Open Access Library Journal
2021, Volume 8, e8061
ISSN Online: 2333-9721
ISSN Print: 2333-9705

GAP Universal One-Step Authentication Protocol

Xianghao Nan

CPK Laboratory, Beijing, China
Email: nanxianghao@bochtec.com

How to cite this paper: Nan, X.H. (2021) GAP Universal One-Step Authentication Protocol. *Open Access Library Journal*, **8**: e8061.
https://doi.org/10.4236/oalib.1108061

Received: October 10, 2021
Accepted: November 12, 2021
Published: November 15, 2021

Abstract

IoT authentication involves not only people, but also things, requiring a universal authentication method. The core authentication technology is the subject authenticity proof, but the traditional proof method based on model reasoning or based on third party trust transferring cannot solve. Therefore, a truth authentication logic based on evidence is created. The Truth Logic is realized by digital signature, and proves the entity authenticity by identifier authentication and ontology authentication, forming a new concept of identifier authentication and proves the event authenticity by acceptance authentication and adoption authentication, where the acceptance authentication is composed of subject and ontology authentication, and the adoption authentication is composed of object authentication, because the acceptance process is always carried out before the acceptance process, thus forming a new concept of "proof before event". Both entity authentication and event authentication are based on identifier authentication, so the GAP universal authentication protocol can be constructed to authenticate all entities in the Internet of Things and all events in the Internet of Events by single-step. As an example, GAP protocol gives the application on the network, a verifiable virtual network can be constituted by identifier authentication, proving traceability, preventing illegal access and DOS attack.

Subject Areas

Information and Communication: Security, Privacy, and Trust

Keywords

Authentication, Password, Entity, Event

1. Introduction

GAP universal authentication protocol creates evidence-based protocol, which is

different from the traditional model-based protocol. An authentication system must be the unification of proving system and verifying system. Digital signature is the core technology, and DSS provides digital signature protocol. However, recent researches have found that DSS digital signature standard only gives the definition of establishing trust relationship, but does not give the preconditions of digital signature. In the original paper, "GAP One-step Authentication Protocol" [1], under the influence of DSS, the given definition of digital signature, identifier and entity authentication was not accurate enough. In this paper, the original paper was revised, the definition of various protocols was redefined, the mathematical expression of protocol was consistent with DSS, and the application scenario was reclassified by entity.

The primary task of information security is authentication. Authentication is the basis of the follow-up work, the security without authentication will be rootless. Cyber space is composed of entities. All entities can be connected by their identities to form Internet of Things (IoT). The interaction of all entities causes events, and the links of events form Internet of Event (IoE). So IoT and IoE security can constitute Cyber security. IoT and IoE are virtual networks. In the era of the Internet of Things and Events, the authentication protocol not only meets the needs of communication and transaction, but also meets the needs of software operation. In the Internet of Things, entities are including address identities, phone identities, user identities, account identities, device identities, etc. Because the entity and event authentication is belong to the same kind of logical category, so the GAP authentication can be established.

2. Traditional Authentication Logic

Traditional authentication Logic includes Blelief Logic [2] based on model reasoning and PKI Certification Logic based on Trust transfer. Suppose an event: subject Alice sends object X to slave Bob, according to the belief logic, Bob proves by reasoning of readability, freshness and jurisdiction that Bob believes that Alice believes X. The logical relationship is that since Alice believes the authenticity of X, Bob also believes the authenticity of X. In terms of the proof of the authenticity of the object, it is obviously true in probability, but it cannot prove that the subject is real. Because there is no proof of subject authenticity in the inference.

The authentication logic of third party CA certification based on trust transfer is widely used on the Internet. The trust transfer theory holds that if different CAs recognize each other, the employees of different CAs enjoy the same trust. If this logic is true, it can lead a joke that a student graduated from A university can go to B university to get his diploma. Because the reflexivity of trust transfer is not established, it can only be a probabilistic inference. For example, the relationship between mother and son is very good, and the relationship between husband and wife is also very good, but it cannot be generally inferred that the relationship between mother-in-law and daughter-in-law must be very good.

