Open Access Library Journal
2021, Volume 8, e7795
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Exploration of Core Technologies of Cyber Security

Xianghao Nan

CPK Laboratory, Beijing, China
Email: nanxh2001@163.com

How to cite this paper: Nan, X.H. (2021) Exploration of Core Technologies of Cyber Security. *Open Access Library Journal*, **8**: e7795.
https://doi.org/10.4236/oalib.1107795

Received: July 27, 2021
Accepted: September 23, 2021
Published: September 26, 2021

Abstract

In order to study the role of key technologies in information security, the main tasks and key technologies defined in different development stages were reviewed in this paper, focusing on exploring the main tasks and core technologies of cyber security. The proof logic of PKI certification system and the digital signature standard DSA were analyzed, subsequently the signature elements are clarified and found that CPK public key could satisfy all the elements, so the evidence-based truth logic of authentication was created, and the new concepts of "identity authentication" and "proof-before-event" were formed. Based on identity authentication technology, a CPK authentication system was established, an independent self-assured network was constructed, a general one-step protocol was formulated, and a feasible technical route for cyber security was formed, and the practical significance of identification was discussed.

Subject Areas

Computer and Network Security

Keywords

Information Security, Authentication, Digital Signature

1. Introduction

The definition of cyber security in this article is the combination of Internet of Things and Events security. That is, it covers static and dynamic entities, concrete and abstract information.

Since the use of the modern cipher machine, it has experienced different development ages, such as communication security age, closed network information security age and open network information security age. In different development stages, different security requirements were put forward, and different main tasks and core technologies were formed. Of course, in some development stages, the requirements were relatively simple and the main tasks and core technologies were self-evident. However, in some development stages, the requirements were very complex and it was difficult to determine the main tasks and core technologies without systematic research. At every stage of development, when the main tasks and key technologies are clear, the business progresses smoothly with fewer detours.

In the development of information security, there has been a major change, this change is caused by the emergence of the open network, has produced a new security theory, new core technology, new security principles, new security policy. This transformation is first proposed by the United States, the United States has been walking in the front, leading the development direction of information security, but suffering from the failure to solve the core technology. This core technology was first solved by the Chinese civilian, and a new security theory was formed. China was not lagged behind the US in their ability to solve practical technical problems. Many technical problems China had already solved, such as LAN information security, identity mapping key distribution and so on, until the Americans brought it up, when we understood it. It explains the gap in our theoretical advancement. Therefore, the future development of China's information security needs the understanding and guidance of the officials in charge.

2. The Evolution of Core Technology Development

In 1970s, China's first electronic cipher machine M06 was developed in the army's high-speed communication "708" project, which pushed China into the era of communication security in which data encryption was taken as main technology. It broke away from the traditional manual operation of the code book and entered the stage of modern cipher operation. The gap has reduced from 40 years to less than 10 years. Encryption and decryption is attached to communication and mutually carried out in a point-to-point line. The whole points use a same key and at the same level, namely single-level control. In the era of communication security, the main task is the design of electronic cipher, and the core technology of electronic cipher is Linear Feedback Shift Register (LFSR). At that time, the United States had the highest level, in the 1960s, it had used a long LFSR in the cipher machine, and India announced 5 levels of LFSR in 65 years. It was not until the 1970s that China mastered the laws of the LFSR, which was the basis for designing electronic cipher. At the same time, block cipher appeared, it has a high complexity by multilayered products of simple algorithm according to the Shannon theory, and the cipher can be made public, which is a leap in the field of data encryption. In 1992, an expert at the Eurocrypt held at the University of Perugia in Italy declared that "cryptography is saturated", and the era of cryptography research as the core technology has gone forever. The U.S. Military's top-secret cipher machine KW-7 has also become a collector's item.

