

# Literature based Cyber Security Topics: Handbook

Dr SRIDHAR SESHADRI

Ex Vice Chancellor and Professor Computer Science & Engineering

Email: drssridhar@yahoo.com

**Abstract:** Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cloud computing has emerged from the legacy data centres. Consequently, threats applicable in legacy system are equally applicable to cloud computing along with emerging new threats that plague only the cloud systems. Traditionally the data centres were hosted on-premises. Hence, control over the data was comparatively easier than handling a cloud system which is borderless and ubiquitous. Threats due to multi-tenancy, access from anywhere, control of cloud, etc. are some examples of why cloud security becomes important. Considering the significance of cloud security, this work is an attempt to understand the existing cloud service and deployment models, and the major threat factors to cloud security that may be critical in cloud environment. It also highlights various methods employed by the attackers to cause the damage. Cyber-attacks are highlighted as well. This work will be profoundly helpful to the industry and researchers in understanding the various cloud specific cyber-attack and enable them to evolve the strategy to counter them more effectively.

**Key words :** Digital Attacks; Network; Cloud Computing; Data Centres; Cyber Attacks; Multi Tenancy; Cloud Service; Sensitive Information; Threat Factors; Cloud Security;

## INTRODUCTION

**Cyber security** is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed. **Information security** protects the integrity and privacy of data, both in storage and in transit. **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella. For various types of attacks, one may refer to the articles listed under references. **Risk Management Regime:** Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to

risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

- Secure configuration: Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.
- Network security: The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.
- Managing user privileges: If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account

will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

- User education and awareness: Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.
- Incident management: All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.
- Malware prevention: Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.
- Monitoring: System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.
- Removable media controls: Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

- Home and mobile working: Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

### **The Importance of Cyber security**

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization. A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It's estimated that, on average, a data breach costs an affected organization \$3.6 million. With high-profile data breaches making media headlines, it's essential that organizations adopt and implement a strong cybersecurity approach.

### **Computer forensics (also known as Computer Forensic Science)**

It is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is accepted as reliable within U.S. and European court systems.

## Forensic process



A portable Tableau write blocker attached to a Hard Drive

Computer forensic investigations usually follow the standard digital forensic process or phases which are acquisition, examination, analysis and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

### Computer Forensics Lab

The computer forensic lab is a safe and protected zone where electronic data can be managed, preserved, and accessed in a controlled environment. There, there is a very much reduced risk of damage or modification to the evidence. Computer forensic examiners have the resources needed to elicit meaningful data from the devices that they are examining.

### Techniques

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular.

### Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

### Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

### Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic

software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

### Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

### Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the images appear identical upon visual inspection, the hash changes as the data changes.

### Mobile Devices Forensics

**Phone Logs:** Phone companies usually keep logs of calls received, which can be helpful when creating timelines and gathering the locations of persons when the crime occurred.

**Contacts:** Contact lists help narrow down the suspect pool due to their connections with the victim or suspect.

**Text messages:** Messages contain timestamps and remain in company servers indefinitely, even if deleted on the original device. Because of this, messages act as crucial records of communication that can be used to convict suspects.

**Photos:** Photos can be critical in either supporting or disproving alibis by displaying a location or scene along with a timestamp of when the photo was taken.

**Audio Recordings:** Some victims might have been able to record pivotal moments of the struggle, like the voice of their attacker or extensive context of the situation.

### Volatile data

**Volatile data** is any **data** that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. **Volatile data** resides in registries, cache, and random access memory (RAM). The investigation of this **volatile data** is called "live forensics". When seizing evidence, if the machine is still active, any information stored solely in RAM that is not

recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, WinDD, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below  $-60^{\circ}\text{C}$  helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination. Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jiggle, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.

However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.

### Analysis tools

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review. Autopsy (software), Belkasoft Evidence Center, COFEE, EnCase are the some of tools used in Digital forensics.

### Hack computer

The **Hack Computer** is a theoretical computer design created by Noam Nisan and Shimon Schocken and described in their book, *The Elements of Computing Systems: Building a Modern Computer from First Principles*. In using the term "modern", the authors refer to a digital, binary machine that is patterned according to the von Neumann architecture model. The Hack computer is intended for hands-on virtual construction in a hardware simulator application as

a part of a basic, but comprehensive, course in computer organization and architecture. One such course, created by the authors and delivered in two parts, is freely available as a massive open online course (MOOC) called *Build a Modern Computer From First Principles: From Nand to Tetris*. In the twelve projects included in the course, learners start with a two input Nand gate and end up with a fully operational virtual computer, including both hardware (memory and CPU) and software (assembler, VM, Java-like programming language, and OS). In addition to the hardware simulator used for initial implementation of the computer hardware, a complete Hack computer emulator program and assembler that supports the projects described in the book and the on-line course is also available at the author's web site.

Instruction set architecture (ISA) and machine language

The Hack computer's instruction set architecture (ISA) and derived machine language is sparse compared to many other architectures. Although the 6 bits used to specify a computation by the ALU could allow for 64 distinct instructions, only 18 are officially implemented in the Hack computer's ISA. Since the Hack computer hardware has direct support for neither integer multiplication (and division) or function calls, there are no corresponding machine language instructions in the ISA for these operations.

Hack machine language has only two types of instructions, each encoded in 16 binary digits.

### A-instructions

Instructions whose most significant bit is "0" are called A-instructions or address instructions. The A-instruction is bit-field encoded as follows:

$0b_{14}b_{13}b_{12}b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2b_1b_0$

0 – the most significant bit of a A-instruction is "0"

$b_{14} - b_0$  - these bits provide the binary representation of a non-negative integer in the decimal range 0 through 32767

When this instruction is executed, the remaining 15 bits are left-zero extended and loaded into the CPU's A-register. As a side-effect, the RAM register having the address represented by that value is enabled for subsequent read/write action in the next clock cycle.

### C-instructions

The other instruction type, known as C-instructions (computation instructions), have "1" as the most significant bit. The remaining 15 bits are bit-field encoded to define the operands, computation performed, and storage location for the specified



computation result. This instruction may also specify a program branch based on the most recent computation result.

The C-instruction is bit-field encoded as follows:

$1x_1x_0ac_5c_4c_3c_2c_1c_0d_2d_1d_0j_2j_1j_0$

1 – the most significant bit of a C-instruction is “1”

$x_1x_0$  – these bits are ignored by the CPU and, by convention, are each always set to “1”

a – this bit specifies the source of the “y” operand of the ALU when it is used in a computation

$c_0-c_5$  – these six control bits specify the operands and computation to be performed by the ALU

$d_2-d_0$  – these three bits specify the destination(s) for storing the current ALU output

$j_2-j_0$  – these three bits specify an arithmetic branch condition, an unconditional branch (jump), or no branching

The Hack computer encoding scheme of the C-instruction is shown in the following tables.

In these tables,

- **A** represents the value currently contained in the A-register
- **D** represents the value currently contained in the D-register
- **M** represents the value currently contained in the data memory register whose address is contained in the A-register; that is,  $M == RAM[A]$

Hack machine language computation function codes and assembly language mnemonics								
a	c <sub>5</sub>	c <sub>4</sub>	c <sub>3</sub>	c <sub>2</sub>	c <sub>1</sub>	c <sub>0</sub>	ALU Output: f(x,y)	Mnemonic
0	1	0	1	0	1	0	Outputs 0; ignores all operands	0
0	1	1	1	1	1	1	Outputs 1; ignores all operands	1
0	1	1	1	0	1	0	Outputs -1; ignores all operands	-1
0	0	0	1	1	0	0	Outputs D; ignores A and M	D
0	1	1	0	0	0	0	Outputs A; ignores D and M	A
1	1	1	0	0	0	0	Outputs M; ignores D and A	M
0	0	0	1	1	0	1	Outputs bitwise negation of D; ignores A and M	!D
0	1	1	0	0	0	1	Outputs bitwise negation of A; ignores D and M	!A
1	1	1	0	0	0	1	Outputs bitwise negation of M; ignores D and A	!M
0	0	0	1	1	1	1	Outputs 2's complement negative of D; ignores A and M	-D
0	1	1	0	0	1	1	Outputs 2's complement negative of A; ignores D and M	-A
1	1	1	0	0	1	1	Outputs 2's complement negative of M; ignores D and A	-M
0	0	1	1	1	1	1	Outputs D + 1 (increments D); ignores A and M	D+1
0	1	1	0	1	1	1	Outputs A + 1 (increments A); ignores D and M	A+1
1	1	1	0	1	1	1	Outputs M + 1 (increments M); ignores D and A	M+1
0	0	0	1	1	1	0	Outputs D - 1 (decrements D); ignores A and M	D-1
0	1	1	0	0	1	0	Outputs A - 1 (decrements A); ignores D and M	A-1
1	1	1	0	0	1	0	Returns M-1 (decrements M); ignores D and A	M-1
0	0	0	0	0	1	0	Outputs D + A; ignores M	D+A
1	0	0	0	0	1	0	Outputs D + M; ignores A	D+M
0	0	1	0	0	1	1	Outputs D - A; ignores M	D-A
1	0	1	0	0	1	1	Outputs D - M; ignores A	D-M

