Proposed on Device Capability based Authentication using AES-GCM for Internet of Things (IoT)

Babar, Sachin D.; Mahalle, Parikshit N.; Prasad, Neeli R.; Prasad, Ramjee

Published in:
Procedings of the 3rd Springer International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec 2011)

Publication date:
2011

Document Version
Early version, also known as pre-print

Proposed on Device Capability based Authentication using AES-GCM for Internet of Things(IoT)

Sachin D. Babar[1] , Parikshit N. Mahalle[1], Neeli R. Prasad[1], Ramjee Prasad[1]

Center for TeleInFrastruktur, Aalborg University , Aalborg , Denmark
{sdb, pnm, np, prasad }@es.aau.dk

Abstract. Economics of scale in Internet of Things (IoT) presents new security challenges for ubiquitous devices in terms of authentication, addressing and embedded security. Currently available cryptographic techniques require further analysis to determine applicability to IoT. We introduce an authentication and encryption protocol which serves as a proof of concept for authenticating device using the Advanced Encryption Standard (AES) – Galois/ Counter Mode GCM as cryptographic primitive. Authenticated encryption is best suited concept for IoT that will provide both message encryption and authentication. Unique part of this work is a novel approach of extending authentication and encryption with cryptographic capabilities.

Keywords: Authentication, Access Control, Capability, Embedded Security, Cryptography, Addressing.

1 Introduction

IoT is service oriented architecture with resource constraints and is a mandatory subset of future internet where every virtual or physical device can communicate with every other device giving seamless service to all stakeholders. IoT is convergence of resource constrained sensors, RFID, smart devices and any object with sensing, computing and communication capability. These devices can interact with the user and among themselves, to provide secure services or information. These interactions will further extend the need for privacy and security models to include how users interact with devices, and how these devices will interact among themselves. In IoT basic challenge is to identify or address and authenticate individual devices. So to identify individual device we need to have some addressing mechanism by which we can address or access particular device. For unique identification already some techniques are available, like for computer system identification, there is ipv4 protocol, but again, as it is 32 bit address, these are less as compared to number of increasing devices. To avoid this limitation new protocol was introduced i.e. IPV6 (128 bit). Challenges for having unique authentication and access control solution for different devices around us like home appliances fridge, mixer, washing machine, Television etc in IoT are daunting.

This paper is structured as follows: Section 2 talks about the Security consideration for IoT. Section 3 analyzes related work. Section 4 describes the AES-GCM which is an efficient authenticated encryption algorithm. Section 5 proposes a device capability

based addressing and authentication protocol which achieves authentication, encryption and access control. Section 6 evaluates the proposed protocol in terms of its efficiency. Section 7 concludes the paper with future scope.

2 Security Considerations for IoT

Devices like RFID or sensor node themselves have no access control function, so they can freely obtain information from each other. As a result, an authentication as well as authorization scheme must be established between devices so as to achieve the security goals for IoT. In RFID, tag security issue related to the scenario, like the communication between a tag and a reader which is by radio, anyone can access the tag and obtains its output, i.e. attackers can eavesdrop on the communication channel between tags and readers, which is a cause of consumer's apprehension. So the authentication scheme employed in RFID must be able to protect the data passing between the tag and the reader, i.e. the security solution itself should have some kind of encryption capability.