In 1980s, The US military launched the project of Defense Secure Network System (DSNS), while the Chinese military launched the project of "918" network security system. The US military put forward the principle of multi-level control in the "Orange Book" [1] of the Ministry of Defense, and managed to achieve the key management of 100,000 levels with traditional end-to-end technology. However, due to the construction of the Internet, the project originally to be completed in 1991 was stopped in the middle of the way. With the DLP double-layer key technology and identity mapping method, PLA has realized the key management of 1 million levels, and entered the era of multi-level control of information security on schedule. However, we did not know what we had achieved. Later, we knew that the multi-level control of the sharing system was information security. We solved the key distribution with identity mapping, but we did not know what it is. In the patent of "Identity-Based Signature Scheme", Shamir proposed the concept of identity-based public key. At that time, we knew that what we realized was the identity-based public key. Therefore, it can be said that China is the first country to use the identity-mapping to solve the key distribution. There is a famous line in Cohen's "Code Breaker": "All secrets reside in the key". Cipher is like a gun, the key is a bullet, and a gun without bullets is like a stick. Cipher and key are not of the same concept, if confused the core technology cannot be found.

In 1990s, the world entered the Internet age. This is a great step forward, moving from collectivized to personalized communication. The Clinton administration of the United States issued the Presidential Directive PDD63 [2], announced that the main task of Internet security is vulnerability analysis, patching, plugging loopholes, also announced that the security of the Internet depends on the security awareness of all Internet users which was so called "Information Assurance policy". The policy was right, but the main task was wrongly defined, the Internet security is understood as system security, while system security is only an integral part of information security, as well as network security, transaction security. However, it is the first time to clearly put forward the concept of relying on the security awareness of Internet users and the concept of information assurance, which is an important concept with historical significance. China has adopted the "follow" policy, but due to the differences in translation and understanding, it has not adopted the open policy of information assurance, and it still remained in unipolar control or remained in a closed policy where information was "guaranteed" by the authorities. This lag in understanding has become the resistance to the development of information security in China.

3. Exploration of Core Technologies for Cyber Security

In the 2000s, Internet security entered the Cyber security era, and the Internet began to penetrate into social production and social life. In addition to person-to-person communication, person-to-object communication also emerged. The President's Information Technology Advisory Committee (PITAC) of the

Bush administration put forward the new concept of Cyber security for the first time in its report "Cyber Security, The Crisis of Prioritization" [3], and made it clear that the priority task is to solve billions of authentication. Since then, the main technology of information security has changed from data encryption to authenticity identification; the security strategy changes from passive defense to active management; the principle of security has changed from "mutual trust" to "mutual suspicion". This is an epoch-making change. From now on, the logic of proof based on subjective trust is discarded, and the new way of proof based on objective evidence is opened up. This is a watershed that will decide future technical approach. However, PITAC only proposed scaled authentication technology as the primary task, but does not address what to authenticate and how to authenticate it. As a result, a study of fingerprints and facial features emerged in the United States, but found that such features did not apply on the Internet. During this period, in order to solve the scale of key management, many new systems appeared in the society, such as GPG, SET, PKI, etc., and produced a new concept of third-party CA certification. Among many technologies, the visualized third-party certification system is easy to understand, so China has entered the era of PKI.

3.1. Analysis of PKI Certification Logic

PKI certification logic is built on the basis of Belief Logic [4] of model reasoning, that is, in the process of "A sends X to B", the Logic tries to make B believe that X is real through readability, freshness and jurisdiction reasoning. According to the agreement, the object authenticity proof can be achieved, which can make B believe the authenticity of X, but how to believe A? Thus, "this is Alice's public key" is given in the CA certificate, but who can prove the authenticity of the CA? It will be an endless evidence-chain. Alice went on the Internet with a real-name CA certificate, but the identity he claimed was a user-name. Then who will prove the oneness of real name and user-name? The number of identities that need to be proved on the Internet of things is so numerous that is hard to be expressed in a single certificate. In the original PKI protocol, the verifier obtained the certificate from LDAP, which reflected some role of the verifier. However, nowadays, the certificate is provided by the signer, which avoids the trouble of accessing the LDAP, but its proof logic is greatly retrogressed, and the key encryption function is lost, too. In addition, with the method of certificate proof, the verification is carried on only between the signer and the CA certificate, has nothing to do with the verifier, which violates the security principle of information assurance and "mutual suspicion", the verifier may recognize or reject the verification results. Of course, under the trust mechanism, the "trust" relationship can be established, but this kind of "trust" does not have the attribute of signature, and it is difficult to be used as evidence when a legal dispute occurs. The Secure Socket Layer (SSL) protocol and the WLAN protocol of Wide Area Network developed later including certificate exchange, but they can only be used for online communication, not single-line communication. It can be seen that the trust relationship established by PKI does not have the attribute of signature, nor can it provide traceability proof and attribute proof, so it cannot be a key technology.