0	0	0	0	1	1	1	Outputs A - D; ignores M	A-D
1	0	0	0	1	1	1	Outputs M - D; ignores A	M-D
0	0	0	0	0	0	0	Outputs bitwise logical And of D and A; ignores M	D&A
1	0	0	0	0	0	0	Outputs bitwise logical And of D and M; ignores A	D&M
0	0	1	0	1	0	1	Outputs bitwise logical Or of D and A; ignores M	D A
1	0	1	0	1	0	1	Outputs bitwise logical Or of D and M; ignores A	D M

Hack machine language computation result storage codes and assembly language mnemonics				
$d_2$	$d_1$	$d_0$	Store ALU output in	Mnemonic
0	0	0	Output not stored	none
0	0	1	M	M
0	1	0	D	D
0	1	1	D and M	DM
1	0	0	A	A
1	0	1	A and M	AM
1	1	0	A and D	AD
1	1	1	A and D and M	ADM

Hack machine language branch condition codes and assembly language mnemonics				
$j_2$	$j_1$	$j_0$	Branch if	Mnemonic
0	0	0	No branch	none
0	0	1	Output greater than 0	JGT
0	1	0	Output equals 0	JEQ
0	1	1	Output greater than or equal 0	JGE
1	0	0	Output less than	JLT
1	0	1	Output not equal 0	JNE
1	1	0	Output less than or equal 0	JLE
1	1	1	Unconditional branch	JMP

## Assembly language

The Hack computer has a text-based assembly language to create programs for the hardware platform that implements the Hack computer ISA. Hack assembly language programs may be stored in text files having the file name extension “.asm”. Hack assembly language source files are case sensitive. Each line of text contains one of the following elements:

- Blank line
- Comment
- Label declaration (with optional end-of-line comment)
- A-instruction (with optional end-of-line comment)
- C-instruction (with optional end-of-line comment)

Each of these line types has a specific syntax and may contain predefined or user defined symbols or numeric constants. Blank lines and comments are ignored by the assembler. Label declarations, A-instructions, and C-instructions, as defined below, may not include any internal white-space characters, although leading or trailing whitespace is permitted (and ignored).

### Comments

Any text beginning with the two-character sequence “//” is a comment. Comments may appear on a source code line alone, or may also be placed at the end of any other program source line. All text following the comment identifier character sequence to end of line is completely ignored by the assembler; consequently, they produce no machine code.

### Symbols and numeric constants

Hack assembly language allows the use of alphanumeric symbols for number of different specific purposes. A symbol may be any sequence of alphabetic (upper and lower case) or numeric digits. Symbols may also contain any of the following characters: under bar (“\_”), period(“.”), dollar sign (“\$”), and colon (“:”). Symbols may not begin with a digit character. Symbols are case sensitive. User defined symbols are used to create variable names and labels (see below).

The Hack assembly language assembler recognizes some predefined symbols for use in assembly language programs. The symbols R0, R1, ..., R15 are bound respectively to the integers 0 through 15. These symbols are meant to represent general purpose registers and the symbols values therefore represent data memory addresses 0 through 15. Predefined symbols SCREEN and KBD are also specified to represent the data memory address of

the start of memory-mapped virtual screen output (16384) and keyboard input (24756). There are a few other symbols (SP, LCL, ARG, THIS, and THAT) that are used in building the operating system software stack.

A string of decimal (0-9) digits may be used to represent a non-negative, decimal constant in the range 0 through 32,767. The use of the minus sign to indicate a negative number is not allowed. Binary or octal representation is not supported.

### Variables

User defined symbols may be created in an assembly language program to represent variables; that is, a named RAM register. The symbol is bound at assembly to a RAM address chosen by the assembler. Therefore, variables must be treated as addresses when appearing in assembly language source code. Variables are implicitly defined in assembly language source code when they are first referenced in an A-instruction. When the source code is processed by the assembler, the variable symbol is bound to a unique positive integer value in beginning at address 16. Addresses are sequentially bound to variable symbols in the order of their first appearance in the source code. By convention, user-defined symbols that identify program variables are written in all lower case.

### Labels

Labels are symbols delimited by left "(" and right ")" parenthesis. They are defined on a separate source program line and are bound by the assembler to the address of the instruction memory location of the next instruction in the source code. Labels may be defined only once, but they may be used multiple times anywhere within the program, even before the line on which they are defined. By convention, labels are expressed in all-caps. They are used to identify the target address of branch C-instructions.

### A-instructions

The A-instruction has the syntax “@xxxx”, where xxxx is either a numeric decimal constant in the range 0 through 32767, a label, or a variable (predefined or user defined). When executed, this instruction sets the value of the A register and the M pseudo-register to a 15-bit binary value represented by “xxxx”. The 15-bit value is left-zero extended to 16-bits in the A register.

The A-instruction may be used for one of three purposes. It is the only means to introduce a (non-negative) numeric value into the computer under program control; that is, it may be used to create program constants. Secondly, it is used to specify a RAM memory location using the M pseudo-register mechanism for subsequent reference by a C-instruction. Finally, a C-instruction which specifies

a branch uses the current value of the A register as the branch target address. The A-instruction is used to set that target address prior to the branch instruction, usually by reference to a label.

### C-Instructions

C-instructions direct the ALU computation engine and program flow control capabilities of the Hack computer. The instruction syntax is defined by three fields, referred to as “comp”, “dest”, and “jump”. The comp field is required in every C-instruction. The C-instruction syntax is “dest=comp;jump”. The “=” and “;” characters are used to delimit the fields of the instruction. If the dest field is not used, the “=” character is omitted. If the jump field is not used, the “;” character is omitted. The C-instruction allows no internal spaces.

The comp field must be one of the 28 documented mnemonic codes defined in the table above. These codes are considered distinct units; they must be expressed in all-caps with no internal spaces. It is noted that the 6 ALU control bits could potentially specify 64 computational functions; however, only the 18 presented in the table are officially documented for recognition by the assembler.

The dest field may be used to specify one or more locations to store the result of the specified computation. If this field is omitted, along with the “=” delimiter, the computed value is not stored. The allowed storage location combinations are specified by the mnemonic codes defined in the table above.

The jump field may be used to specify the address in ROM of the next instruction to be executed. If the field is omitted, along with the “;” delimiter, execution continues with the instruction immediately following the current instruction. The branch address target, in ROM, is provided by the current value of the A register if the specified branch condition is satisfied. If the branch condition fails, execution continues with the next instruction in ROM. Mnemonic codes are provided for six different comparisons based on the value of the current computation. Additionally, an unconditional branch is provided as a seventh

The assembler output, shown in the last column, is a text string of 16 binary characters, not 16-bit binary integer representation.

option. Because the comp field must always be supplied, even though the value is not required for the unconditional branch, the syntax of this instruction is given as “0;JMP”. The branch conditions supported are specified in the table above.

### Assembler

Freely available software supporting the Hack computer includes a command line assembler application. The assembler reads Hack assembly language source files (\*.asm) and produces Hack machine language output files (\*.hack). The machine language file is also a text file. Each line of this file is a 16-character string of binary digits that represents the encoding of each corresponding executable line of the source text file according to the specification described in the section “Instruction set architecture (ISA) and machine language”. The file created may be loaded into the Hack computer emulator by a facility provided by the emulator user interface.

### Example Assembly Language Program

Following is an annotated example program written in Hack assembly language. This program sums the first 100 consecutive integers and places the result of the calculation in a user-defined variable called “sum”. It implements a “while” loop construct to iterate through the integer values 1 through 100 and adds each integer to a “sum” variable. The user-defined variable “cnt” maintains the current integer value through the loop. This program illustrates all of the features of the “documented” assembly language capabilities of Hack Computer except memory-mapped I/O. The contents of the Hack assembly language source file are shown in the second column in bold font. Line numbers are provided for reference in the following discussion but do not appear in the source code. The Hack machine code produced by the assembler is shown in the last column with the assigned ROM address in the preceding column. Note that full-line comments, blank lines, and label definition statements generate no machine language code. Also, the comments provided at the end of each line containing an assembly language instruction are ignored by the assembler.

