Zero Trust, Can Be Simpler!

（May 07, 2021）

"Zero Trust" is a very hot term in the cyber security community. Major security vendors have launched corresponding products and solutions. After a rough understanding of these solutions, the author believes that Zero Trust, using PKI (Public Key Infrastructure) technology, can be simpler! The current solutions are too complicated, the implementation cost is too high, and it may not completely solve the trust problem.

Let me talk about what is Zero Trust first? This concept was first put forward in 2010 by John Kindervag, the chief analyst of Forrester Research at the time. All people and things are untrustworthy, and any request for access to any resource needs to control. Now, as the pressure to protect enterprise business systems and data is increasing, and attacks become more and more complex, CIOs, CISOs and other executives are increasingly agreeing to the concept of Zero Trust and implementing Zero Trust solutions. Solutions that support Zero Trust have gradually become mainstream.

Zero Trust is a security concept, and there is no fixed technology. Its core belief is that organizations should not automatically trust any people and things inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. The Zero Trust model fundamentally contained the old ideas of castles and moats, because new technologies such as cloud computing and mobile office have been widely used, and the methods of protecting castle-and-moat are no longer feasible. It should always be assumed that the network is full of threats, external and internal threats fill the network all the time. You cannot rely solely on network locations to establish trust relationships. All devices, users, and network traffic should be authenticated and authorized to access all systems.

How to implement Zero Trust? The author does not comment on the advantages and disadvantages of a certain provider’s solution, but only proposes solutions that are different from traditional security vendors for reference. Traditional security vendors still focus on protection, and the author’s idea is to directly protect the data, the goal of being protected. The author believes that PKI technology is the most effective and efficient reliable technology to solve trust problems and protect data security. According to the definition of cryptography, it refers to technologies, products and services that use specific transformation methods to encrypt and protect information. The use of cryptographic technology to achieve user authentication and information encryption protection can solve the problems that Zero Trust wants to solve, and at the same time, it can also meet users' compliance requirements of the related laws.

"Zero Trust", in layman's term, means not trusting anyone or anything. The solution proposed by traditional security vendors is to prove that people and things are trustworthy before allowing access. In fact, cryptography can efficiently solve the trust problem. It is very simple. All people and things need to pass the identity validation and issue a trusted identity certificate to prove their trusted identity. When this person or thing is connected to system resources, it does not use insecure username and password authentication, but requires this person and thing to show its identity certificate (digital signature with signing certificate), and only those who conform to the security rules can pass. Only after authentication can the corresponding resources be accessed, which is simple and efficient. Of course, for some important applications, two-way authentication can be used, and the system resources also need to provide their identity certificates (such as website SSL certificate), and the visiting person or thing must also validate the identity of the system. Only then can the person or thing exchange data with the system.

This Zero Trust solution based on PKI technology is similar to real-name flight security management in the real world. It guarantees the safety of airplane travel through real-name certification of passengers and airline qualification certification. The current Zero Trust solutions on the market require complex dynamic continuous trust assessment and dynamic adjustment of access permissions. This is non-real-name authentication that don’t know who the bad guys are, only rely on Sherlock Holmes style continuous screening, the efficiency is too low and may make mistakes.

On the other hand, the goal of Zero Trust protection is to protect the data. The purpose of hacker attacks is to obtain the data. If we use a digital certificate to encrypt the data to be protected, the hacker does not have a digital certificate for decryption. So, the data lost its value for stealing, that is, it truly protects the data resources fundamentally and effectively.

Let’s talk about the email security we are good at. In addition to deploying SSL certificates on the mail server to protect the transmission security, you can also use the signing certificate to achieve strong identity authentication, instead of insecure username and password authentication. MeSign App automatically configures signing certificate with different identity authentication level according to different user identity, which can meet the different identity level requirement of the business system, including the identity that only validates the email control, the identity that validates the individual, the identity that validates the organization and the identity that validates the employee identity of the organization. In this way, the identity authentication system only needs to set a simple access policy to allow people with different identities to access the different resources through authentication.

As for the email data, users can use MeSign App as the email client to send and receive emails, realizing automatic encryption of every email. In this way, the email data stored on the cloud mail server is all ciphertext. Even if it is obtained illegally, the email data is a pile of wastepaper due to the inability to decrypt it, making the email data attacks lose the value for attacking. That is to say, the email data is stored on the mail server in ciphertext, so that the data loses the value of being stolen, then the security of the data is protected.

Regarding the security of documents, in addition to the use of digital certificate authentication technology to achieve strong identity authentication like email security protection, the documents themselves must also be protected. MeSign Technology provides the document signing service, which not only allows users to automatically digitally sign all documents to prove the authenticity of the documents, but also when users digitally sign documents, they can also choose to encrypt the document with the encrypting certificate. In this way, these documents are stored in ciphertext in the cloud system, even if they are illegally leaked or attacked, they cannot be decrypted. It is a pile of wastepaper that makes these attacks lose the value for attacking. That is to say, the documents are stored in the business management system in ciphertext, so that the documents lose the value of being stolen, and the security of the document is protected.

Of course, the core of Zero Trust solution using PKI technology is a must have a PKI system, which requires these systems to issue signing certificate and encrypting certificate. MeSign Technology have built cloud cryptographic infrastructure to empower email client and e-signature tool software, implement automatic email encryption and digital signature, document digital signature and encryption. MeSign Technology also provides cloud cryptographic service, providing users who do not build a PKI system to provide the required cryptographic service, so that user can achieve strong identity authentication and digital signature, encryption, and timestamping service for data to achieve Zero Trust security.

The Zero Trust security solution based on PKI technology can also be used for the security of the Internet of Things, such as the Internet of Vehicles. Each vehicle has a digital certificate to prove its trusted identity. It is used when communicating with vehicles, vehicle and people, and vehicle and things. Digital signature is used to prove their trusted identity, and encrypting certificate is used to encrypt all communications to ensure that the communication content between vehicle, people, and thins will not be illegally stolen and tampered with, thereby protecting the security of Internet of Vehicles communications. In this case, the security protection of the Internet of Vehicles is very simple. The communication receiver must validate the digital signature from the sender, then decide whether to accept or reject the communication according to the security rules. That is to say, the vehicles only receive trusted communications, thus effectively resisting various attacks, without the need for additional complex security protection modules.

Finally, to summarize, due to the widespread application of cloud computing, mobile office, and the Internet of Everything, the boundaries of the enterprise have collapsed, and both the internal network and the external network are insecure. The concept of Zero Trust came into being to solve this problem. However, let us go back to the source of the problem. We want to protect data, the goal of adopting Zero Trust is to protect data. Therefore, we can use PKI technology to build cloud cryptographic infrastructure or use the cloud cryptographic service realizes the trust of the identity of people and things and data encryption, so as to achieve the purpose of simplifying identity management and enhancing data protection. Therefore, Zero Trust, if using of PKI technology, can be simpler, lower implementation costs, and better implementation results!

-- END --

Richard Wang

Digitally signed by Richard Wang
ceo@mesign.com

Want to contact me to discuss this topic? Please use MeSign App (-) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.