https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

Translated English of Chinese Standard: GB/T39205-2020

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 39205-2020

Information security technology - Light-weight authentication and access control mechanism

信息安全技术 轻量级鉴别与访问控制机制

Issued on: October 11, 2020 **Implemented on: May 01, 2021**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

Table of Contents

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

Information security technology - Light-weight authentication and access control mechanism

1 Scope

This Standard specifies the light-weight authentication mechanism and the access control mechanism.

This Standard applies to the design, development and application of authentication and access control mechanisms in resource-constrained application scenarios, such as wireless sensor network, radio frequency identification, and near field communication.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 15629.3-2014, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

GB/T 25069, Information security technology - Glossary

GB/T 32905, Information security techniques - SM3 cryptographic hash algorithm

GB/T 32907, Information security technology - SM4 block cipher algorithm

ISO/IEC 29180:2012, Information technology - Telecommunications and information exchange between systems - Security framework for ubiquitous sensor networks

3 Terms and definitions

Terms and definitions determined by GB/T 25069 and the following ones are applicable to this document.

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

CT: Cryptographic Text

DAE: Destination Access Entity

ET: Encrypted Text

HMAC: Hash Based Message Authentication Code

KD: Key Derivation

MAC: Message Authentication Code

MEK: Message Encryption Key

MIC: Message Integrality Check

MIK: Message Integrality Key

PSK: Pre-Shared Key

SK: Session Key

VP: Valid Period

5 Light-weight authentication mechanism

5.1 Overview

The light-weight authentication mechanism reduces the complexity of calculation and communication in the authentication process while realizing the identity authenticity confirmation between entities. Compared with the usual mechanism, the light-weight authentication mechanism has the following measurement angles:

a) Less occupancy of computing resources;

b) Less interactive messages;

c) Shorter time-consuming;

d) Less required storage space.

5.2 Authentication mechanism based on exclusive OR operation

The authentication mechanism, which is based on the exclusive OR operation, realizes the confirmation of identity authenticity between entity A and entity B through simple exclusive OR and shift operations. The authentication process is shown in Figure 1.

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

Figure 2 -- Schematic diagram of message interaction of the authentication mechanism that is based on the cryptographic hash algorithm

Before authentication, entity A shall have identity information ID_A; entity B shall have identity information ID_B; entity A and entity B shall have pre-shared key PSK; the use of pre-shared key PSK shall meet the needs of specific scenarios; the length of the random number shall be consistent with the PSK length. The authentication process is as follows:

a) Entity A generates a random number N_A, and sends an authentication request message that contains N_A and ID_A to entity B.

b) After entity B receives the authentication request message from entity A, it generates a random number N_B, and uses the pre-shared key PSK with entity A in the key list to calculate $MIK\|SK=KD\text{-}HMAC(PSK,ID_A\|ID_B\|N_A\|N_B)$ according to ID_A, ID_B, N_A, and N_B, where ID_A and ID_B are respectively the identities of entity A and entity B; MIK is the message integrity key between entity A and entity B; SK is the session key between entity A and entity B. Then, entity B uses MIK to calculate the message authentication code $MAC_1=HMAC\ (MIK,\ N_A\|N_B)$, and constructs an authentication response message $N_A\|N_B\|ID_B\|MAC_1$ and sends it to entity A.

c) After entity A receives the authentication response message from entity B, it first checks whether the random number N_A in the authentication response message is consistent with the random number N_A that is sent to entity B in step a). If they are inconsistent, entity A fails to authenticate entity B; if they are consistent, entity A calculates $MIK\|SK=KD\text{-}HMAC(PSK,ID_A\|ID_B\|N_A\|N_B)$, and uses MIK to calculate the message authentication code $MAC_2=HMAC(MIK,N_A\|N_B)$. If $MAC_2\neq MAC_1$, entity A fails to authenticate entity B; if $MAC_2=MAC_1$, entity A saves SK as the session key with entity B, and calculates $MAC_3=HMAC(MIK,N_B)$, to construct an authentication confirmation message $N_B\|MAC_3$, and sends it to entity B. If entity A and entity B use this mechanism and do not contain a key confirmation message, after entity A sends the authentication confirmation message for a period of time or after it correctly decrypts the message that is sent by entity B using the session key, entity A successfully identifies entity B, and entity A enables the session key; if entity A and entity B use this mechanism and contain a key confirmation message, follow step e) to perform subsequent operations.