Line Nbr	Hack Assembly Language Program	Operating Notes	Instruction Type	ROM Addr	Hack Machine Code
01	<b>// Add consecutive integers 1 thru 100</b>	Comment that describes program action	Full-line comment	- - - -	No code generated
02	<b>// sum = 1 + 2 + 3 + ... + 99 + 100</b>	Comments are ignored by assembler	Full-line comment	- - - -	No code generated



03		Blank source lines are ignored by assembler	Blank line	----	No code generated
04	<b>@cnt // loop counter declaration</b>	Variable symbol "cnt" bound to 16	A-instruction	00	0000000000001000
05	<b>M=1 // initialize loop counter to 1</b>	$RAM[16] \leftarrow 1$	C-instruction	01	111011111001000
06	<b>@sum // sum accumulator declaration</b>	Variable symbol "sum" bound to 17	A-instruction	02	0000000000010001
07	<b>M=0 // initialize sum to 0</b>	$RAM[17] \leftarrow 0$	C-instruction	03	1110101010001000
08	<b>(LOOP) // start of while loop</b>	Label symbol bound to ROM address 04	Label declaration	----	No code generated
09	<b>@cnt // reference addr of cnt</b>	$M \leftarrow 16$	A-instruction	04	0000000000001000
10	<b>D=M // move current cnt value to D</b>	$D \leftarrow RAM[16]$	C-instruction	05	111110000010000
11	<b>@100 // load loop limit into A</b>	$A \leftarrow 100$	A-instruction	06	0000000001100100
12	<b>D=D-A // perform loop test computation</b>	$D \leftarrow D - A$	C-instruction	07	1110010011010000
13	<b>@END // load target destination for branch</b>	$M \leftarrow 18$	A-instruction	08	0000000000010010
14	<b>D;JGT //exit loop if D &gt; 0</b>	Conditional branch	C-instruction	09	1110001100000001
15	<b>@cnt // reference addr of cnt</b>	$M \leftarrow 16$	A-instruction	10	0000000000001000
16	<b>D=M // move current cnt value to D</b>	$D \leftarrow RAM[16]$	C-instruction	11	111110000010000
17	<b>@sum // reference address of sum</b>	$M \leftarrow 17$	A-instruction	12	0000000000010001
18	<b>M=D+M // add cnt to sum</b>	$M \leftarrow D + RAM[17]$	C-instruction	13	1111000010001000
19	<b>@cnt // reference addr of cnt</b>	$M \leftarrow 16$	A-instruction	14	0000000000001000
20	<b>M=M+1 // increment counter</b>	$RAM[16] \leftarrow RAM[16] + 1$	C-instruction	15	111110111001000
21	<b>@LOOP // load target destination for branch</b>	$M \leftarrow 4$	A-instruction	16	0000000000000100
22	<b>0;JMP // jump to LOOP entry</b>	Unconditional branch	C-instruction	17	1110101010000111
23	<b>(END) // start of terminating loop</b>	Label symbol bound to ROM address 18	Label declaration	----	No code generated

24	<b>@END // load target destination for branch</b>	$M \leftarrow 18$	A-instruction	18	000000000010010
25	<b>0;JMP // jump to END entry</b>	Unconditional branch	C-instruction	19	1110101010000111

Note that the instruction sequence follows the pattern of A-instruction, C-instruction, A-instruction, C-instruction, ... . This is typical for Hack assembly language programs. The A-instruction specifies a constant or memory address that is used in the subsequent C-instruction. All three variations of the A-instruction are illustrated. In line 11 (@100), the constant value 100 is loaded into the A register. This value is used in line 12 ( $D=D-A$ ) to compute the value used to test the loop branch condition. Since line 4 (@cnt) contains the first appearance of the user-defined variable "cnt", this statement binds the symbol to the next unused RAM address. In this instance, the address is 16, and that value is loaded into the A register. Also, the M pseudo-register also now references this

address, and RAM[16] is made the active RAM memory location.

The third use of the A-instruction is seen in line 21 (@LOOP). Here the instruction loads the bound label value, representing an address in ROM memory, into the A register and M pseudo-register. The subsequent unconditional branch instruction in line 22 (0;JMP) loads the M register value into the CPU's program counter register to effect control transfer to the beginning of the loop. The Hack computer provides no machine language instruction to halt program execution. The final two lines of the program (@END and 0;JMP) create an infinite loop condition which Hack assembly programs conventionally use to terminate programs designed to run in the CPU emulator.

## Computer security

### Related security categories

Computer security, Automotive security, Cybercrime, Cybersex trafficking, Computer fraud , Cybergeddon, Cyberterrorism, Cyberwarfare, Electronic warfare, Information warfare, Internet security, Mobile security, Network security, Copy protection, Digital rights management

### Threats

Adware, Advanced persistent threat, Arbitrary code execution, Backdoors, Hardware backdoors, Code injection, Crimeware, Cross-site scripting, Cryptojacking malware, Botnets, Data breach, Drive-by download, Browser helper objects, Viruses, Data scraping, Denial of service, Eavesdropping, Email fraud, Email spoofing, Exploits, Keyloggers, Logic bombs, Time bombs, Fork bombs, Zip bombs, Fraudulent dialers, Malware, Payload, Phishing, Polymorphic engine, Privilege escalation, Ransomware, Rootkits, Bootkits, Scareware, Shellcode, Spamming, Social engineering (security), Screen scraping, Spyware, Software bugs, Trojan horses, Hardware Trojans, Remote access trojans, Vulnerability, Web shells, Wiper, Worms, SQL injection, Rogue security software, Zombie

### Defenses

Application security , Secure coding, Secure by default, Secure by design , Misuse case, Computer access control , Authentication , Multi-factor authentication, Authorization, Computer security software , Antivirus software, Security-focused operating system, Data-centric security, Code obfuscation, Data masking, Encryption, Firewall, Intrusion detection system , Host-based intrusion detection system (HIDS), Anomaly detection, Security information and event management (SIEM), Mobile secure gateway, Runtime application self-protection



While most aspects of computer security involve digital measures such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering.

### **Computer security, cybersecurity or information technology security**

#### **(IT security)**

It is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field has become of significance due to the expanded reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to the complexity of information systems, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy

### **Vulnerabilities and attacks**

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working attack or exploit exists. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts. To secure a computer system, it is important to understand the attacks that can be made against it,

and these threats can typically be classified into one of these categories below:

#### **Backdoor**

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for many reasons, including original design or poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the operating system of the computer.

#### **Denial-of-service attack**

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

#### **Direct-access attacks**

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

#### **Eavesdropping**

Eavesdropping is the act of surreptitiously listening to a private computer "conversation" (communication), typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (FBI) and NSA

to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon by monitoring the faint electromagnetic transmissions generated by the hardware. TEMPEST is a specification by the NSA referring to these attacks.

### Multi-vector, polymorphic attacks

Surfacing in 2017, a new class of multi-vector, polymorphic cyber threats combined several types of attacks and changed form to avoid cybersecurity controls as they spread.

### Phishing

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words received and discrepancy as recieved and discrepancy, respectively. Although the URL of the bank's webpage appears to be legitimate, the hyperlink points at the phisher's webpage. Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose "look" and "feel" are almost identical to the legitimate one. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized. A more strategic type of phishing is spear-phishing which leverages personal or organization-specific details to make the attacker appear like a trusted source. Spear-phishing attacks target specific individuals, rather than the broad net cast by phishing attempts.

### Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data; or even become "root" and have full unrestricted access to a system.

### Reverse engineering

Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, code, and architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.

### Side-channel attack

Any computational system affects its environment in some form. This effect it has on its environment, includes a wide range of criteria, which can range from electromagnetic radiation, to residual effect on RAM cells which as a consequent make a Cold boot attack possible, to hardware implementation faults that allow for access and or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios, the attacker would gather such information about a system or network to guess its internal state and as a result access the information which is assumed by the victim to be secure.

### Social engineering

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer. This generally involves exploiting peoples trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel, impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such "business email compromise" (BEC) scams had cost US businesses more than \$2 billion in about two years. In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.

### Spoofing

Spoofing is an act of masquerading as a valid entity through the falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. There are several types of spoofing, including:

- Email spoofing, is where an attacker forges the sending (From, or source) address of an email.
- IP address spoofing, where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system.



- MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface controller to obscure their identity, or to pose as another.
- Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user.

### **Tampering**

Tampering describes a malicious modification or alteration of data. So-called Evil Maid attacks and security services planting of surveillance capability into routers are examples.

### **Malware**

Malicious software (malware) installed on a computer can leak any information, such as personal information, business information and passwords, can give control of the system to the attacker, and can corrupt or delete data permanently.

### **Information security culture**

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness toward information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds." Andersson and Reimers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes. Indeed, the Verizon Data Breach Investigations Report 2020, which examined 3,950 security breaches, discovered 30% of cybersecurity incidents involved internal actors within a company. Research shows information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never-ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

- Pre-evaluation: To identify the awareness of information security within employees and to analyze the current security policies.
- Strategic planning: To come up with a better awareness program, clear targets need to be set. Assembling a team of skilled professionals is helpful to achieve it.
- Operative planning: A good security culture can be established based on internal

communication, management buy-in, security awareness and a training program.

- Implementation: Four stages should be used to implement the information security culture.

They are:

1. Commitment of the management
2. Communication with organizational members
3. Courses for all organizational members
4. Commitment of the employees

- Post-evaluation: To assess the success of the planning and implementation, and to identify unresolved areas of concern.

### **Systems at risk**

The growth in the number of computer systems and the increasing reliance upon them by individuals, businesses, industries, and governments means that there are an increasing number of systems at risk.

### **Financial systems**

The computer systems of financial regulators and financial institutions like the U.S. Securities and Exchange Commission, SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illicit gains. Websites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are also prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

### **Utilities and industrial equipment**

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.

### **Aviation**

The aviation industry is very reliant on a series of complex systems which could be attacked. A simple power outage at one airport can cause repercussions worldwide, much of the system relies

on radio transmissions which could be disrupted, and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. There is also potential for attack from within an aircraft. In Europe, with the (Pan-European Network Service) and NewPENS, and in the US with the NextGen program, air navigation service providers are moving to create their own dedicated networks. The consequences of a successful attack range from loss of confidentiality to loss of system integrity, air traffic control outages, loss of aircraft, and even loss of life.

### Consumer devices

Desktop computers and laptops are commonly targeted to gather passwords or financial account information or to construct a botnet to attack another target. Smartphones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. WiFi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach. The increasing number of home automation devices such as the Nest thermostat are also potential targets.

### Large corporations

Large corporations are common targets. In many cases attacks are aimed at financial gain through identity theft and involve data breaches. Examples include the loss of millions of clients' credit card details by Home Depot, Staples, Target Corporation, and the most recent breach of Equifax. Medical records have been targeted in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale. Although cyber threats continue to increase, 62% of all organizations did not increase security training for their business in 2015. Not all attacks are financially motivated, however: security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group, and Sony Pictures was hacked in 2014 with the apparent dual motive of embarrassing the company through data leaks and crippling the company by wiping workstations and servers.

### Automobiles

Vehicles are increasingly computerized, with engine timing, cruise control, anti-lock brakes, seat

belt tensioners, door locks, airbags and advanced driver-assistance systems on many models. Additionally, connected cars may use WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network. Self-driving cars are expected to be even more complex. All of these systems carry some security risk, and such issues have gained wide attention. Simple examples of risk include a malicious compact disc being used as an attack vector, and the car's onboard microphones being used for eavesdropping. However, if access is gained to a car's internal controller area network, the danger is much greater and in a widely publicized 2015 test, hackers remotely carjacked a vehicle from 10 miles away and drove it into a ditch. Manufacturers are reacting in numerous ways, with Tesla in 2016 pushing out some security fixes "over the air" into its cars' computer systems. In the area of autonomous vehicles, in September 2016 the United States Department of Transportation announced some initial safety standards, and called for states to come up with uniform policies.

### Government

Government and military computer systems are commonly attacked by activists and foreign powers. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records, and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

### Internet of things and physical vulnerabilities

The Internet of things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data. Concerns have been raised that this is being developed without appropriate consideration of the security challenges involved. While the IoT creates opportunities for more direct integration of the physical world into computer-based systems, it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyberattacks are likely to become an increasingly physical (rather than simply virtual) threat. If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-

Internet-connected hotel door locks. An attack that targets physical infrastructure and/or human lives is sometimes referred to as a cyber-kinetic attack. As IoT devices and appliances gain currency, cyber-kinetic attacks can become pervasive and significantly damaging.

### Medical systems

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment and implanted devices including pacemakers and insulin pumps. There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks, Windows XP exploits, viruses, and data breaches of sensitive data stored on hospital servers. On 28 December 2016 the US Food and Drug Administration released its recommendations for how medical device manufacturers should maintain the security of Internet-connected devices – but no structure for enforcement.

### Energy sector

In distributed generation systems, the risk of a cyber attack is real, according to Daily Energy Insider. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster. The District of Columbia is considering creating a Distributed Energy Resources (DER) Authority within the city, with the goal being for customers to have more insight into their own energy use and giving the local electric utility, Pepco, the chance to better estimate energy demand. The D.C. proposal, however, would "allow third-party vendors to create numerous points of energy distribution, which could potentially create more opportunities for cyber attackers to threaten the electric grid."

### Impact of security breaches

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from \$13 billion (worms and viruses only) to \$226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to

the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from a cyber/information security breach).

### Attacker motivation

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain. State-sponsored attackers are now common and well resourced but started with amateurs such as Markus Hess who hacked for the KGB, as recounted by Clifford Stoll in *The Cuckoo's Egg*. Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas. The growth of the internet, mobile technologies, and inexpensive computing devices have led to a rise in capabilities but also to the risk to environments that are deemed as vital to operations. All critical targeted environments are susceptible to compromise and this has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these types of actors. Several stark differences exist between the hacker motivation and that of nation state actors seeking to attack based on an ideological preference. A standard part of threat modeling for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home personal computer, bank, and classified military network face very different threats, even when the underlying technologies in use are similar.

### Computer protection (countermeasures)

In computer security, a countermeasure is an action, device, procedure or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Some common countermeasures are listed in the following sections:

#### Security by design

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way, even if an attacker gains access to that part, they only have limited access to the whole system.
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
- Audit trails track system activity so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
- Full disclosure of all vulnerabilities, to ensure that the window of vulnerability is kept as short as possible when bugs are discovered.

### Security architecture

The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services".

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:

- the relationship of different components and how they depend on each other.
- determination of controls based on risk assessment, good practices, finances, and legal matters.
- the standardization of controls.

Practicing security architecture provides the right foundation to systematically address business, IT and security concerns in an organization.

### Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware and software-based.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, the complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security consists mainly of "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet. Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats. However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As a result, as Reuters points out: "Companies for the first time report they are losing more through



electronic theft of data than physical stealing of assets". The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

In order to ensure adequate security, the confidentiality, integrity and availability of a network, better known as the CIA triad, must be protected and is considered the foundation to information security. To achieve those objectives, administrative, physical and technical security measures should be employed. The amount of security afforded to an asset can only be determined when its value is known.

### **Vulnerability management**

Vulnerability management is the cycle of identifying, remediating or mitigating vulnerabilities, especially in software and firmware. Vulnerability management is integral to computer security and network security. Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities, such as open ports, insecure software configuration, and susceptibility to malware. In order for these tools to be effective, they must be kept up to date with every new update the vendor release. Typically, these updates will scan for the new vulnerabilities that were introduced recently. Beyond vulnerability scanning, many organizations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors, this is a contractual requirement.

### **Reducing vulnerabilities**

While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include seL4, and SYSGO's PikeOS but these make up a very small percentage of the market. Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or another piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk, but even in highly disciplined environments (e.g. military organizations), social engineering attacks

can still be difficult to foresee and prevent. Inoculation, derived from inoculation theory, seeks to prevent social engineering and other fraudulent tricks or traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts. It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner and/or hiring people with expertise in security, though none of these guarantee the prevention of an attack. The effects of data loss/damage can be reduced by careful backing up and insurance.

### **Hardware protection mechanisms**

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

- USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs). In addition, a USB dongle can be configured to lock or unlock a computer.
- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.

- Computer case intrusion detection refers to a device, typically a push-button switch, which detects when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves. Tools exist specifically for encrypting external drives as well.
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
- Disconnecting or disabling peripheral devices (like camera, GPS, removable storage etc.), that are not in use.
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), near-field communication (NFC) on non-iOS devices and biometric validation such as thumbprint readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.

