Authentication of Things: Authentication and Access Control for the Entire IoT Device Life-Cycle

Antonio Lemos Maia Neto
Advisor: Leonardo Barbosa e Oliveira
Co-Advisor: Ítalo Fernando Scotá Cunha
Dissertation: `https://shorturl.at/mAG05`

Universidade Federal de Minas Gerais (UFMG)

Abstract. *As the number of Internet of Things (IoT) devices already grows faster than the population, the need for strong authentication and access control mechanisms is greater than ever. Legacy authentication schemes are usually computationally expensive which makes them unsuitable for resource-constrained IoT devices. On the other hand, solutions that target such devices typically base their access control mechanism solely on authentication. In a complex smart environment, however, IoT devices often offer and consume a range of resources, which demands a fine-grained access control mechanism. Besides, the IoT paradigm also beckons safe interoperability among devices that belong to different smart environments. Last, there is a lack of options for authentication and access control solutions that cover the entire IoT device life-cycle, i.e., from device manufacturing to decommissioning.*

In this work, we propose Authentication of Things (AoT), a holistic authentication and fine-grained access control solution for the entire IoT device life-cycle. AoT comprises a suite of protocols which relies on Identity-Based Cryptography (IBC) to distribute keys and authenticate devices as well as Attribute-Based Cryptography (ABC) to cryptographically enforce a fine-grained Attribute-Based Access Control (ABAC). We evaluate an AoT prototype at different security levels implemented on a variety of platforms, representing a wide range of IoT devices, from smartphones to microcontrollers. Our results indicate that AoT performance ranges from affordable on resource-constrained devices to highly efficient on powerful devices.

1. Introduction

The Internet of Things (IoT) can be seen as the pervasive presence of physical objects or "things" that, embedded with computing, storage, and communication capabilities, interact among each other and with other traditional computational entities, such as mobile and cloud computing, to cooperatively provide everyday services for users in a specific context, enabling the so-called smart environments, e.g., smart houses, offices, manufacturing, and cities.

Smart environments are, in fact, part of our daily lives. The number of IoT-connected devices grows faster than both population and Internet users[1], which increases the need for strong authentication and access control mechanisms to guarantee security

[1] `https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html`

in such heterogeneous networks. Besides demanding security inside these diverse technology environments, the IoT paradigm also beckons safe interoperability among devices that belong to different smart environments, e.g., a guest device in a smart house might want access to smart appliances' operations available for visitors.

Due to the highly heterogeneous nature of IoT, ranging from smartphones to smart motion sensors in a smart house context, for instance, traditional authentication schemes based on Public Key Infrastructure (PKI) and certificates, which carry significant processing, memory, storage, communication, and management overheads, are deemed unfit for the devices on the lower end of this range, the resource-constrained IoT devices. Several authentication schemes for IoT especially targeting resource-constrained devices have been proposed as a solution to this problem [Oliveira et al. 2009, Simplicio Jr et al. 2017, Nafi et al. 2020]. Albeit authentication differs in concept and purpose from access control, they are indeed closely related security subjects. Notably, most of these proposals on security that target resource-constrained devices typically base their access control mechanism solely on authentication, which is also known as the all-or-nothing approach, i.e., once authenticated, the entity has full access to any resource on the destination. However, in IoT architectures such as smart environments, IoT devices often offer a range of resources that require different permissions rights, e.g., a kitchen smart appliance has few operations that are available to be safely executed by the kids in a smart house, which demands a fine-grained access control mechanism.

In fact, there are a variety of works that propose alternatives for fine-grained access control for resource-constrained devices in IoT [Lunardi et al. 2018, Ding et al. 2019, Khalid et al. 2020]. The existing approaches usually delegate the access control decision to an external trusted entity, taking such a decision out of the IoT device. On the one hand, the access control processing burden is removed from the resource-constrained device. On the other hand, it creates a third-party dependency on a supposed direct device-to-device operation, which impacts user experience in cases of instability or unavailability on the authorization service.

