Scientific Report

First name / Family name	Antonis Michalas
Nationality	Greek
Name of the *Host Organisation*	SICS
First Name / family name of the *Scientific Coordinator*	Christian Gehrmann
Period of the fellowship	13/01/2014 to 13/01/2015

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

While the cloud computing model is maturing, the increasing complexity of the underlying technology introduces many new security risks and challenges. The list of risks is long, and the relevant threats and mitigation technologies have been under intensive scrutiny in recent years, while the industry is investing in enhanced security solutions and issuing best practice recommendations to the business actors. Nevertheless, decision makers hesitate to move critical information systems to public cloud environments, mainly due to security concerns.

Security is a multifaceted process and beyond best practices there is no “one size fits all” solution for all cloud usage scenarios. Indeed, different models have distinct attack surfaces, and the required level of security heavily depends on the end-applications' requirements and the relevant trust model.

During my ERCIM fellowship, my research mainly focused in the field of Infrastructure-as-a-Service (IaaS) cloud security. To this end, along with my colleagues, we introduced an overview of requirements that must be considered when an organization migrates to the cloud. This cloud migration guide, was coupled with a list of security threats that must be considered when moving to the cloud and can be used as a walkthrough to avoid common pitfalls and design even better and more secure IaaS environments.

Furthermore, we extended previous work on applying Trusted Computing technologies to strengthen infrastructure cloud security. As a result, end-users can place hard security requirements on the cloud infrastructure, while maintaining exclusive control of the security critical information assets. To this end, we designed a holistic security framework which consists of three major building blocks:

- Protocols for secure launch of virtual machine instances on infrastructure clouds;
- Key management and encryption enforcement functions for virtual machines, providing transparent encryption of persistent data storage in the cloud;
- Key management and security policy enforcement by a specific trusted anchor point - the Trusted Third Party (TTP);

Next, we identified the absence of a secure access control for the above mentioned framework. We tried to fill this gap, by introducing an XML-based language framework that allows users to define role-based access control in order to grant access, based on permissions, to other users in the IaaS cloud. Our protocol allows a granular access rights management per VM instance and storage device.

Last but not least, one problem that caught our attention is the data geolocation in the cloud. Lately, along with the already traditional questions about the safety of cloud environments we have also seen concerns about the physical location of data and its availability in different jurisdictions. By storing data in the cloud, users hand it over to a provider that may have data centres in different geographical locations, countries or even continents. However, organizations that work with sensitive data, such as health records, or financial data, need complete control over the physical storage location and data access. As a result, storing sensitive data in the cloud complicates adherence to regulatory compliance laws, since such data may fall under different regulations depending on where it is physically stored. If for example data is moved to a different country, a different set of rules may apply.

Based on that, we presented a theoretical analysis of the existing trusted geolocation systems for the cloud. We used this analysis to demonstrate the inefficiencies as well as the strengths of existing protocols and redefine the important research questions in cloud data geolocation in the

hope to spawn further research in the area.

Finally, as a continuation of my PhD research, I designed a privacy-preserving reputation system for participatory sensing applications. Recent advances in sensing, computing, and networking have paved the way for the emerging paradigm of mobile sensing. The openness of such systems and the richness of user data they entail (collect valuable data, practically from everywhere) raise significant security and privacy concerns. Having this in mind, I designed a protocol that allows users to keep their real identity hidden, while at the same time they have a reputation score for which they cannot lie about or shed. Additionally, the proposed protocol provides accountable anonymity. Users are able to exchange information in a lawful manner without being tracked while on the other hand, misbehaving users will lose their anonymity and they will encounter the repercussions that are defined from the community regarding malicious behaviours.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Nicolae Paladi, Antonis Michalas and Christian Gehrmann. "*Providing End-User Security Guarantees in Public Infrastructure Clouds*". IEEE Transactions on Cloud Computing, a special issue on Cloud Security Engineering, IEEE, 2015. **(Under Submission)**
Abstract: The infrastructure cloud (IaaS) service model provides resource flexibility and increased availability; tenants are insulated from the minutiae of hardware maintenance and can purchase computational, network and storage resources to deploy and operate complex systems. Large-scale services running on IaaS platforms demonstrate the viability of this model. Nevertheless, many organizations operating on sensitive data do not migrate operations to IaaS platforms due to security concerns.

