INTELLIGENT VEHICLE NETWORKING CROSS DOMAIN AUTHENTICATION METHOD AND SYSTEM BASED ON MASSIVE IDENTIFIER PARSING

Field of the Invention

The present invention relates to the field of intelligent vehicle networking cross domain authentication technology, specifically an intelligent vehicle networking cross domain authentication method and system based on massive identifier parsing.

Background to the Invention

In order to accelerate the construction of a strong transportation country, a strong technology country, a strong network country, and a digital China, and to build a cross disciplinary collaborative and open intelligent connected vehicle technology system, in July 2023, the Ministry of Industry and Information Technology and the National Standardization Management Committee jointly revised and formed the "Guidelines for the Construction of National Connected Vehicle Industry Standard System (Intelligent Connected Vehicles) (2023 Edition)". The formulation of this document not only adapts to the new trends, characteristics, and demands of the development of intelligent connected vehicles in China, but also accelerates the pace of building a new standard system for intelligent connected vehicles in China. On October 8, 2023, the China Association of Automobile Manufacturers predicted that the sales of new energy passenger vehicles in China would be 8.5 million units in 2023, with a narrow definition of passenger vehicle sales of 23.5 million units. Therefore, how to ensure the communication security, authentication, road traffic conditions, digital identity identification and other issues of massive vehicles during driving has become a key problem that urgently needs to be

solved in the Internet of Vehicles;

In order to meet the digital identity identification, secure communication and identity authentication, data transmission and other functions of massive intelligent vehicles in high-speed driving, high bandwidth and low latency are required to meet this demand. Therefore, it is necessary to build a new V2X management system that enables vehicles, people, roadside units, and cloud facilities in the system to authenticate and exchange information with each other, regardless of which security field they come from, to achieve intelligent management of traffic and achieve the perceptual collaborative development of "vehicle-road-human-cloud". As a way to break the information barrier and realize data exchange, the current identification resolution technology has been highly valued by the Internet of Vehicles and the industrial Internet. However, the existing cross domain authentication methods of the intelligent Internet of Vehicles have the following shortcomings:

1. Cross domain authentication is costly;

2. Does not meet the requirements of large-scale key management;

3. Low efficiency in verifying the authenticity of identification;

4. The authentication speed of the identification source is slow.

Statement of Invention

The purpose of this section is to outline some aspects of the embodiments of the present invention and briefly introduce some preferred embodiments. Simplification or omission may be made in this section, as well as in the abstract and title of the present application, to avoid blurring the purpose of this section, abstract, and title, and such simplification or

omission cannot be used to limit the scope of the present invention.

Therefore, the purpose of the present invention is to provide an intelligent vehicle networking cross domain authentication method and system based on massive identifier parsing. Based on the autonomous and controllable identifier authentication combination public key CPK technology, an intelligent vehicle networking network security guarantee system is constructed based on security technologies such as access control, authorization management, data encryption transmission, and trusted computing. Combined with machine learning algorithms, network data is analyzed for security, forming threat situation, threat intelligence, security events, security situation, attack events, risk assessment and other information, providing management departments with a global security situation awareness and self protection ability evaluation means, comprehensively improving the security level and protection ability of the intelligent vehicle networking network.

To solve the above technical problems, according to one aspect of the present invention, the present invention provides the following technical solution:

An intelligent vehicle networking cross domain authentication method based on massive identifier parsing, characterized by the following steps:

S1、 system initialization, assigning composite identifiers to all entities, and deploying the global CPK public key matrix $SM \perp \{n \times m\} S$ through the cloud, with edge nodes preloading the hotspot domain matrix;

S2、 terminal preparation, input electrical signals on the device, HSM relies on the identification specification of S1, activates PUF to generate device fingerprints, loads CPK private key components based on S1's preset data, constructs dynamic credentials, and describes the initialized T-Box;

S3、domain authentication request, input the credential generated in S2, and send it to the edge node through TSN channel, the edge node verifies the validity of the timestamp and queries the bendingCPK matrix deployed in S1 to verify the signature, and outputs a temporary Token;

