Department of

Computer Science

ELSEWEDY UNIVERSITY OF TECHNOLOGY
- POLYTECHNIC OF EGYPT -

Hacking The Future

Research Report

Ahmed Eldesouki - 230100444

Fady mahros - 230103236

Marwan Hossam - 230104805

Omar Ahmed - 230104579

Mobarak Yehia - 230104617

Abstract

In light of recent trends and statistics on cyber-crimes, this report brings the reader to the expansion of cybersecurity at its core, analyzing the distinct phases of development of this area, its current state, and its possible directions for the coming years. Starting with outlining the characteristic of cybersecurity and its major objectives, the report indicates that there are three major ways to attain these objectives, which are: compliance-based, risk-based, and ad hoc. Possessing a comprehensive nature, the report begins with a historical perspective on various cyber threats that date back to the 19th century and extends to any future developments. It also delves into various types of modern cyber threats such as Denial-of-Service (DoS) attacks, phishing, malware, and ransomware. This report predicts disturbing possibilities with quantum computing and its correlating influence on cybersecurity and its solutions, denoting that both can be improved or undermined at the same time. While elucidating the current state of IoT, potential threats like supply chain attack and breaching are analyzed as well. Lastly in conclusion, the report explicitly emphasizes the importance of a continual process of researching and advancing different branches of cybersecurity in order to effectively tackle new forms of threats. It points out the necessity for better solutions and more innovative responses to emerging challenges in such an important field.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Overview

Cybersecurity as a whole is the technology and practice used to protect computer systems, applications, devices, and data from cyberattacks, damage, or unauthorized access. It ensures that data remains private, accurate, and accessible. To achieve this goal, three main approaches are commonly used:

- Compliance-based: A set of rules created to protect systems from common threats.
- Risk-based: A method designed after identifying risks in a system to apply specific solutions for those threats.
- Ad hoc: A flexible approach where a tester tries to break into the system repeatedly, improving it until no more weaknesses can be found.

Figure 1. the three main cybersecurity approaches

1.2 Importance of Cybersecurity in the New World

With cyber threats evolving at a fast rate, cybersecurity is more important than ever before. It stops identity theft, protects national security, keeps private information like banking details safe, and safeguards business secrets from competitors' hackers.

2. The Evolution of Cyber Threats

2.1 History of Cyber Threats

The first known cyberattack happened in France in 1834. Two thieves broke into the telegraph system to steal financial information.

The first computer virus, known as the "RABBITS Virus," was created in 1969 at the University of Washington Computer Center. Its creator remains unknown.

Kevin Mitnick, often called the first true cybercriminal, accessed some of the world's most secure networks between 1970 and 1995.

2.2 Current Shape of Cyber Threats

Due to cyber threats evolving at a fast rate, the list of approaches to gain unauthorized access to data has become large. Some of the new methods to get them include.

- DoS (Denial of Service) attacks: This type of attack sends traffic to the target to lower the performance quality of the service.
- Phishing: This type of attack works by sending an email with a link to a fake web page that looks the same as a login page of a real site (Facebook, Instagram) so that when the target inputs his email and password, the hacker is able to get them for himself.
- Malware: Malware is a dangerous software/virus that steals data and harms the device if the owner of the device is tricked into either downloading the virus or clicking a link containing the virus.
- Ransomware: is a software/virus that blocks access to data on a device and won't stop until a sum of money is paid.

Table 1. Types of Cyber Threats

Threat Type	Description	Example
DoS	Overwhelms a system to make it inaccessible	Targeting websites or servers
Phishing	Deceptive emails to trick users into revealing sensitive information	Fake banking emails
Malware	Malicious software designed to disrupt or damage systems	Trojans, worms, etc.
Ransomware	Encrypt files and demands payment to restore access	WannaCry attack

2.3 Emerging Threats and Trends

In the future, Artificial Intelligence could help with attacks. Hackers would use Artificial Intelligence to attack enemy countries, stealing important information like locations and strategies of the army.

3. Future of cybersecurity

3.1 The Effect of Quantum Computing on cybersecurity

Unlike regular computers that translate input as 0 and 1 individually, (0, 0, 1, 0, 1,1), Quantum computers can take in the 0s and 1s in groups, (00, 10, 01, 11), therefore they can process data at a much faster rate than regular computers. And with the help of quantum computing, the encryption of data is more efficient and secure.