Although the enormous attention authentication and access control for IoT has received from the research community, there is scant literature covering the entire IoT device life-cycle [Yousefnezhad et al. 2020], i.e., from the beginning-of-life, when the device is manufactured then deployed in a smart environment, passing through the middle-of-life, when it communicates not only with other devices in its smart context but also with its manufacturer to potentially be updated, and, last, the end-of-life, when it is disposed [Kärkkäinen et al. 2003]. The majority of the authentication and access control proposals for IoT on the literature, even without being explicit, approach the middle-of-life of IoT devices, i.e, when the device is cooperatively providing its operations in its smart environment domain. However, neither a trusted relationship with the manufacturer nor a secure decommissioning process for end life are usually contemplated. The lack of the former has a high probability of leaving IoT devices out to date, potentially vulnerable to security threats, which, in turn, might lead to devastating consequences since it puts all devices in the smart environment connected to them at risk [Abdul-Ghani et al. 2018]. The absence of the latter, on the other hand, gives adversaries access to consumers' personal information and to the cryptographic material from their trusted environments, which might be used to abuse the trusted relationships, also becoming a potential threat

to the other devices in the smart environment [Khan et al. 2018].

2. Goal

In this work, we aim at designing, developing, and evaluating a holistic authentication and fine-grained access control solution for IoT. Our solution, *Authentication of Things* (AoT), provides authentication and access control to all stages in an IoT device's life-cycle (Figure 1), in particular: pre-deployment, ordering, deployment, functioning, and retirement. AoT targets the highly heterogeneous and interoperable nature of IoT smart environments, where IoT devices: (i) operate each other in what we call a local domain of trust, where the operations demand fine-grained access control permissions; (ii) do not have any dependency on third parties during the authentication and access control processes; (iii) can operate as guest devices in a foreign domain, i.e., not originally their local domain of trust; and (iv) interact with a remote server in a manufacturer domain of trust, which represents the trust relationship between the devices and their manufacturer during their life-cycle.

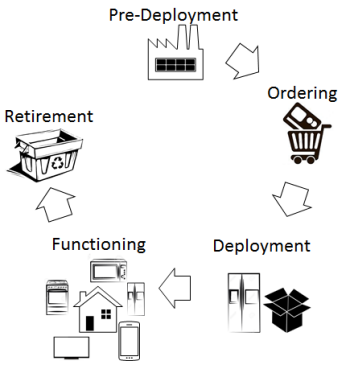

Figure 1. Entire IoT device life-cycle.

3. Approach

In order to accomplish our goals, AoT protocols rely on Identity-Based Cryptography (IBC) [Shamir 1984] to distribute keys and authenticate devices as well as Attribute-Based Cryptography (ABC) [Goyal et al. 2006] to cryptographically enforce a fine-grained Attribute-Based Access Control [Yuan and Tong 2005]. We chose these cryptosystems because they are certificate-free and thus do not impose certificate-related overheads on devices.

Our key insight to tackle the key escrow problem of IBC is a two-domain architecture (Figure 2). More precisely, our solution comprises two distinct IBC setups, namely: a manufacturer (*Cloud*) setup and a local (*Home*) setup. They respectively define manufacturer-to-device and domestic device-to-device trust relationships. There is no overlap in these trust relationships and thus an artifact generated in the Cloud domain is invalid in the Home domain and vice-versa. Note that the key escrow still holds in each IBC setup individually; however, the escrow now is no longer a major problem. For the Cloud's IBC keys escrow, this is because the user's privacy is preserved in that requests originating from the Cloud domain are null in the Home domain. For the Home's IBC

and ABC keys escrows, the context of where it takes place already deals with the problem. Nevertheless, the compromising of such a device leads to the compromising of the entire Home Domain, which means the device itself should integrate further protection mechanisms. In this sense, standard techniques can be used to protect the cryptographic material, like employing a Hardware Security Module (HSM) or Trusted Platform Module (TPM).

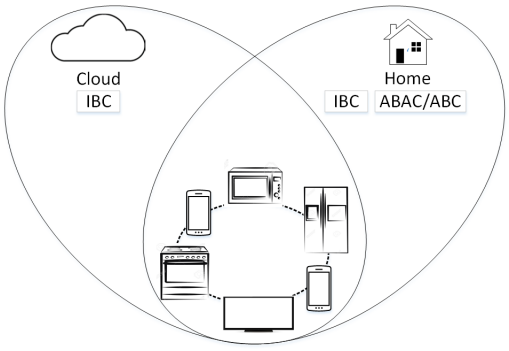

Figure 2. AoT two-domain architecture.

