Utilizing The DLBAC Approach Toward a ZT Score-based Authorization for IoT Systems

Safwa Ameer
Institute for Cyber Security and NSF C-SPECC Center
Department of Computer Science
The University of Texas at San Antonio
safwa.ameer@utsa.edu

Ram Krishnan
Institute for Cyber Security and NSF C-SPECC Center
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
Ram.Krishnan@utsa.edu

Ravi Sandhu
Institute for Cyber Security and NSF C-SPECC Center
Department of Computer Science
The University of Texas at San Antonio
ravi.sandhu@utsa.edu

Maanak Gupta
Department of Computer Science
Tennessee Technological University
mgupta@tntech.edu

abstract

The internet of Things (IoT) refers to a network of physical objects that are equipped with sensors, software, and other technologies in order to communicate with other devices and systems over the internet. IoT has emerged as one of the most important technologies of this century over the past few years. To ensure IoT systems' sustainability and security over the long term, several researchers lately motivated the need to incorporate the recently proposed zero trust (ZT) cybersecurity paradigm when designing and implementing access control models for IoT systems. This poster proposes a hybrid access control approach incorporating traditional and deep learning-based authorization techniques toward score-based ZT authorization for IoT systems.

Keywords

Access control, Score-based, IoT, Zero Trust

ACM Reference Format:
Safwa Ameer, Ram Krishnan, Ravi Sandhu, and Maanak Gupta. 2023. Utilizing The DLBAC Approach Toward a ZT Score-based Authorization for IoT Systems. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY '23), April 24–26, 2023, Charlotte, NC, USA. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3577923.3585046

1 INTRODUCTION AND MOTIVATION

IoT is the term used to describe physical objects (or groups of objects) with sensors, processing capability, software, and other technologies that connect and exchange data over the Internet or other networks [19]. The number of connected smart devices is projected to reach over 25 billion by 2025 [2, 20].

Security and privacy in IoT are primary factors that will enable wide adoption of IoT especially at the consumer level. One of the critical security services in IoT that mostly all researchers agree upon is access control. Providing an appropriate access control model for IoT services is a vital but challenging topic. In IoT, the deployment of resource constrained devices, along with the adoption of a plethora of technologies, enlarges the attack surface and introduces new security vulnerabilities [11, 14]. Furthermore, the complexity of IoT systems outpaces legacy perimeter-based network security methods since there are no easily recognizable perimeters for an IoT system. As a result, the critical question is how we can have trust in such a complex system. Recently researchers have suggested that the solution is not to trust and to incorporate the recently proposed Zero Trust (ZT) cybersecurity paradigm in IoT [1, 4, 7, 8, 17]. Zero trust (ZT) paradigm provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. This technology has emerged in response to current enterprise trends, which include remote users, bring your own device, and IaaS/SaaS cloud services [15]. IoT systems also exhibit these trends, along with additional complexities. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes ZT concepts and encompasses component relationships, workflow planning, and access policies [15]. An integrated zero trust IoT system is the network infrastructure (physical and virtual) and operational policies that are in place for an IoT system as the result of a ZTA plan [1]. Recently, Ameer et al. [1] have proposed a set of authorization requirements that should be taken into account when designing a ZT authorization policy model. They conducted a study to analyze IoT systems based on these requirements. According to their findings, maintaining ZT principles in IoT systems requires an access control model that is contextually aware and able to : (i) incorporate actors, targets, action, action-target, and context characteristics' (ii) continuously perform ongoing authorization, and (iii) dynamically decide on access requests based on calculated score (confidence level) rather than on static access control policies. Accordingly, they introduced a preliminary framework for score-based authorization in terms of basic components and their interactions, where actual development of the access control policy models, enforcement models, and implementation mechanisms are left for future investigation. Score-based authorization is the type of authorization that computes a confidence level (score) for the requested access. As long as the score exceeds the threshold value configured or calculated for

CODASPY '23, April 24–26, 2023, Charlotte, NC, USA

ACM ISBN 979-8-4007-0067-5/23/04.
https://doi.org/10.1145/3577923.3585046

the resource, access to the resource is granted, or the action is performed. Otherwise, the request is declined, or access privileges are reduced [1, 15]. Depending on the application system, there could be different types of score and threshold calculation algorithms. They may be probabilistic, heuristic, simple mathematical functions, or utilizing machine learning techniques. On the other hand, recent researchers [10] have proposed an automated and dynamic access control mechanism leveraging advances in deep learning technology. This approach denoted as Deep Learning Based Access Control (DLBAC), addresses some major limitations of classical access control approaches such as attributes engineering, policy engineering, and generalization. DLBAC produces a trained neural network that makes access control decisions based on user and resource metadata. Rather than using policies to control access, it relies on a neural network for decision-making. Moreover, they conducted a comparison between their proposed DLBAC model and some ML based policy mining algorithms which are used traditional AC approaches. They have shown that a DLBAC approach can make more accurate access control decisions and generalize better than ML based policy mining algorithms. In concluding that research, the authors advocated that DLBAC could be effectively integrated to work in conjunction with traditional access control models to better meet authorization requirements.

