Remme Whitepaper

Abstract

Nowadays, the main method of accessing various local and network resources is a password, that has proven itself as a way of identifying and securing users and resources. However, it has one serious drawback: in case of stealing a password, an attacker gets access to all the data of the user who owned this password. In addition, users usually have the same password for multiple services, the situation
gets even worse because these passwords can be weak or even be a subject for vocabulary attack. Password databases from a variety of resources periodically fall
into open access. In general, even if the resource provides the ability to change the password, this method is somewhat vulnerable, since the user's mailboxes are usually protected by a password, often the same as that used on other resources. Thus, the password can not serve as a sufficient instrument for protecting user data
and guarantee the security of the user session.

An approach to this problem is password managers. This software, which provides
a secure storage for passwords, and, in the case of integration as a browser extension, is able to withstand numerous ways of stealing passwords. Also, password managers are often able to generate secure passwords that are unique to each resource, which takes security to a new level. The obvious drawback of such protection is that the storage is protected with a master password (Lastpass, 1Password), and in case of theft or brute force the master password, it all boils down to the previous thesis.

Two-factor authentication provides a partial solution of password problems. For two-factor authentication, in addition to the password, it is required to provide the
resource with some more data that should be available only to a particular user. Examples of the second factor:
1) One-time passwords that are generated every n seconds are the most common option. Usually implemented with TOTP protocol.
2) One-time passwords sent in the message. Usually, SMS or instant messengers is used.
3) Hardware tokens.

Archived copy · cryp2nova.com

Another way of authorizing a user into the system is SSL/TLS certificates, which are
widely adopted in enterprise solutions, such as banking, tax services, etc.
A system of Public Key Infrastructure supports the creation, distribution and identification of public encryption keys, enabling users and systems to both securely exchange data over untrusted environment such as the Internet as well as
verify the identity of the other party of conversation. PKI provides possibilities for digital signature (confirmation of authentication, non-repudiation and message integrity), data encryption (confidentiality during data storing, transfer and processing) and authorization in one complex system.

The core of PKI – the public key encryption systems (a private key for encryption, a
public key for decryption) based on strong mathematical approaches. But simple presence of public/private key is not enough for trust. There should be a complex and comprehensive system with all functions listed above.

Typically PKI consists of a lot of controls beginning from policies and standards through administration and management to software and hardware. PKI can be realized in different architectures: simple, network, hierarchy etc. But we should understand that the heart of PKI is digital certificates. A digital certificate is a document designed to affirm the identity (user, system etc.) of the certificate subject and bind that identity to the public key contained in the certificate.

The typical scheme of PKI includes next elements:
• Certification Authority (CA) – a trusted party provides services for issue digital certificates.
• Registration Authority (RA) – a trusted party responsible for accepting requests for digital certificates and authenticating the entity making the request. Sometimes RA also called subordinate CA.
• Validation Authority (VA) – a trusted party provides a service used to verify the validity of a digital certificate. It's clear that different VA should has database of valid certificates, revoked certificates and communication with different CA.

As we can see, functioning of PKI based on trusted authorities with different functions.

From our point of view we should focus on several core issues. First of all, PKI now
is government regulated or business driven ecosystem depends on a sector of application. Government CA and PKI at all usually are not acceptable for wide public or SMB use according to different limitations and application lockin. For example, specific CA works with specific tax reporting software. Services of

Archived copy · cryp2nova.com

business CA very often expensive and there is a collusion between software vendors and CA for including specific CA into a list of trusted for this software. For example, web browsers don't accept all certificates issued by different CA. Sometimes ago it was a brilliant vision named "web of trust" were most of noted problems could be resolved with teamwork of count of CA/VA/RA. Unfortunately, it left just as vision according to the disagreement s CA to work in a single network
of trust.

Our team works on solving those problems by implementing decentralized public key infrastructure based on blockchain technology. The chosen approach will give our end customers the way of managing their PKI with a high level of security and all advantages of decentralized and distributed system, including fault tolerance.

Advantages of REMME:
1. There is no centralized database of certificates and keys that could be compromised.
2. There are no technology lockin and API limitations. Easy integration with existing systems.
3. There are no additional fees for different certificates/credentials in different CA.
4. There are no possibilities for collusion between software/hardware vendors and limited count of CAs.
5. Fast and protected public key distribution process.
6. Fast and protected certificate revocation process.
7. Single point of trust for different systems: easy single-sign-on implementation, decentralized worldwide available authorization.
8. There are no legal limitations and government cooperation issues.
Additional advantages:
1. Acceptable for different types multi-factor authentication.
2. Full anonymity.
3. It allows to track all issued certificates, provides complete and transparent control.

REMME is bringing blockchain to PKI infrastructure providing immutability of data stored there.

For simple user it could look complicated, but all is simple: you don't need to remember count of login and passwords, you don't need to pay five or ten authorities for certificates used in tax, legal, bank, technical or other types of software, you don't need to control the live time of each password/certificate/key.

Remme Website
Remme Whitepaper

Archived copy · cryp2nova.com

Social

Archived copy · cryp2nova.com