Basic Computer Science and Cyber Defense Terms

This document provides a comprehensive glossary of basic computer science and cyber defense terms, combining information from various sources to offer a clear and accessible understanding of these fundamental concepts[1].

Introduction to Computer Science

Computer science is the study of computers and computational systems. It encompasses a wide range of topics, from the theoretical foundations of information and computation to the practical applications of designing and building computers and software[14]. This section explores fundamental computer science terms, providing a foundation for understanding how computers work and how they are used to solve problems.

A Brief History of Computing

The history of computing can be traced back to ancient times when tools like the abacus were invented. However, the concept of the modern computer emerged in the 1930s with Alan Turing's theoretical work on computation. The development of the electronic computer in the 1940s marked a significant milestone, leading to the rapid evolution of computing technology. From bulky, slow machines to the ultra-fast, portable devices we use today, computers have transformed the way we live, work, and interact with the world.

Key Computer Science Terms

Abstraction: Simplifying complex systems by focusing on essential features and omitting unnecessary details. This allows for easier understanding and management of complex concepts. For example, representing a complex object with a simple icon or symbol.

Algorithm: A step-by-step procedure or set of rules for solving a problem or performing a computation. Algorithms are essential in computer science for designing efficient programs and are used in various applications, from sorting data to finding the shortest route on a map.

Application: A self-contained program that performs a specific function for end-users. Examples include web browsers, word processors, and games.

Binary: A number system that uses only two symbols, typically 0 and 1. It is the foundation of data representation and computation in digital systems. Each binary digit (bit) represents an on or off state, enabling computers to store and process information.

Bit: A contraction of "Binary Digit." It is the single unit of information in a computer, typically represented as a 0 or 1. Bits are used to represent data and instructions in computers[2].

Bug: An error in a program that prevents it from running as expected. Bugs can cause unexpected

behavior, crashes, or incorrect results. Debugging is the process of finding and fixing these errors.

Byte: A group of 8 bits. It is the most common fundamental unit of digital data. Bytes are used to represent characters, numbers, and other data types[2].

Code: The language that programmers create and use to tell a computer what to do. Code consists of instructions and commands that the computer can understand and execute[2].

Command: An instruction for the computer. Many commands put together makeup algorithms and computer programs. Commands can be used to perform various actions, such as opening a file, running a program, or displaying information[2].

Compiler: A software tool that translates high-level programming code (written in languages like C++, Java, or Python) into machine code that a computer can execute. Compilers analyze the code, check for errors, and generate an executable file[1].

Computer Science: The study of computers and algorithmic processes, including their principles, hardware and software designs, applications, and impact on society. It encompasses a wide range of topics, from theoretical foundations to practical applications[2].

Conditional Statements: Statements that only run under certain conditions. They allow programs to make decisions and execute different code blocks based on specific criteria. For example, an "if" statement checks if a condition is true and executes a block of code only if it is.

Data: Information. Often, quantities, characters, or symbols that are the inputs and outputs of computer programs. Data can be in various forms, such as numbers, text, images, or sound.

Data Structures: Ways to organize and store data in a computer so that it can be accessed and used efficiently. Different data structures are suited for different kinds of tasks. Common data structures include arrays, linked lists, stacks, queues, trees, graphs, and hash tables.

Database: An organized collection of data, typically stored electronically. Databases allow for efficient storage, retrieval, and management of large amounts of data.

Debugging: Finding and fixing problems in an algorithm or program. Debugging is an essential part of software development, ensuring that programs work correctly and produce the desired results[2].

Digital Citizen: Someone who acts safely, responsibly, and respectfully online. Digital citizenship encompasses ethical and responsible use of technology, including respecting privacy, protecting data, and communicating appropriately online[2].

Encryption: The process of converting plaintext or readable data into an encoded form (ciphertext) to protect it from unauthorized access or tampering. Encryption techniques use algorithms and keys to transform data into a format that can only be deciphered with the corresponding decryption key[1].

Function: A piece of code that can be easily called over and over again. Functions perform specific tasks and can be reused throughout a program, improving code organization and efficiency[2].

Hardware: The physical components of a computer system, such as the monitor, keyboard, mouse, and

internal components like the CPU and memory[14].

HTML (Hypertext Markup Language): The standard markup language used for creating web pages and applications. It defines the structure and layout of content on a webpage, using tags and attributes to format and organize text, images, links, and other elements[1].

HTTP (Hypertext Transfer Protocol): The protocol used for transmitting hypertext over the internet. It defines the rules and conventions for how web browsers and servers communicate and exchange data[1].

Input/Output (I/O): The communication between a computer system and external devices or data sources. Input refers to receiving data from external sources, such as a keyboard, mouse, or network. Output refers to sending data from the computer to devices like displays, printers, or network connections[1].

