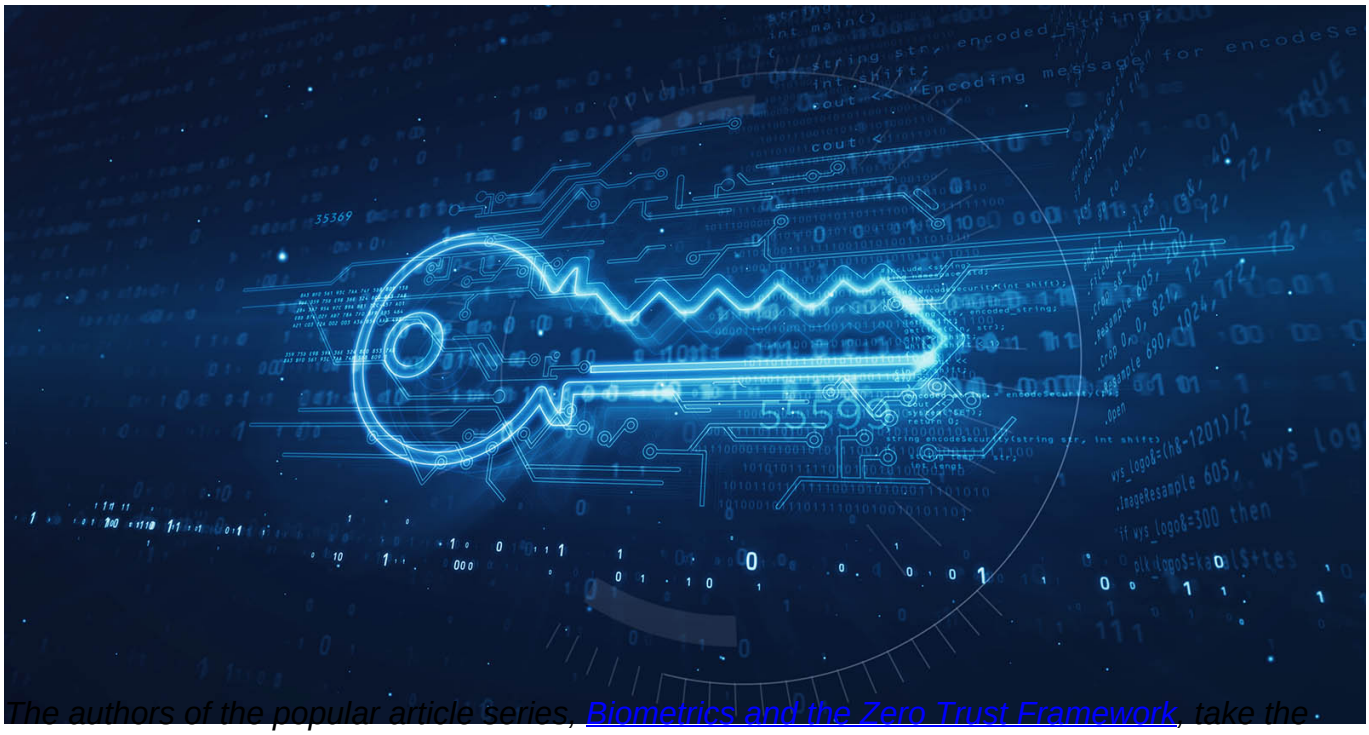
ZTF: The Secret to Seamless Authentication: Part 1

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). This excerpt from the book, you'll learn 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.

Cryptography plays a crucial role in protecting sensitive information and ensuring the privacy and security of data and communications. In this section, we will discuss three major cryptographic applications: protecting data, communications, and identities.

There are three major things achieved by Cryptography: Protecting Data, Protecting Communications and Protecting Identities.

Protecting Data

Cryptography is commonly used to protect the confidentiality of data stored on computers and servers. Data encryption algorithms such as the one we described like, AES, or even some ones that we did not mention such as Rivest Cipher 4 (RC4) are used to encrypt the data, making it unreadable to unauthorized users. Encrypted data can only be decrypted by someone who has the correct decryption key. In the event that the encrypted data is stolen, it will be unreadable to the attacker and the confidentiality of the data will be maintained.

Protecting Communications

Cryptography is also used to protect the privacy of communication between two parties. The most common example of encrypted communication is Secure Sockets Layer (SSL) and its

successor, Transport Layer Security (TLS), which are used to secure the communication between a web browser and a website. When a user visits an SSL/TLS-protected website, the browser and website use a cryptographic protocol to negotiate an encryption key. This encryption key is used to encrypt all subsequent communication between the browser and the website, providing privacy and security for the user's data.