In this poster, we propose a score-based authorization framework for ZT IoT systems that utilizes the concept of DLBAC to build a score engine that works together with a traditional authorization approach to decide on access. This framework will maintain the ZT requirements for IoT authorization systems introduced in [1]. Furthermore, it will leverage the deep learning-based access control precision and generalization feature.

2 SCORE-BASED AUTHORIZATION

According to the zero trust NIST document [15], depending to how input factors are evaluated to decide whether or not an access request will be approved. There are two types of AC models: criteria-based and score-based. Criteria-based authorization models imply that specific requirements (conditions, roles, attributes, etc.) must be met in order to gain access to a resource (for instance, read/write access). Resource access or action is only granted if all requirements are met. ABAC models [9], RBAC[18] , UCON [12], ReBAC [3], and ACON [13], are all considered criteria-based authorization models. The score-based model, however, calculates a confidence level (score) for the requested access. When the calculated score exceeds the threshold value configured or calculated for the resource, access to the resource is granted, or the action is carried out. Otherwise, the request is declined, or access privileges are reduced. Since score-based authorization models provide a current confidence level for the requesting actor, they are more dynamic and more flexible than criteria-based models, as they adjust to changing factors more quickly than static policies modified by humans [1, 15]. The authors in [1] have investigated IoT access control requirements. They concluded that the need arises for a contextually aware access control model incorporating score-based technology to meet IoT authorization requirements. The main reason behind this conclusion is that IoT systems are highly dynamic. The communication between people, connected devices, data, utility, and the changing nature of the system and environment characteristics in a smart IoT connected system necessitates that actors' rights and access requirements change accordingly. Furthermore, a lot of consumer IoT devices lack certifications and do not undergo rigorous security tests. As a result, they may be exposed to unforeseen or unknown security threats. In addition, many of the sensor inputs are subjective and probabilistic rather than definitive. In light of this, it is crucial that IoT authorization models take into account the confidence level of different access requests and that they can accommodate subjective information.

3 DEEP LEARNING-BASED AUTHORIZATION

Nobi et al. [10] have recently motivated the need for deep learning based access control (DLBAC) models. They have shown that traditional access control models (e.g. ABAC, RBAC, ReBAC, ACAC, ACON) have their benefits. However, in the context of dynamic, complex, and large-scale modern systems, it is dificult for traditional access control models to maintain an accurate access control state in the system for a human administrator. They demonstrated that leveraging significant advances in deep learning technology may be a potential solution. DLBAC addresses three major limitations of classical access control approaches, these limitations are as following: (i) Attribute engineering: In traditional access control mechanisms, metadata of the system components are rarely meaningful access control attributes. As a result, administrators need to engineer attributes that can be used to express access control rules. This is a very complicated task, and as described in [16], it is, at best an art involving semi-formal design and requirements engineering processes. On the other hand, DLBAC is an end-to-end access control approach. It does not need attribute engineering. (ii) Policy engineering: In traditional AC approaches the administrator needs to engineer the policy rules. This is accomplished through either a manual engineering process or automated mining techniques (including ML mining techniques) [6]. In contrast, DLBAC does not need a policy engineering step since it utilizes users and resources metadata to train a deep neural network. DLBAC produces a trained neural network that makes access control decisions based on user and resource metadata. Rather than using policies to control access, it relies on a neural network for decision-making. It is shown in [10] that DLBAC captures the access control state in complex systems more precisely than policy mining and classical machine learning mining techniques. (iii) Generalization: Traditional access control approaches do not support generalization [5]. The ability to make access control decisions when examining attributes that haven't been explicitly analyzed during mining. The DLBAC, however, is innately capable of making reliable predictions as long as the test sample and training data are aligned. In [10], the authors found that engineered rules often make poor access control decisions for users and resources associated with metadata that isn't explicitly visible to the mining process. In this context, are DLBACs capable of replacing traditional forms of access control in a short period of time? According to the authors in [10], DLBAC can effectively be integrated with traditional access control models. The challenge, however, is how to accomplish this.

