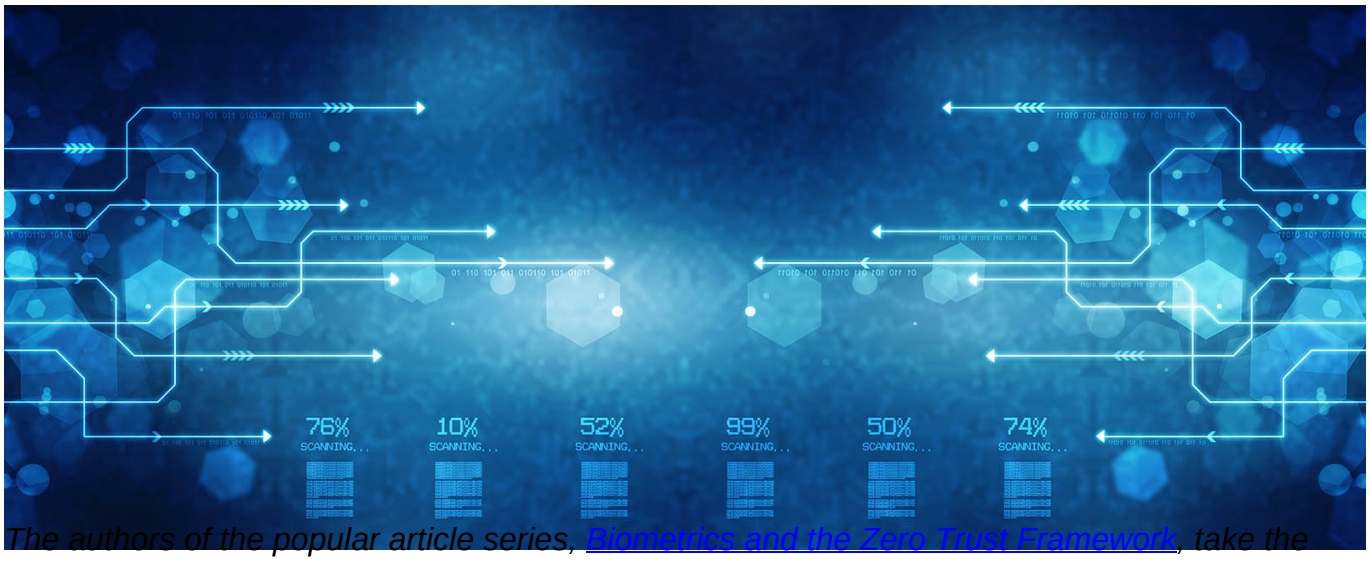
ZTF: The Secret to Seamless Authentication: Part 2

Author :



The authors of the popular article series, Biometrics and the Zero Trust Framework, take the topic to the next level in their new book, ZTF: The Secret To A Seamless Authentication Experience (on Amazon). Previously, the authors explained how cryptography is used to protect data, communications, and identity—as well as the types of cryptographic attacks and counterattacks that play out in Cyberspace.

Here, they consider the future of cryptography by examining emerging trends and advances.

The Future of Cryptography: Emerging Trends and Advances

With the advancements in technology and the growing need for secure communication and data protection, cryptography is becoming increasingly important.

Here are some emerging trends and advances in cryptography:

- **Quantum Cryptography:** Quantum cryptography uses the principles of quantum mechanics to securely transmit information. Unlike traditional encryption methods, quantum cryptography provides guaranteed secure communication as it is based on the laws of physics. The key feature of quantum cryptography is the use of quantum bits, or qubits, instead of classical bits. These qubits can be in multiple states at the same time, making it impossible for an eavesdropper to intercept the information without altering it. This makes quantum cryptography highly secure and is expected to be widely adopted in the future. We will see more about quantum cryptography in the following chapters.
- **Post-Quantum Cryptography:** As quantum computers become more advanced, they are expected to be able to break traditional encryption methods. To prepare for this, a new generation of cryptography algorithms is being developed, known as post-quantum cryptography. These algorithms use mathematical problems that are believed to be resistant to quantum computers, ensuring the security of communication even in the presence of a quantum computer.

- **Homomorphic Encryption:** Homomorphic encryption is a type of encryption that allows computations to be performed on ciphertext, producing an encrypted result which, when decrypted, is equivalent to the result of the computation performed on plaintext. This enables sensitive information to be processed without having to first decrypt it, thus maintaining the privacy of the data.
- **Zero-Knowledge Proofs:** Zero-knowledge proofs are a concept in cryptography that allows one party (the prover) to prove to another party (the verifier) that they know a specific piece of information, without revealing the information itself. In other words, zero-knowledge proofs allow for verifiable statements to be made without revealing any underlying data.

The importance of zero-knowledge proof lies in their ability to protect privacy while still allowing for verifiable statements to be made. They have a wide range of applications in areas such as finance, identity verification, and voting systems. In finance, zero-knowledge proofs can be used to prove the authenticity of financial transactions without revealing the underlying details, such as account balances or the identities of the parties involved. In identity verification, zero-knowledge proofs can be used to prove that a person is over a certain age without revealing their date of birth. And in voting systems, zero-knowledge proofs can be used to ensure the privacy and integrity of voting results.

Zero-knowledge proofs are based on mathematical algorithms that allow for the creation of proof systems. These proof systems are designed to be both computationally sound (i.e., it is not possible to generate false proofs) and zero-knowledge (i.e., no information is revealed during the proof process). The most well-known zero-knowledge proof system is called ZK-SNARK, which stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge." ZK-SNARKs have been widely adopted in various applications, including cryptocurrency and blockchain technology.

