PhD Forum: Trust Management for Context-aware Access Control Systems in IoT

Shirin Kalantari
imec-DistriNet, KU Leuven
Leuven, Belgium
shirin.kalantari@kuleuven.be

Andreas Put
imec-DistriNet, KU Leuven
Leuven, Belgium
andres.put@kuleuven.be

Bart De Decker
imec-DistriNet, KU Leuven
Leuven, Belgium
bart.dedecker@kuleuven.be

***Abstract*—The PhD project presented in this paper aims to design a trust management infrastructure that allows to assess the trustworthiness of context data in the scope of access control with the IoT. The main requirements for this design are independence from the underlying access control model and flexibility of trust calculation schemes based on application needs.**

***Index Terms*—Internet of Things, Access Controller, Context-awareness, Trust Management.**

I. Introduction

It is estimated that in 2020, more than 20 billion Internet of Things (IoT) devices have already been connected to the Internet [1]. In the coming years, the number of these devices will increase and they will become more commonplace. We will shortly arrive at an era in which we could have a *digital twin* for every entity in our physical world. This network of connected devices enables us to develop applications that contains detailed information not only on events of interests, but also the context in which they take place. Moreover, this context can be used to improve existing applications with regard to safety, security and usability.

In the literature, several well-known access control models have been adapted to become context-aware [2]. In addition, context has been used to refine different aspects of AC systems. This includes improving the core functionalities such as entity identification and authentication [3], [4], expressing contextual conditions in authorization rules [5], [6], leveraging context data to facilitate fallback authentication [7], and for enabling and auditing emergency accesses [8].

While most research papers focus on *the usage of context* for improving access control systems, context-awareness brings in new issues that might hinder the security of the systems. Consider the following automation policy in a smart home, based on CO concentration "if $|CO| \geq \theta$, unlock the front door". By manipulating the data from the gas leak detector, an attacker can unlock the victim's front door. Hence, the security of the access controller heavily relies on its "trust assumptions" regarding the gas leak detector's readings. In most research papers, the consequences of using context on the trust assumptions of the access control system is disregarded.

Every AC system makes certain trust assumptions regarding the core techniques and principles that it uses. For example, when using certificates, the system *assumes* the trustworthiness of the issuer, when using passwords for entity authentication, the AC system *assumes* that "knowing the password" accurately proves "having a certain identity" and when considering the authorization policies, the system *assumes* that these policies are specified by authorities who have jurisdiction over a particular access request.

Trust assumptions substantially change when the system uses context data from sources that are external to the access controller. The context data might be unintentionally inaccurate (e.g., due to device or communication failures) or manipulated by an attacker (e.g., spoofing, replaying and relaying attacks). Hence, it is necessary to evaluate the trustworthiness of context-data before using it in an AC decision. The goal of this PhD project is to design a trust management infrastructure that allows to assess the trustworthiness of context data in the scope of access control.

II. Constraints and Requirements

In most access controllers trust assumptions are incorporated into the model during the system design or deployment. While these assumptions might change during the life-time of the system, the changes are often triggered and resolved by factors external to the AC. For example, the system administrator might revoke all current passwords if the password file is compromised and then revise the authentication method. When considering trust assessment of context data in IoT there are many hurdles to overcome:

a) Heterogeneity of devices: Most of the context data originates from IoT devices that have different capabilities and characteristics. These devices might have different sensing accuracy and use different network protocols. Some might lack a trusted computation module and suffer from outdated software or unpatched vulnerabilities.

b) Heterogeneity of application requirements: Whether context information is trusted also depends on the application that is using it. For example, in some healthcare applications the access controller might want to receive all the available data concerning a patient's vital health parameters regardless of the security of transportation channel or data authenticity because the risk of missing an emergency is higher than accepting inaccurate or even malicious data.

c) Cross-domain applications: Many IoT applications use shared devices or services. These infrastructural elements are often owned and controlled by different self-interested

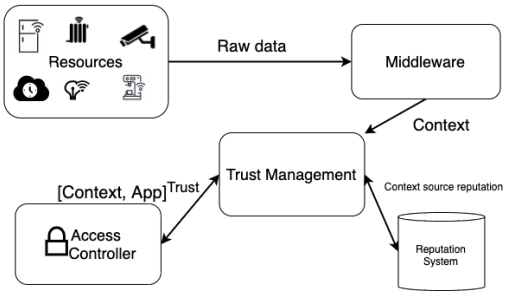

Fig. 1. From raw data to verified context data.

organizations. Trustworthiness of data that comes from these resources is dependent on the level of trust that the application has on the owner of that resource.

d) Lack of security administrators: Many IoT applications are now deployed, configured and maintained by users who lack in-depth knowledge of security, in domains such as smart home and wearables. Applications in these domains should be accompanied with support tools that are easy to use for non-technical users. For example, the system should help the user to understand the security problem of the automation rule "if $|CO| \geq \theta$, unlock the front door" when the gas leak detector lacks the required security features.

