In the real world, the most secure systems are all zero trust systems

I don't know if readers still have an impression for "The Story of Lenin and the Guard". This is a real-world story that only recognizes "credential" but not "people”, this is strictly enforced every day in all secure systems. Another example is traveling by plane, which is also a zero-trust system. Everyone must buy tickets with their real names, must hold a trusted credential (ID card or passport), and pass the security check after passing the real-name authentication with a boarding pass. At the same time, the boarding and disembarking passages must also be dedicated passages (covered bridges and shuttles). These are zero trust, zero trust for personal identity and zero trust for transmission channel.

The process of traveling by plane corresponds to the digital world, which is a cryptographic based zero trust security solution. Each user must have a digital certificate to prove their trusted identity, this digital certificate must be issued by a CA certificate trusted by the system. For network resources access, user need to use its digital identity certificate to complete the digital signature verification. Only after passing the trusted identity authentication, can user access the required data. The data delivery must also be transmitted through a dedicated HTTPS encrypted channel and can also be encrypted with the user's public key. Only the user can decrypt the received data with the private key.

The real-world banking system is also a zero-trust system. Bank employees must hold specific identity documents to enter specific work areas and use specific identity cards to log into systems with specific permissions. Online banking users must have a USB Key to prove their trusted identity and to log into the online banking system, the digital certificate in the USB Key must be used to sign the login behavior data. The banking system can only log into the online banking system after verifying the signature. At the same time, all communication channels must be encrypted with https. The user's money transfer instruction in the online banking must also be signed and encrypted with the user's digital certificate and sent to the bank payment system.

The author will not give much more examples. You must have experienced and discovered many such systems in the real world. It can be said that the application of zero trust in the cyber world is a replica application in the real world. From this point, we can also see the application prospect of zero trust in the cyber world.

In the real world, everyone has different credentials, and different credentials need to be showed in different scenarios. Commonly used ID cards can be used for most application scenarios, while passports are used for overseas travel. Community access cards or office building work cards are used to enter the community and office buildings, and the pass for large-scale conferences is only used for one-time participation in the conference. The same is true in the digital world. Users can also have digital identities with different validation levels, and users can use different identity certificates for identity authentication according to different application scenarios. There are identity certificates that only validate email addresses or mobile phone numbers, identity certificates that validate personal identity, identity certificates that validate the identity of an organization, and an identity certificates that validate both the identity of the organization and the identity of employees of the organization. Users can have multiple identities, while business systems can require the user using different validation level identity certificate to access the data according to the access policy.

The first traffic in the cyber world is website, and its identity is identified by an SSL certificate. If a website is not deployed with an SSL certificate, all browsers will display it as "Not secure". This is not only because of cleartext transmission, but also because of the identity of the website has not been validated. Website identity has 4 different levels. The DV SSL certificate that only validates the domain name control is the lowest level of website identity validation because the real identity of the website owner is not validated, the subject in the DV SSL certificate only displays the website domain name. If the website owner is an individual, the SSL certificate issued after validating the website owner's personal identity is called "IV SSL certificate". This certificate name is not common because personal websites generally only apply for cheap DV SSL certificates. If the website owner is an organization, the SSL certificate issued after validating the identity of the website owner is called "OV SSL certificate", and the subject in the OV SSL certificate will display the name of the organization. There is also an extended validation for organization users, that is, the SSL certificate issued after validating the identity of the website owner more strictly in accordance with international standards is called "EV SSL certificate", and the browser address bar is displayed as a green address bar, allowing website visitors to get a very visible look at the trusted identity of the website owner. With these 4 different levels of website identity validation, website visitors can easily identify the real identity of the website, so as to make correct security decisions for website access.

The most secure system in the real world is a zero-trust system. The application of the zero-trust concept to the cyber world is a wonderful application of human wisdom in the cyber world. This has been tested and verified in practice, and it is the most efficient concept for solving cyber security problems. Coupled with the zero-trust security implementation using cryptographic technology, it will definitely become a powerful tool for solving cyber security and can effectively guarantee the security of the Internet and the Internet of Everything.

Richard Wang

June 1, 2022
In Shenzhen, China