In AoT, the life-cycle of an IoT device comprises five main stages, namely: (1) *pre-deployment*, (2) *ordering*, (3) *deployment*, (4) *functioning*, and (5) *retirement*. By the way of example, consider a given device life-cycle. In the *pre-deployment*, the cryptographic material of the Cloud domain is loaded into the device at the factory, i.e., during its manufacturing process. Next, in *ordering*, the (about to become) owner of the device purchases it and gets a PIN that grants the owner the initial access to the device. *Deployment*, as its name suggests, is when the device is deployed in its Home domain for the very first time and therefore is the stage responsible for bootstrapping security in such a context. During deployment, the owner uses the PIN to access the device, which puts it in setup mode. The device, in turn, uses the owner's personal device to establish a trust relationship with the Home server. (The Home server is the trusted home authority in charge of managing keys and orchestrating access control inside the home domain. For instance, the Home server issues IBC and ABC keys as well as advertises access permissions over the domestic network.) Finally, during this stage, the device is also bound to a user in the Cloud domain. Now, the way is paved for *functioning*, which corresponds to the daily operation of the device. At this point, users request the device's operations, and the latter reacts based on users' clearance levels. *Retirement* is the end point of a device life-cycle. It takes place whenever its owner will no longer use the device. During this stage, there is a wipeout cryptographic material held by the device and the owner is unbound from the device in the Cloud domain.

AoT has also some complementary features. For instance, AoT enables a inter-domain interactions between devices on different Home domains, meaning that devices from different Home domains may interoperate seamlessly as long as their respective Home servers have previously agreed on some parameters. This strategy is appealing because it neither violates the identity-based nature of AoT, nor requires key escrow across the participating domains. Our suite of protocols also address device reassignment, enabling a user to trade or give away one or more of his devices.

We design AoT as a composition of cryptographic protocols and primitives,

therefore, we base its modeling and security analysis under the Universal Composability paradigm [Canetti 2001]. In this context, we extend a specific functionality [Küsters and Rausch 2017] to support a set of cryptographic primitives which, in turn, supports the analysis of the identity-based authenticated key agreement protocols categorized into the same family of protocols proposed by [McCullagh and Barreto 2005] under the Universal Composability paradigm.

We implement an AoT prototype, at different security levels, on different platforms, varying computational resources, representing a wide range of IoT devices. We use a recently launched Android mobile phone, a Google Pixel 6, as a representative of smartphones that could be used in a smart environment supported by AoT. Other powerful entities in a smart environment are represented by a Raspberry Pi3, a low-cost programmable computer. We represent intermediate smart devices with Raspberry Pi1. Last, as our representative of microcontrollers that could be used on low-end appliances supporting AoT, we use an Arduino Due. We use our prototype to quantify CPU, memory, storage, and communication overheads imposed by AoT protocols. Our results indicate AoT performance ranges from affordable on resource-constrained devices like the Arduino Due to efficient on intermediate devices like the Rapsberry Pi1, and highly efficient on powerful devices like the Raspberry Pi3 and on smartphones like the Google Pixel 6.

4. Contributions

The majors contributions of our work are summarized as follows.

- An authentication and access control solution that cover all the stages in an IoT device life-cycle, i.e., from device manufacturing to decommissioning.
- A fine-grained Attribute-Based Access Control mechanism cryptographically enforced by Attribute-Based Cryptography.
- An extension of a functionality [Küsters and Rausch 2017] in the Universal Composability framework which ends up supporting the analysis of identity-based authenticated key agreement protocols [McCullagh and Barreto 2005].

We also have the following minor contributions:

- A two-domain architecture that allows separated device-to-manufacturer and device-to-device trust relationships during the IoT device life-cycle.
- A protocol for device ownership reassignment and a protocol for authentication and access control between devices from different domains of trust.
- Device-to-device authentication and access control processes' decision without any delegation to third parties.