3.2. Analysis of DSA under Trust Mechanism

The traditional logic of trust was based on such a logic that "what you have, I have" or "what you encypts, I can decrypts". Digital Signature Algorithm DSA [5] provides a good mathematical formula to prove public-private key pairings, the signature is signed with the private key, and the verification is verified with the public key:

$$k*G=(x,y)\rightarrow c;\quad s=k^{-1}(h+sk)$$

$$s^{-1}(hG+PK)=k*G\rightarrow c'$$

If $c=c'$, then it is proved that "I have a public-key, you have a corresponding private-key", thus the trust relation can be built, but it doesn't have the meaning of a signature, because anyone can generate a key pair, signs to any object at will. Therefore, whether DSA can be a signature algorithm depends on the definition of key. For a signature to be meaningful, there must be a claim, that is, who claims to have signed it. In fact, for any event, the claim goes first. When one makes a call, he says "this is xxx" first. When a station broadcasts, it says "this is xxx station" first. When a terminal sends a message, it claims "the IP-addr is xx". Proof of the authenticity of a claim is "identity authentication", because what the subject claims is the identity. Here, identity is a concrete noun, *i.e.*, the claimed name of an entity. If a person uses his or her identity as a digital seal, the identity claimed is his or her real identity. If a person makes a phone call, the identity claimed is a phone number. If he or she sends an email, the identity claimed is a user identity. It is easy to claim, but hard to prove, even harder to verify, it has been an international conundrum. The reason why the proof of claim is so difficult is because the claim proof have special request for key pair: the private-key used must be derived from identity that is claimed, and forms a one-to-one mapping relation between the identity and private-key; The reason why the verification of claims is harder, because the public-key used must be derived personally by the verifier from the identity that is to be verified, and forms a one-to-one mapping relation between the identity and public-key, therefore the digital signature needs to be redefined. A DSA can be a digital signature protocol only when the key pair meets the preceding two conditions. In other words, a digital signature must contain proof of claim, otherwise it cannot be called a digital signature.

3.3. Invention of CPK Combined Public Key

CPK combined public key [6] was originally studied to solve the scale of key and the problem of public key distribution. The basic working principle is as follows:

CPK is composed of combination matrix and mapping function. The matrix is divided into private matrix $a_{sk} = \left(r_{i,j} \right)$ and public matrix $A_{PK} = \left(R_{i,j} \right)$. The private matrix is kept in KMC, and the public matrix is published. The coordinates of the matrix are indicated by the YS:

$$YS = \text{Hash}\left(\text{Alice}\right) = v_0, v_1, \cdots, v_{31}$$

$$sk_{\text{Alice}} = \sum_{i=0}^{31} r_{[v_i,i]} \bmod n \text{ or } PK_{\text{Alice}} = \sum_{i=0}^{31} R_{[v_i,i]}$$

v_i is taken as the row coordinate, the column coordinate adopts the natural order, and the corresponding variables are taken from the matrix and added. The sum of the private matrix variables is the private-key, and the sum of the public matrix variables is the public-key.

The key pair not only provides digital signature, but also provides key encryption. Its digital signature can provide the authenticity proof of identity, entity and object; its key encryption can form closed environment between any two points on the open network achieving the minimum granularity, which makes regional closure is no longer needed.

