Identity-based authentication scheme for the Internet of Things

Conference Paper · June 2016

DOI: 10.1109/ISCC.2016.7543884

5 authors, including:

Ola Salman
American University of Beirut
9 PUBLICATIONS **41** CITATIONS
SEE PROFILE

Sarah Abdallah
American University of Beirut
7 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Imad H. Elhajj
American University of Beirut
168 PUBLICATIONS **1,417** CITATIONS
SEE PROFILE

Ali Chehab
American University of Beirut
239 PUBLICATIONS **1,027** CITATIONS
SEE PROFILE

Identity-Based Authentication Scheme for the Internet of Things

Ola Salman Sarah Abdallah Imad H. Elhajj Ali Chehab Ayman Kayssi
Department Electrical and Computer Engineering
American University of Beirut
Beirut 1107 2020, Lebanon
{oms15, saa78, ie05, chehab, ayman}@aub.edu.lb

***Abstract* — Security and privacy are among the most pressing concerns that have evolved with the Internet. As networks expanded and became more open, security practices shifted to ensure protection of the ever growing Internet, its users, and data. Today, the Internet of Things (IoT) is emerging as a new type of network that connects everything to everyone, everywhere. Consequently, the margin of tolerance for security and privacy becomes narrower because a breach may lead to large-scale irreversible damage. One feature that helps alleviate the security concerns is authentication. While different authentication schemes are used in vertical network silos, a common identity and authentication scheme is needed to address the heterogeneity in IoT and to integrate the different protocols present in IoT. We propose in this paper an identity-based authentication scheme for heterogeneous IoT. The correctness of the proposed scheme is tested with the AVISPA tool and results showed that our scheme is immune to masquerade, man-in-the-middle, and replay attacks.**

Keywords—Authentication; Security; Internet of Things; Fog Computing; SDN.

I. Introduction

The Internet of Things (IoT) presents several challenges that hinder its wide deployment. Nevertheless, the technology is evolving with tens of billions of things will be connected to the Internet by 2020 [1]. IoT will span a wide range of distinct communication technologies used in the different islands of networks of things, and will also result in a large amount of data referred to as "IoT Big Data". In IoT, the concern related to Big Data is not particularly related to the size of the data, but rather to the heterogeneity of the data in terms of format, type, and semantics. Security and privacy are also additional concerns and constitute essential IoT limitations [2]. Applying security schemes in IoT requires careful consideration since the requirements and device capabilities are different than in traditional networks. Moreover, these schemes have to be scalable in order to span the tens of billions of things; thus a new management paradigm ought to be invoked.

Software Defined Networking (SDN) offers a new centralized control and management structure for networks; an SDN controller monitors and manages all the network elements, and the management and supervision functions are enforced globally and seamlessly. IoT can benefit from SDN and the notion of fog computing to deploy a set of gateways that can support an authentication security layer for the things. These gateways will be in turn managed and authenticated by a central authority, in this case the SDN controller.

The rest of this paper is organized as follows: In section II, we survey related work. In section III, we present our proposed authentication scheme, then show an evaluation of this scheme in section IV, together with its overhead. Finally, we conclude in section V.

II. Related Work

IoT has been studied thoroughly in the literature, where researchers tackled aspects starting from device identification and authentication, up to device management, and more generally the IoT architecture. Shivraj et al. rely on the One Time Password (OTP) technique developed with Elliptic Curves Cryptography (ECC) [3]. The scheme was shown to be more efficient and secure than other existing methods since the Key Distribution Center (KDC) does not store private and public keys of devices, it only stores their IDs. Sungchul et al. built their authentication technique on an ID-based authentication scheme (IBA) in the context of RESTful web services. The proposed scheme uses the URIs as unique IDs for generating the keys using ECC [4]. Another authentication scheme for IoT is presented in [5] and is based on the association of things with a registration authority. This method is useful for limited-capability things. In [6], Bamasag et al. presented a new technique that avoids the use of public key cryptography and the computational burden associated with it. Their technique relies on an algorithm [7] that allows the recovery of a secret key from chunks of this latter. Turkavonic et al. also introduced a new approach for IoT authentication, where users and nodes authenticate themselves directly and not through a gateway. The scheme was presented in a WSN context, where most of the nodes are of limited capability and only few of them are powerful gateway nodes (GWN)[8]. In [9], Crossman and Liu approached the two-step authentication scheme and instead of using a verification code sent to a mobile phone, the authors proposed the use of a smartcard for generating keys on the devices directly. Their proposed scheme tries to separate data and encryption keys.