5. Results

We evaluate versions of an AoT prototype at 100- and 128-bit security levels, on different platforms, varying computational resources, representing a wide range of IoT devices. We use a recently launched Android mobile phone, a Google Pixel 6, as a representative of smartphones that could be used in a smart environment supported by AoT. Other powerful entities in a smart environment are represented by a Raspberry Pi3, a low-cost programmable computer. We represent intermediate smart devices with Raspberry Pi1. Last, as our representative of microcontrollers that could be used on low-end appliances

Resouce	Google Pixel 6	Raspberry Pi3	Raspberry Pi1	Arduino Due
CPU arch.	arm64-v8a	armv7-a	armv6	armv7-m
Word size	64 bits	64 bits	32 bits	32 bits
Clock	1.8 GHz	1.2 GHz	700 MHz	84 MHz
Cores	8	4	1	1
RAM	12 GB	1 GB	512 MB	96 KB
Storage	256 GB	8 GB	4 GB	512 KB
OS	Android 12	Linux raspberry 4.9.59-v7+	Linux raspberry 5.10.17+	None

Table 1. Summary of devices used in experimental evaluation.

supporting AoT, we use an Arduino Due. Table 1 presents the computation resources of each platform.

Tables 2 and 3 summarizes run times for the cryptographic primitives used in AoT at 100- and 128-bit security levels, respectively. In the tables, "Enc", "Dec", "Sign", and "Ver" are abbreviations for encryption, decryption, signature generation, and signature verification, respectively. The abbreviations IBE, IBS, and ABS refer to Identity-based Encryption, Identity-based Signature, and Attribute-based Signature. In case of IBE, we consider a 32 bytes length message. In IBS, we use messages with 1KB, covering all cases IBS is used in AoT. In ABS, we consider predicates of the form $\boldsymbol{A} \wedge \boldsymbol{B}$, i.e., with two attributes and a single "and" operator. We observe that at 100-bit security level, the cryptographic primitives in Arduino Due execute in reasonable time. IBE encryption, for instance, is executed in 0.5s, and an ABS signature is generated in 1.2s and verified in 1.5s.

100-bit sec. level	IBE.Enc	IBE.Dec	IBS.Sign	IBS.Ver	ABS.Sign	ABS.Ver
Google Pixel 6	5ms	2ms	0.2ms	1ms	11ms	13ms
Raspberry Pi3	21ms	10ms	1ms	7ms	45ms	58ms
Raspberry Pi1	86ms	43ms	5m s	24ms	184ms	222ms
Arduino Due	551ms	264ms	34ms	190ms	1.2s	1.5s

Table 2. Summary of experimental evaluation at 128-bit security level.

As expected, at 128-bit security level, the run time results are high on the Arduino Due. IBE encryption is executed in 2.8s, and ABS signature is generated in 4.8s and verified in 6.2s. Even with high run times, most of the primitives are not frequently executed in AoT, therefore they are acceptable for resource-constrained devices executing our prototype at 128-bit security level. However, as ABS algorithms are executed in each access control of a device operation, the ABS run times for this version of our prototype on the Due fulfill the timing requirements of a narrow range of IoT applications. It is important mention, however, that at 128-bit security level we do not implement any optimization using assembly code for the underlying elliptic curve. We estimate that using such an optimized code, the Arduino Due would take around 2.7s to generate an ABS signature for a predicate of the form $A \wedge B$, and 4s to verify it.

We observe that in the other platforms AoT imposes negligible overhead. For

128-bit sec. level	**IBE.Enc**	**IBE.Dec**	**IBS.Sign**	**IBS.Ver**	**ABS.Sign**	**ABS.Ver**
Google Pixel 6	14ms	7ms	0.5ms	3ms	25ms	33ms
Raspberry Pi3	59ms	30ms	2ms	13ms	101ms	136ms
Raspberry Pi1	184ms	94ms	8ms	42ms	314ms	421ms
Arduino Due	2.8s	1.4s	110ms	550ms	4.8s	6.2s

Table 3. Summary of experimental evaluation at 128-bit security level.

instance, ABS signature verification for predicates of the form $A \wedge B$, the most expensive operation in our experiments, is executed in 33ms in Google Pixel 6, in 136ms in Raspberry Pi3, and in 421ms in Raspberry Pi1.