Trust is a sociological term that cannot be used as evidence in the system of proof, just like concepts such as morality, recognition and consensus. Especially in the research of network warfare, password and trust transfer become the main means of network attack. The transfer of trust leads to the transfer of rights, which finally leads to the consequence that rights are taken over. As stated in the report of "Cyber Security, The crisis of Prioritization" [3] by PITAC, the principle of Cyber Security is "mutual suspicion", it is an epoch-making statement.

3. Evidence-Based Authentication Logic

The authentication logic based on objective evidence is called Truth Logic. The Truth Logic can only be implemented in an identifier-based public key system, where public and private keys are directly derived from identities to ensure the unity of the key and identities. For example, under the CPK [4] system:

$$\text{Entity identity}(\text{Alice}) \rightarrow \begin{cases} \sigma\left(r_{i,j}\right) \rightarrow \text{private key } sk_{[\text{Alice}]} \\ \sigma\left(R_{i,j}\right) \rightarrow \text{public key } PK_{[\text{Alice}]} \end{cases}$$

where σ is combined transformation, $(r_{i,j})$ is private matrix kept secret in KMC to generate private-key, $(R_{i,j})$ is public matrix, published for the calculation by relying party and signed by KMC to determine its scope. CPK can be realized on existiing ECC, DLP, RSA and BLP.

Only in the identifier-based public key system, digital signature standard DSS can prove the authenticity of the identifier claimed by the subject and have the real digital signature function. Otherwise, it can only be used to establish trust relationship and cannot be used as evidence.

The Internet of Things is made up of entities, and each Entity has a unique identifier that distinguishes it from other entities. Entities include people and things, and things include intelligent and unintelligent. If the authenticity of each entity can be proven, then the authenticity of all entities in the Internet of Things can be proven. Interactions between entities trigger events, and if the authenticity of each event can be verified, then the authenticity of all events in the Internet can also be verified. Since cyberspace is made up of entities and events, if the authenticity of all entities and events can be proved, then of course all authentication problems in cyberspace can be solved.

Evidence-based authentication protocols fall into two categories: entity authentication and event authentication.

3.1. Entity Authentication

Entities consist of identifier and ontology:

$$\text{Entity} = \text{identifier} + \text{ontology}$$

Entity authentication protocol consists of identifier authentication and ontology authentication:

$$\text{Entity auth} = \{\text{identifier auth, ontology auth}\}$$

Identifier authentication is the product of the inverse of a random number k and the private key (sk_{Alice}) of claimed identifier, the signature code is (c, s):

$$kG = (x, y) \to c, \quad s = k^{-1} sk_{\text{Alice}} \bmod n$$

where, G is the generator of ECC, (x, y) is a point, $kG = (x, y) \to c$ is any one-way function, such as $(x + y) \to c$. s is sign code, c is checking code, and n is te order of additive group.

Identifier verification is the product of the inverse of the sign code and the public key (PK_{Alice}):

$$s^{-1} PK_{\text{Alice}} = kG = (x, y) \to c'$$

Ontology authentication is the product of the sum of ontology h and private key (sk_{Alice}) of the inverse of random number k, and the signature is (s, c):

$$kG = (x, y) \to c, \quad s = k^{-1} (h + sk_{\text{Alice}}) \bmod n$$

Ontology verification is the product of the inverse of the sign code and the sum of the public key (PK_{Alice}) and h timed G:

$$s^{-1} (hG + PK_{\text{Alice}}) = kG = (x, y) \to c'$$

Ontology can be replaced by ontology features.

3.2. Event Authentication

The interaction of entities causes events, and the interacting entities are divided into subject and slave. Events exist in the form of process, which can be divided into accept process and adopt process:

Event = (accept process, adopt process)

Therefore, event authentication consists of accept authentication and accept authentication:

Event Auth = (accept auth, accept auth)

1) Accept Authentication

Accept authentication has three forms, first is the subject authentication the second is the entity authentication, the third is the slave authentication:

Accept auth = (subject auth, entity auth, slave auth)