CPK also provides a general method to change the common public key into an identity-based public key system. Only when the current public key is changed to an identity-based public key can it have the identity authentication function, that is, it can provide proof for the claim, attribute and traceability. CPK has experienced the development and perfection process from original type, improved type to enhanced type. Existing RSA (integer factorization), ECC (elliptic curve), DLP (discrete logarithms), BLP (bi-linear pairing) and so on can be changed to identity-based public keys. As long as it is changed to identity-based public key, the meaning of its digital signature has a qualitative leap, and it is easy to prove the claims.

3.4. Establishment of CPK Truth Logic

Since there is identity-based CPK public key, we can build an evidence-based truth logic. Evidence must be objective, and subjective factors such as trust and consensus should no longer be regarded as evidence, just as morality, though accepted, cannot be used as evidence. Identity-based signature has the following characteristics, taking Alice's signature to object and verification as an example:

Signature: $kG = \left(x, y\right) \to c$; $k^{-1}\left(\text{object} + sk_{[\text{Alice}]}\right) \bmod n = s$; sign code is ($s$, c)

Verification: $s^{-1}\left(\text{object} * G + PK_{[\text{Alice}]}\right) \to c'$

If $c = c'$, then it proves that the public and private keys are paired; Since the key is derived from the identity, the unity of the key and identity is established; Signed by an authenticated key, the object is real. Obviously, the proof has a concept of order. In the order, identity authenticity proof has nothing to do with object, on the contrary, the object authenticity proof relies on identity authentication, which gives rise to the concept of "identity authentication". Thus, truth logic can be designed according to different order.

The Truth Logic is evidence-based logic, which is different from the trust logic based on behavior and the belief logic based on model reasoning in the past. The evidence on which proof is based is objective, and the proof result is only yes or no without ambivalence and subjectivity. The objects of truth logic are only entity and event.

Entity is composed of identity and ontology:

$$\text{entity} = \text{identity} + \text{ontology}$$

So the entity authentication is composed of identity authentication and ontology authentication. Identity authentication is the private key of the identity claimed by the subject signs to object 0. Since the identity has nothing to do with the object, In the DSA signature protocol $s^{-1}\left(h+sk\right)$, the object h can be set to 0:

$$kG=\left(x,y\right)\to c\text{;}\quad k^{-1}sk_{[\text{alice}]}\bmod n=s$$

The sign code is (s, c). The verification is the validation of the signature by the public-key created from the identity that the subject claimed. The public-key is calculated by the verifier, which embodies the principle of information assurance:

$$s^{-1}PK_{[\text{Alice}]}\to c'$$

when identity signatures replace "password certification", no personal information is exposed.

Ontology authentication is the signature and verification of ontology h by the identity claimed by the subject:

$$k*G=\left(x,y\right)\to c\text{;}\quad k^{-1}\left(h+sk_{[\text{alice}]}\right)\bmod n=s$$

$$s^{-1}\left(hG+sk_{[\text{Alice}]}\right)\bmod n\to c'$$

The entity authentication is equal to ontology authentication, but it is different from identity authentication. If one claims: "I am Bob", its proof belongs to identity authentication; if one claims: "I am a professor", the proof is ontology authentication.

Event is composed of accepting process and adopting process, hence the concept of "ex ante authentication" was formed. Event authentication is also composed of accepting authentication and adopting authentication. If A gives X Dollars to B, then a payment event occurs in A and a collection event occurs in B, the payer provides two evidences, one for ex ante authentication and the other for subsequent authentication. The evidence used for ex ante authentication is the signature of the payer to the payee, while the evidence used for later authentication is the signature of the payer to the object.

The verification is carried out in two steps. The first step is to verify the authenticity of the evidence for ex ate authentication, namely A and B, in the accepting stage. The second step is to verify the evidence for later authentication, namely object x, in the adopting stage. Accept and adopt is used as a term of transaction, while in communication it is called access and receive process.