### Secure operating systems

One use of the term "computer security" refers to technology that is used to implement secure operating systems. In the 1980s, the United States Department of Defense (DoD) used the "Orange Book" standards, but the current international standard ISO/IEC 15408, "Common Criteria" defines a number of progressively more stringent Evaluation Assurance Levels. Many common operating systems meet the EAL4 standard of being "Methodically Designed, Tested and Reviewed", but the formal verification required for the highest levels means that they are uncommon. An example of an EAL6 ("Semiformally Verified Design and Tested") system is INTEGRITY-178B, which is used in the Airbus A380 and several military jets.

### Secure coding

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such

systems are secure by design. Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system; important for cryptographic protocols for example.

### Capabilities and access control lists

Within computer systems, two of the main security models capable of enforcing privilege separation are access control lists (ACLs) and role-based access control (RBAC). An access-control list (ACL), with respect to a computer file system, is a list of permissions associated with an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Role-based access control is an approach to restricting system access to authorized users, used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC).

A further approach, capability-based security has been mostly restricted to research operating systems. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open-source project in the area is the E language.

### End user security training

The end-user is widely recognized as the weakest link in the security chain and it is estimated that more than 90% of security incidents and breaches involve some kind of human error. Among the most commonly recorded forms of errors and misjudgment are poor password management, sending emails containing sensitive data and attachments to the wrong recipient, the inability to recognize misleading URLs and to identify fake websites and dangerous email attachments. A common mistake that users make is saving their user id/password in their browsers to make it easier to log in to banking sites. This is a gift to attackers who have obtained access to a machine by some means. The risk may be mitigated by the use of two-factor authentication.

As the human component of cyber risk is particularly relevant in determining the global cyber risk an organization is facing, security awareness training, at all levels, not only provides formal compliance with regulatory and industry mandates but is considered essential in reducing cyber risk and protecting individuals and companies from the great majority of cyber threats.

The focus on the end-user represents a profound cultural change for many security practitioners, who have traditionally approached cybersecurity exclusively from a technical perspective, and moves along the lines suggested by major security

centers to develop a culture of cyber awareness within the organization, recognizing that a security-aware user provides an important line of defense against cyber attacks.

### Digital hygiene

Related to end-user training, **digital hygiene** or **cyber hygiene** is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimize the risks from cyber threats. The assumption is that good cyber hygiene practices can give networked users another layer of protection, reducing the risk that one vulnerable node will be used to either mount attacks or compromise another node or network, especially from common cyberattacks. Cyber hygiene should also not be mistaken for proactive cyber defence, a military term.

As opposed to a purely technology-based defense against threats, cyber hygiene mostly regards routine measures that are technically simple to implement and mostly dependent on discipline or education. It can be thought of as an abstract list of tips or measures that have been demonstrated as having a positive effect on personal and/or collective digital security. As such, these measures can be performed by laypeople, not just security experts.

Cyber hygiene relates to personal hygiene as computer viruses relate to biological viruses (or pathogens). However, while the term computer virus was coined almost simultaneously with the creation of the first working computer viruses, the term cyber hygiene is a much later invention, perhaps as late as 2000 by Internet pioneer Vint Cerf. It has since been adopted by the Congress and Senate of the United States, the FBI EU institutions and heads of state.

### Response to breaches

Responding to attempted security breaches is often very difficult for a variety of reasons, including:

- Identifying attackers is difficult, as they may operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymizing procedures which make back-tracing difficult - and are often located in another jurisdiction. If they successfully breach security, they have also often gained enough administrative access to enable them to delete logs to cover their tracks.
- The sheer number of attempted attacks, often by automated vulnerability scanners and computer worms, is so large that

organizations cannot spend time pursuing each.

- Law enforcement officers often lack the skills, interest or budget to pursue attackers. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, which may be difficult or time-consuming to obtain.

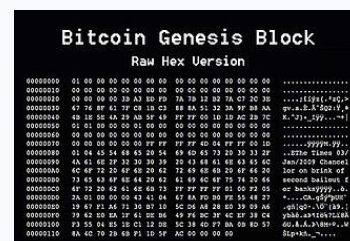
Where an attack succeeds and a breach occurs, many jurisdictions now have in place mandatory security breach notification laws.

### Types of security and privacy

- Access control
- Anti-keyloggers
- Anti-malware
- Anti-spyware
- Anti-subversion software
- Anti-tamper software
- Anti-theft
- Antivirus software
- Cryptographic software
- Computer-aided dispatch (CAD)
- Firewall
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Log management software
- Parental control
- Records management
- Sandbox
- Security information management
- Security information and event management (SIEM)
- Software and operating system updating
- Vulnerability Management

### Cryptocurrency

A logo for Bitcoin, the first decentralized cryptocurrency



The genesis block of Bitcoin's blockchain, with a note containing The Times newspaper headline. This note has been interpreted as a comment on the instability caused by fractional-reserve banking.

A **cryptocurrency**, **crypto-currency**, or **crypto** is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as

a government or bank, to uphold or maintain it. It is a decentralized system for verifying that the parties to a transaction have the money they claim to have, eliminating the need for traditional intermediaries, such as banks, when funds are being transferred between two entities. Individual coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. Despite their name, cryptocurrencies are not considered to be currencies in the traditional sense and while varying treatments have been applied to them, including classification as commodities, securities, as well as currencies, cryptocurrencies are generally viewed as a distinct asset class in practice. Some crypto schemes use validators to maintain the cryptocurrency. In a proof-of-stake model, owners put up their tokens as collateral. In return, they get authority over the token in proportion to the amount they stake. Generally, these token stakers get additional ownership in the token over time via network fees, newly minted tokens or other such reward mechanisms.

Cryptocurrency does not exist in physical form (like paper money) and is typically not issued by a central authority. Cryptocurrencies typically use decentralized control as opposed to a central bank digital currency (CBDC). When a cryptocurrency is minted or created prior to issuance or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database. Traditional asset classes like currencies, commodities, and stocks, as well as macroeconomic factors, have modest exposures to cryptocurrency returns. The first decentralized cryptocurrency was Bitcoin, which first released as open-source software in 2009. As of March 2022, there were more than 9,000 other cryptocurrencies in the marketplace, of which more than 70 had a market capitalization exceeding \$1 billion.

## Cryptocurrency

### Formal definition

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:

1. The system does not require a central authority; its state is maintained through distributed consensus.
2. The system keeps an overview of cryptocurrency units and their ownership.

3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

In March 2018, the word cryptocurrency was added to the Merriam-Webster Dictionary.

### Altcoins

Tokens, cryptocurrencies, and other digital assets other than Bitcoin are collectively known as alternative cryptocurrencies, typically shortened to "altcoins" or "alt coins", or disparagingly "shitcoins". Paul Vigna of The Wall Street Journal also described altcoins as "alternative versions of Bitcoin" given its role as the model protocol for altcoin designers.



The logo of Ethereum, the second largest cryptocurrency

Altcoins often have underlying differences when compared to Bitcoin. For example, Litecoin aims to process a block every 2.5 minutes, rather than Bitcoin's 10 minutes, which allows Litecoin to confirm transactions faster than Bitcoin. Another example is Ethereum, which has smart contract functionality that allows decentralized applications to be run on its blockchain. Ethereum was the most used blockchain in 2020, according to Bloomberg News. In 2016, it had the largest "following" of any altcoin, according to the New York Times. Significant rallies across altcoin markets are often referred to as an "altseason".

### Stablecoins

Stablecoins are cryptocurrencies designed to maintain a stable level of purchasing power. Notably, these designs are not foolproof, as a number of stablecoins have crashed or lost their



peg. For example, on 11 May 2022, Terra's stablecoin UST fell from \$1 to 26 cents. The subsequent failure of Terraform Labs resulted in the loss of nearly \$40B invested in the Terra and Luna bitcoins. In September 2022, South Korean prosecutors requested the issuance of an Interpol Red Notice against the company's founder, Do Kwon.

### Architecture

Cryptocurrency is produced by an entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly stated. In centralized banking and economic systems such as the US Federal Reserve System, corporate boards or governments control the supply of currency. In the case of cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which cryptocurrencies are based was created by Satoshi Nakamoto.

Within a proof-of-work system such as Bitcoin, the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners. Miners use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme. In a proof-of-stake blockchain, transactions are validated by holders of the associated cryptocurrency, sometimes grouped together in stake pools.

Most cryptocurrencies are designed to gradually decrease the production of that currency, placing a cap on the total amount of that currency that will ever be in circulation. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.

### Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given

block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.