Subject authentication is the identifier authentication of the subject, whose signature and verification are as follows:

$$kG = (x, y) \to c, \quad s = k^{-1} sk_{\text{Alice}} \bmod n$$

$$s^{-1} PK_{\text{Alice}} = kG = (x, y) \to c'$$

Entity authentication is the signature and verification of ontology features by identifier of subject:

$$kG = (x, y) \to c, \quad s = k^{-1} (h + sk_{\text{Alice}}) \bmod n$$

$$s^{-1} (hG + PK_{\text{Alice}}) = kG = (x, y) \to c'$$

Slave authentication is the signature and verification of subject identifier (Alice) to slave identifier (Bob):

$$kG = (x, y) \to c, \quad s = k^{-1}(\text{Bob} + sk_{\text{Alice}}) \bmod n$$

$$s^{-1}(\text{Bob} * G + PK_{\text{Alice}}) = kG = (x, y) \to c'$$

2) Adopt Authentication

Adopt authentication is the authentication of subject to object:

$$\text{Adopt auth} = (\text{object auth})$$

Object identification is the signature and verification of subject to object:

$$kG = (x, y) \to c, \quad s = k^{-1}(\text{Object} + sk_{\text{Alice}}) \bmod n$$

$$s^{-1}(\text{Object} * G + PK_{\text{Alice}}) = kG = (x, y) \to c'$$

In event authentication, accept authentication always takes place before the adopt process, which is called proof-before-event and the adopt authentication is called proof-after-event.

4. Application of GAP Protocol

GAP authentication protocol is actually a signature protocol, which can be used for identifier authentication, entity authentication, and the entity authentication is further divided into subject authentication, slave authentication and object authentication. The digital signature used by GAP protocol has the functions of authenticity proof, traceability proof and attribute proof. It can construct digital equivalent currency, digital seal, anti-counterfeiting label, software trademark, etc., therefore, it is needed to choose an appropriate authentication function according to the requirement.

4.1. Application of Subject Authentication

"Password certification" is a classic example of traditional trust-based subject authentication. The logic of authentication is symmetry, that is: "what you have, I have; what you know, I know". Password has been the simplest and most effective means of access control. The US DoD has launched a project of "Zero trust Architecture" [5] to achieve a strong password with multi-factor authentication. it illustrates the importance of password, however, it also shows that the US DoD has not solved the key problem of information security, and can only resort to image logic, forgetting PITAC's epoch-making security principle of "mutual suspicion" in 2005, and still not free from the restraint of trust logic. The concept of "zero trust Architecture" has also begun to ferment in China, claiming that "to achieve true trust from zero trust". The debate to construct a "trusting system" or an "proving system" looks set to continue. The image logic of stopgap medicine is not unable to solve the problems, but cannot solve the fundamental problem.

The subject authentication of GAP protocol is carried out by identifier authen-

tication technology. Identifier authentication directly proves the authenticity of the identifier claimed by the subject, so the identifier certificate code can be used as a password on the network and as a signature on paper, but the certificate is needed to be typed out with two-dimensional code.

How the identifier authentication of GAP protocol replaces the traditional password is described as follows:

Subject Alice first issues the signature code s of the identifier as a password. The private key sk_{Alice} is corresponding to the identifier claimed by the subject. For example, the identifier will be the phone number when calling; and will be the account name when paying, etc.

First, subject Alice selects a random number k to calculate the password:

$$kG = (x, y) \to c$$

$$s = k^{-1} sk_{\text{Alice}}$$

To package s and c, take (s, c) as Alice's password.

Suppose Bob receives Alice's password (s, c).

Bob first computes Alice's public key and computes the checking code with Alice's password s:

$$s^{-1} PK_{\text{Alice}} = kG = (x, y) \to c'$$

Under the action of random number k, password code s changes once, so there is no need for encryption protection; Password checking is carried out by operation, without comparison, the verifier does not need to retain the other party's password;

From password issuing to authentication, no private information is divulged.

The traditional password is to meet the need of "login", but the login mechanism is the bane of the right takeover caused by trust transfer, and is not a security mechanism. GAP protocol is of an on-spot authentication, namely "one thing one proof" to put an end to the trust transfer. The password has been replaced by identifier authentication and there is no need to exist.

4.2. Application of Slave Authentication

Communication authentication consist of sender and receiver. The sender is the subject of the event, and the receiver is the slave of the event. The identifier claimed by the subject in the network is the IP address. The private-key used is corresponded to the address. Suppose that the subject is Alice and the slave is Bob, then the slave authenticity is the signature and verification of the subject to the slave:

$$kG = (x, y) \to c, \quad s = k^{-1} (\text{Bob} + sk_{\text{Alice}}) \bmod n$$

$$s^{-1} (\text{Bob} * G + PK_{\text{Alice}}) = kG = (x, y) \to c'$$

The subject authenticity proof has been included in the slave authentication , so there is no need to prove it.

