Four misunderstandings of Zero Trust Security

Zero trust is very hot now in the cybersecurity world, but the concept of zero trust was not proposed by cybersecurity giants, but by John Kindervag, chief analyst of market research firm Forrester, in 2010. It is neither a technology nor a product, but a new security concept whose basic principle is "Never Trust, Always Verify". This provides unlimited imagination space for manufacturers who join this field. Everyone can develop their own zero trust security products and solutions according to their own specialties and products. However, overall, zero trust security is still ecologically decentralized and barbaric growing, different providers have different understandings of the basic concepts and technical paths of zero trust. The author has been engaged in Internet trust services for 17 years. From how to solve the trust problem, I will talk about the four misunderstandings of zero trust security in this article.

Misunderstanding #1: Ignoring the always verification of website identity

Speaking of zero trust, everyone knows that the identity of the user needs to be always verified. The author believes that all the zero trust solutions on the market currently ignore the always verification of one important element, that is, the always verification of the website identity, which is a huge mistake in technical direction, this is the number one misunderstanding.

Websites are the largest traffic on the Internet. If the always verification of website identity is ignored, the user's always verification will lose any meaning, because if the user's identity that has passed the always verified is trusted, but this trusted user visited a fake fraudulent website, that is very insecure access, and a real identity fell into the hands of the fraudulent website.

How to realize always verifying the identity of the website, of course, you must first validate the identity of the website, and always verify the identity every time you visit. It is the SSL certificate that implements this always-validate, and it is the browser that performs the always-verify task. Therefore, all browsers now display websites that have not passed identity validation as "Not secure". Only through identity validation can an SSL certificate be issued and deployed on the website to achieve https encrypted transmission, and the browser will not display as "Not secure", the security padlock is displayed instead. Because the SSL certificate has the dual function of proving the identity of the website and encrypting the transmission.

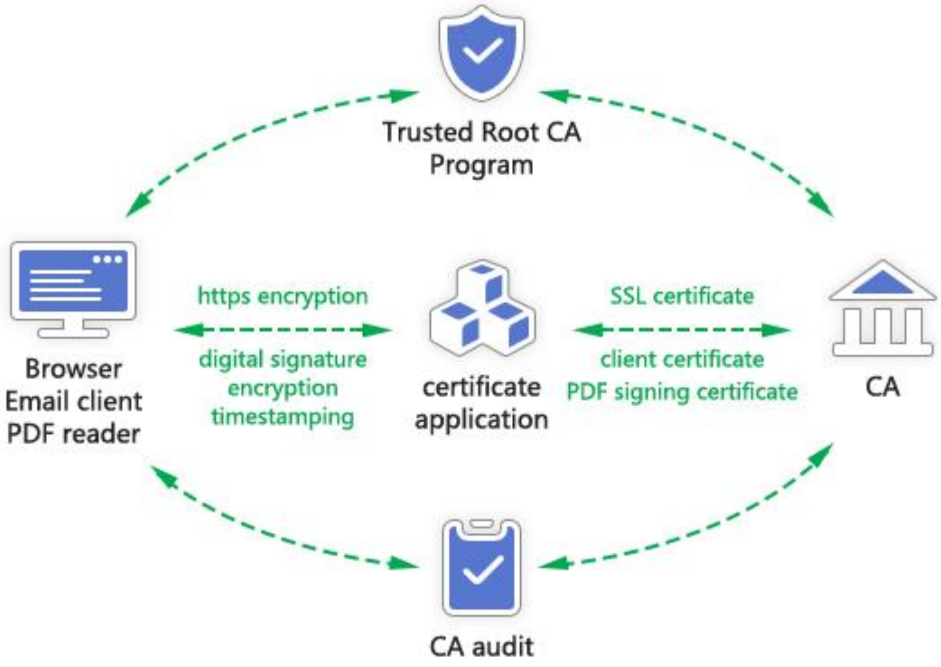
The first principle of zero trust should be never trust websites that are not validated by third parties, and the second is never trust the identity of the user who wants to visit the website and always verify the user's identity. This order cannot be wrong, nor can it be emphasized that only the identity of the user is verified. Only when the website has passed the identity validation by a third party (such as a CA), deployed an SSL certificate to realize https encryption, and then verified the user's identity every time, this is a complete zero trust security chain, can it truly ensure that the "right person" has accessed the "right" website.

The number one misunderstanding of zero trust is that it only cares about always verifying the identity of the user, while ignoring the always verification of the identity of the website on the server side.