Internet: A global network of computers which are linked, allowing the exchange of data[5].

JavaScript: A programming language used primarily for web development. It is a client-side scripting language that runs in web browsers, allowing interactive and dynamic elements to be added to web pages[1].

Kernel: The central component of an operating system that manages system resources and provides a bridge between software applications and the underlying hardware. The kernel is responsible for memory management, process scheduling, device drivers, and handling system calls[1].

Loop: A programming structure that repeats a sequence of instructions as long as a specific condition is true. Loops are used to automate repetitive tasks and iterate over data[2].

Memory: The internal storage location where data and information are stored on a computer. Memory can be volatile (RAM) or non-volatile (hard drives, SSDs)[11].

Network: A group of two or more computer systems linked together. Networks allow computers to communicate with each other and share resources. There are different types of networks, such as:
* LAN (Local Area Network): Connects devices in a limited area, such as a home, office, or school.
* WAN (Wide Area Network): Covers a larger geographical area, such as a city, country, or the entire world. The internet is an example of a WAN5.
Operating System (OS): The program that enables the computer to start and access different sorts of software on the computer. Examples include Microsoft Windows and iOS for Mac[5].

Programming: Designing, writing, and debugging computer programs that can complete a process or solve a problem. Programming involves using programming languages and algorithms to create software applications[14].

Programming Language: A formal language for representing statements, or commands, and data values used in a program. A programming language has a precise syntax that defines the valid ways for combining the symbols used to denote variables and data values. Examples used in schools include Scratch, Python and SmallBASIC[5].

Programming languages often adhere to different paradigms, or ways of structuring programs. One common paradigm is **object-oriented programming**, which structures software around data, or objects,

rather than functions and logic[25].

Software: The programs and other operating information used by a computer. Software can be categorized into system software (like operating systems) and application software (like web browsers and word processors)[5].

Software Engineering: The application of engineering principles to the design and development of software systems. It involves a systematic approach to building and maintaining software, ensuring that it is reliable, efficient, and meets the needs of its users[13].

Variable: A named storage location that holds a value. Variables are used to store data that can be accessed and manipulated by a program[24].

Key Insight: Algorithms and programming languages are closely related. Algorithms are the foundation of programs, providing the step-by-step procedures for solving problems. Programming languages provide the tools to express those algorithms in a way that computers can understand and execute[1].

Introduction to Cyber Defense

Cyber defense is the practice of protecting computer systems and networks from unauthorized access, use, disclosure, disruption, modification, or destruction[18]. With the increasing reliance on technology and the rise of cyber threats, cybersecurity has become more critical than ever. This section explores fundamental cyber defense terms, providing a foundation for understanding the key concepts and techniques used to protect information and systems.

Key Insight: The importance of cybersecurity is growing rapidly due to the increasing reliance on technology in all aspects of life and the rise of sophisticated cyber threats. Organizations and individuals must prioritize cybersecurity to protect their sensitive data and maintain the integrity and availability of their systems[16].

Key Cyber Defense Terms

Access Control: The practice of regulating who or what can view or use resources in a computing environment. Access control mechanisms ensure that only authorized users and devices can access sensitive data and systems[5].

Advanced Persistent Threat (APT): A sophisticated and stealthy cyber attack conducted by skilled adversaries, such as nation-state actors or organized cybercrime groups. APTs often involve prolonged and targeted attacks to steal sensitive information or disrupt critical infrastructure[5].

Antivirus Software: Software designed to detect, prevent, and remove malicious software (malware) from computers and networks. Antivirus software uses various techniques, such as signature-based detection and behavioral analysis, to identify and neutralize malware threats[3].

Authentication: A security process that ensures and confirms a user's identity when attempting to access a system, resource, or application, often requiring credentials such as passwords, tokens, or biometric verification[11].

Authorization: The process of granting an authenticated user permission to access specific data, resources, or capabilities within a system, based on predefined rules and policies[16].

Backdoor: A hidden method for bypassing normal authentication or encryption in a computer system, a program, or a whole computer network. Backdoors can be used by attackers to gain unauthorized access to systems and data[5].

Baiting: A social engineering attack where a victim is enticed with the promise of a reward to provide confidential information or to perform an action, like downloading malicious software[7].

Botnet: A network of compromised devices infected with malicious software controlled by a remote attacker, often to launch coordinated cyber attacks, distribute malware, and so on[8].

Bring Your Own Device (BYOD): A company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities[7].

Brute-force attack: A cyber attack method where attackers attempt to gain unauthorized access to a system, application, or account by systematically trying all possible combinations of usernames, passwords, or encryption keys until the correct one is found[8].