III. Proposed Authentication Scheme

A. The General Architecture

The assumption that all things have IPv6 addresses and support the TCP/IP protocol stack is not realistic in the broadest IoT scenario. In fact, IoT is a network of networks, i.e. it is made of islands running different communication and networking protocols. Therefore, a gateway layer is mandatory to support this heterogeneity which consists of fog-distributed nodes, and to ensure the communication between different vertical silos and to ease authentication. A trusted certificate authority implemented on an SDN controller is used to manage all security parameters.

978-1-5090-0679-3/16/$31.00 ©2016 IEEE

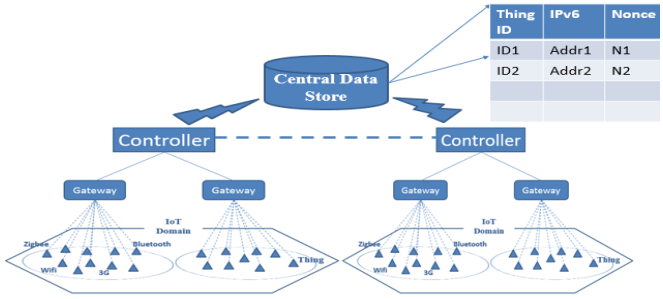

Figure 1: General Architecture

In SDN, all control is relayed to a central controller, which is all-pervading in the network [10]. Deploying SDN in IoT networks provides many advantages especially that having a centralized control hides the management complexities incurred in IoT. While the centralization of control has been introduced many years ago, and although it faces scalability and availability limitations, the automation provided by the softwarization outweighs these shortcomings. In fact, the logical centralization of control with physically distributed controller instances, makes the scalability issue easier to address. For these reasons, we introduce SDN with IoT, in a hierarchical and distributed deployment of SDN control.

Although different SDN security concerns exist, they have been thoroughly addressed in the literature: DoS and DDoS attacks at the control plane and the data plane are very likely to happen [11]. However, those and other attacks have been analyzed and countermeasures have been proposed, as in [12, 13]. Nonetheless, the security aspects added by the introduction of SDN outweigh the limitations that already exist in today's networks. Having a global view of the whole network, the controller can detect any misbehavior. The time and overhead of sharing the security-related statistical information in the distributed networking paradigm are reduced. Additionally, the functions of firewalls and intrusion detection systems (IDS) are henceforth included in the manageable switches. With this in mind, we present our SDN based IoT architecture as well as the corresponding authentication scheme. This architecture is divided into domains, as shown in Figure 1. In our scheme, the controller retains the most important security role and has full knowledge of its managed domains. It may be a collection of distributed instances that share a whole view of the entire network and has access to a central database, with one instance of the controller will be in charge of one IoT domain.

B. Authentication of Things

Many authentication schemes consider only the direct communication between things in a specific type of network, such as WSN, where power consumption has been commonly considered. Although this is a big concern in the WSN context, other concerns are encountered in IoT, the most important being the heterogeneity in the types and nature of the things.

The IoT things must be uniquely identifiable [15], so they could be authenticated autonomously, if they are capable enough or if they associate themselves with a more powerful node in their own network. IPv6 has been designated as a suitable identity scheme, however, IPv6 hasn't been widely adopted yet. Our proposed scheme assigns a virtual IPv6-based identity to the thing via the controller.

The key establishment method in our proposal is based on ECC, as it is the most widely used method in IoT due to its efficiency and economical nature. We assume that the root controller public key is hardcoded in each thing when manufactured. The controller generates the public keys for things using ECC. The gateway also generates its own pair of public/private keys using ECC. In the following, we describe the message flow in the phases of authentication (Figure 2).