In this paper, we describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. The framework description is followed by an extensive theoretical analysis where we formally prove protocol resistance against attacks in the defined threat model. The protocols allow to establish trust by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data kept in remote storage, with the encryption keys being kept outside of the IaaS domain. The analysis is coupled with experimental results demonstrating the validity and efficiency of the proposed protocols. The framework prototype was implemented on a test bed operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments.

Antonis Michalas, Nicolae Paladi and Christian Gehrmann. "*Security Aspects of e-Health Systems Migration to the Cloud*". In the 16th International Conference on E-health Networking, Application & Services (Healthcom), October 15 - 18, 2014, Natal, Brazil. **(Presented)**
Abstract: As adoption of e-health solutions advances, new computing paradigms - such as cloud computing - bring the potential to improve efficiency in managing medical health records and help reduce costs. However, these opportunities introduce new security risks which can not be ignored. Based on our experience with deploying part of the Swedish electronic health records management system in an infrastructure cloud, we make an overview of major requirements that must be considered when migrating e-health systems to the cloud. Furthermore, we describe in-depth a new attack vector inherent to cloud deployments and present a novel data confidentiality and integrity protection mechanism for infrastructure clouds. This contribution aims to encourage exchange of best practices and lessons learned in migrating public e-health systems to the cloud.

Nicolae Paladi, Antonis Michalas and Christian Gehrmann. "*Domain Based Storage Protection with Secure Access Control for the Cloud*". The 2014 International Workshop on Security in

Cloud Computing, held in conjunction with the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), June 3, 2014, Kyoto, Japan. **(Presented)**
Abstract: Cloud computing has evolved from a promising concept to one of the fastest growing segments of the IT industry. However, many businesses and individuals continue to view cloud computing as a technology that risks exposing their data to unauthorized users. We introduce a data confidentiality and integrity protection mechanism for Infrastructure-as-a-Service (IaaS) clouds, which relies on trusted computing principles to provide transparent storage isolation between IaaS clients. We also address the absence of reliable data sharing mechanisms, by providing an XML-based language framework which enables clients of IaaS clouds to securely share data and clearly define access rights granted to peers. The proposed improvements have been prototyped as a code extension for a popular cloud platform.

Antonis Michalas and Nikos Komninos. "*The Lord of the Sense: A Privacy Preserving Reputation System for Participatory Sensing Applications*". In the 19th IEEE Symposium on Computers and Communications (ISCC), June 23 - 26, 2014, Madeira, Portugal. **(Presented)**
Abstract: Electronic devices we use on a daily basis collect sensitive information without preserving user's privacy. In this paper, we propose the lord of the sense (LotS), a privacy preserving reputation system for participatory sensing applications. Our system maintains the privacy and anonymity of information with the use of cryptographic techniques and combines voting approaches to support users' reputation. Furthermore, LotS maintains accountability by tracing back a misbehaving user while maintaining k-anonymity. A detailed security analysis is presented with the current advantages and disadvantages of our system.

Nicolae Paladi and Antonis Michalas. "*"One of Our Hosts in Another Country": Challenges of Data Geolocation in Cloud Storage*". In the 6th IEEE Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), May 11 - 14, 2014, Aalborg, Denmark. **(Presented)**
Abstract: Physical location of data in cloud storage is an increasingly urgent problem. In a short time, it has evolved from the concern of a few regulated businesses to an important consideration for many cloud storage users. One of the characteristics of cloud storage is fluid transfer of data both within and among the data centres of a cloud provider. However, this has weakened the guarantees with respect to control over data replicas, protection of data in transit and physical location of data. This paper addresses the lack of reliable solutions for data placement control in cloud storage systems. We analyse the currently available solutions and identify their shortcomings. Furthermore, we describe a high-level architecture for a trusted, geolocation-based mechanism for data placement control in distributed cloud storage systems, which are the basis of an on-going work to define the detailed protocol and a prototype of such a solution. This mechanism aims to provide granular control over the capabilities of tenants to access data placed on geographically dispersed storage units comprising the cloud storage.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

- 6th IEEE Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), May 11 - 14, 2014, Aalborg, Denmark.
- 19th IEEE Symposium on Computers and Communications (ISCC), June 23 - 26, 2014, Madeira, Portugal.
- 16th International Conference on E-health Networking, Application & Services (Healthcom), October 15 - 18, 2014, Natal, Brazil.
- ABCDE seminar IV, October 23 - 24, 2014, Pisa, Italy.