Cyber espionage: The unauthorized access to computer systems or networks to gain secret information. This can involve stealing sensitive data, such as intellectual property, government secrets, or financial information[5].

Cyber hygiene: The practice of maintaining good cyber security habits and behaviours, such as keeping software up to date, using strong passwords, enabling MFA, avoiding suspicious links or attachments, and regularly backing up data to reduce the risk of cyber attacks and data breaches[8].

Cybersecurity: The application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies[16].

Data Breach: The unauthorized access, disclosure, or exposure of sensitive or confidential information, such as personal data, financial records, or intellectual property, often resulting from cyber attacks, insider threats, or accidental leaks[5].

Data Integrity: A broad term that refers to the maintenance and assurance of data quality. This includes the accuracy and consistency of data over its entire lifecycle[6].

Denial of Service (DoS) attack: A cyber attack that aims to disrupt the availability of a network, system, or service by overwhelming it with traffic or exploiting vulnerabilities, making it inaccessible to legitimate users[9].

Encryption: The process of converting plain text or data into ciphertext using cryptographic algorithms and keys to protect it from unauthorised access or interception, ensuring confidentiality, integrity, and privacy during storage, transmission, or processing[8].

Exploit: A malicious application or script that can be used to take advantage of a computer's

vulnerability. Exploits can allow attackers to gain control of systems, steal data, or disrupt services[7].

Firewall: A network security mechanism that controls network access by monitoring outgoing and incoming packets and either passing or blocking them based on source and destination IP addresses, protocols, and ports. Firewalls act as a barrier between a private internal network and external networks, filtering and blocking potentially malicious or unauthorized access attempts[1].

Hacking: Hacking refers to an unauthorised intrusion into a computer or a network. Hacking can be done for various purposes, including stealing data, disrupting services, or gaining unauthorized access to systems[7].

Honeypot: A decoy computer system used to attract and trap attackers, gather information about their activities, and divert them from real targets. Honeypots can help organizations understand attacker tactics and improve their security defenses[5].

Identity theft: Identity theft is a crime in which someone uses personally identifiable information in order to impersonate someone else[5].

Malware: Malware is software designed to harm or exploit any programmable device, service, or network. Common types of malware include viruses, worms, ransomware, and spyware[11].

Man-in-the-middle attack: A type of attack where an attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. This allows the attacker to eavesdrop on the conversation, steal data, or manipulate the communication[22].

Multi-Factor Authentication (MFA): MFA is an extra layer of security that requires multiple verification methods to confirm a user's identity. For example, you might need to enter a password followed by a code sent to your phone. MFA is increasingly recommended as a way to protect online accounts[8].

Password: A string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces[12].

Phishing: Phishing is a method of trying to gather personal information using deceptive e-mails and websites. Phishing attacks often aim to trick users into revealing sensitive information, such as login credentials or financial data[7].

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid. Ransomware attacks can encrypt data, lock users out of their systems, or disrupt critical services[3].

Social Engineering: Social engineering is the art of manipulating people, so they disclose confidential information. Social engineering attacks often exploit human psychology and trust to trick individuals into revealing sensitive information or performing actions that compromise security[7].

Spyware: Software that secretly monitors your computer activity and collects personal information, such as browsing habits or passwords, without your consent. Spyware is often used for malicious purposes, like

identity theft[3].

Trojan Horse: A type of malware that disguises itself as a legitimate program or file to trick users into installing it. Once installed, a Trojan horse can give attackers access to the system, steal data, or cause other harm[11].

Virus: A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions. Viruses can spread from one computer to another by attaching themselves to files or programs[7].

Vulnerability: A weakness or flaw in a system that can be exploited by attackers to gain unauthorized access or cause harm. Vulnerabilities can exist in software, hardware, or configurations[7].

Zero-Day: Zero-Day refers to a recently discovered vulnerability that hackers can use to attack systems. Zero-day vulnerabilities are particularly dangerous because they are unknown to the software vendor or security researchers, leaving systems vulnerable until a patch is developed and deployed[7].

Types of Cyber Attacks

Attack Type	Description
Malware	Malicious software designed to harm or exploit a system. Includes viruses, worms, ransomware, and spyware.
Phishing	Deceptive emails or websites used to gather personal information.
Denial-of-service attack	Disrupts the availability of a network, system, or service by overwhelming it with traffic.
Man-in-the-middle attack	An attacker secretly intercepts and relays messages between two parties.
Social engineering	Manipulating people to reveal confidential information or perform actions that compromise security.

