VILNIUS UNIVERSITY
FACULTY OF MATHEMATICS AND INFORMATICS
INSTITUTE OF COMPUTER SCIENCE
DEPARTMENT OF COMPUTATIONAL AND DATA MODELING

Term project for informational security management course

Biometric authentication

Done by:
Kazimieras Vitkus

Vilnius
2024

Contents

Abbreviations

Biometrics - yada yada yada,
Apple touch ID - bin bang

Introduction

Biometrics, the science of identifying individuals based on their unique physical or behavioral characteristics, has gained significant attention in recent years. With the increasing reliance on digital systems and the growing threat landscape in the cyber world, the integration of biometrics into cybersecurity has become a crucial area of research and development.

In this work, we explore the intersection of biometrics and cybersecurity, focusing on the challenges, opportunities, and implications of using biometric authentication systems in safeguarding sensitive information. We delve into the various biometric modalities, such as fingerprints, iris scans, voice recognition, and facial recognition, and analyze their strengths and vulnerabilities in the context of cybersecurity.

The objective of this study is to provide a comprehensive understanding of the role of biometrics in enhancing security measures and mitigating cyber threats. We examine the potential benefits of biometric authentication, including increased convenience, improved accuracy, and resistance to traditional attack vectors. However, we also address the potential risks and limitations associated with biometric systems, such as privacy concerns, spoofing attacks, and the possibility of data breaches.

By examining real-world case studies and current research advancements, we aim to shed light on the practical implications of biometric technologies in the realm of cybersecurity. Furthermore, we discuss the ethical and legal considerations surrounding the use of biometrics, emphasizing the need for responsible implementation and adherence to privacy regulations.

In conclusion, this work aims to provide a comprehensive overview of biometrics from a cybersecurity perspective. By understanding the strengths, weaknesses, and potential risks associated with biometric authentication systems, we can make informed decisions in designing secure and reliable systems that protect sensitive information in an increasingly interconnected world.

1 Understanding biometric authentication

Looking at biometrics from completely technical perspective it could be defined as the measurament and evaluation of the individual specimens unique biological parameters. By looking at the definition, this technology does not seem as it would be available or even created for humans. However, this is not the case, as biometrics is used in various fields, such as authentication, identification, and access control. Biometrics encompasses the science and technology of measuring and analyzing these distinct traits, enabling accurate and reliable authentication processes. Many people do not even realize how much of their daily activities include biometrics.

1.1 Biometrics for authentification

Biometric authentication is a process of verifying the identity of an individual based on their unique biological characteristics. Biometric authentication relies on a diverse array of physiological and behavioral traits, each possessing unique characteristics that distinguish individuals from one another. Physiological biometrics include fingerprints, iris patterns, facial features, and DNA, while behavioral biometrics encompass patterns such as typing rhythm, voice patterns, and gait. These traits are captured and processed using specialized sensors and algorithms, converting them into digital templates for comparison and verification (Jain, Ross, & Nandakumar, 2016).

The adoption of biometric authentication spans various domains, offering enhanced security and convenience. In access control systems, biometrics replace traditional methods like passwords or access cards, mitigating ecurity risks and improving user experience (Li, Ye, & Wang, 2019). Biometrics also find applications in financial services, border security, healthcare, and consumer electronics, where they play pivotal roles in fraud prevention, identity verification, and user authentication (Amin, Malik, & Gohar, 2020).

1.2 Advantages of biometric authentication

Biometric authentication offers several advantages over traditional authentication methods. First of all, it is more secure due to reliance on unique biological traits or behaviours, which are difficult to replicate or forge. Moreover, biometric authentication tends to be more accurate and reliable than other methods of authentication, once the trait is set up, it is there to stay, but typing in the password 10 times in a row with no mistakes could be challenging.

Biometric methods of authentication offers increased convenience. Users do not need to memorize complex passwords, carry access keys or cards. Including biometrics in the authentication process, could also improve the ergonomics of the devices, for example fingerprint scanner on the back of the phone: unlocking the device while pulling it out of the pocket. Biometric authentication systems also reduce the administrative burden associated with managing passwords, access cards, and other authentication tokens.

Biometric authentication raises users awareness while enlisting for new services - the process of being verified by fulfilling the tasks while on camera requires users to be present and aware of the process.

Identity theft is becoming a growing concern in the digital age, with cybercriminals exploiting vulnerabilities in traditional authentication methods to gain unauthorized access to sensitive information. Biometric authentication offers a robust defense against identity theft, as biometric traits are unique to each individual and cannot be easily replicated or stolen. However, the risk of identity

theft emerges again, with the development of machine learning algorithms, that are getting better at replicating biometric traits, such as facial features.

2 Biometric systems, components and processes

There are various biometric systems, components, and methods that are used to capture, process, and analyze biometric data. These systems are designed to identify and authenticate individuals based on their unique biological traits or behavioral patterns. In this section, we explore the different types of biometric systems, the components that make up these systems, and the methods used to extract and analyze biometric data.

2.1 Biometric sensors

Biometric sensors are specialized devices that capture and analyze unique physiological or behavioral characteristics of individuals for authentication purposes. These sensors are designed to detect and measure specific biometric traits, such as fingerprints, iris patterns, facial features, voice patterns, or hand geometry.

3 Concerns with biomteric applications

4 Future for biometric authentication

Conclusions and Recommendations

Išvados bei rekomendacijos.

References