Trust Management for Vehicular Cloud Computing

Marcela Roxana Farcasescu
West University of Timisoara, Department of Informatics and Mathematics, Bd. Vasile Parvan, Timisoara, Romania

1 RESEARCH PROBLEM

In the last years, the business model of cloud computing has spread viral in several domains, promising to change the way we think about computing and data storage. One of the biggest concerns in cloud adoption since 2009, is considered to be the trust offered from both perspective – cloud-end user and cloud provider. A new and challenging field that highlights the need of defining the trust management concept is vehicular cloud computing.

Stephen Olariu and his team have define the vision of vehicular cloud computing as a pool of resources which need to be carefully handled by a trusted interested party.

This is why the current paper is going to combine two of the main challenges in Vehicular Cloud Computing by creating trust models: the authentication of the owner of the car and the geolocation data sharing. The infotaiment unit of a vehicle will soon have installed an accesible operating system which is already used for our mobiles, tablets, gadgets, etc. In this way, all the current applications that can be installed on our gadgets will soon be adapted to the infotaiment unit, which means that the vehicular cloud will become a necesity. With this in mind, the authentication of the owner of a car will become an important security issue, while the geolocation data sharing will remain a critical privacy concern.

The innovative approach is to build trust models based on driver's behavior as the owner of his vehicle, using the geolocation as a strategical item in validating the user's actions and requests. The attacks simulation will consider the scenario of loosing ownership of the vehicle and providing fake geolocation data.

2 OUTLINE OF OBJECTIVES

The main activities of the research will be to:

- Outline the security challenges in cloud computing but also in vehicular cloud environments
- Mitigate the importance of a trust management in a cloud environment
- Build trust models for driver identification and vehicle's localization
- Apply the trust models and analyse the results
- Perform attack simulations: attacker as a driver and fake geolocation received
- Interpretation of the results by providing a final conclusion on the confirmed or infirmed theory

The research will be conducted from two main directions: how to trust the information provided by the driver and how to trust the services used in communication (the information requested by the service will be used only for obtaining the needed data and not for other purposes).

Before getting into the exact details, the main concepts used, need to be defined.

3 STATE OF THE ART

Concepts review:

- Cloud Computing

Cloud computing combines in a successful recipe the advantages of the grid computing with the service-oriented. This introduces an elastic and rapid provisioning service consumption model. Cloud computing can overcome the running out of capacity, capacity excess costs, tied-up capital. The main characteristics of the cloud computing concept are: on-demand self-service or pay-as-you-go, rapid elasticity, resource pooling, measured service[Bernd Grobauer]. In order to adopt cloud computing, a cloud model should be chosen that will cover the business needs (SaaS, PaaS, IaaS), the provider roles and capabilities should be analysed, determine the dependencies on the cloud provider, establish and negotiate the SLA (Service Level Agreement), have an exit strategy – in case the cloud provider will disappear from the cloud ecosystem.

Cloud Security is a sub-domain of the computer security that includes all the policies, controls,

Farcasescu, M.
Trust Management for Vehicular Cloud Computing.
In *Doctoral Consortium (DCCLOSER 2016)*, pages 14-17

deployment techniques used in the infrastructure of the cloud computing. Cloud based security refers to the services present in the cloud environment. The focus of this research paper relies on the sub-domain of cloud based security.

- Vehicular Cloud Computing

Vehicular cloud computing represent an extension of the cloud computing paradigm describing: "a group of largely autonomous vehicles whose corporate computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users"[Md Whaiduzzaman]. A shorter definition redesigns the concept of a vehicle in the cloud computing context, describing it as driver's dependent entities, service providers and communication tools. The differences between cloud computing and vehicular cloud computing are

The main challenges of both of the paradigms are establishing a reliable trust context for each vehicle involved in the communication, but also to trust the information provided by those entities. This is why the trust management concept is required when discussing about the security and privacy concerns of the vehicular cloud computing.