S4、 cross domain query, input the taeget domain in S3, the edge node requests the target domain parameters from the cross domain center, and returns the encrypted public key matrix fragment based on the TLS channel established in S1, outputting the target domain authentication parameters;

S5、 bidirectional authentication, input the target domain parameters obtained in S4, the server relies on the Token from S2 to send a challenge, and the client uses the private key HSM loaded in S2 to calculate the response and output a signed response packet;

S6、 verification decision, input the response packet of S5, rely on the public key matrix of S4, and output the authentication structure based on the real-time access control policy of the domain policy in S4;

S7、 secure channel establishment, input the successful result of S6, derive the session key based on the nonce value of S5, and use the algorithm suite preset in S1 to negotiate transmission parameters and output an encrypted communication channel.

As a preferred solution for the intelligent vehicle networking cross domain authentication method based on massive identifier parsing according to the present invention, wherein: the composite identifier in step S1 consists of the following parts:

Static part: equipment manufacturer code + international mobile device identification;

Dynamic part: random sequence generated based on PUF physical unclonable function + timestamp allocated by edge nodes;

The composite identifier is bound to the coordinates in the CPK public key matrix through a hash chain, forming a verifiable topological relationship.

As a preferred solution for the intelligent vehicle networking cross domain authentication method based on massive identifier parsing according to the present invention, wherein: the domain authentication request in S3 includes a zero knowledge proof process of dynamic credentials as follows:

When the client sends a Credential through the TSN channel, attach the ciphertext of the PUF response value generated by HSM;

After verifying the timestamp of the edge node, the hash commitment of the Credential is calculated based on the hotspot domain matrix and homomorphic compared with the PUF response value;

If the verification is successful, a Token carrying the target domain permission declaration will be issued, otherwise, the composite identifier reconstruction process of S1 will be triggered.

As a preferred solution for the intelligent vehicle networking cross domain authentication method based on massive identifier parsing according to the present invention, wherein: the cross domain query in S4 adopts a hierarchical key distribution mechanism:

Maintain a second level CPK matrix across domain centers, and encapsulate its fragments using the SM9 identification public key of the target domain edge node when encrypted and transmitted through TLS channels;

After receiving the encrypted fragment, the edge node decrypts and verifies the fragment signature through local HSM, and synchronously updates it to the cache area of the hotspot domain matrix;

The target domain parameters include matrix coordinate offset and validity period, which are used for real-time policy verification in S6.

An intelligent vehicle networking cross domain authentication system based on massive identifier parsing, comprising:

Central processing module, as the nervous center of the system, performs maintenance and updates of the global CPK public key matrix, and handles routing and arbitration of cross domain authentication requests, as well as real-time dynamic load balancing;

Edge authentication proxy module, connected to the central processing unit, is used to perform caching of hotspot domain public key evidence and perform localized identification parsing to achieve traffic classification;

Security control module, connected to the central processing unit and is used to generate and protect CPK private key components, perform high-speed password transport, and provide PUF fingerprint extraction services;

Protection module, connected to the central processing unit and is used to analyze and authenticate traffic patterns, block malicious authentication requests, and generate security event logs;

Data management module, connected to the central processing unit, is used to execute the mapping relationship between storage device identification and public key, and supports multi-dimensional queries, providing version based data snapshots;

Blockchain certificate storage module, connected to the central processing unit, is used to record key authentication events, provide certificate chain completion services, and achieve cross domain consensus verification;

Communication transmission module, connected to the central processing unit, used as a

data transmission channel to achieve data information transmission between modules;

Message bus module, connected to the central processing unit, is used to perform priority scheduling of authentication messages, ensure deterministic transmission of control instructions, and achieve loosely coupled communication between modules.

