Public key infrastrcture: A literature survey

Andrei Titu

November 14, 2023

Abstract

Embraced by both small enterprises and large corporations alike, public key infrastructure (PKI) serves as a cybersecurity technique for verifying, validating, and safeguarding digital information. Authentication, validation, and authorization of identities play a pivotal role in the realm of cybersecurity for all types of organizations. Originally stemming from the British intelligence community in the early 1970s, employing PKI for authentication and encryption has been in practical use within commercial contexts for more than two decades. However, choosing or designing the suitable PKI remains an unsolved problem as there simply isn't a one-fits-all solution. One must inquire whether there exists a one-fits-most solution nevertheless.

1 Introduction

The implications of public key cryptography extend far beyond individual transactions or secure email exchanges. Its integration into the fabric of digital infrastructure has ushered in transformative shifts in the realms of e-commerce, secure communication protocols, and the very structure of our digital identities. It underpins the security and authenticity of websites we visit daily, safeguarding our personal information from prying eyes. Public key infrastructure (PKI), which manages the creation, distribution, and revocation of digital certificates, has emerged as a crucial component of digital trust. Moreover, public key cryptography plays a pivotal role in the development of blockchain technology, enabling the creation of decentralized, tamper-proof ledgers underpinning cryptocurrencies and smart contracts.

The literature survey presented in this essay will offer a panoramic view of the academic, technological, and practical landscape surrounding public key cryptography and its integration into digital infrastructure. By synthesizing key insights, trends, and debates, this paper aims to provide a comprehensive understanding of the current state of knowledge in this dynamic field. Additionally, this reading will delve into the challenges and open questions, as well as the latest developments and future prospects, highlighting the ever-evolving nature of public key cryptography in a world where secure communication and data protection have become indispensable.

2 Background

Before diving deeper into security solutions it is important to understand the actual problems which need solving and define a lens through which alternatives will be looked at. This lens is an evaluation model which will start from the requirements which need to be fulfilled, will look into the extent to which these requirements are fulfilled and the incurred costs for achieving these levels. Most readers will be interested to optimise the balance between increasing the level of guarantees for certain requirements while keeping the cost within some boundaries. In order to systematically introduce this analytic view, the current section will present a very brief history of the space and introduce the required security concepts.

2.1 History

The history of cryptography is a long and fascinating journey, starting well before the Enigma machine and continuing to the present day. Here's a chronological overview of some key developments in the history of cryptography:

Ancient Ciphers: Cryptographic techniques have been used for thousands of years. Early civilizations, such as the Egyptians, Greeks, and Romans, employed simple substitution ciphers to encode messages.

Caesar Cipher: Julius Caesar is known to have used a simple substitution cipher known as the Caesar Cipher, where each letter is shifted a fixed number of positions down or up the alphabet.

Vigenère Cipher (16th century): Blaise de Vigenère created a more complex polyalphabetic cipher that used a keyword to determine the shift for each letter, making it harder to crack.

Frequency Analysis: In the 9th century, the Arab polymath Al-Kindi wrote a treatise on cryptography that included the earliest known description of frequency analysis, a technique used to break monoalphabetic ciphers by analyzing the frequency of letters in a language.

The Great Cipher (17th century): The Great Cipher of Louis XIV, developed by Antoine and Bonaventure Rossignol, was a polyalphabetic substitution cipher that remained unbroken for over 200 years.

Playfair Cipher (19th century): Developed by Charles Wheatstone and independently by Lyon Playfair, this digraph substitution cipher was widely used in the 19th and early 20th centuries.

World War I: Both sides in World War I used various cryptographic techniques to protect their communications. Notably, the Germans used the ADFGVX cipher, which was broken by the French.

Enigma Machine (20th century): Developed by the Germans during World War II, the Enigma machine was a complex electromechanical cipher machine. Allied codebreakers, including British mathematician Alan Turing, successfully cracked the Enigma code, a significant turning point in the war.

Public Key Cryptography (1970s): Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography, a revolutionary advancement that allowed for secure communication over insecure channels. This laid the foundation for modern encryption methods like RSA and ECC.

Data Encryption Standard (DES): In the 1970s, the U.S. National Institute of Standards and Technology (NIST) introduced the Data Encryption Standard, a widely used symmetric-key encryption algorithm.

Rise of Internet Cryptography: With the growth of the internet, encryption became crucial for securing online communications. Protocols like SSL/TLS and cryptographic algorithms like RSA and AES were developed to ensure data security online.

Advanced Encryption Standard (AES): AES became the successor to DES and is widely used for encrypting data today.

Elliptic Curve Cryptography (ECC): ECC is a popular asymmetric encryption technique used in modern cryptographic systems. It offers strong security with smaller key sizes.

