Let cryptography add another firewood to zero trust

Zero trust is very hot now. The establishment of ZoTrus Technology is to let cryptographic technology add another firewood to zero trust and make zero trust even more hot.

At present, the zero trust security participants in the market are basically major security vendors and Internet giants, and their solutions are zero trust security solutions based on their respective professions and expertise. The author concludes that these solutions are "Sherlock Holmes" security mode for continuous threat analysis and screening, this mode is still designed based on the concept of traditional security protection, and it still cannot escape the magic circle of constant game of "As virtue rises one foot, vice rises ten".

The author has been engaged in CA operation and cryptographic application for 17 years, and the business that has been engaged in is trust service. In Europe, CA company is called trust service provider (TSP). Therefore, we firmly believe that: to solve the trust problem, of course, digital certificates, PKI (Public Key Infrastructure) and cryptographic technology are inseparable. The concept of zero trust is put forward to solve the problem of cyber trust, of course, PKI and cryptography cannot be absent. Because PKI and cryptography are born to solve the problem of cyber trust and data security. Therefore, the birth of ZoTrus Technology is to add a different one to the hundreds of zero trust security solutions. ZoTrus Technology, an innovative zero trust security provider based on cryptographic technology.

One of the core logic components of zero trust described in SP 800-207 "Zero Trust Architecture" released by the National Institute of Standards and Technology (NIST) of United States in August 2020 is PKI, although there is no specific PKI application description. On January 26, 2022, the Office of Management and Budget (OMB) of United States officially released the "Federal Zero Trust Strategy", which detailed that the US federal government agencies must gradually shift to a security architecture based on zero trust principals. There are many actions such as https encryption and email encryption, which are the core applications of PKI and cryptographic technology.

The China Cryptography Law clearly requires that critical information infrastructure must be protected by commercial cryptography, which means that cryptographic technology must be used to achieve security authentication and encryption protection of information. This is literally zero trust, never trust the entities identities and information that are not using cryptographic technology. In other words, zero trust is inseparable from cryptography, and cryptographic technology is the foundation and cornerstone of zero trust security.

The three concepts of ZoTrus are “Never trust, always verify, always encrypt”, and the five principals of ZoTrus are:

First, never trust http websites that transmit cleartext, and only trust https encrypted and identity validated websites.

Second, never trust cleartext emails, but only trust encrypted and digitally signed emails.

Third, never trust the electronic documents without trusted identities, and only trust the electronic documents with trusted digital signatures and timestamps.

Fourth, never trust applications without a trusted identity, but only trust applications with trusted digital signatures and timestamps.

Fifth, never trust the entities without validated identities, and only trust the digital identities of validated entities.

Zero trust is a kind of life wisdom to ensure the safety of daily life. ZoTrus Technology is a security practice to ensure the security of the Internet of Everything. ZoTrus Technology, make zero trust zero threshold and make cryptographic at fingertips, making the zero trust journey easier and more efficient.

Richard Wang

Dec 20, 2021
In Shenzhen, China
June 1, 2022, Updated