Compared with existing technologies, the present invention has the following beneficial effects:

Based on the autonomous and controllable identifier authentication combination public key CPK technology, an intelligent vehicle networking network security guarantee system is constructed based on security technologies such as access control, authorization management, data encryption transmission, and trusted computing. Combined with machine learning algorithms, network data is analyzed for security, forming threat situation, threat intelligence, security events, security situation, attack events, risk assessment and other information, providing management departments with a global security situation awareness and self protection ability evaluation means, comprehensively improving the security level and protection ability of the intelligent vehicle networking network.

Brief Description of the Drawings

In order to more clearly illustrate the technical solution of the embodiments of the present invention, the present invention will be described in detail below in conjunction with the accompanying drawings and detailed embodiments. It is obvious that the accompanying drawings described below are only some embodiments of the present invention. For those skilled in the art, other drawings can be obtained based on these drawings without creative labor. Among them:

FIG. 1 is a flowchart of the cross domain authentication method for intelligent vehicle

networking of the present invention;

FIG. 2 is a schematic diagram of calculating keys based on MAC according to the present invention;

FIG. 3 is a detailed parameter schematic diagram of the central network connection of the present invention.

Detailed Description

In order to make the above objectives, features, and advantages of the present invention more obvious and understandable, the specific embodiments of the present invention will be described in detail below in conjunction with the accompanying drawings.

In the following description, many specific details are elaborated to facilitate a full understanding of the present invention. However, the present invention can also be implemented in other ways different from those described herein. Those skilled in the art can make similar generalizations without violating the connotation of the present invention. Therefore, the present invention is not limited by the specific embodiments disclosed below.

Secondly, the present invention will be described in detail in conjunction with the schematic diagram. When describing the embodiments of the present invention, for ease of explanation, the cross-sectional view representing the device structure will not be enlarged to a general scale, and the schematic diagram is only an example, which should not limit the scope of protection of the present invention. In addition, in actual production, the three-dimensional spatial dimensions of length, width, and depth should be included.

In order to clarify the purpose, technical solution, and advantages of the present invention,

the embodiments of the present invention will be further described in detail with reference to the accompanying drawings.

The present invention provides a intelligent vehicle networking cross domain authentication method based on massive identifier parsing. Please refer to Figures 1-3, which includes the following steps:

S1、 system initialization, assigning composite identifiers to all entities, and deploying the global CPK public key matrix $SM \perp \{n \times m\}S$ through the cloud, with edge nodes preloading the hotspot domain matrix;

S2、 terminal preparation, input electrical signals on the device, HSM relies on the identification specification of S1, activates PUF to generate device fingerprints, loads CPK private key components based on S1's preset data, constructs dynamic credentials, and describes the initialized T-Box;

S3、domain authentication request, input the credential generated in S2, and send it to the edge node through TSN channel, the edge node verifies the validity of the timestamp and queries the bendingCPK matrix deployed in S1 to verify the signature, and outputs a temporary Token;

S4、 cross domain query, input the taeget domain in S3, the edge node requests the target domain parameters from the cross domain center, and returns the encrypted public key matrix fragment based on the TLS channel established in S1, outputting the target domain authentication parameters;

S5、 bidirectional authentication, input the target domain parameters obtained in S4, the server relies on the Token from S2 to send a challenge, and the client uses the private key HSM loaded in S2 to calculate the response and output a signed response packet;

S6、 verification decision, input the response packet of S5, rely on the public key matrix of S4, and output the authentication structure based on the real-time access control policy of the domain policy in S4;

S7、 secure channel establishment, input the successful result of S6, derive the session key based on the nonce value of S5, and use the algorithm suite preset in S1 to negotiate transmission parameters and output an encrypted communication channel.