III. Initial Design

The definition of trust is known to be context-dependent. Hence, it is difficult to design a generic trust management module that is suitable for every application. In the literature, several trust management modules have been proposed which operate at different layers of the IoT stack and target specific applications [9], [10]. The relevant literature for our system includes trust management systems for access controllers [11], [12], context verification [13], [14] and quality of context [15] schemes. There are two main approaches for trust management: policy-based and reputation-based trust. In policy-based systems trust is specified based on predefined rules. The reputation-based approach establish trust based on previous interactions of community members with a service or device.

The approach adapted in this PhD project leverages a reputation-based trust management. The overview of our scheme is illustrated in Figure 1. Our trust management scheme relies on a middleware framework to process the raw input data and capture the relevant parts in an explicit context model. The reputation system utilizes community feedback and provides information about the quality of services related to each context source e.g., response time and accuracy. The trust management module itself is inspired by the study of Miao and Chen [16] in which the final trust score is application-dependent and is composed of: a *static* and a *dynamic* part. The static part represents trust attributes that are the same for different entities such as physical properties associated with a context source, the service type and the communication protocols. The dynamic part adapts the trust calculation to the applications' requirements and relies on information that might differ for each application e.g., trust relationships between organizations or the device owners. This part also enables application to specify strategies for escalation of trust. For example, the trust score of context data received over an unencrypted channel can be increased by crosschecking and involving third parties.

IV. Conclusion

The goal of this PhD project is to design a reputation-based trust management infrastructure that allows to assess the trustworthiness of context data in the scope of access control systems in an IoT environment. We are currently working on developing a decentralized reputation system that forms the basis of our trust calculations.

References

[1] M. Hung, "Leading the iot, gartner insights on how to lead in a connected world," 2017.

[2] A. S. M. Kayes, R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha, and I. Kumara, "A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues," *Sensors*, vol. 20, no. 9, 2020.

[3] H. Khan, U. Hengartner, and D. Vogel, "Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, Jul. 2015, pp. 225–239.

[4] D. Preuveneers and W. Joosen, "Smartauth: Dynamic context fingerprinting for continuous user authentication," in *SAC '15: Proceedings of the 30th Annual ACM Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2015, p. 2185–2191.

[5] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments," in *The Semantic Web - ISWC 2006*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 473–486.

[6] A. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Generation Computer Systems*, vol. 93, 2019.

[7] A. Hang, A. D. Luca, M. Smith, M. Richter, and H. Hussmann, "Where have you been? using location-based security questions for fallback authentication," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015, pp. 169–183.

[8] D. Van Bael, S. Kalantari, A. Put, and B. De Decker, "A context-aware break glass access control system for iot environments," in *The 7th IEEE International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2020)*. IEEE Xplore, 2020.

[9] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Computer Communications*, vol. 160, pp. 475 – 493, 2020.

[10] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, 2014.

[11] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trust management in decentralized iot access control system," in *2020 IEEE International Conference on Blockchain and Cryptocurrency*, 2020.

[12] B. Lang, "A computational trust model for access control in p2p," *SCIENCE CHINA Information Sciences*, vol. 53, pp. 896–910, 05 2010.

[13] A. Put and B. De Decker, "Iotsear: A system for enforcing access control rules with the iot," in *The Twelfth International Conference on Evolving Internet (INTERNET 2020)*. Xpert Publishing Services, 2020.

[14] S. Al-Rabiaah and J. Al-Muhtadi, "Consec: Context-aware security framework for smart spaces," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, ser. IMIS '12. USA: IEEE Computer Society, 2012, p. 580–584.

[15] A. Toninelli, A. Corradi, and R. Montanari, "A quality of context-aware approach to access control in pervasive environments," in *MobileWireless Middleware, Operating Systems, and Applications*. Springer, 2009.

[16] Chunyu Miao and Lina Chen, "Trust-based dynamic access control policy for ubiquitous computing," in *2010 3rd IEEE International Conference on Ubi-Media Computing*, 2010, pp. 277–281.