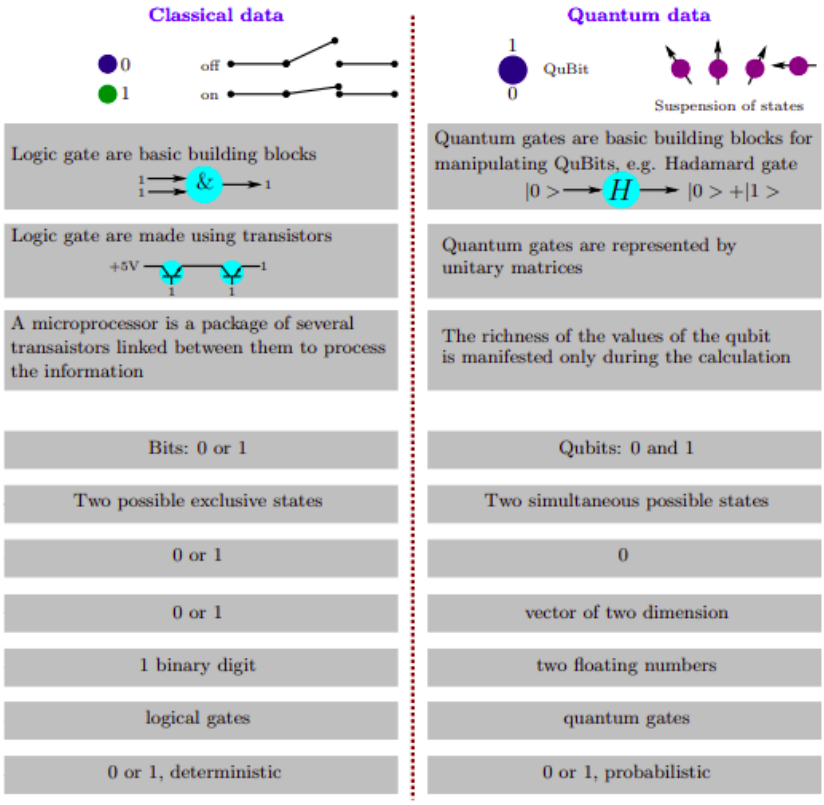

Figure 2. Quantum Computing Process

3.2 The Internet of Things (IoT) and Associated Risks

IoT devices are devices that are connected through a network so that they can easily share data. But the same connection through a network can be abused by cybercriminals, just like how one can easily share data; someone can share a virus just as easily, and so a cybercrime can infect multiple devices by infecting one device that will share the virus on accident. This type of threat is called a supply chain attack.

Table 2. IoT Risks and Mitigation

Risk	Impact	Mitigation
Supply Chain Attacks	Virus spreads across connected devices	Regular software updates
Unauthorized Access	Data theft or manipulation	Strong passwords, encryption

3.3 Possibilities for New Ideas in Cybersecurity

The digital world is constantly changing and so is the wider relevance and concerned to use refined and original means to secure cyberspace. Not only enterprises but also individuals and critical infrastructures are now being targeted as aggressors in the cyber domain, which poses many threats. This ever-changing paradigm presents numerous challenges to the status quo and opens up exciting new avenues to rethink how we protect our vital assets and resources in the cyber space.

- Artificial Intelligence and Machine Learning (AI/ML): Threats can be detected more rapidly, vulnerabilities can be predicted, and action can automatically be taken in response to cyber incidents thanks to the use of AI systems. Big data powered algorithms will be able to sift through large volumes of data sets to look for trends that support anticipated pro-active security expectations.

- Quantum-Resilient Encryption: The rise of quantum computing puts traditional cryptography in great danger of becoming behind the academia itself. Improvements made quantum encryption methods will help secure parties against future quantum threats and maintain critical communications.

- Zero-Trust Architectures: It enables trust to be built on the continuous authentication mechanism, which lowers the dependency on perimeter models due to the insecure upon every access request. Identity and Access Management is itself an enabler and will complement the success of this paradigm shift in business practices.