Limitations and Approaches in Access Control and Identity Management for Constrained IoT Resources

Shantanu Pal
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
shantanu.pal@hdr.mq.edu.au

***Abstract*—The Internet of Things (IoT), smart sensors and mobile wearable devices are helping to provide services that are more ubiquitous, smarter, faster and easily accessible to users. However, security is a significant concern for the IoT, with access control and identity management are being two major issues. With the growing size and presence of these systems and the resource constrained nature of the IoT devices, an important question is how to manage policies in a manner that is both scalable and flexible. In this research, we aim at proposing a fine-grained and flexible access control architecture, and to examine an identity model for constrained IoT resources. To achieve this, first, we outline some key limitations in the state of the art access control and identity management for IoT. Then we devise our approach to address those limitations in a systematic way.**

I. Introduction and Background

The Internet of Things (IoT) is a digital ecosystem that connects devices, objects, resources and users, allowing them to communicate, collaborate and process data in new and innovative ways. New services and applications (e.g. smart healthcare, smart transportation, smart agriculture, etc.) are rapidly being made available through the IoT. It is predicted that the Internet will include 50 billion connected devices by 2020. While such a convergence of digital-physical systems can provide better services, reduced cost of applications and improved user experience, it also leads to numerous challenges in security and privacy [1].

Attacks on IoT systems are becoming more sophisticated. This is not limited to simply infecting network traffic with malicious code. For instance, a patient's pacemaker can be used to generate a fatal shock or a drug infusion pump (e.g. insulin or antibiotics) can be controlled by an attacker to change the drug dosage [2]. Unfortunately, characteristics of the IoT, e.g. low-powered devices, small memory capacity and limited processing power, are major issues in creating secure IoT systems. This means that it is impractical to enforce heavy weight security mechanisms in these devices while the scale of the systems argues against fully centralized solutions. From a communication point of view, heterogeneous network environments, wireless communication mediums, high mobility of *things*, dynamic network topology and availability of infrastructure for communication present further issues.

II. Research Summary

A. Problem Statement

In an IoT system, with its large scale, open technologies and resource constrained nature of the devices, managing the resources and users of the system and enforcing appropriate policies is a complex and challenging issue. IoT systems can also not afford single point of failure risks from over-centralization but conversely require high levels of security due to the sensitive nature of these systems and the scale of data to be handled. These, and other characteristics, require solutions specifically designed for the IoT arena [3]. In particular, access control and identity management have been identified as pressing issues in this context. IoT systems will need policies and mechanisms to support authorization (i.e. determining whether an entity can access a resource) and authentication (i.e. identifying an entity). With the range and scale of *things* in an IoT system, the scale of the policies required for access control and the management of those policies, must be considered.

B. Key Research Issues

- *Flexible and Fine-Grained Policy Management:* A number of well-known access control models and mechanisms, e.g. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Capability-Based Access Control (CapBAC) [4], have been proposed for use in IoT systems. Each of them, in isolation, has its drawbacks when enforcing policies for a large scale dynamic system like the IoT. RBAC provides effective policy management but it is dependent on a highly centralized system. It also typically requires explicit user-assignment to roles, and supports only predefined and static policies. This is inflexible in a highly dynamic context like the IoT. ABAC improves flexibility in policy management as explicit user identities are not specified in the policies, rather users are identified based on attributes they possess. The use of attributes in ABAC assists in the enforcement of fine-grained access control policies in real-time. However, there are questions around how many policies are required and where they are evaluated. If one set of attributes is to give access to multiple resources, and this evolves over time, either multiple policies, or significant policy re-writes, will be required. CapBAC simplifies the distribution of permissions and is decentralized by nature. However, previous proposals for the use of CapBAC in the IoT have ignored the question of policy management at a fine-grained level.
- *Light Weight Communication and Authentication:* Several approaches have discussed communication and authentication issues for IoT systems. However, the majority of them are highly centralized and use Public Key Infrastructure (PKI)

based systems, which are not ideal bases for IoT systems. From the protocol point of view, there are multiple options that could potentially be adopted in resource constrained IoT networks. On the one hand, new communication protocols can be implemented for IoT on top of the IPv6 infrastructure. On the other hand, existing light weight protocols could be used to provide interoperability with the existing infrastructure. We argue that, a light weight protocol (using symmetric key cryptography) could achieve both authentication as well as authorization (without using public key cryptography). However, extensive efforts are lacking on how to employ light weight protocols for achieving authentication in IoT systems.