6. Scientific Production

- Neto, A. L. M., Souza, A.L., Cunha, I., Nogueira, M., Nunes, I. O., Cotta, L., Loureiro, A. A. F., Aranha, D. F., Oliveira, L. B. (2016). AdC: um Mecanismo de Controle de Acesso para o Ciclo de Vida das Coisas Inteligentes. *Brazilian Symposium on Information and Computer System Security (SBSeg)*.
- Neto, A. L. M., Souza, A.L., Cunha, I., Nogueira, M., Nunes, I. O., Cotta, L., Loureiro, A. A. F., Aranha, D. F., Oliveira, L. B. (2016). Aot: Authentication and Access Control for the Entire IoT Device Life-Cycle. *ACM Conference on Embedded Network Sensor Systems (SenSys).*
- Oliveira, L. B. E., Loureiro, A. A. F., Neto, A. L. M. (2019). U.S. Patent No. 10,523,437. *Washington, DC: U.S. Patent and Trademark Office. United States Patent Application Publication US 2017/0214529 A1.*
- Neto, A. L. M., Pereira, Y. L., Souza, A. L., Cunha, I., Oliveira, L. B. (2018). Attribute-based authentication and access control for IoT home devices. *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN).*
- Neto, A. L. M., Oliveira, L. B. (2018). AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle. *2018 Google Latin America Research Awards.*
- Neto, A. M., Richardson, S., Horowitz, M., Oliveira, L. (2019). Aceleração de Assinaturas baseadas em Atributos para Internet das Coisas. *Brazilian Symposium on Information and Computer System Security (SBSeg)*.
- Neto, A. L. M., Cunha, I., Oliveira, L. B. Uma Extensão de Framework de Análise de Protocolos de Composibilidade Universal para Acordo de Chaves com Autenticação Baseado em Identidade. *Brazilian Symposium on Information and Computer System Security (SBSeg)*.
- Neto, A. L. M., Cunha, I., Oliveira, L. B. Short Talk - Análise Modular de Segurança de Protocolos Fundamentados em Criptografia Baseada em Identidade. *Digital Identity Management Workshhop - Brazilian Symposium on Information and Computer System Security (SBSeg)*.

References

Abdul-Ghani, H. A., Konstantas, D., and Mahyoub, M. (2018). A comprehensive iot attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*.

Canetti, R. (2001). Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE.

Ding, S., Cao, J., Li, C., Fan, K., and Li, H. (2019). A novel attribute-based access control scheme using blockchain for iot. *IEEE Access*.

Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *Conference on Computer and Communications Security (CCS)*.

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., and Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Cluster Computing*.

Khan, W. Z., Aalsalem, M. Y., and Khan, M. K. (2018). Five acts of consumer behavior: A potential security and privacy threat to internet of things. In *IEEE international conference on consumer electronics (ICCE'18)*.

Küsters, R. and Rausch, D. (2017). A framework for universally composable diffie-hellman key exchange. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 881–900. IEEE.

Kärkkäinen, M., Holmström, J., Främling, K., and Artto, K. (2003). Intelligent products—a step towards a more effective project delivery chain. *Computers in Industry*. Advanced Web Technologies for Industrial Applications.

Lunardi, R. C., Michelin, R. A., Neu, C. V., and Zorzo, A. F. (2018). Distributed access control on iot ledger-based architecture. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*.

McCullagh, N. and Barreto, P. S. L. M. (2005). A New Two-party Identity-based Authenticated Key Agreement. In *International Conference on Topics in Cryptology (CT-RSA)*.

Nafi, M., Bouzefrane, S., and Omar, M. (2020). Matrix-based key management scheme for iot networks. *Ad Hoc Networks*.

Oliveira, L. B., Kansal, A., Priyantha, B., Goraczko, M., and Zhao, F. (2009). Secure-TWS: Authenticating Node to Multi-user Communication in Shared Sensor Networks. In *International Conference on Information Processing in Sensor Networks (IPSN)*.

Shamir, A. (1984). Identity-based Cryptosystems and Signature Schemes. In *International Cryptology Conference on Advances in Cryptology (CRYPTO)*.

Simplicio Jr, M. A., Silva, M. V., Alves, R. C., and Shibata, T. K. (2017). Lightweight and escrow-less authenticated key agreement for the internet of things. *Computer Communications*.

Yousefnezhad, N., Malhi, A., and Främling, K. (2020). Security in product lifecycle of iot devices: A survey. *Journal of Network and Computer Applications*.

Yuan, E. and Tong, J. (2005). Attributed Based Access Control (ABAC) for Web Services. In *International Conference on Web Services (ICWS)*.