### Nodes

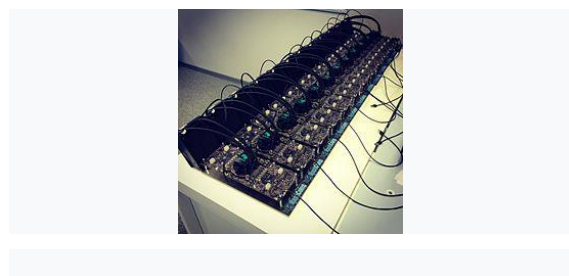
A node is a computer that connects to a cryptocurrency network. The node supports the cryptocurrency's network through either; relaying transactions, validation or hosting a copy of the blockchain. In terms of relaying transactions each network computer (node) has a copy of the blockchain of the cryptocurrency it supports. When a transaction is made the node creating the transaction broadcasts details of the transaction using encryption to other nodes throughout the node network so that the transaction (and every other transaction) is known. Node owners are either volunteers, those hosted by the organization or body responsible for developing the cryptocurrency blockchain network technology, or those who are enticed to host a node to receive rewards from hosting the node network.

### Timestamping

Cryptocurrencies use various timestamping schemes to "prove" the validity of transactions added to the blockchain ledger without the need for a trusted third party. The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and script. The other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11.

Another method is called the proof-of-stake scheme. Proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it. Some cryptocurrencies use a combined proof-of-work and proof-of-stake scheme.

### Mining



### Hashcoin mine

On a blockchain, mining is the validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and script. This arms race for cheaper-yet-efficient machines has existed since Bitcoin was introduced in 2009.

With more people venturing into the world of virtual currency, generating hashes for validation has become more complex over time, forcing miners to invest increasingly large sums of money to improve computing performance. Consequently, the reward for finding a hash has diminished and often does not justify the investment in equipment and cooling facilities (to mitigate the heat the equipment produces), and the electricity required to run them. Popular regions for mining include those with inexpensive electricity, a cold climate, and jurisdictions with clear and conducive regulations. By July 2019, Bitcoin's electricity consumption was estimated to be approximately 7 gigawatts, around 0.2% of the global total, or equivalent to the energy consumed nationally by Switzerland. Some miners pool resources, sharing their processing power over a network to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share" is awarded to members of the mining pool who present a valid partial proof-of-work.

As of February 2018, the Chinese Government has halted trading of virtual currency, banned initial coin offerings and shut down mining. Many Chinese miners have since relocated to Canada and Texas. One company is operating data centers for mining operations at Canadian oil and gas field sites, due to low gas prices. In June 2018, Hydro Quebec proposed to the provincial government to allocate 500 megawatts of power to crypto companies for mining. According to a February 2018 report from Fortune, Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity.

In March 2018, the city of Plattsburgh, New York put an 18-month moratorium on all cryptocurrency mining in an effort to preserve natural resources and the "character and direction" of the city. In 2021, Kazakhstan became the second-biggest crypto-currency mining country, producing 18.1% of the global hash rate. The

country built a compound containing 50,000 computers near Ekibastuz.

### GPU price rise

An increase in cryptocurrency mining increased the demand for graphics cards (GPU) in 2017. The computing power of GPUs makes them well-suited to generating hashes. Popular favorites of cryptocurrency miners such as Nvidia's GTX 1060 and GTX 1070 graphics cards, as well as AMD's RX 570 and RX 580 GPUs, doubled or tripled in price – or were out of stock. A GTX 1070 Ti which was released at a price of \$450 sold for as much as \$1,100. Another popular card, the GTX 1060 (6 GB model) was released at an MSRP of \$250, and sold for almost \$500. RX 570 and RX 580 cards from AMD were out of stock for almost a year. Miners regularly buy up the entire stock of new GPU's as soon as they are available.

Nvidia has asked retailers to do what they can when it comes to selling GPUs to gamers instead of miners. Boris Böhles, PR manager for Nvidia in the German region, said: "Gamers come first for Nvidia."

### Wallets

An example paper printable Bitcoin wallet consisting of one Bitcoin address for receiving and the corresponding private key for spending. A cryptocurrency wallet is a means of storing the public and private "keys" (address) or seed which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet. There exist multiple methods of storing keys or seed in a wallet. These methods range from using paper wallets (which are public, private or seed keys written on paper), to using hardware wallets (which are hardware to store your wallet information), to a digital wallet (which is a computer with a software hosting your wallet information), to hosting your wallet using an exchange where cryptocurrency is traded, or by storing your wallet information on a digital medium such as plaintext.

### Anonymity

Bitcoin is pseudonymous, rather than anonymous; the cryptocurrency in a wallet is not tied to a person, but rather to one or more specific keys (or "addresses"). Thereby, Bitcoin owners are not immediately identifiable, but all transactions are publicly available in the blockchain. Still, cryptocurrency exchanges are often required by law to collect the personal information of their users. Some cryptocurrencies, such as Monero, Zerocoin, Zerocash, and CryptoNote, implement additional measures to

increase privacy, such as by using zero-knowledge proofs.

### Economics

Cryptocurrencies are used primarily outside banking and governmental institutions and are exchanged over the Internet.

### Block rewards

Proof-of-work cryptocurrencies, such as Bitcoin, offer block rewards incentives for miners. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the blockchain, but a study suggests that this may not be the case under certain circumstances. The rewards paid to miners increase the supply of the cryptocurrency. By making sure that verifying transactions is a costly business, the integrity of the network can be preserved as long as benevolent nodes control a majority of computing power. The verification algorithm requires a lot of processing power, and thus electricity in order to make verification costly enough to accurately validate public blockchain. Not only do miners have to factor in the costs associated with expensive equipment necessary to stand a chance of solving a hash problem, they further must consider the significant amount of electrical power in search of the solution. Generally, the block rewards outweigh electricity and equipment costs, but this may not always be the case.

The current value, not the long-term value, of the cryptocurrency supports the reward scheme to incentivize miners to engage in costly mining activities. Some sources claim that the current Bitcoin design is very inefficient, generating a welfare loss of 1.4% relative to an efficient cash system. The main source for this inefficiency is the large mining cost, which is estimated to be US\$360 Million per year. This translates into users being willing to accept a cash system with an inflation rate of 230% before being better off using Bitcoin as a means of payment. However, the efficiency of the Bitcoin system can be significantly improved by optimizing the rate of coin creation and minimizing transaction fees. Another potential improvement is to eliminate inefficient mining activities by changing the consensus protocol altogether.

### Transaction fees

Transaction fees for cryptocurrency depend mainly on the supply of network capacity at the time, versus the demand from the currency holder for a faster transaction. The currency holder can choose a specific transaction fee, while network entities process transactions in order of highest offered fee to lowest. Cryptocurrency exchanges can simplify the process for currency holders by offering priority alternatives and thereby determine which

fee will likely cause the transaction to be processed in the requested time. For Ether, transaction fees differ by computational complexity, bandwidth use, and storage needs, while Bitcoin transaction fees differ by transaction size and whether the transaction uses SegWit. In September 2018, the median transaction fee for Ether corresponded to \$0.017, while for Bitcoin it corresponded to \$0.55. Some cryptocurrencies have no transaction fees, and instead rely on client-side proof-of-work as the transaction prioritization and anti-spam mechanism.

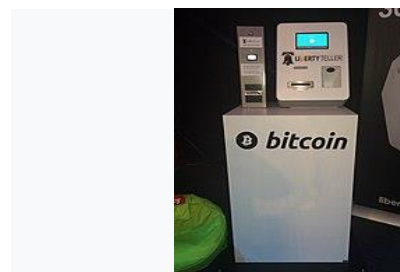
### Exchanges

Cryptocurrency exchanges allow customers to trade cryptocurrencies for other assets, such as conventional fiat money, or to trade between different digital currencies. Crypto marketplaces do not guarantee that an investor is completing a purchase or trade at the optimal price. As a result, many investors take advantage of this by using arbitrage to find the difference in price across several markets.

### Atomic swaps

Atomic swaps are a mechanism where one cryptocurrency can be exchanged directly for another cryptocurrency, without the need for a trusted third party such as an exchange.

### ATMs



### Bitcoin ATM

Jordan Kelley, founder of Robocoin, launched the first Bitcoin ATM in the United States on 20 February 2014. The kiosk installed in Austin, Texas, is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities.