• *Managing IoT Identity at Scale:* In the IoT, identity needs to capture all the constituent *things*. However, the majority of the existing approaches do not address the issues of identity and its management precisely, keeping in mind the correlation between the dynamic nature, scale and the resource constrained nature of the *things*. Most studies are concerned with how identities can uniquely identify a particular entity. This is true even when identity is based on attributes (e.g. name, age, location, etc). We argue that such an approach is not sufficiently flexible for a large and highly dynamic system like IoT. When considering issues e.g. policy management and delegation in the IoT, we need to be able to flexibly handle questions of identity. It cannot always be known in advance which entities will access which services or devices or which devices will be available at the time when access is requested.

III. Proposed Approach

• *Addressing Fine-Grained and Flexible Policy Management:* In [5], we propose a novel partially decentralized access control architecture which improves policy management by reducing the required number of authentication policies in an IoT system while providing fine-grained access control. We use a hybrid approach by employing attributes, roles and capabilities for our authorization design to achieve streamlined policy management. Our approach solves the policy management issue by combining the strengths of RBAC, ABAC and CapBAC. Part of this is issuing parameterized capabilities based on attributes, allowing fine-grained access control with a minimum number of policy specification. We apply attributes for role membership assignment and in permission evaluation. Membership of roles grants capabilities. The capabilities which are issued may be parameterized based on further attributes of the user and are then used to access specific services provided by IoT devices. We have developed a formal representation of our proposed model. We demonstrate that our approach significantly reduces the number of policies required for specifying access control settings. Our evaluation also highlights that the proposal has clear advantages in performance compared to the other capability based mechanisms used for IoT access control.

• *Addressing Light Weight Communication and Authentication:* In [6], we extend the architecture of [5] for providing fine-grained policy decisions based on capabilities to the users using symmetric key cryptography. The major motivation of this study is to investigate the suitability of applying a light weight protocol for access control framework for IoT-enabled constrained healthcare resources. We also aim to reduce the number of polices within the system. Our experimental evaluation confirmed that our proposal achieves better performance for IoT systems using such light weight security mechanisms. We discuss a detailed system design and provide a detailed implementation using physical test-bed setup.

• *Approach for Managing IoT Identity at Scale:* In [7], we devise a novel idea of *things-centric* identity management approach for the IoT. To achieve this, at first, we survey and classify the various representations of digital identities in a detailed and comprehensive manner. Then we illustrate a formal model of IoT identity based on the different components of an identity management framework in a more systematic fashion. We argue that the scope and nature of an IoT system mean that insisting on definitive, unique, identity in every case is overly restrictive. While in some circumstances such unique identification will be required, in other cases less defined identities will suffice for the needs of application functionality and policy specification. Unique identities will not always be known in advance (for example, which customers may enter a shop or purchase a movie ticket), however partial identities (e.g. age) may be able to be defined in advance. With specific use-case examples we demonstrate the suitability of our proposed model in real-world IoT scenarios.

IV. Conclusion and Future Work

In this research, we try to address the issues of access control and identity management for constrained IoT resources. Our proposed architecture is flexible, as role membership is based on attributes, not an a priori knowledge of which roles the users are assigned to. This allows a degree of flexibility and conciseness in policy specification unachievable in most other proposed systems. In future, we plan to examine a delegation model and how to incorporate the notion of trust when interacting between different entities in an IoT system.

Acknowledgement

The author would like to acknowledge Michael Hitchens, Macquarie University, Australia and Vijay Varadharajan, University of Newcastle, Australia. The research is supported by the International Macquarie University Research Excellence Scholarship.

References

[1] M. Ammar et al.,“Internet of things: A survey on the security of iot frameworks,” *Information Security and Applications*, vol. 38, 2018.

[2] WIRED, “How the Internet of Things got Hacke,” Available Online, 2015.

[3] S. Pal, M. Hitchens, and V. Varadharajan, “On the design of security mechanisms for the internet of things,” in *ICST*, IEEE, 2017.

[4] A. Ouaddah et al., “Access control in the internet of things: Big challenges and new opportunities,” *Computer Networks*, vol. 112, 2017.

[5] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, “On Design of A Fine-Grained Access Control Architecture for Securing IoT-Enabled Smart Healthcare Systems,” in *MobiQuitous*, 2017.

[6] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, “Policy-based access control for constrained healthcare resources,” in *WoWMoM*, 2018.

[7] S. Pal, M. Hitchens, and V. Varadharajan, “Modeling identity for the internet of things: Survey, classification and trends,” in *ICST*, IEEE, 2018.