In the context of blockchain technology, zero-knowledge proofs play a crucial role in maintaining the privacy and security of the network. For example, in the cryptocurrency ZCash, zero-knowledge proofs are used to ensure that transactions can be verified without revealing any information about the sender, receiver, or amount involved. This allows for greater privacy and security compared to other cryptocurrencies that store all transaction information on a public ledger.

The future of zero-knowledge proofs is bright, with ongoing research and development aimed at improving their efficiency and scalability. With the increasing importance of privacy and security in the digital world, zero-knowledge proofs are poised to play an increasingly significant role in a variety of industries and applications. Additionally, the development of new zero-knowledge proof systems, such as ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge), holds the potential to further improve the efficiency and scalability of zero-knowledge proofs.

They are a powerful tool for ensuring privacy and security in a wide range of applications and allow for verifiable statements to be made without revealing any underlying information, and their importance is likely to continue to grow as privacy concerns increase in the digital world. With ongoing research and development, the future of zero-knowledge proofs looks bright, and it will be exciting to see where this technology goes in the coming years.

- **Blockchain Cryptography:** Blockchain technology is a decentralized ledger that uses cryptography to secure transactions and protect information. The use of cryptography in blockchain allows for secure and transparent record-keeping, making it ideal for various applications, such as digital currencies and supply chain management.

Blockchain Cryptography refers to the use of cryptographic techniques and algorithms to secure and validate transactions within a blockchain network. The purpose of these cryptographic methods is to ensure the integrity, privacy, and confidentiality of data stored in the blockchain.

Blockchains use public key cryptography to secure and validate transactions. In this method, a pair of public and private keys are used to encrypt and decrypt information. The public key is used for encryption and is shared among the network participants, while the private key is kept secret and is used to decrypt information.

A common cryptographic algorithm used in blockchains is SHA-256, which is a secure hash function that generates a unique digital fingerprint of data. This fingerprint is used to verify the authenticity and integrity of data stored in the blockchain. When a transaction is initiated, the sender uses their private key to encrypt the data, and the recipient uses the sender's public key to decrypt the information.

Another cryptographic technique used in blockchains is called digital signatures. Digital signatures are used to prove that the person who initiates a transaction is indeed the owner of the private key associated with the transaction. Digital signatures use public key cryptography to generate a unique signature for each transaction, which is then verified using the corresponding public key.

Blockchains also use consensus algorithms to validate transactions and add new blocks to the chain. A consensus algorithm is a mechanism that ensures all participants in the network agree on the state of the blockchain. Some common consensus algorithms used in blockchains include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

Proof of Work (PoW) is a consensus algorithm where participants compete to solve a complex mathematical problem. The first participant to solve the problem is allowed to add a new block to the blockchain, and the solution to the problem is included in the block as proof of work. It is used by the Bitcoin network to validate transactions and secure the network.

Proof of Stake (PoS) is a consensus algorithm where participants are selected to validate transactions and add new blocks to the chain based on the amount of cryptocurrency they hold in the network. In PoS, participants are incentivized to act honestly and validate transactions truthfully, as their stake in the network is at risk if they act maliciously.

Delegated Proof of Stake (DPoS) is a consensus algorithm where participants vote for a limited number of delegates to validate transactions and add new blocks to the chain. DPoS aims to balance security, scalability, and decentralization, and is used by many blockchain networks, including EOS and TRON.

Blockchain cryptography also helps to ensure the privacy of transactions and the confidentiality of data stored in the blockchain. One common method used to achieve privacy in blockchains is called zero-knowledge proofs. Zero-knowledge proofs are cryptographic techniques that allow one party to prove to another party that a statement is true without revealing any information beyond the fact that the statement is true.

For example, a person can use zero-knowledge proof to prove they are over 18 years old without revealing their actual age. This same principle can be applied to blockchains to prove that a transaction is valid without revealing the details of the transaction. Zero-knowledge proofs are used by many privacy-focused blockchain networks, such as Zcash and Monero.

Cryptography is a rapidly evolving field with new trends and advances emerging all the time. From quantum cryptography to homomorphic encryption, these developments are helping to ensure the security of communication and data in our digital world. These technologies are expected to play a critical role in the future of cryptography, ensuring that information remains secure and private even as technology continues to advance.

Next up: *The next excerpt in this series will address the topic of Privileged Access Management (PAM), which gives human users as well as non-human users (such as applications and machine identities) special access or abilities above and beyond that of a standard user in an enterprise setting.*

Sources/References:

https://purplesec.us/resources/cyber-security-statistics/, February 2023

Aumasson, Jean-Philippe (2021), Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographer. No Starch Press, 2021

Aumasson, Jean-Philippe (2017), Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017

Falconer, John (1685). Cryptomenysis Patefacta, or Art of Secret Information Disclosed Without a Key.

Ferguson, Niels, and Schneier, Bruce (2003). Practical Cryptography, Wiley

Goldreich, Oded (2001 and 2004). Foundations of Cryptography. Cambridge University Press.

Katz, Jonathan and Lindell, Yehuda (2007 and 2014). Introduction to Modern Cryptography

1. J. Menezes, P. C. van Oorschot, and S. A. Vanstone (1996) Handbook of Applied Cryptography

https://www.proofpoint.com/us/resources/threat-reports/state-of-phish , February 2023

Kahn, David – The Codebreakers (1967)

Join the conversation.

GO

Visit Keesing Technologies