1. Microkernel: In computer science, a **microkernel** (often abbreviated as **μ-kernel**) is the near-minimum amount of software that can provide the mechanisms needed to implement an operating system (OS). These mechanisms include low-level address space management, thread management, and inter-process communication (IPC).

Contents [hide]

- Kernel (computer science)
  - Hybrid kernel
  - Loadable kernel module
  - Monolithic kernel
- Microservices
- Tanenbaum–Torvalds debate
- Trusted computing base
- Unikernel
- Multi-Environment Real-Time

2. Software Portability: **Portability** in high-level computer programming is the usability of the same software in different environments. The prerequirement for portability is the generalized abstraction between the application logic and system interfaces. When software with the same functionality is produced for several computing platforms, portability is the key issue for development cost reduction.

Contents [hide]

- Cross-platform software
- Hardware-dependent Software
- C (programming language)
- Language interoperability
- Portability testing
- Source-to-source compiler

3. MINIX 3: **Minix 3** is a project to create a small, high availability, high functioning Unix-like operating system. It is published under a BSD license and is a successor project to the earlier versions, Minix 1 and 2.

Contents [hide]

- Comparison of operating system kernels
- MINIX file system
- List of computing mascots
- Category:Computing mascots

4. My resident memory size at first is **728 KB:**

```
16710 erx       20   0    4340    728    656 T   0.0  0.0   0:00.00 a.out
```

After increasing the array by 10x and each malloc to 10,000, my new resident memory size is **5012KB:**

```
16889 erx       20   0   14072   5012   1016 T   0.0  0.2   0:00.00 a.out
```

The memory size is not 10x the old one.

5. After running the program, my resident memory size is **732 KB:**

```
17194 erx       20   0    4340    732    660 T   0.0  0.0   0:00.00 a.out
```

The resident memory was pretty similar to the previous one.

6. For the third test, I ran the program and my resident memory size is **640KB:**

```
17206 erx       20    0     4340     640     568 T   0.0  0.0    0:00.00 a.out
```

7. For the pre-test (without assigning), I got a resident memory size of **628KB:**

```
17515 erx       20    0     4340     628     556 T   0.0  0.0    0:00.00 a.out
```

After assigning the pointers, I got a resident memory size of **636KB:**

```
17485 erx       20    0     4340     636     568 T   0.0  0.0    0:00.00 a.out
```

After increasing the size, I got a resident memory size of **1824KB:**

```
17499 erx       20    0     5264    1824     996 T   0.0  0.1    0:00.00 a.out
```

After increasing the size, the size does increase (by around 3x).

8. Denial of service (DOS): In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]

Contents [hide]

- Application layer DDoS attack
- BASHLITE
- Billion laughs
- Botnet
- Blaster (computer worm)

- Dendroid (malware)
- Fork bomb
- High Orbit Ion Cannon (HOIC)
- Hit-and-run DDoS
- Industrial espionage
- Infinite loop
- Intrusion detection system
- Low Orbit Ion Cannon (LOIC)
- Network intrusion detection system
- October 2016 Dyn cyberattack
- Paper terrorism
- Project Shield
- ReDoS
- Resource exhaustion attack
- SlowDroid
- Slowloris (computer security)
- UDP Unicorn
- Virtual sit-in
- Warzapping
- Web shell
- Wireless signal jammer
- XML denial-of-service attack
- Xor DDoS
- Zemra
- Zombie (computer science)

9. Keystroke Logging: **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **keylogger** can be either software or hardware.

Contents [hide]

- Anti-keylogger
- Black-bag cryptanalysis
- Computer surveillance
- Digital footprint
- Hardware keylogger
- Reverse connection
- Session replay
- Spyware
- Trojan horse
- Virtual keyboard

10. Cryptography: **Cryptography** or **cryptology** (from Ancient Greek: κρυπτός, romanized: *kryptós* "hidden, secret"; and γράφειν *graphein*, "to write", or -λογία *-logia*, "study", respectively[1]) is the practice and study of techniques for secure communication in the presence of third parties called adversaries.[2] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages;[3] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation[4] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Contents [hide]

- Outline of cryptography
  - List of cryptographers
  - List of important publications in cryptography
  - List of multiple discoveries
  - List of unsolved problems in computer science
- A Syllabical and Steganographical table – first cryptography chart
- Comparison of cryptography libraries
- Crypto Wars
- Encyclopedia of Cryptography and Security
- Global surveillance
- Information theory
- Strong cryptography
- W3C's Web cryptography API

11. Authentication: **Authentication** (from Greek: αὐθεντικός *authentikos*, "real, genuine", from αὐθέντης *authentes*, "author") is the act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate,[1] determining the age of an artifact by carbon dating, or ensuring that a product or document is not counterfeit.

Contents [hide]

- Access Control Service
- AssureID
- Atomic authorization
- Authentication Open Service Interface Definition
- Authenticity in art
- Authorization
- Basic access authentication
- Biometrics
- CAPTCHA
- Chip Authentication Program
- Closed-loop authentication
- Diameter (protocol)
- Digital identity
- EAP
- Electronic authentication
- Encrypted key exchange (EKE)
- Fingerprint Verification Competition
- Geolocation
- Hash-based message authentication code
- Identification (information)
- Java Authentication and Authorization Service
- Kantara Initiative
- Kerberos
- Multi-factor authentication
- Needham–Schroeder protocol
- OAuth – an open standard for authorization
- OpenAthens
- OpenID Connect – an authentication method for the web

- OpenID – an authentication method for the web
- Provenance
- Public-key cryptography
- RADIUS
- Reliance authentication
- Secret sharing
- Secure Remote Password protocol (SRP)
- Secure Shell
- Security printing
- SQRL
- Strong authentication
- Tamper-evident technology
- TCP Wrapper
- Time-based authentication
- Two-factor authentication
- Usability of web authentication systems
- Woo–Lam

12. Biometrics: **Biometrics** is the technical term for body measurements and calculations. It refers to metrics related to human characteristics . Biometrics authentication (or realistic authentication)[note 1] is used in computer science as a form of identification and access control.[1][2] It is also used to identify individuals in groups that are under surveillance.[3]

Contents [hide]

- Aadhaar
- Access control
- AFIS
- AssureSign
- BioAPI

- Biometric passport
- Biometric voter registration
- Biometrics in schools
- BioSlimDisk
- Facial recognition system
- Fingerprint recognition
- Fuzzy extractor
- Gait analysis
- Government database
- Hand geometry
- Handwritten biometric recognition
- Identity Cards Act 2006
- International Identity Federation
- Iris recognition
- Keystroke dynamics
- Multiple Biometric Grand Challenge
- Private biometrics
- Retinal scan
- Signature recognition
- Smart city
- Speaker recognition[84]
- Surveillance
- Vein matching
- Voice analysis