- Trust Management

Similar to the cloud computing, the trust concept has multiple definitions, because it can be seen from different perspectives: customer's and cloud vendor's point of views. Trust is "the subjective probability by which an individual, expects that another individual, performs a given action on which its welfare depends"[Talal H]. Trust represents "more than the authorized nature of security relations between human societies, from a stable and healthy operation to a large extent thanks to the trust relationship between the individuals, groups and organizations."[R. K. L. Ko, P. Jagadpramana]

Marsh was one of the first researchers of the computational trust. In the trust model that he proposed as a direct interaction between agents, he divided trust in three categories [Marsh S.]:

- Basic Trust - based on experiences from the past
- General Trust - the trust that an agent has in other agent
- Situational Trust - the amount of trust that an agent has in other agent in a specific situation

The bidirectional relationship between two agents can be described at any moment by using the degree of trust represented by the three categories. Trust management represents the trust analysis between agents using trust metrics that rely on reputation, deception, persuasion and the optimal decisions taken according to the trust level found. The trust management techniques can be classified in four main categories: policy, recommendation, reputation, prediction. For each category, specific trust models can be created. A trust model can be described by a set of rules that reflect the relationship between the cloud provider and customer.

4 METHODOLOGY

4.1 Building the Trust Models

The trust models will be created as sets of rules established by the cloud provider or end-cloud user using a Rule Based Engine (for example the Business Rule Engine from WSO2). The set of rules will reflect a specific policy or recommendation.

The trust models will be used later on at the authentication and geographical location identification phases. The geo-location can be also used as a second authentication factor.

From the authentication perspective, we would like to try to focus on personal gadget (owned device) usage as an authentication method in order to gain access to the infortaiment (the entertainment unit from the vehicle) data. If the owner of the car is not recognized, the current driver should have limited access to the information presented on the infotaiment unit. The recognition will be done using the sensors of the owned device which will interpretate the user behaviour in the vehicle. On the other side, geo-location can be used to confirm that the driver behaviour.

Geo-location is a concept used in "information systems security cycles to extrapolate the geographical location of a subject (person or system)". There are several Location-Based Service (LBS) applications on different platforms that currently challenge the user's trust levels and privacy. The LBS application use the geolocation data to obtain other information for the user. Usually are installed on personal devices and help in researching for specific points of interest (eg. restaurants, museums, etc). The main difference between Geolocation Services and Location-Based Services is that the first ones don't require an accurate user address and the primary objective is to protect the user's privacy.

For the Geolocation model, the GPS data will be collected using driver's gadgets and the infotaiment unit. After establishing a set of rules for each cloud provider, a trust score will be associated considering

the number of touched rules per policy (a rule will be considered "touched" if the condition or criteria used in the rule was fully respected).

4.2 Collecting the Data

The data will be collected using mobile phones, tablets, other gadgets sensors. Usually the devices have built-in sensors that measure motion, orientation, and various environmental conditions. The sensors will provide raw data with high precision and accuracy, monitoring three-dimensional device movement or positioning, or ambient environment changes. The sensors can be classified as: environmental, motion and position sensors.

The purpose of the collected data is to be used as an input for the trust models created in order to approve or decline further access through the cloud ecosystem.

After collecting the data, an heuristic approach will be used in identifying similarities and use the input data as a further authentication schemas.

4.3 Attack Simulations

The next steps will be to prove by simulating attacks that the heuristics chosen are actually providing the expected results and try to improve those to address possible attack scenarios.

A. Stolen Device

A possible scenario can be considered when the drivers gadget or owned device it's now in attacker's hands. An attack graph will be created looking at the chances of the attacker to gain full access to the infotaiment data using the stolen device.

B. Fake Geolocation Data

Another possible scenario is when the attacker which already stolen the device from the driver is sending fake geolocation data. An attach graph will be created to analyse all the possible scenarios.

