces, especially in terms of privacy has prevented many workload from moving into the cloud. Hence, the quest of a trusted execution environment within that would give us confidentiality and integrity guarantees for our computation has been a highly sought after security property.

Intel guard extensions which are a processor based security extension give the promise of achieving such guarantees. However, a number of research papers have shown how the confidentiality guarantees can be compromised by side channel attacks. While a number of mitigation techniques have been proposed in order to guard against these side channel attacks, most of them are not practical enough as they add a lot of overhead to the running application, especially if it is a real time one. The speaker presented in this paper a defence strategy that can achieve higher computational efficiency with a small trade-off in privacy protection. This is mainly achieved by adding noise to traces of memory access observed by an adversary, with the use of dummy data instances