# Formal UML-based Modeling and Analysis for Securing Location-based IoT Applications


Hector Cardenas
*Texas A&M International University*
*hector_cardenas@dusty.tamiu.edu*

Ryan Zimmerman
*Columbus State University*
*zimmerman_ryan@columbusstate.edu*

Antonio Rosales Viesca
*Texas A&M International University*
*antoniorosales@dusty.tamiu.edu*

Mustafa Al Lail
*Texas A&M International University*
*mustafa.allail@tamiu.edu*

Alfredo J. Perez
*University of Nebraska at Omaha*
*alfredoperez@unomaha.edu*



***Abstract*—In this work we present a process and a tool to apply formal methods in Internet of Things (IoT) applications using the Unified Modeling Language (UML). As there are no best practices to develop secured IoT systems, we have developed a plug-in tool that integrates a framework to validate UML software models and we present the design of a location-based IoT application as a use case for the validation tool.**


## 1. Introduction

The notion that everyday Internet-connected devices such as baby monitors or child toys are secured and cannot be used to spy on their users is antiquated and naive [1], making the security (and privacy) of these systems an essential issue. Because no standardized best practices for securing Internet of Things (IoT) systems exist yet [2], in this work, we have applied modeling techniques as a way to standardize and validate secure IoT systems in their design phase. As test case for our approach, we created three basic location-based application models with varying levels of security constraints to validate their security using our own developed UML-based analysis tool [3] to verify system behavior. We leverage the processes and UML/SysML extension described in IoTsecM [1], whose creators have identified five actors and fourteen security elements relevant to the IoT ecosystem [2]. Our analysis process implements the work proposed in [4], consisting of a framework for analyzing UML class diagrams and specified requirements. If the analysis finds a scenario in which the system violates its constraints, the tool returns a detailed summary that can be used by designer/developer to improve the design of the IoT system.

## 2. Methods and Contributions

### 2.1. Location Application Models

We based our models on a simple Android application we have named *Where Am I?* whose only functionality is to obtain the user's current latitude and longitude and show it in the screen. Two classes, *MainActivity* and *GpsTracker* provide the main functionality in tandem with various helper and security classes related to location collection and the IoTsecM nomenclature. The GpsTracker class is in control of creating the necessary provider whose type dictates the security elements required by a given system state. By using the formal classification method to identify IoT vulnerabilities proposed by Neshenko et al. [1], we recognize the most prominent attack surfaces related to gathering the user's location in Android, namely the Network location provider and GPS provider, which are responsible for the GNSS and non-GNSS location services [5]. We used SecurITree (an attack-tree design software developed by Amenaza Technologies) to build an attack tree (illustrated in figure 1) to model spoofing and jamming-based attack sequences that a given provider may face [6]. Ultimately, we used seven elements specified in the IoTsecM profile in our model: the behavior monitor (BEHM), to emulate an intrusion prevention system (IPS) or an intrusion detection system (IDS), and six elements related to the public key infrastructure (PKI). Figure 2 shows the class diagram of our application, including its security elements.