Quantum Cryptography: As quantum computing technology advances, quantum-resistant cryptography is becoming an area of active research to protect against potential threats posed by quantum computers to existing encryption methods.

Blockchain and Cryptocurrencies: Technologies like blockchain and cryptocurrencies such as Bitcoin rely heavily on cryptographic principles to provide security and enable decentralized transactions.

Post-Quantum Cryptography: Researchers are actively working on post-quantum cryptographic algorithms that can withstand the potential threat of quantum computers. NIST is leading standardization efforts in this area.

2.2 Public Key Cryptography (PKC)

Public key cryptography, also known as asymmetric cryptography, is a cryptographic system that uses a pair of keys: a public key and a private key, to secure digital communication and data. Each key in the pair has a specific role:

Public Key: This key is intended to be shared openly and is used for encryption. Anyone can use the public key to encrypt a message or data, but only the holder of the corresponding private key can decrypt it. Public keys are used for confidentiality and data protection.

Private Key: The private key is kept secret and known only to the owner. It is used for decryption and digital signature generation. When someone receives an encrypted message or digital signature created with the public key, they use their private key to decrypt it or verify the signature's authenticity.

Real world problems which are currently solved with PKC: symmetric key exchange, secure communication, SSL/TLS connections, S/MIME encrypted email, secret management, access control, secure data storage, code signing, document sharing, enforcing regulations and compliance, secure remote access (via SSH keys), Bitcoin etc.

2.3 Security requirements

Nowadays, in the case of most projects the security requirements which need to be fulfilled stem out of five root concepts: authentication, integrity, confidentiality, non-repudiation and, in some cases, authorization.

Confidentiality: Definition: Confidentiality ensures that information remains private between the parties for which its exposure was intended. Systems leverage both public (asymmetric) and secret (symmetric) cryptography for confidentiality. While public key cryptography is less efficient for large data, it is suitable for encrypting small data objects, such as symmetric encryption keys. Secret key cryptography is often used in PKIs for bulk data encryption, providing actual confidentiality.

Integrity: This concept ensures that data cannot be corrupted or modified, and the integrity of transactions remains intact. For this task, PKIs use public key cryptography along with hashing algorithms (e.g., SHA-1 or MD5). For example, a Message Authentication Code (MAC) can be generated using secret key cryptography in a PKI environment. However, using symmetric cryptographic systems for integrity in a PKI may not scale well, so public key cryptography, combined with hashing, is typically more efficient.

Authentication: Authentication involves verifying the identities of entities using public key certificates and digital signatures. As a result, plain PKC can't guarantee the authenticity of a sender after a certain extent, but PKIs excel at it.

Non-Repudiation: This concept ensures that data cannot be denied or transactions disavowed. It is achieved through digital signatures in public key cryptography. Non-repudiation is a crucial security service in e-commerce, legal, and contractual negotiations. It is a by-product of using public key cryptography. When data is cryptographically signed with a private key, anyone with the corresponding public key can verify that only the key's owner could have signed the data. This underscores the importance of securely protecting private keys used for digital signatures.

Public key cryptography ensures all of the above to some degree, but by itself is vulnerable to a range of attacks, particularly with regard to authenticity. The hard question is: how can someone know for sure that the public key they are encrypting their precious data with really belongs to the intended receiver? For gaining insights into what a secure system needs to watch out for, some studied adversarial models will be reviewed.

2.4 Adversarial models

Equally notable is the existence and perpetual development of attack models looking to exploit insufficient guarantees in one of the 5 concepts from above.

Confidentiality

Eavesdropping: Attackers intercept and monitor data transmission, attempting to decrypt or gain access to sensitive information.

Brute Force Attacks: Attackers attempt to break encryption by trying all possible decryption keys, particularly with symmetric encryption.

Integrity

Data Tampering: Attackers modify data during transmission, potentially altering the content of messages, documents, or transactions.

Replay Attacks: Attackers capture legitimate data and replay it, causing actions to be performed multiple times, potentially leading to unauthorized operations.

Authentication:

Man-in-the-Middle (MitM) Attacks: Attackers intercept communication between two parties, potentially altering or eavesdropping on the messages, while both parties believe they are securely communicating with each other. This is usually the most encountered and feared attack when it comes to large ecosystems with a lot of communicating actors.

To guarantee the authenticity of a public key, the traditional PKC uses a certificate that is a digitally signed statement binding an entity and his public key. Since the amount of keys to manage and operations to perform seem to multiply, here is where the need for some designated architecture come in. This architecture is what's been refferred to as public key infrastructure.