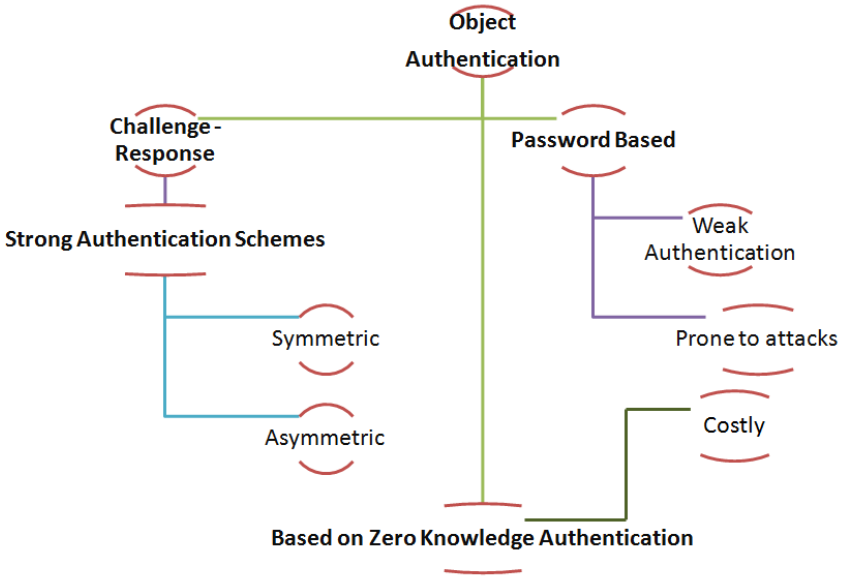

Fig. 1. Authentication schemes

Authentication is related to secure identification of devices in which there is need for verification of identity possession. Every act of an access control will enable authentication process. So, secure identity establishment is a promising in nomadic IoT which prone to many threats [1-2]. Authentication with encryption can solve all of the former mentioned security threats in IoT scenario like RFID and sensor Networks applications.

Broadly there are three authentication schemes: password systems (weak authentication), challenge-response authentication (strong authentication), and customized and zero-knowledge authentication [3]. Password systems offers a weak level of security and zero-knowledge techniques are often related to "strong" mathematical problems which are very costly in calculation and implementation. So we aim for the second type, the challenge-response techniques, which are broadly used. There are asymmetric and symmetric challenge-response techniques. The disadvantage of asymmetric authentication methods is that they are very time consuming and costly to implement in hardware. So, they are not the first choice for resource constraints devices. This classification is shown in figure 1.

3 Related Work

A number of different authentication and access control schemes exist in the literature but each addressing different devices. In sensor networks a multitude of sensors communicate as peers with each other and each sensor is constrained in its computational power, which precludes use of asymmetric cryptography. Here secret key schemes are used to create authenticated communication relations between certain nodes. Due to the peer-to-peer communication model there are multiple possible paths between each node. Statistical considerations are used to reduce the number of necessary node-pair secrets while still guaranteeing secure paths between any arbitrary pair of nodes. The main research focus in sensor network authentication is on resiliency in the face of partly compromised network [4]. In [5], author proposes two factor time efficient authentication schemes with session key establishment only for users and devices are left unaddressed. In [6] and [7] , author have proposed authentication and access control protocol which is prone to active attacks and message interception and not suited to resource constrained IOT. Hash function based mutual authentication protocol for RFID is given in [8] but key management issue is left unaddressed as it is most important issue as per [9]. Researchers have proposed numerous protection mechanisms, but none prevents an attacker from retrieving secure information [10]. There are many protocol proposals that use hash functions and mutual authentication [11], [12] but they perform weakly during tracking and are not suitable for resource constrained devices. There are other proposals like SPKI [13], [14] which is a public key based authentication and access control protocol and authentication message format. Main focus is on sophisticated rights delegation and derivation algorithms. SPKI provides no means for session protection against tampering or replay and it is not suited for private IoT. SAML [15] is an XML based syntax for encoding capabilities, which may potentially be used within the context of the protocol described in this paper to transport capabilities, but is limited due to the fact that standard SAML can only express yes/no type of access decisions, no complex permission statements and policy enforcement.
Aforementioned literature shows that there is advancement in research for authentication and encryption, but device to device communication is left unaddressed. Also solution for incorporating on device security in the resource constrained devices is an open issue.

4 Authentication and encryption using AES-GCM

Authenticated encryption is evolving as a relatively new concept that will provide both message encryption and authentication which can be adapted for embedding security in device. AES-GCM is one of the latest authenticated encryption algorithms providing both confidentiality and authenticity suitable for hardware implementation. AES-GCM accepts four inputs namely symmetric key, Initialization vector (IV), Plaintext and an optional field for authenticating data. The output of AES-GSM is the cipher text and the message. The Initialization Vector (IV) is generated by the device performing the authenticated encryption operation. It can also be a nonce within the scope of any authenticated encryption key with uniqueness. Repeating nonce for two different messages encrypted with the same key destroys the security properties. The optional additional authenticated data can be used to authenticate plaintext packet headers. AES-GCM makes use of the AES block cipher in counter mode to provide encryption. When used properly, counter mode provides strong confidentiality [16]. GCM uses universal hashing in the finite field $GF(2^w)$ for generating a message authentication code (MAC). The additional merit of using $GF(2^w)$ is that the computation cost of multiplication under $GF(2^w)$ is less than integer multiplication. AES-GCM provides high security suitable for hardware implementation. Therefore, the use of AES-GCM is the best solution for resource constrained device to meet the security needs of IoT devices [17, 18]. Implementing AES-GCM on resource constrained devices with hardware software co-design approach will surely match the Security requirements for IoT enhancing the speed and storage area parameters. For prevention against replay attacks, use of different session key for encryption of plaintexts will help to guarantee confidentiality which can be done through GCM. Proposed protocol is using capability based addressing [19, 20] along with AES-GCM for access control of devices. Capability corresponds to row view of access control matrix [21].