d) After entity B receives the authentication confirmation message from entity A, it checks whether the random number N_B in the authentication confirmation message is consistent with the random number N_B that is sent to entity A in step b). If they are inconsistent, entity B fails to authenticate entity A; if they are consistent, entity B calculates the

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

the length of the random number shall be consistent with the PSK length. The authentication process is as follows:

a) Entity A generates a random number N_A, and sends an authentication request message that contains N_A to entity B;

b) After entity B receives the authentication request message from entity A, it generates random numbers N_{B1} and N_{B2}, calculates $CT_1 \| MIC_1 = E(PSK, N_A \| N_{B1} \| N_{B2})$, and sends an authentication response message that contains $N_A \| CT_1 \| MIC_1$ to entity A;

c) After entity A receives the authentication response message from entity B, it first determines whether the N_A in the message is consistent with the N_A that is sent to entity B in step a). If they are inconsistent, entity A fails to authenticate entity B; if they are consistent, entity A uses PSK to decrypt and verify $CT_1 \| MIC_1$. If the verification of MIC_1 fails, entity A fails to authenticate entity B; if the verification of MIC_1 passes, it further verifies whether the decrypted N_A is consistent with the N_A that is sent to entity B in step a). If they are inconsistent, entity A fails to authenticate entity B; if they are consistent, entity A authenticates entity B successfully; entity A uses the decrypted NB_2 as the session key with entity B, and calculates $CT_2 \| MIC_2 = E(N_{B2}, N_{B1})$, and sends an authentication response confirmation message to entity B, which includes the field $N_{B1} \| CT_2 \| MIC_2$;

d) After entity B receives the authentication response confirmation message from entity A, it first determines whether the N_{B1} in the message is consistent with the N_{B1} that is sent to entity A in step b). If they are inconsistent, entity B fails to authenticate entity A; if they are consistent, entity B uses N_{B2} to decrypt and verify $CT_2 \| MIC_2$. If the MIC_2 verification fails, entity B fails to authenticate entity A; if the MIC_2 verification passes, further verify whether the decrypted N_{B1} is consistent with the N_{B1} that is sent to entity A in step b). If they are inconsistent, entity B fails to authenticate entity A; if they are consistent, entity B authenticates entity A successfully, and entity B uses N_{B2} as the session key with entity A.

Note: E is a block encryption algorithm; CT‖MIC=E(KEY,S) means using KEY to encrypt S and calculating the integrity check code, where CT stands for cryptographic text, MIC stands for integrity check code; the separation of CT and MIC depends on the specific application. In some modes, it is necessary to first derive the message integrity check key and the message encryption key according to the KEY, and then respectively use the two keys to calculate the integrity check code and the cryptographic text. In the decryption verification, the sequence of verifying the integrity check code and decrypting may be different according to the different used modes.

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

a) Before the User sends an access request to the DAE in the network, it first sends an authentication request message to the DAE, which mainly contains the random number N_1 that is generated by the User;

b) After DAE receives the authentication request message from the User, it generates a random number N_2, and uses the shared key $K_{ACr,\ DAE}$ with ACr to calculate $ET_1=E(K_{ACr,DAE},N_1)$; send $N_1\|N_2\|ET_1$ as authentication response message to the User, where E is the symmetric encryption algorithm;

c) After the User receives the authentication response message from DAE, it first judges whether the random number N_1 in the message is the random number that is selected by the User; if it is not, discard the message directly; if it is, use the shared key $K_{ACr,\ User}$ with ACr to calculate $ET_2=E(K_{ACr,User},N_1)$; calculate the message authentication code $MIC_1=HMAC(K_{ACr,User},N_1\|ID_{DAE}\|ET_1\|ET_2)$; construct an entity authentication request message $N_1\|ID_{DAE}\|ET_1\|ET_2\|MIC_1$; send it to ACr, where ID_{DAE} is the identity of DAE;