Identity Theft: Attackers impersonate a legitimate entity by stealing or compromising private keys, allowing them to masquerade as the entity.

Non-repudiation:

Key Compromise: If a private key is compromised, an attacker may falsely sign data, leading to non-repudiation failures.

Forgery: Attackers may create counterfeit digital signatures or manipulate digital signatures, leading to false non-repudiation claims.

2.5 Required Infrastructure

A few suplimentary measures can go a long way in raising security guarantees in each of the aforementioned security services. A few of these measures are: digital certificates, multi-factor authentication (MFA), role-based access control, auditing, security information and event management (SIEM), zero trust security model, intrusion detection and prevention systems (IDPS), vulnerability scanning etc. All these various endeavours will require infrastructure so they can exist. On the other hand, the clear need for public key infrastructure supporting certificates is considered the main difficulty in the deployment and management of traditional PKC.

However, it is important to understand that a such infrastructure is not by itself an authentication, authorization, auditing, privacy, or integrity mechanism. Rather, a it is mearly an enabling factor that supports these various business and technical needs. For example, a PKI does not infer trust by itself, but requires the establishment of a trust base, on which the PKI can rely. This requirement means that the basis of trust must be established on a personal, business, or other level, before it can be accepted by the PKI. The problem of firstly authenticating a entity will remain a hard one, and must be tackled in isolation.

3 Traditional PKI

A PKI enables the establishment of a trust hierarchy. This is one of the primary principles of a PKI. In Internet-based e-commerce, formal trust mechanisms must exist to provide risk management controls. The concept of trust, relative to a PKI, can be explained by the role of the CA. In the Internet environment, entities unknown to each other do not have sufficient trust established between them to perform business, contractual, legal, or other types of transactions. The implementation of a PKI using a CA provides this trust.

A Public Key Infrastructure (PKI) is a comprehensive system of hardware, software, policies, standards, and practices that work together to provide a framework for secure communications and authentication. It is used to manage digital keys and certificates. PKIs are commonly used for tasks like securing email communications, establishing secure connections over the internet (e.g., SSL/TLS), and for digital signatures. Here are the key components of a PKI:

Certificate Authority (CA):

Root CAs are the highest-level CAs in the hierarchy. It issues and signs intermediate CAs' certificates. Intermediate CA: These CAs are subordinate to the root CA and issue certificates to end entities. They can also sign other intermediate CA certificates. End Entities: These are the users, devices, or servers that require certificates issued by the PKI to authenticate themselves or secure communications.

Digital Certificates: Certificates bind a public key to the entity's identity. They include information such as the public key, the entity's name, the digital signature of the issuing CA, and the certificate's expiration date.

Public and Private Key Pairs: End entities generate and keep private keys secure. Public keys are shared widely and included in certificates.

Registration Authority (RA): The RA verifies the identity of entities before they are issued a certificate. It acts as an interface between the end entity and the CA.

Certificate Repository: A secure location for storing issued certificates, making them available for validation and lookup.

Certificate Revocation Lists (CRLs): Lists of certificates that have been revoked by the CA before their expiration date. Clients and applications can use CRLs to check the status of certificates.

Certificate Policy and Practice Statements (CP/CPS): These documents outline the PKI's operational and security practices, including how certificates are issued, managed, and revoked.

Key Management System: A system for securely generating, storing, and managing cryptographic keys. It should ensure the security of private keys.

Security Protocols and Standards: The PKI should adhere to industry-standard security protocols and standards, such as X.509 for certificate formats, TLS for secure communications, and OCSP for real-time certificate status checks.

Secure Hardware: The CA's private key should be stored securely, often in hardware security modules (HSMs), to protect against theft or tampering.

Auditing and Monitoring: Regular monitoring of the PKI infrastructure to detect and respond to security incidents or anomalies.

Backup and Recovery: Procedures for backup and recovery of CA keys and data in case of hardware failure or disaster.

Cross-Certification: When operating in a distributed environment, PKIs may need to establish trust with external PKIs through cross-certification.

Compliance and Legal Requirements: Compliance with relevant laws and regulations, including data protection and privacy laws, may be required. Additionally, adherence to any industry-specific standards or requirements is essential.

User Education and Training: Training and education programs for users to understand how to use certificates and secure communication channels.

Scalability and Redundancy: The PKI should be designed to scale as the organization grows, and it should incorporate redundancy for high availability.

Lifecycle Management: This involves the management of certificate lifecycles, including issuance, renewal, and revocation.

Secure Communication: All communication within the PKI should be secure, including the transmission of certificates, CRLs, and certificate revocation information.

Policy Enforcement: Ensure that policies regarding certificate issuance, usage, and revocation are consistently enforced.