An intelligent vehicle networking cross domain authentication system based on massive identifier parsing, comprising:

Central processing module, as the nervous center of the system, performs maintenance and updates of the global CPK public key matrix, and handles routing and arbitration of cross domain authentication requests, as well as real-time dynamic load balancing;

Edge authentication proxy module, connected to the central processing unit, is used to perform caching of hotspot domain public key evidence and perform localized identification parsing to achieve traffic classification;

Security control module, connected to the central processing unit and is used to generate and protect CPK private key components, perform high-speed password transport, and provide PUF fingerprint extraction services;

Protection module, connected to the central processing unit and is used to analyze and authenticate traffic patterns, block malicious authentication requests, and generate security event logs;

Data management module, connected to the central processing unit, is used to execute the mapping relationship between storage device identification and public key, and supports multi-dimensional queries, providing version based data snapshots;

Blockchain certificate storage module, connected to the central processing unit, is used to record key authentication events, provide certificate chain completion services, and achieve cross domain consensus verification;

Communication transmission module, connected to the central processing unit, used as a data transmission channel to achieve data information transmission between modules;

Message bus module, connected to the central processing unit, is used to perform priority scheduling of authentication messages, ensure deterministic transmission of control instructions, and achieve loosely coupled communication between modules.

Identity authentication process design:

Unidirectional identity authentication generally refers to the authentication of the client by the server, mainly based on the authentication and authorization of the client's identity. The main process is that the client first initiates an authentication request to the server. After receiving the request, the server will initiate an authentication challenge to the client, and the client must send back the correct response to confirm that they are an authorized administrator. After the client's authentication is approved, the server responds to the request.

Bidirectional identity authentication adds authentication from the client to the server on the basis of single authentication, mainly to prevent server forgery and achieve the goal of mutual recognition between the client and server. For example, a phishing website is a fake well-known website that attracts customers to log in and obtain sensitive information such as passwords. The main process is as follows: the client first initiates an authentication request to the server. After receiving the request, the server will initiate an authentication challenge to the client. The client must send back the correct response to confirm that they are an authorized administrator. After the client's authentication is passed,

the server sends an authentication response to the client and also sends authentication information containing proof of the server's identity. After receiving the response from the server, the client verifies the legitimacy of the authentication information from the server and completes the two-way identity authentication.

As shown in Figure 2, C is the client, S is the server, IDc is the client identity, K is the key, R is the random number challenge code, and MAC is the challenge response code. The client identity authentication system is responsible for authenticating the identities of participating entities such as clients and servers. The authentication of clients by servers can use authentication protocols based on KBC, X.509 public key certificates, CPK algorithm, etc;

The authentication process consists of multiple messages exchanged between the client and server. The message includes the challenge sent by the server to the client for authentication, the challenge response sent by the client in response to the server challenge, the verification request and response message in the case of symmetric key authentication. The messages exchanged during authentication are associated with a unique<SessionId>set by the server. For each authentication session, the server needs to maintain state information, including server challenge, client challenge response, and original client request;

Border defense technology based on the integrated SDK of the Internet of Vehicles:

For the intelligent connected vehicle terminal security SDK, after being implanted into the connected vehicle network boundary terminal devices, it can actively monitor and protect the device terminal ECU in the intelligent connected system, monitor network intrusion behavior at the terminal, and form a complete collection, monitoring, protection, warning and disposal of the entire intelligent connected system, as shown in Figure 3;

The security SDK for in vehicle network boundary devices aims to connect the security application scenarios of in vehicle, mobile, and cloud connected vehicles. On the vehicle side, manage the local control security and data security of key components in the vehicle, configure secure communication channels connected to the TSP cloud service platform, verify encryption keys, execute control instructions, perform security upgrades and audits, etc; On the mobile end, configure a secure communication channel to connect to the TSP cloud service platform and verify signature certificates to execute mobile phone security control commands; In the cloud, manage the lifecycle of in vehicle security components and application data, perform threat analysis, vulnerability assessment, situational warning, and emergency response for connected vehicle terminals and platforms;

Design of in vehicle central security gateway:

Hardware architecture - The EEA3.0 architecture based on in vehicle Ethernet has become the preferred choice for major automotive manufacturers, and other domain controllers need to be interconnected through a central gateway. The V2X connection controller can be an independent T-Box or a wireless connection device integrated into the central gateway. As the communication and scheduling hub for the entire vehicle, the central gateway involves communication management and command coordination between various domain controllers of the vehicle. Key vehicle information and some or even all V2X communication information need to pass through the central gateway;