5 The Proposed Protocol

In this work, we propose on device capability based authentication and access control protocol. Novelty of this protocol is in its cryptographic capability which acts as a ticket to access other device. This capability is then encrypted using AES–GCM which strongly provides both encryption and authentication for resource constrained devices. This protocol is mutual authentication protocol and it also addresses capability based access control. Conceptually, a capability is a token, ticket, or key that gives permission to access an device. A capability is implemented as a data structure that contains items like a unique device identifier, access rights and a random number, as shown in figure 2. The identifier addresses or names are single to device in IoT. Any device, in this context, can be equipped with RFID tags or sensor nodes. The access rights define the operations that can be performed on that device.

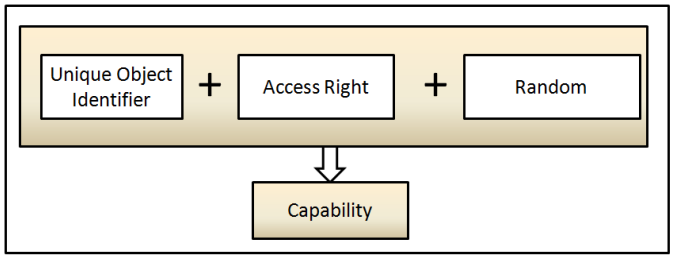

Fig. 2. Capability Structure

For simplicity, it is sufficient to examine the case where a capability describes a set of access rights for the device. Device may also contain security attributes such as access rights or other access control information. A classic capability is represented as a ticket as:

(Device, Rights, Random)

in which the first item is the name / id of the device, second is the set of access rights and the third is a random number to prevent forgery. Algorithm for one way hash function can be made publicly available. It should be secret keys independent because key distribution introduces other difficulties. Benefits of using one way hash function are that it is computationally infeasible to inverse hash function and, given a pair of input and matching output it is infeasible to find a second input which gets the same output. When an access request arrives together with a capability consisting of object id, the one-way function is run to check the result against the random number to detect tampering. If the capability is valid, the access is granted [22].

Working of this protocol is shown in figure 3. Refer table 1 for the notations used in this protocol. There are two components of this protocol: first is the creation of capability and second component is an application of AES – GCM.

Device 1 creates its capability which is a function of device id and access rights which is then encrypted and hashed along with a random number to prevent forgery. Underlying algorithm for encryption is AES-GCM. Cipher text which is created is sent to device 2. Device 2 receives the capability of device 1 in encrypted form which is decrypted using symmetric key. Tampering of received cipher text is verified using one way hash function. If the generated hash value and the received hash value do not match then it is evident that the communication has been tampered and some other device is trying to impersonate and the authentication is violated. If there is a match in generated hash value and received hash value after decryption, then device 1 is authenticated to device 2. Encryption and its hardware implementations are efficient in resource constrained devices due to features of AES-GCM. The computations overhead on device are less optimizing energy.
As it is a mutual authentication protocol, device 2 have to authenticate itself to device 1. For this, device 2 creates its capability by same method as explained above and uses the same random number sent by device 1 to prevent from replay attacks. After receiving this response at device1, it decrypts this cipher text and checks the integrity and compares the random number to ensure that this message is coming from the

same device which is authenticated by device 1. After successful decryption and comparison, device 2 is authenticated to device 1 and they are free to communicate with each other over secure channel. It is very important to note that, access right has been communicated to each other securely to achieve secure access control. This protocol is challenge response type of protocol which alleviates the overhead on both the devices.