Phase 1 - Gateway public key certification: Each gateway acquires a public key certificate from the controller. By sending its ID (ID_G) along with its public key (Ku_G), the gateway gets a certificate signed by the controller's private key, Kr_C: $E(Kr_C, [ID_G||Ku_G||H_1(ID_G||Ku_G)]$. This certificate is used by the gateway to authenticate itself to the controller.

Phase 2-Thing registration: The thing starts by sending an authentication request to the gateway containing its ID (ID_T) (specific to each type of network: IP, MAC, Zigbee address, etc.) and a randomly generated nonce (N_1) which will be used as private key encrypted by the controller public key: $E(Ku_C, N_1)$, and another nonce (N_2) that is sent to prevent replay attacks. Upon receiving the partial identity of the thing, the gateway, which is aware of the different communication protocols, can verify if the technology-specific source address matches the one in the registration request. After this preliminary identity check, the gateway sends the request to the controller, along with its certificate, to be authenticated by the controller. The controller generates an IPv6 address and a public key for the thing using ECC with the received nonce (N_1) as private key. The hash of the IPv6 address, $H(IPv6)$, the thing's public key, Ku_T, the gateway's public key encrypted by the thing's private key all encrypted by the gateway public key:

$$E(Ku_G, H(IPv6)||Ku_T||E(N1, [Ku_G]))$$

The gateway receives this message, decrypts it and stores the hash identity $H(IPv6)$ and the corresponding thing's public key. Then, the gateway sends to the thing: the thing's public key, the hashed address, and the gateway's public key encrypted by the thing's private key. The thing makes sure that it has been registered with the controller by receiving the gateway's public key encrypted by its own private key. So, it decrypts it and stores the gateway's public key.

Phase 3 - Authentication Phase: When the thing wants to authenticate itself, it sends the stored $H(IPv6)$ along with a nonce (N_3) signed by the gateway's public key to prevent replay attacks and to authenticate the gateway. Upon receiving the identity of the thing, the gateway looks for its public key in its local storage. Then, the gateway replies by sending back (N_3) along with a new nonce (N_4), both encrypted by the thing's public key. To be authenticated, the thing has to reply by sending back N_4 encrypted by the gateway's public key. Thus, the couple ($H(IPv6)$, N_1) serve to provide a unique identity to the thing to be authenticated by the gateway and hence to be granted access permissions. Therefore, if the thing moves to another gateway domain, the gateway will not find the $H(IPv6)$ in its local database, and will ask the controller if this thing is registered. The controller, having access to the global database, searches for the hash. If found, it returns it to the gateway along with the public key of the thing. The gateway then decrypts the nonce, stores it and authenticates the thing. If not, the thing is considered as an outsider.

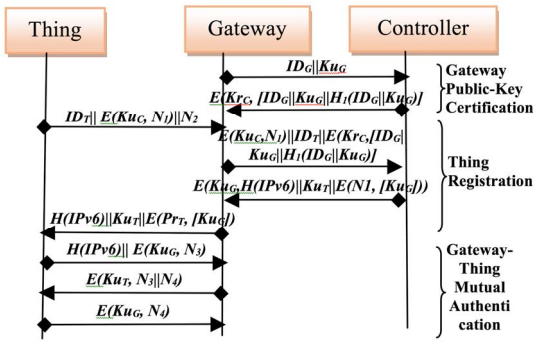

Figure 2: Protocol Message Flow

IV. Evaluation & Results

Testing was performed using the SPAN/AVISPA tool. In our experiment, we have three roles: **Thing (T), Gateway (G),** and **Controller (C).** Each role has certain knowledge, initial state, and several transitions defined in its role section and three security goals are defined in the environment role; these are the secrecy of the nonce (N_1), the authentication of the thing through *H(IPv6)* and (N_4), and the authentication of the gateway by the thing on receiving the nonce (N_3). The analysis, which is fully automated and results showed that our scheme is **SAFE** against attacks.