4. The Achievement of Identity Authentication

4.1. Establishment of CPK Authentication System

The concepts of "identity authentication" and "ex ante authentication" formed in truth logic are the core and basic concepts of information security, which have very important significance. Because the digital signature cannot be realized without the authenticity proof of the identity claimed by the subject; it is difficult to prevent illegal access and DOS attacks without ex ante authentication. Because the basic unit of proof is entity and event, which can naturally adapt to different environments, such as network environment, computing environment, transaction environment, etc. The new authentication system based on evidence should be different from the traditional certification system based on trust transfer. The authentication system takes "mutual suspicion" as the security principle and evidence as the criterion to ensure the completeness of proof.

To achieve completeness, the elements to be proved by the system should include: First, the identity authenticity proof claimed by the subject; Second, the slave authenticity proof claimed by the subject; Third, the object authenticity proof claimed by the subject; Fourth, the public matrix authenticity proof claimed by KMC. The public matrix is published by the KMC with the evidence of authenticity. Any verifier can check the authenticity of the public matrix. The KMC establishes the scope within which the integrity of the digital signature is guaranteed. The signature published by KMC is (s, c), when verifying, the user calculates the KMC's public-key $PK_{[\mathrm{KMC}]}$ and then computes:

$$\mathrm{Hash}\left(\mathrm{Matrix}\right)=h\,,\quad s^{-1}\left(hG+PK_{[\mathrm{KMC}]}\right)\rightarrow c'$$

This verification only checks once when the system is set up.

4.2. Construction of Self-Assured Network

Identity authentication is a logic to prove who the subject claims to be. Since the truth logic is created, it is natural to enter into the research of constructing self-assured authentication network. In 2010, the Obama administration realized that identity authentication was the real core technology among many authentication technologies, and officially took it as a national development strategy. However, it still failed to find a solution, let alone solve the identity authentication, and stalled. The IoT network is a virtual network connected from any identity to any identity, realizing "proof-before-event authentication", constructing an independent and provable network, replacing password certification with access protocol, and replacing login mechanism with access protocol. According to the experience of cyber warfare [7], the login mechanism is the bane of the trust transfer, which leads to the takeover of power. It can be seen that the security measures under the trust mechanism have become security threats in the IoT era. Assurance policy is the base of cyber security. The technology realizes how the information system is only controlled by myself and not by others. "My security is up to me" is easier said than done. To achieve assurance control, we must first identify "friends or foe". Identity authentication actually identifies "friends", "either friends or foe". To Identify true or false is the primary task of information security. The authentication must be carried out before the occurrence of the object event. Therefore, the proof-before-event' technology is also the basic technology to realize the assurance policy. In the study of assurance policy, it is found that the independence of authentication technology is no longer constrained by the communication protocol. For example, when A receives a letter from B, A cares about the authenticity of the letter and does not care about how the letter came. The independence of the authentication technology provides an independent path for the implementation in the system. The realization of information assurance has brought great changes to the way of thinking about security: to turn passive into active without being afraid of the occurrence of illegal access, malicious software intrusion, and the existence of loopholes, backdoors, because self-assured controlling technology can make it meaningless, just like digital currency without being afraid of losing, because the same currency in the other's hands will be meaningless.

4.3. Formulation of Universal GAP Protocol

The IoT is a network of virtually interconnected entities, and the IoE (Internet of Events) a network of virtually interconnected events. Therefore, the way of thinking about security needs to be improved from the image logic of physical connection to the abstract logic of virtual connection. The Internet of Things and Events has the same properties of entities, the only difference is static entity or dynamic entity. Because the entity authentication is the basic technology, since the self-assured authentication network is established, a universal GAP one-step authentication protocol can be created [8]. GAP protocol has only four signature forms, which can meet the authenticity proof requirements of Internet of Things and Internet of Events:

Identity signature: $\left(k^{-1}sk_{[\text{alice}]}\right)\bmod n = s$

Entity signature: $\left(k^{-1}\left(\text{ontology} + sk_{[\text{alice}]}\right)\right)\bmod n = s$

