Attribute-Based Access Control to Secure IoT Devices in the Home

Jacqueline Brown
College of Engineering and Computer Science
Marshall University
Huntington, West Virgina, USA
brown1062@marshall.edu

William LeMaster
College of Engineering and Computer Science
Marshall University
Huntington, West Virgina, USA
lemaster82@marshall.edu

Kaleb Weekley
College of Engineering and Computer Science
Marshall University
Huntington, West Virgina, USA
weekley48@marshall.edu

***Abstract*—Internet of Things (IoT) applications and services are revolutionizing the capabilities of the Internet with billions of connected devices, yet also becoming more readily available in our everyday life. These devices are commonly referred to as smart things enabling smart environments, such as Smart Home, Smart Health, Smart Transportation, and overall Smart Communities, together with key enabling technologies like Cloud Computing, Artificial Intelligence (AI) and Machine Learning (ML). That said, the need for proper authentication and authorization is becoming more critical as these smart things need appropriate security for the transfer of sensitive information. Access control is a common way to achieve better security. Access control determines the use of resources only to the specified and authorized users based on appropriate policy enforcement. IoT demands more sophisticated access control in terms of its usability, scalability, and efficiency in protecting sensitive information. In this project, we discuss the potential for employing protocol-based access control for IoT systems and examine how attribute-based access control (ABAC) can overcome the limitations of traditional access control mechanisms. We will also focus on the key benefits and constraints of this integration.**

Keywords—Internet of Things, Access Control, Network Security, Home IoT environment.

I. INTRODUCTION

The Internet of things describes physical objects that are embedded with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. The home IoT environment presents interesting and complex challenges in terms of security due to heterogeneous devices connected through multiple types of networks. These devices provide different services to the user and can operate independently or in collaboration with other IoT devices. For example, a smart home environment controller might require the light bulbs to indicate their current luminescence values and adjust them to suit the current visibility of the rooms. Another illustration is a smart IoT monitoring device that might periodically query different devices for their connectivity and report failures to the user. There are many more IoT devices such as air quality monitors, motion sensors, video doorbells, water leakage detectors, fire detectors, smart vacuum cleaners, smart washers and so on, that share data with controllers and mobile phone apps. Broadly speaking, an IoT network can be viewed as numerous operating environments (OEs) within a single computing ecosystem wherein each device acts as an independent OE and provides data services (DS). Clearly, there is need for access control in such an environment and traditional access control methods, such as discretionary access control or role-based access control, are not suitable as multiple attributes of users and devices are needed to make access control decisions. IoT devices are becoming more and more important in terms of global economic distribution. The total amount spent on IoT devices climbed by 12.1 percent in the previous year [1]. The total money which was spent in the fiscal year itself IoT devices was $128.9 billion which goes to show exactly how integral the collection of devices is to the economy. The market's expenditure is expected to grow at a staggering 26.7 percent each year over the following four years [1]. Access control is the process of restricting connections and access to resources in order to guarantee that only trustworthy sources are utilized and that only the information transfers that are intended are carried out. Because of how well internet connections are incorporated into our daily interactions as humans, this is extremely important. Attribute-based access control (ABAC) is seen as the next generation access control model for achieving logical, fine-grained and context-aware access control in complex heterogeneous systems. IoT device authentication is fundamental to ensure connected devices can be trusted to be what they purport to be. Thus, access control can police what resources can be accessed and used and in which context to minimize the risk of unauthorized actions, or proceedings.. In this paper, we will explore the enforcement of ABAC within a home IoT environment. We will address the various challenges posed by implementing ABAC as an access control solution.

II. PREVIOUS WORKS

We are basing the protocol algorithm off of existing works of:

A. Securing Home IoT Environments with Attribute-Based Access Control

To overcome the shortfalls of IoT authentication the authors of this work implement ABAC in a home IoT context using the NIST NGAC standard architecture.
Their approach divides the entities in the home IoT environment into subject and object categories, and then list the numerous attributes.

The authors also discuss various types of policies that are appropriate for use in a home IoT system. These policy categories are intended to be generic, and they should work for the majority of home IoT networks and show how to implement them using the NIST NGAC architecture [2].

B. *Attributed-Based Authentication and Access Control for IoT Home Devices*

In this paper, the authors demo explains how IoT devices will be maintained and controlled using thier cryptographically implementation approach to authenticate an Attribute-Based Access Control (ABAC) mechanism. Their demo uses an underlying cryptographic technique, Attribute-Based Cryptosystem (ABC) [3].

III. Proposed Research

Our objective is to analyze and compare the modern standard model for ABAC (XACML) and the ABAC model itself to determine the efficacy of the algorithms. This will be accomplished by using various analytical tools for algorithms which will provide individual components of the overall effectiveness of the algorithms themselves such as energy efficiency, run-time, and security properties. What will also be discussed is the constraints of each of the algorithms and the plausible and existing ramifications of said flaws.

A. *Algorthim Protocols*

eXtensible Access Control Markup Language (XACML) Model.

The XACML standard specifies a policy specification language as well as an infrastructure. Subject attributes, resource attributes, action attributes, and environment attributes make up a XACML access request. The environmental attributes, which are frequently current time, day, or threat level, are independent of the subject or resource attributes. A Policy Set is a collection of XACML policies, and a XACML policy is a collection of XACML policies. The majority of XACML policies are made up of a mix of Policy Sets and policies. A pre-condition is included with each Policy Set or policy that is assessed on the characteristics presented to check whether the appropriate policy applies to the access request. XACML has been widely used as the de facto access control architecture [4].

Attribute Based Access Control Model (ABAC)

The ABAC is a conceptual model that draws upon the principles of access control systems. It features an elegant and expressive set of attributes that define the policies and logical relationships among various entities. The attributes can be used to identify various things, such as users, resources, and environment variables. They can also be used to interact with an action, such as signing in or revoking. ABAC can also be used to identify the various resources that are related to an object type, such as a music player or a temperature sensor. It can also capture various details about an individual, such as their age and current role. Under ABAC, access decisions can be made without requiring changes to the relationships between the object and the subject. This capability allows for more flexible access control management. Sometimes, the attributes can be used to predict the actions that a user will perform in order to trigger the appropriate access policies [5].

References

[1] Wegner, P., “Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security," IoT Anayltics, 16 June 2021. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/.

[2] Bezawada, B., Haefner, K., & Ray, I. (2018). Securing Home IoT Environments with. Association for Computing Machinery, 43-53.

[3] A. L. Maia Neto, Y. L. Pereira, A. L. F. Souza, I. Cunha and L. B. Oliveira, "Demo Abstract: Attributed-Based Authentication and Access Control for IoT Home Devices," 2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2018, pp. 112-113, doi: 10.1109/IPSN.2018.00019.

[4] 2013. OASIS. eXtensible Access Control Markup Language (XACML) Version 3.0. Oasis standard, Or-ganization for the Advancement of Structured Information Standards. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os- en.html.

[5] Hu, C., Ferraiolo, D. , Kuhn, D. , Schnitzer, A. , Sandlin, K. , Miller, R. and Scarfone, K. (2019), Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-162.