### Initial coin offerings

An initial coin offering (ICO) is a controversial means of raising funds for a new cryptocurrency venture. An ICO may be used by startups with the intention of avoiding regulation. However, securities regulators in many jurisdictions, including in the U.S., and Canada, have indicated that if a coin or token is an "investment contract" (e.g., under the Howey test, i.e., an investment of money with a reasonable expectation of profit



based significantly on the entrepreneurial or managerial efforts of others), it is a security and is subject to securities regulation. In an ICO campaign, a percentage of the cryptocurrency (usually in the form of "tokens") is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, often Bitcoin or Ether.

According to PricewaterhouseCoopers, four of the 10 biggest proposed initial coin offerings have used Switzerland as a base, where they are frequently registered as non-profit foundations. The Swiss regulatory agency FINMA stated that it would take a "balanced approach" to ICO projects and would allow "legitimate innovators to navigate the regulatory landscape and so launch their projects in a way consistent with national laws protecting investors and the integrity of the financial system." In response to numerous requests by industry representatives, a legislative ICO working group began to issue legal guidelines in 2018, which are intended to remove uncertainty from cryptocurrency offerings and to establish sustainable business practices.

### Price trends

The market capitalization of a cryptocurrency is calculated by multiplying the price by the number of coins in circulation. The total cryptocurrency market cap has historically been dominated by Bitcoin accounting for at least 50% of the market cap value where altcoins have increased and decreased in market cap value in relation to Bitcoin. Bitcoin's value is largely determined by speculation among other technological limiting factors known as blockchain rewards coded into the architecture technology of Bitcoin itself. The cryptocurrency market cap follows a trend known as the "halving", which is when the block rewards received from Bitcoin are halved due to technological mandated limited factors instilled into Bitcoin which in turn limits the supply of Bitcoin. As the date reaches near of a halving (twice thus far historically) the cryptocurrency market cap increases, followed by a downtrend. By June 2021, cryptocurrency had begun to be offered by some wealth managers in the US for 401(k)s.


### Volatility

Cryptocurrency prices are much more volatile than established financial assets such as stocks. For example, over one week in May 2022, Bitcoin lost 20% of its value and Ethereum lost 26%, while Solana and Cardano lost 41% and 35% respectively. The falls were attributed to warnings about inflation. By comparison, in the same week, the Nasdaq tech stock index fell 7.6 per cent and the FTSE 100 was 3.6 per cent down. In the longer term, of the 10 leading cryptocurrencies identified by the total value of coins in circulation in January 2018, only four (Bitcoin, Ethereum, Cardano

and Ripple (XRP)) were still in that position in early 2022. The total value of all cryptocurrencies was \$2 trillion at the end of 2021, but had halved nine months later. The Wall Street Journal has commented that the crypto sector has become "intertwined" with the rest of the capital markets and "sensitive to the same forces that drive tech stocks and other risk assets", such as inflation forecasts.

### Databases

There are also centralized databases, outside of blockchains, that store crypto market data. Compared to the blockchain, databases perform fast as there is no verification process. Four of the most popular cryptocurrency market databases are CoinMarketCap, CoinGecko, BraveNewCoin, and Cryptocompare.Cybercrime

Criminology

Main Theories
Conflict theory, Criminalization, Differential association, Integrative criminology, Rational choice theory, Structural functionalism, Subcultural theory, Symbolic interactionism
Methods
Comparative, Profiling, Critical theory, Ethnography, Uniform Crime Reports, Crime mapping, Positivist school, Qualitative, Quantitative, BJS, NIBRS
Subfields and other major theories
American, Anthropological, Biosocial criminology, Conflict, Criminology, Critical, Culture, Cyber, Demography, Development, Environmental, Experimental, Organizational, Political, Public, Radical criminology
Browse
Bibliography, Index, Journals, Organizations, People

A **cybercrime** is a crime that involves a computer or a computer network. The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances. There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in



cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare. Warren Buffett describes cybercrime as the "number one problem with mankind" and said that cybercrime "poses real risks to humanity."

A 2014 report sponsored by McAfee estimated that cybercrime resulted in \$445 billion in annual damage to the global economy. Approximately \$1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1% of global GDP, close to \$600 billion, is lost to cybercrime each year. The World Economic Forum 2020 Global Risk Report confirmed that organized cybercrimes bodies are joining forces to perpetrate criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1% in the US

### **Computer fraud**

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system. If computer fraud involves the use of the Internet, it can be considered Internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorisation.

Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams. Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crimes often result in the loss of private or monetary information.

### **Cyberterrorism**

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by means such as computer viruses, computer worms, phishing, malicious software, hardware methods, or programming scripts can all be forms of cyberterrorism. Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. Within the United States, there is a growing concern among government

agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security holes in critical systems.

### **Cyberextortion**

Cyberextortion is a type of extortion that occurs when a website, e-mail server, or computer system is subjected to or threatened with attacks by malicious hackers, such as denial-of-service attacks. Cyberextortionists demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate, and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack. However, other cyberextortion techniques exist, such as doxing, extortion, and bug poaching. An example of cyberextortion was the attack on Sony Pictures of 2014.

### **Ransomware**

Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. The Kaspersky Lab 2016 Security Bulletin report estimated that a business falls victim to ransomware every 40 minutes, and predicted that number would decrease to 11 minutes by 2021. With ransomware remaining one of the fastest-growing cybercrimes in the world, global ransomware damage is predicted to cost up to \$20 billion in 2021.

### **Cybersex trafficking**

Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam. Victims are abducted, threatened, or deceived and transferred to "cybersex dens". The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection. Perpetrators use social media networks, videoconferences, dating pages, online chat rooms, apps, dark web sites, and other platforms. They use online payment systems and cryptocurrencies to hide their identities. Millions of reports of its occurrence are sent to authorities annually. New legislation and police procedures are needed to combat this type of cybercrime. An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

## Cyberwarfare

The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic significance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the military commanders will adapt the concept of cyberspace operations impact in the future.

### Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, are towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. They are seldom committed by loners, instead usually involving large syndicate groups.

Crimes that primarily target computer networks include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

### Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the like existed before the development of computers and the internet. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

Crimes that use computer networks or devices to advance other ends include:

Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)

- Information warfare

- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware. Or, they may contain links to fake online banking or other websites used to steal private account information.

### Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

### Ad-fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are less likely to be prosecuted and are particularly lucrative cybercrimes. Jean-Loup Richet, Professor at the Sorbonne Business School, classified the large variety of ad-fraud observed in cybercriminal communities into three categories: (1) identity fraud; (2) attribution fraud; and (3) ad-fraud services. Identity fraud aims to impersonate real users and inflate audience numbers. Several ad-fraud techniques relate to this category and include traffic from bots (coming from a hosting company or a data center, or from compromised devices); cookie stuffing; falsifying user characteristics, such as location and browser type; fake social traffic (misleading users on social networks into visiting the advertised website); and the creation of fake social signals to make a bot look more legitimate, for instance by opening a Twitter or Facebook account.

Attribution fraud aims to impersonate real users' behaviors (clicks, activities, conversations, etc.). Multiple ad-fraud techniques belong to this category: hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns; click farms (companies where low-wage employees are paid to

click or engage in conversations and affiliates' offers); incentivized browsing; video placement abuse (delivered in display banner slots); hidden ads (that will never be viewed by real users); domain spoofing (ads served on a website other than the advertised real-time bidding website); and clickjacking (user is forced to click on the ad). Ad fraud services are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud. Services can involve the creation of spam websites (fake networks of websites created to provide artificial backlinks); link building services; hosting services; creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign. A successful ad-fraud campaign involves a sophisticated combination of these three types of ad-fraud—sending fake traffic through bots using fake social accounts and falsified cookies; bots will click on the ads available on a scam page that is faking a famous brand.

### Online harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, or sexual orientation. There are instances where committing a crime using a computer can lead to an enhanced sentence. For example, in the case of *United States v. Neil Scott Kramer*, the defendant was given an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct." Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term "computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

In the United States, over 41 states have passed laws and regulations that regard extreme online harassment as a criminal act. These acts can be punished on a federal scale, such as US Code 18 Section 2261A, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken. Several countries outside of the United States have also created laws to combat online harassment. In China, a country that supports over 20 percent of the world's internet users, the Legislative Affairs

Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine. The United Kingdom passed the Malicious Communications Act, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine. Australia, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the Criminal Code Act of 1995. Using telecommunication to send threats or harass and cause offense was a direct violation of this act. Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact, spoken or written "true threat" speech or text is criminalized because of "intent to harm or intimidate". That also applies to online or network-related threats in written text or speech. Cyberbullying has increased drastically with the growing popularity of online social networking. As of January 2020, 44% of adult internet users in the United States have "personally experienced online harassment". Children who experience online harassment deal with negative and sometimes life-threatening side effects. In 2021, reports displayed 41% of children developing social anxiety, 37% of children developing depression, and 26% of children having suicidal thoughts.