Misunderstanding #2: **Ignoring the existing Internet trust ecosystem**

The existing Internet trust ecosystem is the WebTrust system, which is to solve the problem of Internet trust. To put it simply, the SSL certificate is issued by the CA to prove the trusted identity of the website and is used for https encryption of the website transmission. The operating system manufacturer or browser manufacturer has a root certificate trust program that trusts the SSL certificates issued by some CAs. The "CA/Browser Forum", an international organization jointly formed by CA and browser manufacturers, is responsible for formulating technical standards for CA business, and Canadian CPA is responsible for formulating auditing standards based on the technical standards. This standard is WebTrust for CA, Canada CPA certifies some accounting firms to be qualified to engage in WebTrust audit business, CA companies need to be audited by the WebTrust auditor every year, after passing the audit, CA can get the WebTrust audit report, and submit it to the browser manufacturer to include the CA root certificate or continue to be trusted, then CA can continue to issue publicly trusted SSL certificates and other certificates.

This is a closed-loop trust authentication delivery eco-mechanism, it ensures the normal operation of the WebTrust system, thereby ensuring the secure and rapid development of the global Internet. The CA company is called a Trust Service Provider (TSP) in Europe, because the CA company is responsible for using cryptographic technology (PKI) to issue digital identity certificates for users to solve trust problems. Now that the concept of zero trust security has emerged, the existing well-functioning global Internet trust ecosystem cannot be ignored and must be supplemented and expanded on this basis.



Misunderstanding #4: Forgetting or not knowing what technology is really for solving trust problems

In misunderstanding #2, I told you how the Internet currently solves the problem of trust, which can be extended to the Internet of Everything. The only reliable technologies to solve the trust problem are cryptographic and PKI technology. PKI (public key infrastructure) was born to solve the trust problem and to solve the data security. PKI technology completely solves (1) the confidentiality of data (**Privacy**); (2) the identity authenticity of data producers and users (**Authentication**); (3) the integrity of data (**Integrity**); (4) data generation behavior and usage behavior non-repudiation (**Non-repudiation**), the four headaches (**PAIN**) data security problems. The solution to these headaches is to solve the problem of trust and data security. PKI is the only reliable technology to solve the problem of trust. Only when the concept of zero trust is closely combined with PKI can the problem of trust and the target of the of trust - data security be truly and completely solved.

The zero trust security solution of ZoTrus Technology is the security practice of zero trust principle plus cryptographic technology. Our solution is not to replace the existing cyber security solutions and discard the existing security protection devices and systems, but to plan and implement zero trust security solutions on existing protection devices and systems, transforming existing systems gradually support zero trust security.

Misunderstanding #4 Forgetting why zero trust is implementing

The reason why zero trust is only popular after 10 years is because the current cyber security protection mechanism has hit the ceiling. It is no longer possible to get out of the dead cycle of "as virtue rises one foot, vice rises ten", especially due to the work-at-home caused by the pandemic, users have to think about how to solve the traditional firewall and internal-external network security mechanisms that can no longer work, because the traditional security mechanism is unlimited trust for one-time authentication and unlimited trust for the intranet, but now there is no intranet, what to do? In this way, the concept of zero trust has been recognized by everyone.

Because it is very popular, of course, everyone will rush to chase this so-called "air outlet", and various solutions have also appeared on the stage! However, there are many solutions that may really forget why zero trust is implemented. Some seemingly very complex and dazzling zero trust identity security solutions have indeed achieved "never trust, always verify", but after verification, the user data is transmitted to the user in http cleartext, such a zero trust identity authentication scheme is useful? Even some zero trust authentication systems based on usernames and passwords do not deploy SSL certificates to ensure the security of usernames and passwords! Can such a solution work?

The goal of any security solution is to protect data, to allow the "right person" to access the "right server" and get the "right data".

The same is true for the purpose of zero trust security, which is to protect user data from being illegally obtained and used illegally, not just for identity authentication! This is the second biggest misunderstanding of zero trust, forgetting why we want to implement zero trust.

In conclusion, zero trust always-verify is not the purpose, protecting data assets and ensuring data security is the purpose. The zero trust system must be that both the user on the client side and the website on the server side need to be always verified, and both sides can use digital certificates to achieve always-verify. Zero trust security based on cryptographic technology is not only suitable for Internet security, but also for Internet of Things security, Internet of Vehicles security, and Industrial Internet security. Zero trust is a journey, and cybersecurity is actually constantly evolving towards zero trust.

Richard Wang

Dec 24, 2021
In Shenzhen, China