Security in remote access, based on Zero Trust Model concepts and SSH authentication with signed certificates

Cristina-Raluca IȚĂ, Rodica-Claudia CONSTANTINESCU, Alexandru VLĂDESCU, Bogdan ALEXANDRESCU
Faculty of Electronics, Telecommunications and Information Technology, Polytechnic University of Bucharest, Bd. Iuliu Maniu, Nr. 1-3, Sector 6, Romania

Introduction

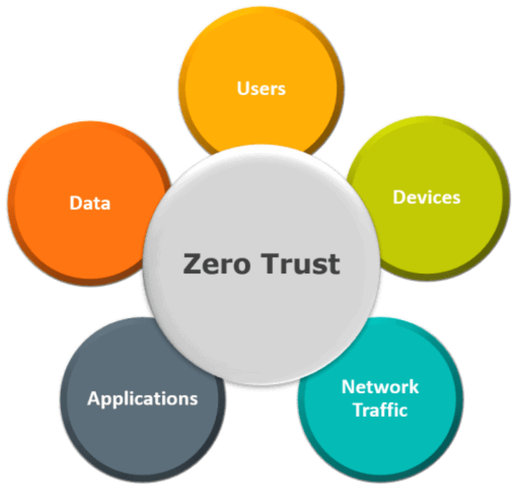
Most organizations have been faced with the need to allow employees, contractors or business partners to use telecommuting technologies to perform tasks from external locations. In order to do this, they use remote access solutions for non-public resources.

When the employee is allowed to access the company's resources through personal devices (laptop, tablet, mobile phone), an additional security analysis is required, even if there is an agreement between the organization and third parties to force these devices to be sure. Such problems are limited to the application of security policies on the equipment and these are generally not applied immediately, which leads to the possibility of introducing a virus into the company's private network.

The organization must assume that external facilities, the Internet, and devices contain threats that will attempt to access the organization's resources and information.

Zero Trust Model

The Zero-Trust model starts from the premise that the entire network is insecure, and protection must be provided from the access area. According to this approach, we cannot trust the devices of users who want to connect to the network, so we need to create mechanisms that build trust.



Zero trust architecture is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

Components of risk analysis

The right approach to identifying the right solutions must be based on a systematic analysis that identifies and addresses the risks.To identify risks, security engineers must identify: protected assets, existing vulnerabilities and possible threats.

Public key infrastructures

Regardless of the methods chosen to secure the transmitted or stored data, data encryption is always a must.

Symmetric key cryptography

It involves using the same key for encryption and decryption.

• The advantage of symmetric key cryptography is the speed of encryption.

• The big disadvantage of symmetric key cryptography is the way the key is distributed.

Asymmetric algorithms

The principle of using public key cryptography or asymmetric cryptography is that each entity generates two keys: a private key and an associated public key.

• The private key, as the name suggests, must be in the possession of the entity that generates and protects it (any incident related to the loss of the private key leads to a change of pair),

• The public key, as the name suggests, is public (can be distributed on unsafe channels).

The relationship between the two keys is as follows: everything that is encrypted with the public key can be decrypted using the private key and vice versa.

The disadvantage of public key encryption is that it is slow and cannot be used to encrypt large volumes of data.

The advantage of public key encryption is related to how the key can be distributed.

Principle and importance of secure access to resources

Consistent security controls and high reliability are common expectations for any system administrator. Most standard solutions require a compromise in at least one of these areas.

Most system administrators use industry standard Secure Shell to access systems. We take advantage of features to use SSH in a way that is reliable, secure, and manageable. SSH, more precisely OpenSSH, has a great way to provide both the security and the reliability we need.

In addition to the risks of central management failure, opting for public path authentication instead of user passwords means managing public passwords on all servers. If the administrative header was not long enough, it is not uncommon to compromise your own person who publishes unknowns in authorized_keys files. In addition, authorized_keys require the definition of trust by individual key pairs, which are not scalable.

Importance and configuration

From the configuration point of view, there are some key steps that are followed:

• Creating a certification authentication by defining a private key and a public key

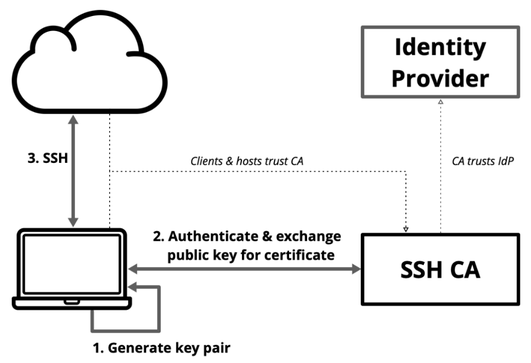
• Distribution of the public key to all servers involved

• Configure servers to trust the created authority

• Customer certificates are generated

• Subsequently, authentication is performed on any of the servers that allow this type of authentication.

The steps to follow are not very complicated, but of course they will be automated through scripts and the solution will be integrated with other company solutions.



Conclusions

The aim of the project is to make an analysis based on basic security concepts but also by analyzing the new concepts that appeared in the module, which is based on the principle of not trusting any device and any person, regardless of location. from which data is accessed. Most security solutions already developed raise the issue of remote access only to resources, without ensuring a verification of devices in private networks.

The access solution on the proposed remote resources, achieved through a certificate-based authentication, offers both security and ease of account management. Representing a first step in the development of architectures based on the Zero Trust model.

There is a lot of information on this subject, so I think a summary of the key points of such access is absolutely necessary.

Literature cited

- NIST Special Publication 800-207
- NIST Special Publication 800-114
- Allison Wylde, "Zero trust: Never trust, always verify", Published in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),
- DOI: 10.1109/CyberSA52016.2021.9478244, Electronic ISBN:978-1-6654-2529-2, Print on Demand(PoD) ISBN:978-1-6654-3092-0, Date of Conference: 14-18 June 2021, Conference Location: Dublin, Ireland.
- Sourabh Chandra; Sk Safikul Alam; Smita Paira; Goutam Sanyal; "A comparative survey of symmetric and asymmetric key cryptography", Published in: 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Date of Conference: 17-18 Nov. 2014, Conference Location: Hosur, India, DOI:10.1109/ICECCE.2014.7086640, Electronic ISBN: 978-1-4799-5748-4

ATOM-N 2022