Synthesis and Conclusion

This glossary provides a foundational understanding of key terms in computer science and cyber defense. By familiarizing yourself with these concepts, you can gain a better understanding of how computer systems work, how they are used to solve problems, and how to protect them from cyber threats. This knowledge is essential for anyone who interacts with technology, whether in their personal or professional lives.

Computer science provides the building blocks for the digital world, encompassing concepts like algorithms, data structures, and programming languages. These concepts are essential for developing software, analyzing data, and solving complex problems using computers.

Cyber defense focuses on protecting these systems and the information they hold from various threats. Understanding different types of cyber attacks, such as malware, phishing, and denial-of-service attacks, is crucial for implementing effective security measures.

The fields of computer science and cyber defense are closely interconnected. As technology advances and new threats emerge, it is vital to stay informed and adapt security practices accordingly. By staying vigilant and adopting good cyber hygiene practices, you can help protect yourself and your organization from cyber attacks and ensure a safe and secure online experience.

Works cited

1. Computer Science Terms: A to Z Glossary - Coursera, accessed March 4, 2025, https://www.coursera.org/collections/computer-science-terms
2. Glossary - Code.org, accessed March 4, 2025, https://code.org/curriculum/docs/k-5/glossary
3. 200 Most Useful Computer Terms For Beginners - PC Tips, accessed March 4, 2025, https://www.pctips.com/computer-terms/
4. What are common terms used in computer science? - FutureLearn, accessed March 4, 2025, https://www.futurelearn.com/info/courses/teaching-computing/0/steps/14831
5. Cybersecurity Glossary of Terms - Security Compass, accessed March 4, 2025, https://www.securitycompass.com/glossary/
6. Glossary of Cyber Security Terms - SANS Institute, accessed March 4, 2025, https://www.sans.org/security-resources/glossary-of-terms/
7. Cyber Security Terminology | Essential Cyber Security Terms - MetaCompliance, accessed March 4, 2025, https://www.metacompliance.com/cyber-security-terminology
8. An A-Z glossary of cyber security terms and definitions - Charity Digital, accessed March 4, 2025, https://charitydigital.org.uk/topics/an-a-z-glossary-of-cyber-security-terms-and-definitions-11473
9. 100+ Cybersecurity Terms & Definitions You Should Know - Allot Communications, accessed March 4, 2025, https://www.allot.com/100-plus-cybersecurity-terms-definitions/
10. Cyber security terminology | Cyber.gov.au, accessed March 4, 2025, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-terminology
11. Cybersecurity Terminology - U.S. Army Cyber Command, accessed March 4, 2025, https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2686075/cybersecurity-terminology/
12. Common Information Security / Compliance Terms, accessed March 4, 2025, https://is.wfu.edu/infosec/common-information-security-compliance-terms/
13. What Is Computer Science: Exploring Its Core Concepts - OPIT, accessed March 4, 2025, https://www.opit.com/magazine/what-is-computer-science/
14. Computer Science for beginners – Everything you need to know - Codedamn, accessed March 4,

2025, https://codedamn.com/news/programming/computer-science-for-beginners
15. Computer Science Definition - Iowa Department of Education, accessed March 4, 2025, https://educate.iowa.gov/pk-12/standards/instruction/computer-science/definition
16. What is Cyber Security? Definition & Best Practices - IT Governance, accessed March 4, 2025, https://www.itgovernance.co.uk/what-is-cybersecurity
17. The Fundamentals of Cyber Security | Online - The University of Adelaide, accessed March 4, 2025, https://online.adelaide.edu.au/blog/cyber-security-fundamentals
18. What is Cyber Security? Types, Importance & How to Stay Safe (2025 Guide), accessed March 4, 2025, https://www.geeksforgeeks.org/what-is-cyber-security/
19. Network Security 101: Understanding the Basics - NordLayer, accessed March 4, 2025, https://nordlayer.com/learn/network-security/basics/
20. Cybersecurity Glossary of Terms - Global Knowledge, accessed March 4, 2025, https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/
21. Glossary | CSRC - NIST Computer Security Resource Center, accessed March 4, 2025, https://csrc.nist.gov/glossary
22. Top 35+ Cybersecurity Terms You Need to Know - Simplilearn.com, accessed March 4, 2025, https://www.simplilearn.com/top-cybersecurity-terms-you-need-to-know-article
23. 30 Cybersecurity Terms Everyone Should Know To Stay Safe Online - ThriveDX, accessed March 4, 2025, https://thrivedx.com/resources/article/25-cyber-security-terms
24. Online Computer Science Glossary | QuickBase, accessed March 4, 2025, https://www.quickbase.com/articles/online-computer-science-glossary
25. Glossary of Coding Terms for Beginners, accessed March 4, 2025, https://onlinegrad.syracuse.edu/blog/coding-terms-for-beginners/