4 UTILIZING THE DLBAC APPROACH TOWARD A ZT SCORE-BASED AUTHORIZATION FOR IOT SYSTEMS

This section proposes a score-based access control framework that integrates DLBAC with traditional access control models for smart ZT IoT systems. This framework is inspired from the score-based authorization framework for ZT systems proposed in [1]. In this framework, we utilize the concept of DLBAC to build a scoring engine that works with traditional access control policies to decide on an access request. We aim to develop a ZT score-based authorization model for IoT systems that combines traditional and deep learning-based access control features. Figure 1 illustrates the framework. Here, actors create sessions through which they can trigger or perform specific actions on specific targets. Context states is a set of states. Each state represents a picture of the context that we want to describe at a given time instant. Different states represent different time instants, such as current, yesterday, etc. Context includes environment context, system context, and threats and logs information. The actors, the sessions, the states of the context, the targets, and the actions each have characteristics that are used as attributes in the authorization decision. Access is determined based on a predefined access policy and accepted trust level (score), not just a proper comparison of attributes. The predefined authorization engine uses predefined authorization policies to evaluate access requests. Defining the authorization policy should be done using formal policy definition language and will probably utilize different types of attributes in the system. There are two main components of the score engine: the score calculation function and the threshold calculation function. Score engines receive access requests from ADE engines and return scores and threshold values associated with access requests. The score is described as a real time, measured determination of trust granted to the input access. This function implements a deep learning based score calculation algorithm to calculate different access requests' scores. The threshold is described as a real-time, measured determination of acceptable trust level for the requested resource at the current instant of time. This function implements a deep learning based threshold calculation algorithm to calculate different requested resources' thresholds. The access decision enforcement (ADE) engine decides on different access requests. It executes the following steps: (i) Receives the request from the actor. (ii) Sends the request to the score engine and the predefined policies authorization engine. (iii) Receives the authorization engine's output, the calculated access request score, and the calculated resource threshold. (iv) Depending on its algorithm, grants or denies the actor's access request.

5 CONCLUSION AND FUTURE DIRECTIONS

We introduce a score-based access control framework that integrates DLBAC with traditional access control models for smart ZT IoT systems. Several research directions need to be considered in the future, as follows. A formally defined, abstract, mathematically based model for the predefined policies authorization engine needs to be developed so that there is a precise and rigorous specification for the intended behavior. Deep learning-based score calculation and threshold calculation algorithms, as well as an ADE engine algorithm, should be developed. Moreover, a comparison between this combined score-based authorization approach on the one hand and traditional access control, as well as pure deep learning-based approaches on the other hand, needs to be conducted.

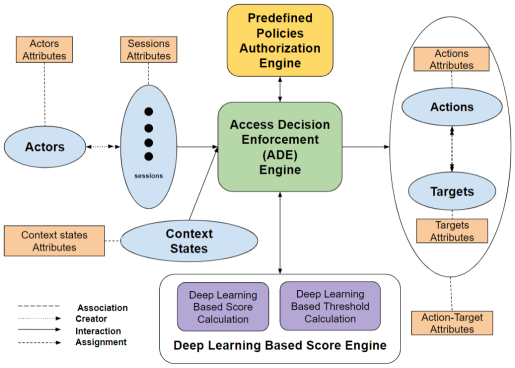

Figure 1: DLBAC Score-based Authorization Model

6 ACKNOWLEDGMENT

This work is supported by NSF CREST-PRF Award 2112590 and NSF CREST Grant HRD1736209.

References

[1] S. Ameer, et al. 2022. BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies. 235–244.
[2] S. Bhatt and R. Sandhu. 2020. ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies.
[3] Y. Cheng, et al. 2012. Relationship-based access control for online social networks: Beyond user-to-user relationships. In SocialCom. IEEE.
[4] P. Colombo, et al. 2021. Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era. In 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA) . IEEE, 159–166.
[5] C. Cotrini, et al. 2018. Mining ABAC rules from sparse logs. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 31–46.
[6] S. Das, et al. 2018. Policy Engineering in RBAC and ABAC. From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday (2018), 24–54.
[7] S. Dhar and I. Bose. 2021. Securing IoT devices using zero trust and blockchain. Journal of Organizational Computing and Electronic Commerce 31, 1 (2021), 18–34.
[8] T. Dimitrakos, et al. 2020. Trust aware continuous authorization for zero trust in consumer internet of things. In TrustCom. IEEE.
[9] X. Jin, et al. 2012. A unified attribute-based access control model covering DAC, MAC and RBAC. In IFIP Annual Conf. on Data and App. Sec.
[10] M. N. Nobi, et al. 2022. Toward deep learning based access control. In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy. 143–154.
[11] A. Ouaddah, et al. 2017. Access control in the Internet of Things: Big challenges and new opportunities. Comp. NW 112 (2017).
[12] J. Park and R. Sandhu. 2004. The UCONABC usage control model. ACM transactions on information and system security (TISSEC) 7, 1 (2004), 128–174.
[13] J. Park, et al. 2011. Acon: Activity-centric access control for social computing. In ARES. IEEE.
[14] S. Ravidas, et al. 2019. Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications 144 (2019), 79–101.
[15] S. Rose, et al. 2020. Zero trust architecture. Technical Report NIST Special Publication (SP) 800-207. National Institute of Standards and Technology.
[16] Z. Sainan and Z. Changyou. 2019. Research and Application of Rigorous Access Control Mechanism in Distributed Objects System. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 1166–1169.
[17] M. Samaniego and R. Deters. 2018. Zero-trust hierarchical management in IoT. In 2018 IEEE international congress on Internet of Things (ICIOT). IEEE, 88–95.
[18] R. Sandhu. 1998. Role-based access control. In Advances in computers. Vol. 46.
[19] M. Shafiq, et al. 2022. The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks. Wireless Communications and Mobile Computing 2022 (2022), 1–12.
[20] B. Tang, et al. 2019. Iot passport: A blockchain-based trust framework for collaborative internet-of-things. In SACMAT '19.