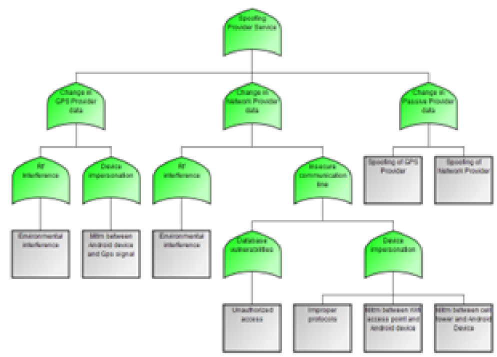


Figure 1: SecurITree model of a spoofing attack

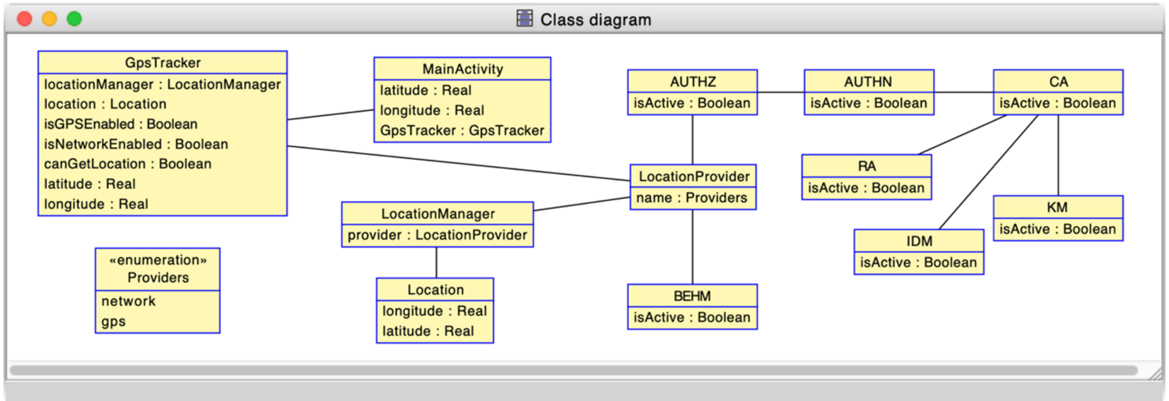


Figure 2: *Where Am I?* class diagram

## 2.2. Analysis Plug-in Tool

Working towards analyzing the location-based models, we developed a plug-in for the UML-based Specification Environment (USE). This tool allows users to specify a software system and its structural requirements in UML and the Object Constraint Language (OCL) [7] respectively. Our plug-in implements the analysis framework proposed by Al Lail [4]. In the background, the plug-in performs two transformations. The first transformation converts input UML models into equivalent UML models that facilitate analysis of their behavior. The second transformation translates UML properties/constraints to the Object Constraint Language (OCL) which is required to analyze the models. The plugin implements an optimization technique proposed by Al Lail [4] to reduce the computational costs of analyzing large UML models. We added this plug-in to USE (a tool that allows users to specify information systems using UML and OCL [8]]). We implemented a command-line interface and a Graphical User Interface (GUI) to interact with the plugin. The inputs for the plug-in consist of two files: one that contains the model to be analyzed and another containing its specified behavioral requirements. Using this plug-in, we transformed the location-based applications in a suitable format for analysis. At this point we are in the process of validating the analysis done by the tool.

## 3. Conclusion and Future Work

In this work we presented the use of UML class diagrams to create designs of IoT systems with security constraints in mind. To illustrate the use of this formal methods framework, we created a design of a location-based IoT application with security elements. In the future, we expect to analyze the models by using our developed USE plug-in, thus contributing to the design and standardization of security (and privacy) in IoT systems.

## Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1950416. Hector Cardenas, Ryan Zimmerman and Antonio Rosales want to thank our mentors, Dr. Mustafa Al Lail and Dr. Alfredo Perez, for their guidance throughout this REU. The authors want to acknowledge Dr. Lars Hamann for his help with the analysis plug-in and Terry Ingoldsby for providing our team with a license to use the SecurITree software.

## References

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[2] P. J. Escamilla-Ambrosio, D. A. Robles-Ramírez, T. Tryfonas, A. Rodriguez-Mota, G. Gallegos-García, and M. Salinas-Rosales, "Iotsecm: A uml/sysml extension for internet of things security modeling," *IEEE Access*, vol. 9, pp. 154 112–154 135, 2021.

[3] Omg unified modeling language (2017). [Online]. Available: https://www.omg.org/spec/UML/2.5.1/About-UML/

[4] M. Al Lail, "A unified modeling language framework for specifying and analyzing temporal properties," Ph.D. dissertation, Colorado State University, 2018.

[5] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala *et al.*, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[6] Amenaza techologies. [Online]. Available: https://amenaza.com

[7] Object constraint language (2014). [Online]. Available: https://www.omg.org/spec/OCL/2.4/About-OCL/

[8] A uml-based specification environment (6.0.0). [Online]. Available: https://sourceforge.net/projects/useocl/