4.4 Preparing for Vehicular Cloud Computing Outages

The outage concept refers to the unavailability of a service that usually it is a consequence of a server loss of electricity power or malware blockages[Nicholas Car]. Outages could be a serious security vulnerability for a cloud ecosystem. When an outage occurs in cloud computing, there are two key factors: the type of outage and the time needed for service recovery.

Outages can be scheduled or unexpected. If the cloud provider is scheduling an outage for administration reasons each month at the same date time, the service outage can be easily tracked and used in malicious scopes. An unexpected outage can occur due to a malware attack that takes down the DNS servers. When an outage is analyzed, security issues must be considered in order to detect the root causes. After an outage in cloud computing, the cloud vendor should present the problem and explain the identified issue. If this is not possible, the viability of the cloud services will be usually questioned. The focus of the cloud provider is to prepare for outages, not to avoid them. Prediction might also be beneficial, but it implies processing a lot of monitoring data and might result in too many false-positive alarms.

In particular for vehicular cloud computing, an outage is actual represented by a missed communication between the vehicle and the cloud which means that the data from the vehicle to the cloud is not transferred anymore or the vehicle doesn't receive anymore data from the cloud. This situation can occur while driving in the areas where the communication is not possible (depending on the channel used).

5 EXPECTED OUTCOME

The expected outcome is to confirm the advantages and disadvantages of using the trust management in vehicular cloud environments by analysing the obstacles and proposed -solutions. The expected results will highlight the need of implementing the trust models for the vehicular cloud computing environment.

6 STAGE OF THE RESEARCH

A few attempts for building the trust models were already perform in order to extract the difference between what the customer provided and what the services collect with or without the end-user's approval.

Currently, I am in the process of collecting the data from several owned devices like tablets, mobile phones, fitness braces. After collecting the data the next step will be to implement the trust models

which will contribute to the driver identification.

ACKNOWLEDGEMENTS

This work was supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS-UEFISCDI, project number PN-II-RU-TE-2014-4-1501(2015-2017).

REFERENCES

Stephan Olariu, Gongjun Yan, Ding Wen, Michele C.Weigle, 2012, "*Security Challenges in Vehicular Cloud Computing*" IEEE Transactions on intelligent transportation systems.

Md Whaiduzzaman, Mehdi Sookhak, Adbullah Gani, Rajkumar Buyya, 2014, *"A survey on vehicular cloud computing",*Journal Network and Computer Applications.

Mario Gerla, 2012, *"Vehicular Cloud Computing",*Vehicular Communications and Applications Workshop.

Talal H. Noor, Quan Z.Sheng, Sherali Zeadally, Jian Yu, 2013, "*Trust Management of Services in Cloud Environments: Obstacles and Solutions*", ACM Computing Surveys, Vol 46, No1, Article 12, Publication Date: October 2013.

Bernd Grobauer, Tobias Walloschek, Elmar Stocker, 2010,"*Understanding Cloud-Computing Vulnerabilities*", Proceedings of the 2010 IEEE Security and Privacy,pp. 1-14.

Cloud Security Alliance, August 23, 2012, "*Cloud Computing Vulnerability Incidents: a statistical overview*", Cloud Vulnerabilities Working Group.

Josang, A., Keser, C., and Dimitrakos, T. , 2005. "*Can We Manage Trust?"* In: P. Herrmann et al. (Eds.): iTrust, LNCS 3477, 2005, pp. 93-107.

S. Marsh, 1994 "*Formalising trust as computational concept*", PhD Thesis, Department of Computer Science, University of Stirling, 1994, pp.56-59.

R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, et al.,2011 "*TrustCloud - A Framework for Accountability and Trust in Cloud Computing*," in IEEE 2nd Cloud Forum for Practitioners (IEEE ICFP 2011), Washington DC, USA, pp. 1-5.

Nicholas Carr, 2008,"*The Big Switch - Rewiring the world, from Edison to Google*", Second Edition, W.W. Norton & Company Inc, New York, Part 1, Chapter 1, pp. 14-25.