Slave signature: $\left(k^{-1}\left(\text{slave} + sk_{[\text{alice}]}\right)\right)\bmod n = s$

Object signature: $\left(k^{-1}\left(\text{object} + sk_{[\text{alice}]}\right)\right)\bmod n = s$

Because it is a sentence protocol, a unified authentication of Internet of things and event can be implemented realizing "one thing one proof", "one event one proof", put an end to all trust transfer, and making the proof have the nature of "ex ante", one stepped, universality and on-spot. One-step authentication protocol is a significant improvement over the traditional Secure Socket Layer (SSL) protocol, which can only be used for online communication but requires six responses back and forth, while GAP can be completed in one step, so it is used for communication or transaction, online or offline. The universe is made up of entities and events, and of course entities can be compound entities, and events can be compound events, but any entity or event is classified naturally by identities, so the proof of security is as simple as pushing a building block. If proof of authenticity could be provided for every entity and every event, the whole problem of cyber security could be solved. This may be is the so called "Silver Bullet" that experts around the world dream of.

5. Prospect and Significance of Identity Authentication

Entity authenticity cannot be established without identity authentication. This shows, in many authentication technologies, only the identity authentication can be independent, to provide the proof of claims, attribute, traceability. Signature to an object is only effective on the base of identity authentication. One signature provides the proof of claim, attribute, and traceability at the same time, but it belongs to the subsequent authentication, because it can only be provided after an object event has occurred. The authenticity proof of any entity and any event is inseparable from the proof of the claimed identity, without which the security of the claimed item proof is without roots. Without proof of claim, digital currency can't be designed, because it can't prove which bank's currency. Without proof of claim, digital seal can't be designed, because it can't prove which entity's seal. Identity authentication is not only the core technology of cyber security, but also the core technology of social management. The Ministry of Public Security issued a "resident ID card", which is an innovation in China, but the identity, address, and the issuer's claims are not proved, the checking system needs a huge background supporting system. If the claim can be proved, it can allow everyone to verify the authenticity directly without any other support.

Practice has proved that GAP protocol is used in communication, can control access, provide traceability proof, not afraid of illegal access and DoS attack; Applied to computer kernel, can control the download, installation, invoking, execution of unauthorized software, not afraid of malware intrusion and backdoor; Applied to transactions, digital currencies can be constructed for payment and settlement without fear of loss and the need for a vault; used in office, it can construct digital seal of online and offline communication to open the bottleneck of electronic office; Used in logistics to construct anti-counterfeiting labels; Used in signal system, it can accurately control all kinds of signals in complex remote control signal environment. If the results of each certificate are gathered together, the operation situation diagram of the whole network will be automatically formed.

6. Summary

The process of exploring key technologies is a process of continuous abstraction.

At present, the composition of cyber space has been abstracted into static and dynamic entities, and the entities have been decomposed into identity and ontology. This is the basic element of information security research. The solution process of key technology is the process of continuous innovation, including theory and technology.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] TCSEC U.S. DoD (1983) Orange Book, Rainbow Series Verified Protection Mandatory Protection Security Domains Superseded Common Criteria.

[2] President's Information Technology Advisory Committee (1997) Protecting America's Critical Infrastructures (PDD 63). Presidential Decision Directive.

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

[4] Brurros, M., Abadi, M. and Needham, R. (1989) A Logic of Authentication. *Proceedings of the* 12*th ACM Symposium on Operating Systems Principles*, New York, 3-6 December, 1989, 1-13. https://doi.org/10.1145/74850.74852

[5] National Institute Standard and Technology (1994) Digital Signature Standards, U.S. Department of Commerce, NIST PUB 186.

[6] 南湘浩, 陈钟. 网络安全技术概论[M]. 北京: 国防工业出版社, 2003.

[7] Wilson, C. (2004) Information Warfare and Cyber War: Capabilities and Related Policy Issues. CRS Report for Congress.

[8] 南湘浩. GAP 一步协议[J]. 通信技术, 2020, 53(12): 3030.