d) After ACr receives the User's entity authentication request message, it first judges the integrity of the message according to MIC_1. If the verification fails, discard the message; if the verification passes, use the shared key $K_{ACr,\ DAE}$ with DAE to decrypt ET_1. If the decrypted N_1 is not equal to the N_1 that is sent by the User in step c), ACr constructs an entity authentication response message $N_1\|ID_{DAE}\|RES(DAE)\ \|MIC_2$ and sends it to the User, where $MIC_2=HMAC(K_{ACr,User},N_1\|\ ID_{DAE}\|RES(DAE))$, Res(DAE)=Failure indicates that ACr fails to identify DAE; if the decrypted N_1 is equal to the N_1 that is sent by the User in step c), ACr uses the shared key $K_{ACr,\ User}$ with the User to decrypt ET_2. If the decrypted N_1 is not equal to the N_1 that is sent by the User in step c), the authentication is terminated; if the decrypted N_1 is equal to the N_1 that is sent by the User in step c), ACr generates the session key $K_{DAE,\ User}$ between the User and DAE, and queries ACL according to the User's identity; obtain the User's access control information ACL_{User}, together with the User's access period T_V; use $K_{ACr,\ DAE}$ to calculate $ET_3=E(K_{ACr,DAE},ID_{User}\|K_{DAE,User}\|T_V\|ACL_{User})$; use $K_{ACr,User}$ to calculate $ET_4=E(K_{ACr,User},K_{DAE,User})$; calculate $MIC_2=HMAC(K_{ACr,User},N_1\|ID_{DAE}\|RES(DAE)\|ET_3\|ET_4)$; construct entity authentication response message $N_1\|ID_{DAE}\|RES(DAE)\ \|ET_3\|ET_4\|MIC_2$; sent it to User, where RES(DAE)=True means that ACr successfully authenticates DAE;

e) After the User receives the entity authentication response message from ACr, it first judges whether the random number N_1 is the random number that is selected by the User; if it is not, discard the message; if it is, judge the integrity of the message according to MIC_2; if the verification fails,

https://www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~9 minutes.

U_ID in the ACL list to all entities in the network in a secure manner; the entity saves the ACL_{U_ID} before the user's VP expires; if the user is not registered, ACr discards the user's identity certification request message.

Note: The secure manner refers to protecting the confidentiality and integrity of the message by means of encrypted transmission. The pre-shared key can be used between entities to realize encrypted transmission; the specific implementation method is not limited, the same below.

b) Before the user accesses the destination access entity, it first sends an identity authentication request message to the network. At this time, all entities in the user's single-hop communication area in the network constitute a temporary access control gateway to authenticate the user. The process is as follows:

1) After the temporary access control gateway receives the user's identity authentication request message, the entity in the temporary access control gateway first determines whether the user's ACL_{U_ID} information is stored. If this information is stored, it indicates that the user is within the valid period. The entity performs an authentication of the user according to the user AI in the ACL_{U_ID}. If the entity authenticates the user authentication successfully, it casts a PASS vote and broadcasts the PASS vote. If the number of PASS votes that are received by the entity in the temporary access control gateway is larger than or equal to the threshold value P, it indicates that the user authentication is successful. If the PASS votes that are received by the entity in the gateway is less than the threshold value P, it indicates that the authentication fails and the user's access is terminated; the threshold value P is defined by the network owner; it can be a fixed value of the number of PASS votes, or a proportional value of PASS votes;

2) After the successful authentication, during the process when the user accesses the network, the entity in the current temporary access control gateway shall calculate the location where the user shall reach according to the user's movement direction, movement speed, etc., and constructs the next temporary access control gateway through all entities in all single-hop areas with the location, where the measured users will reach, as the center. The entity in the current temporary access control gateway sends the successful user authentication message to the entity in the next temporary access control gateway after time t; the next temporary access control gateway determines whether the user is successfully authenticated according to whether the number of received successful user authentication messages reaches the threshold P. If the user is still within the valid period VP, and the

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------