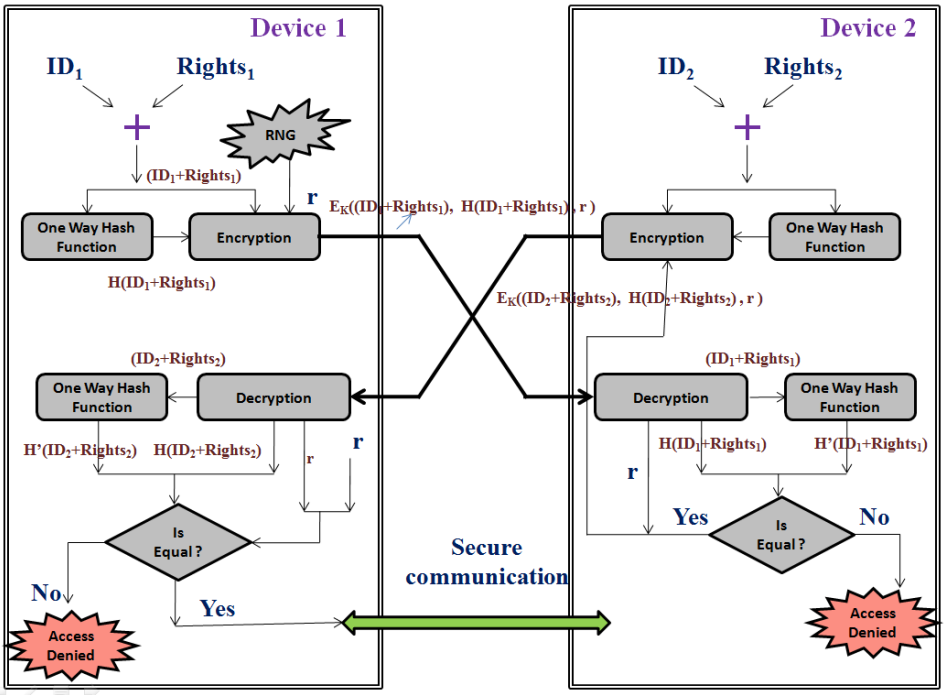

Fig. 3. Proposed Protocol

Table 1: Notations used in the protocol

Table 1. Notations used in the protocol	
Notation	**Description**
ID_1	Unique device 1 identifier
$Rights_1$	Access Rights of Device 1
r	Random number generated by Device 1
ID_2	Unique device 2 identifier
$Rights_2$	Access Rights of Device 2
H()	one-way hash function
E()	Encryption using AES-GCM
K	Secret Key
RNG	Random Number Generator

6 Evaluation

Here we evaluate the proposed protocol in terms of its mutual authentication process, resistance to attack and efficiency.

6.1 Mutual authentication

Only legitimate devices can generate and verify capabilities as it is based on secret key, one way hash function .As device identifiers and secret key are private and are being sent in encrypted form over communication channel, it is being prevented from forgery. AES-GCM provides encryption and authentication to capabilities and hence mutual authentication is successfully validated.

6.2 Replay attack resistance

This resist-attack model is secure for replay attacks, as every challenge and response is encrypted with the random number.

6.3 Computational, traffic and storage cost

The proposed protocol keeps computational costs low by requiring only four hashes to validate tampering. To guarantee that the device is legitimate, challenge and response protocol proposed here sends only three parameters. Thus the traffic cost between two devices is low. Device needs storage cost only for storing device identifier and secret key. We assume here that appropriate key management is being used.

7 Conclusions and Future work

Our protocol ensures authentication and access control by adding the capabilities as a second line of defense. It uses a secret value S, random number r, and hash function h() as both static and dynamic security guards. Only a authenticated devices can recognize the right values of these numbers and access control is achieved correctly. Novelty of this protocol is in use of AES –GCM to provide both authentication and encryption with efficient low cost implementation in resource constrained devices.
Future work will consist in the examination of advanced authentication protocols for mutual authentication. Other authentication methods (e.g. asymmetric techniques) should be analyzed for the suitability for resource constrained devices. The application range for IoT will be pushed further. To extend further, plan is to evaluate this protocol for different types of attacks and proposing generic and interoperable solution for these attacks.