The central security gateway adopts NXPS32g as the main control chip to develop and mass produce a central gateway hardware platform for EEA3.0. After the maturity of domestic automotive grade replacement chips, it will switch to the national production plan. At the same time, a domestic hardware security management HSM (Hardware Security Management) module will be added to strengthen information security functions, while

reducing the processing burden of S32g chips for information security processing, in order to reserve more resources to handle normal functional calculations and ensure functional security requirements;

The hardware architecture of the central security gateway is shown in Figure 4, with the main control chip using S32g. To support at least 4 domains of on-board Ethernet access, the SJA1110A switching chip is used to expand the Ethernet interface, while also supporting standard bus access such as traditional CAN, LIN, SPI, Flexray, etc; At the same time, the central gateway is planned to support Time Sensitive Networking (TSN) to meet the demand for strong real-time control; And provide real-time transmission technology for next-generation network audio and video, namely AVB protocol, in the high-end version gateway. The detailed parameters of the central network are shown in the table;

There are two different application requirements for the software architecture intelligent vehicle Ethernet connection function. One is traditional network transmission, such as vehicle cloud communication, especially entertainment information, which usually has a large amount of data but allows for a certain degree of latency and fluctuation; The second is the communication of control information between various domains of the vehicle body, which usually has a small amount of data but requires real-time arrival. Therefore, the central gateway platform needs to support both traditional Ethernet to access the cloud and mobile devices; And support time sensitive networks to provide low latency and low fluctuation communication support for vehicle applications;

In terms of algorithm strategy, to address the issue of coexistence of multiple types of high traffic data and high real-time short instructions, data stream queue shaping and application and data type aware selective transmission algorithms are adopted to achieve

adaptive data routing in different scenarios. To address the global time issue in the vehicle network, we plan to comprehensively apply mechanisms such as the optimal master clock selection algorithm, path delay compensation, clock frequency matching and adjustment to achieve clock synchronization between various domain controllers and the central gateway. Furthermore, a time triggered synchronous channel allocation mechanism is adopted in the logical link control layer of the communication network. In order to ensure the safe and stable operation of the central security gateway, a central security gateway security subsystem is embedded in the above software system;

Design of Security Enhanced T-BOX:

The hardware architecture of the intelligent connected vehicle security enhanced T-Box is shown in Figure 8, taking into account the computing power, access capability, real-time data processing capability, and special application requirements of the vehicle level environment required for T-Box to solve various information security threats. The intelligent connected vehicle safety enhanced T-Box mentioned in this technical solution uses NXPMPC5748G as the main control device. The MPC5748G includes two PowerPC architecture Z4 (160MHz * 2) cores and one Z2 (80MHz) core internally. In addition, the chip also integrates an information security dedicated coprocessor HSM module for the implementation of various information security related algorithms. The Huawei MH50005G communication module is used for network communication between T-Box and cloud TSP platform. The MH5000 also integrates WIFIAP functionality, providing access capability for in car mobile devices to access external data. The GPS/Beidou positioning module and three-axis acceleration sensor are used to collect vehicle position and pose information, completing the collection of vehicle operating status information on the cloud TSP platform. Three CAN interfaces are connected to different functional domain CAN bus networks inside the vehicle to collect onboard information, such as vehicle speed, engine speed,

door lock status, air conditioning status, etc. In addition, this T-Box also integrates LIN, BLE modules, RTC clock, audio codec, and Ethernet interface, making it easy for different devices to access. Due to compatibility requirements, T-Box can use Ethernet interfaces to exchange data between the vehicle's internal and external networks through a central gateway, or directly connect to the vehicle's CAN network through a CAN interface. However, considering that CAN networks typically involve vehicle control data, additional security measures need to be taken for this type of access method;