In order to understand encrypted communications, let's use the example of Bob and Alice. Bob wants to send a message to Alice securely, so he encrypts the message using Alice's public key. The encrypted message can only be decrypted using Alice's private key, ensuring that only Alice can read the message. Alice can then reply to Bob using the same process, encrypting her response with Bob's public key.

Protecting Identities

Cryptography is also used to protect the identities of individuals and organizations in a variety of applications. For example, digital certificates are used to verify the identity of websites and ensure that users are communicating with the correct website. Digital certificates contain the public key of the website, along with information about the website's identity and the identity of the certificate authority that issued the certificate. When a user visits a website, the website's digital certificate is verified by the user's browser, ensuring that the user is communicating with the correct website.

Cryptographic Attacks and Countermeasures

Cryptographic systems are the backbone of secure communication and information protection in the digital world. Despite the many advantages of cryptography, it is not immune to attacks and vulnerabilities. This article will provide an overview of the different types of cryptographic attacks and the countermeasures that can be used to protect against them.

- **Brute Force Attack:** A brute force attack is a straightforward and simple method of trying all possible possibilities of a given security measure. An example is trying all combinations of characters in a password to determine the correct one. The attacker starts with the simplest combination, such as "a", and then moves on to the next, such as "aa", and so on, until the correct password is found. This type of attack can be mitigated by using long and complex passwords, and by using password managers to generate and store strong passwords, as well as rate limiters.
- **Dictionary Attack:** A dictionary attack is similar to a brute force attack, but instead of trying all possible combinations of characters, the attacker uses a dictionary of commonly used passwords to try and guess the correct one. This type of attack can be mitigated in the same way.
- **Man-in-the-Middle Attack:** A man-in-the-middle attack occurs when an attacker intercepts and alters communications between two parties. The attacker intercepts the communication, modifies it, and then passes it on to the intended recipient. This type of attack can be mitigated by using encryption and digital signatures to verify the authenticity of communications. It can be seen with multiple names and acronyms, such as monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle, meddler-in-the-middle, manipulator-in-the-middle (MITM), person-in-the-middle (PITM) or adversary-in-the-middle (AiTM) attack, depending on the bibliography. These types of attacks can be very sophisticated and even conducted by state sponsored hackers.

- **Side-Channel Attack:** A side-channel attack is an attack that exploits weaknesses in the implementation of a cryptographic system rather than the cryptography itself. Side-channel attacks take advantage of information leaked by the implementation of a cryptographic algorithm, such as the timing of encryption or the power consumption of a device. This type of attack can be mitigated by implementing secure and efficient cryptography algorithms, and by ensuring that the implementation of these algorithms does not leak sensitive information.
- **Cryptanalysis:** Cryptanalysis is the process of analyzing and breaking cryptographic systems. Cryptanalysis attacks can be divided into two categories: theoretical attacks and practical attacks. Theoretical attacks are mathematical attacks that aim to break the cryptography by analyzing the underlying mathematical structure of the algorithm. Practical attacks are attacks that exploit weaknesses in the implementation of cryptography, such as poor key management or weak random number generation. This type of attack can be mitigated by using strong encryption algorithms, implementing secure key management, and using strong random number generation.
- **Social Engineering Attack:** A social engineering attack is an attack that relies on human interaction and deception. The attacker manipulates or convinces individuals to disclose confidential information or to perform actions that compromise the security of a system. This type of attack can be mitigated by raising awareness of the dangers of social engineering, providing training on how to identify and respond to social engineering attacks, and implementing security controls that limit the access of sensitive information.

According to PurpleSec, 98% are involved in social engineering on some level. It could involve pretending to be a trusted contact to encourage an employee to click a malicious link, pretending to be a reliable institution, like a bank, to capture login credentials, or similar activities designed to gain entry into target systems.

Cryptographic attacks pose a significant threat to the security of cryptographic systems, and it is important to understand and be aware of the different types of attacks that exist and the countermeasures that can be taken to prevent or mitigate them. By using strong encryption algorithms, secure key management, and other security controls, organizations can protect their information and ensure the confidentiality, integrity, and availability of their data.

Next up: *The next article in this series will consider the future of cryptography by examining emerging trends and advances.*

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

Join the conversation.

GO

Visit Keesing Technologies