References

1. Parikshit Mahalle, Sachin Babar, Neeli R. Prasad and Ramjee Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges" , The Third International Conference on Network Security and Applications (CNSA 2010), India, Springer Berlin Heidelberg, 2010, Volume 89, Part 2, 430-439.
2. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)" , The Third International Conference on Network Security and Applications (CNSA 2010), India, Springer Berlin Heidelberg, 2010, Volume 89, Part 2, 420-429.
3. Feldhofer, Martin, Dominikus, Sandra, Wolkerstorfer, Johannes, "Strong Authentication for RFID Systems Using the AES Algorithm" , Cryptographic Hardware and Embedded Systems - CHES 2004, Lecture Notes in Computer Science 2004, Springer Berlin-Heidelberg, 85-140, Volume 3156.
4. H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, “On the distribution and revocation of cryptographic keys in sensor networks,” IEEE Transactions on dependable and secure computing, vol. 2, no. 3, pp. 233–247, July/September 2005.
5. Das, M.L.; , "Two-factor user authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on , vol.8, no.3, pp.1086-1090, March 2009 doi: 10.1109/TWC.2008.080128
6. H. S. Kim and S. W. Lee, “Enhanced Novel Access Control Protocol over Wireless Sensor Networks,” IEEE Trans. on Consumer Electron., vol.55, no. 2, pp. 492-498, May 2009.
7. Jian Shen; Sangman Moh; Ilyong Chung; , "Comment: "Enhanced novel access control protocol over wireless sensor networks"," Consumer Electronics, IEEE Transactions on , vol.56, no.3, pp.2019-2021, Aug. 2010.
8. Wei, Chia-Hui; Hwang, Min-Shiang; Chin, Augustin Yeh-hao; , "A Mutual Authentication Protocol for RFID," IT Professional , vol.13, no.2, pp.20-24, March-April 2011.
9. R. Housley, S. Bellovin Request for Comments: 4107, “Guidelines for cryptographic key management”, http://www.ietf.org/rfc/rfc4107.txt
10. D.N. Duc et al., “Enhancing Security of EPC Global GEN-2 RFID Tag against Tractability and Cloning,” Proc. 2006 Symp. Cryptography and Information Security (SCIS 06), Springer, 2006, pp. 17–20.
11. L. Lamport, “Password Authentication with In-secure Communication,” Comm. ACM, Nov. 1981, pp. 770–772.
12. N.C. Wu et al., “Challenges to Global RFID Adoption,” Technovation, vol. 6, no. 12, 2007, pp. 257–278.
13. C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas, and T. Ylonen, “Simple Public Key Certificate,” draft-ietf-spki-cert-structure06.txt, July 1999.
14. C. M. Ellison, “SPKI Requirements,” RFC 2692, September 1999.
15. J. Hughes and E. Maler, “Security Assertion Markup Language (SAML) V2.0 Technical Overview,” sstc-saml-tech-overview-2.0-draft-08, September 2005.
16. Hori, Y.; Satoh, A.; Sakane, H.; Toda, K.; , "Bitstream encryption and authentication with AES-GCM in dynamically reconfigurable systems," Field Programmable Logic and Applications, 2008. FPL 2008. International Conference on , vol., no., pp.23-28, 8-10 Sept. 2008
17. Gang Zhou; Michalik, H.; Hinsenkamp, L.; , "Efficient and High-Throughput Implementations of AES-GCM on FPGAs," Field-Programmable Technology, 2007. ICFPT 2007. International Conference on , vol., no., pp.185-192, 12-14 Dec. 2007

18. Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation:Galois / Counter Mode (GCM) and GMAC." , U.S. National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
19. J. B. Dennis and E. C. van Horn. Programming Semantics for Multiprogrammed Computations. Communications of the Association for Computing Machinery, 9(3):143–155,Mar. 1966.
20. R. S. Fabry. “Capability-based addressing” Communications of the ACM, 17(7), 1974, p.403–412
21. Lampson, Butler W. (1971). "Protection". Proceedings of the 5th Princeton Conference on Information Sciences and Systems. pp. 437.
22. Li Gong, "A Secure Identity-Based Capability System," Security and Privacy, IEEE Symposium on, p. 56, 1989 IEEE Symposium on Security and Privacy, 1989