The software architecture - Intelligent Connected Vehicle Security Enhanced T-Box software architecture is shown in Figure 9. The overall software design adopts a logical layering and functional block based approach. From top to bottom, they are the application layer, BSP layer, SDK layer, and hardware layer. The application layer consists of four software modules, each running within the four CPU cores of the MCU. The Z4_1 core serves as the main CPU core, on which the real-time operating system FreeRTOS is deployed, responsible for the allocation and scheduling of tasks throughout the T-box software system. The T-BoxAPP runs on the Z4-1 core application layer and is responsible for implementing the basic functions of the T-BoxT-Box core;

The Z4_2 core Diagnosis APP application is responsible for implementing the remote diagnosis function of vehicles. Implementation of GB_32960APP application for dedicated communication protocol GB_32960 between vehicle terminal and cloud TSP platform. HSM stands for Hardware Security Module, which, as a coprocessor, can implement various encryption and decryption algorithms related to information security in software. BSPLayer, the board level support layer, mainly encapsulates the programming interface of the SDK middleware layer and implements basic inter core data communication functions.

SDK Layer mainly consists of three parts: FreeRTOS, underlying hardware driver layer, and middleware layer. The hardware driver layer consists of hardware processor related code, while the middleware layer consists of Comms (Z4_1 core, some shared code), Safety (Z2 core), and Misc (HSM and Z4_2 core). Provided API programming interfaces for the application layer and implemented software abstraction for the underlying hardware.

Due to the weak computing power of the security enhanced T-BOX device, the current implementation method is to add domestic security encryption chips to the T-BOX to provide secure computing capabilities, assist the CPU in completing password operations, and provide common security measures based on password security. At the same time, the built-in security encryption chip can be used in conjunction with CPKSDK and the vehicle networking based boundary protection SDK to achieve password isolation, prevent data from being sniffed or tampered with during transmission, and ensure the security of data transmission. The security SDK for in vehicle network boundary devices is designed to meet network security requirements such as ROOT prevention, reverse engineering, tampering prevention, illegal instruction injection and control, and sensitive data leakage prevention. From the perspective of firewall, blacklist and whitelist, data forwarding and filtering, the security enhanced T-BOX is subjected to security detection and protection. To achieve security enhanced T-BOX that meets security requirements such as firewall policies and reasonable configuration of security parameters. Relying on the boundary security SDK, remote upgrade security can also be achieved, signing and publishing security enhanced T-BOX software upgrade packages to ensure that terminal software code is not illegally tampered with and to ensure data and OTA upgrade security;

Design of CPKSDKAPI interface functions based on CPK:

The CPKSDK API implements a set of API interface functions for a security system based

on a combination of public keys, including different operating system versions such as Windows, x86_ Linux, ARM_ Linux, Android, etc. Provides functions such as device management, access control, file management, and password services.

Device management: mainly responsible for opening, closing, and obtaining device serial numbers. Users do not need to know the device type and specific driving mode, they only need to complete device management through the provided interface.

Access control: divided into two levels (superuser and user), each with different access control permissions. Super users are responsible for establishing application files, importing, updating, and initializing keys, unlocking user PIN codes, and reinstalling PIN codes. Users have the right to use the device, use the functions provided by the device, and store their own private data.

File management: Used to meet the needs of application developers for secondary development based on specific applications, including creating, writing, reading, and deleting files.

Password service: refers to operations directly related to cryptography, including generating random numbers, CPK digital signatures and verification signatures, CPK encryption and decryption (core is key transfer protocol), and some auxiliary functions.

Although the present invention has been described with reference to embodiments in the preceding text, various improvements can be made and components can be replaced with equivalents without departing from the scope of the present invention. Especially, as long as there is no structural conflict, the various features disclosed in the embodiments of the present invention can be combined with each other in any way. The lack of exhaustive description of these combinations in this specification is only for the sake of omitting space and saving resources. Therefore, the present invention is not limited to the specific

embodiments disclosed herein, but includes all technical solutions falling within the scope of the claims.