Subject and slave authentication can be carried out before object event (data transmission) occurs, so it is the most effective way to prevent illegal access and DOS attack.

4.3. Application of Object Authentication

The payment event consists of the payer, payee and amount, where the payer is subject, the payee is the slave and the amount is object. The identifier claimed by the subject in the transaction is the account name or account number. The private-key used is corresponded to the account name or account number.

Suppose the subject account name is Alice, the slave account name is Bob, and the object is amount, then:

The authenticity proof of slave is the signature and verification of the subject to the slave:

$$kG = (x, y) \to c_1, \quad s = k^{-1}\left(\text{Bob} + sk_{\text{Alice}}\right) \bmod n$$

$$s^{-1}\left(\text{Bob} * G + PK_{\text{Alice}}\right) = kG = (x, y) \to c_1'$$

The authenticity proof of object is the signature and verification of subject to object:

$$kG = (x, y) \to c_2, \quad s = k^{-1}\left(\text{amount} + sk_{\text{Alice}}\right) \bmod n$$

$$s^{-1}\left(\text{amount} * G + PK_{\text{Alice}}\right) = kG = (x, y) \to c_2'$$

In cases where the accept process and the adopt process are separated, the authenticity proof of slave and object can be separated. If there is no need for separate authentication, the slave and object can be combined into a composite object, and the subject can sign to and verify the composite object:

$$\text{data} = \text{Slave} \,//\, \text{amount}$$

$$kG = (x, y) \to c, \quad s = k^{-1}\left(\text{data} + sk_{\text{Alice}}\right) \bmod n$$

$$s^{-1}\left(\text{data} * G + PK_{\text{Alice}}\right) = kG = (x, y) \to c'$$

The composite object associates the amount with the payee, and it has no meaning to be taken by a third party, so it is not afraid of loss. If the account is settled with this kind of bill, then the account will be without fear of loss or theft.

Objects often require privacy, when the whole bill is changed into a package:

$$\text{Dada}_1 = \left(\text{subject} \,//\, \text{slave} \,//\, \text{object} \,//\, \text{signature}\right)$$

Then data1 can be encrypted: Alice selects random number r, calculates data encrypting key: rG = key, and encrypts object data_1 with with the symmetric key:

$$E_{\text{key}}\left(\text{data}_1\right) = \text{code}$$

Alice calculates $r * PK_{\text{Bob}} = \beta$ with Bob's public-key PK_{Bob} and sends (code, β) to Bob.

Bob receives the cipher-text, he uses his private-key sk_{Bob} to decipher it first:

$$sk_{\text{Bob}}^{-1}\beta = rG = \text{key}$$

$$D_{\text{key}}(\text{code}) = \text{data}_1$$

where, E and D are symmetric encryption and decryption functions.

5. Summary

In this paper, a one-step universal authentication protocol was used to build a verifiable virtual network to solve entity authentication of IoT and event authentication of IoE. The GAP protocol completes the authentication function by only one step, to achieve on-the-spot proof, put an end to the transfer of trust. GAP protocol has universality, can provide traceability, and attribute proof. If applied to the network, its identifier authentication can replace the traditional password certification and prevent illegal access and DOS attacks, applied to payment, a digital currency can be designed that is not afraid of losing, applied to the kernel, malicious software intrusion and execution can be prevented without afraid of back door.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Nan, X.H. (2020) GAP One-Step Authentication Prtocol. *Communications Technology*, **53**, 3030-3033.

[2] Brurros, M., Abadi, M. and Needham, R. (1989) A Logic of Authentication. *ACM Transactions on Computer Systems*, November 1989, 1-13. https://doi.org/10.1145/74850.74852

[3] (2005) President's Information Technology Advisory Committee. Cyber Security. A Crisis of Prioritization.

[4] Nan, X.H. and Chen, Z. (2003) A Profile to Network Security. Defense Industry Publishing House, Beijing.

[5] Department of Defense (DOD) (2021) Zero Trust Reference Architecture, Version 1.0.