The main concept of the checkers in the SPAN tool is that they look for possible attacks simulating the role of an intruder. The analysis considers the channels as insecure mediums and all unencrypted messages or encrypted messages with attainable keys can be perceived by the intruder. These testing algorithms then try to check if the defined security goals in design can be violated by introducing the intruder role or not. Upon the analysis, they decide if the protocol is SAFE, UNSAFE, or INCONCLUSIVE. The main attacks that are considered by these testing/verification algorithms are: masquerade, man-in-the-middle and replay attacks.

To reduce the overhead in our scheme, we tried to decrease the computation and storage overhead on the things and waived these tasks to more powerful nodes (gateways and controller). Essentially, the thing has to store its private key, the public key of the controller, the public key of the gateway and its virtual identity (hash of its generated IPv6 address). Also the thing has to generate the private key (N_1), the nonce (N_2) for preventing replay attacks, and the nonce (N_3) used during the authentication phase, and finally send the registration request which contains the encrypted private key. When receiving the reply, it has to decrypt the gateway's public key. At the authentication phase, it has to encrypt the nonce (N_3). Then, when receiving the reply, it has to decrypt the message, check if the nonce (N_3) is received correctly, and it has to encrypt the other nonce (N_4). Totally, it has to do three encryption operations and two decryption operations, send three messages and receive two.

The overhead at the gateway and controller can be similarly estimated, and it shows that our scheme is well designed in terms of managing security data (keys, certificates, and identities) but it presents some challenges in term of computation needed to be done by the thing. However, as stated before, a thing that cannot perform these tasks can associate itself to a more powerful node in its local network.

V. Conclusions

Security is a crucial concern in networks. In particular, with IoT, security implications are even more pronounced since the impact of attacks is more drastic, mainly because IoT includes a wide range of applications from simple location awareness to very critical healthcare uses. In this paper, we proposed an identification and authentication scheme for heterogeneous IoT networks based on SDN. The central SDN controller translates the different technology-specific identities from the different silos into a shared identity based on virtual IPv6 addresses and authenticates devices and gateways. Results showed that the scheme is safe against masquerade, man-in-the-middle, and replay attacks.

Acknowledgments

Research funded by TELUS Corp., Canada

References

[1] D. Evans, "'The Internet of Things How the Next Evolution of the Internet Is Changing Everything", Cisco White Paper, April 2011.

[2] S. William and W. Stallings, "'Cryptography and Network Security, Fifth Edition", 2011.

[3] Shivraj, V. L., M. A. Rajan, Meena Singh, and P. Balamuralidhar. "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)". In IEEE 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW 2015), pp. 1-6. KSA, 2015.

[4] Sungchul L., Ju-Yeon J. and Yoohwan K., "Method for secure RESTful web service". In IEEE/ACIS, 14th International Conference on Computer and Information Science (ICIS 2015), pp. 77-81. Las Vegas-USA, 2015

[5] Liu J., Xiao Y. and Chen C.L.P., "'Authentication and Access Control in the Internet of Things". In IEEE 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW 2012), pp. 588-592. China, 2012.

[6] Bamasag, O. O., & Youcef-Toumi, K. "Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme". In Proceedings of the WESS'15: Workshop on Embedded Systems Security, p.1. The Netherlands, 2015.

[7] A. Shamir, "'How to share a secret," *Commun ACM*, vol. 22, no. 11, pp. 612-613.

[8] Turkanović, M., Brumen, B., & Hölbl, M. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion". Ad Hoc Networks, 2014, vol. 20, 96-112.

[9] M.A. Crossman and Hong Liu, "Study of authentication with IoT testbed". In IEEE International Symposium on Technologies for Homeland Security (HST 2015), pp. 1-7, Massachusetts-USA, 2015.

[10] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "'OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69-74.

[11] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes, "'Software-defined networking security: pros and cons," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 73-79.

[12] D. Kreutz, F. Ramos and P. Verissimo, "'Towards secure and dependable software-defined networks," In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 55-60. ACM, 2013.

[13] M. Coughlin, "A Survey of SDN Security Research."

[14] M.S. Farash, M. Turkanović, S. Kumari and M. Hölbl, "'An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, Part 1, 1, pp. 152-176.

[15] R. Minerva, A. Biru and D. Rotondi, "'Towards a definition of the Internet of Things (IoT) ", IEEE Internet Initiative, May 2015.