The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group's mobile spyware Pegasus for mass surveillance. Prominent activists and journalists were targeted as part of the campaign, including Ahmed Mansoor, Princess Latifa, Princess Haya, and more. Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment. Oueiss filed a lawsuit against UAE ruler Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online. The defendants, including the UAE ruler, filed motions to dismiss the case of the hack-and-leak attack.

### Drug trafficking

Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers. The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011. It was permanently shut down in 2014 by the FBI and Europol. After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace

named Diabolus Market, that used the name for more exposure from the brand's previous success. Darknet markets have had a rise in traffic in recent years for many reasons, one of the biggest contributors being the anonymity offered in purchases, and often a seller-review system. There are many ways in which darknet markets can financially drain individuals. Vendors and customers alike go to great lengths to keep their identities a secret while online. Commonly used tools are virtual private networks, Tails, and the Tor Browser to help hide their online presence. Darknet markets entice customers by making them feel comfortable. People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome. However, actually gaining access to an illicit market is not as simple as typing it in on a search engine like one would with Google. Darknet markets have special links that change frequently, ending in .onion as opposed to the typical .com, .net, and .org domain extensions. To add to privacy, the most prevalent currency on these markets is Bitcoin. Bitcoin allows transactions to be anonymous, with the only information available to the public being the record that a transaction occurred between two parties. One of the biggest issues the users who use marketplaces face is when vendors or the market itself are exit scamming. This is when usually a vendor with a high rating will act as if they are still selling on the market and have users pay for products they will not receive. The vendor will then close off their account after receiving money from multiple buyers and never send what they purchased. The vendors all being involved in illegal activities have a low chance of not exit scamming when they no longer want to be a vendor. In 2019, an entire market known as Wall Street Market had allegedly exit scammed, stealing 30 million dollars from the vendors' and buyers' wallets in bitcoin.

Federal agents have cracked down on these markets. In July 2017, federal agents seized one of the biggest markets, commonly called Alphabay, which later re-opened in August 2021 under the control of DeSnake, one of the original administrators. Commonly, investigators will pose as a buyer and order products from darknet vendors in the hopes that vendors leave a trail the investigators can follow. One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses. The investigators were able to make over a dozen arrests during this six-month investigation. Another one of law enforcement's biggest crackdowns is on vendors selling fentanyl and opiates. With thousands of people dying each year due to drug overdose, investigators have made it a priority. Many vendors do not realize the extra criminal charges that go

along with selling drugs online. Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor. In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife. Although many investigators spend large amounts of time tracking down people, in 2018, only 65 suspects who bought and sold illegal goods on some of the biggest markets were identified. This is compared to the thousands of transactions taking place daily on these markets.

### Cyber Security

**Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

- Risk Management Regime: Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.
- Secure configuration: Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.
- Network security: The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.



- Managing user privileges: If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.
- User education and awareness: Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.
- Incident management: All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.
- Malware prevention: Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.
- Monitoring: System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.
- Removable media controls: Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable

media and apply appropriate security controls to its use.

- Home and mobile working: Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

### **The Importance of Cybersecurity**

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization.

A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It's estimated that, on average, a data breach costs an affected organization \$3.6 million. With high-profile data breaches making media headlines, it's essential that organizations adopt and implement a strong cybersecurity approach.

### **Fintech**

#### **Finance**



Fintech meetup at Hilton Colombo in Sri Lanka

**Fintech**, a portmanteau of "**financial technology**", refers to firms using new technology to compete with traditional financial methods in the delivery of financial services. Artificial intelligence, Blockchain, Cloud computing, and big data are regarded as the "ABCD" (four key areas) of FinTech. The use of smartphones for mobile banking, investing, borrowing services, and cryptocurrency are examples of technologies designed to make financial services more accessible to the general public. Financial technology companies consist of both startups and established financial institutions and technology companies trying to replace or enhance the usage of financial services provided by existing financial companies. A subset of fintech companies that focus on the insurance industry are collectively known as **insurtech** or **insuretech** companies.

### Definition

After reviewing more than 200 scientific papers citing the term "fintech", a study on the definition of fintech concluded that "fintech is a new financial industry that applies technology to improve financial activities." Fintech is the new applications, processes, products, or business models in the financial services industry, composed of one or more complementary financial services and provided as an end-to-end process via the Internet.

### Academics

Artificial Intelligence (AI), Blockchain, Cloud Computing, and Big Data are considered the four key areas of FinTech. Artificial intelligence refers to the intelligence demonstrated by machines, in contrast with "natural intelligence" displayed by humans and animals. AI is assuming an increasingly important role in traditional banking as it provides technologies such as voice recognition, natural language processing, and computer vision for user-account management and fraud detection, machine learning methods and deep learning networks for anti-moneylaundering and credit modeling. Mobile and internet payment systems are closely connected to cloud computing. The past ten years have witnessed increasing adoption of cloud computing by financial institutions around the globe.

### FinTech Industry

Financial technology has been used to automate investments, insurance, trading, banking services and risk management. The services may originate from various independent service providers including at least one licensed bank or insurer. The interconnection is enabled through open APIs and open banking and supported by regulations such as the European Payment Services Directive. Robo-advisers are a class of

automated financial adviser that provide financial advice or investment management online with moderate to minimal human intervention. They provide digital financial advice based on mathematical rules or algorithms, and thus can provide a low-cost alternative to a human advisers.

Global investment in financial technology increased more than 12,000% from \$930 million in 2008 to \$121.6 billion in 2020. 2019 saw a record high with the total global investment in financial technology being \$215.3 billion, of which Q3 alone accounted for \$144.7 billion in investment. In H1 2021, Fintech deal volume hit 2,456 deals accounting for \$98 billion in investment. Global VC investment was higher than \$52 billion in H1'21, close to the annual record of \$54 billion seen in 2018. H1'21 saw \$21 billion in corporate-affiliated VC investment. CVC deal volume reached a high of 284 in Q1'21, and then grew further to 312 in Q2'21. The Americas saw about \$51.4 billion of fintech investment in H1'21, with the US alone accounting for \$42.1 billion. In the EMEA region, investment in fintech was very robust at \$39.1 billion. In Asia-Pacific, fintech investment grew between H2'20 and H1'21 — rising from \$4.5 billion to \$7.5 billion, although it was subdued in comparison with previous record highs.

The nascent financial technology industry in London has seen rapid growth over the last few years, according to the office of the Mayor of London. Forty percent of the City of London's workforce is employed in financial and technology services. As of April 2019, about 76,500 people form the UK-wide FinTech workforce, and this number is projected to rise to 105,500 by 2030. Of the current fintech workforce in the UK, 42% of workers are from overseas. In Europe, \$1.5 billion was invested in financial technology companies in 2014, with London-based companies receiving \$539 million, Amsterdam-based companies \$306 million, and Stockholm-based companies receiving \$266 million in investment. After London, Stockholm is the second highest funded city in Europe in the past 10 years. Europe's fintech deals reached a five-quarter high, rising from 37 in Q4 2015 to 47 in Q1 2016. Lithuania is starting to become a northern European hub for financial technology companies since the news in 2016 about the exit of Britain from the European Union. Lithuania has issued 51 fintech licenses since 2016, 32 of those in 2017. Fintech companies in the United States raised \$12.4 billion in 2018, a 43% increase over 2017 figures.



Christine Lagarde, Managing Director of the International Monetary Fund addressing in 2018 at the Singapore FinTech Festival, the largest FinTech festival in the world.

In the Asia Pacific region, the growth will see a new financial technology hub to be opened in Sydney, in April 2015. According to KPMG, Sydney's financial services sector in 2017 creates 9 per cent of national GDP and is bigger than the financial services sector in either Hong Kong or Singapore. A financial technology innovation lab was launched in Hong Kong in 2015. In 2015, the Monetary Authority of Singapore launched an initiative named Fintech and Information Group to draw in start-ups from around the world. It pledged to spend \$225 million in the fintech sector over the next five years. While Singapore has been one of the central Fintech hubs in Asia, start ups in the sector from Vietnam and Indonesia have been attracting more venture capital investments in recent years. Since 2014, Southeast Asian Fintech companies have increased VC funding from \$35 million to \$679 million in 2018 and \$1.14 billion in 2019. Africa's overall FinTech sector has expanded quickly. There were more over 1000 active businesses as of April 2022, up from 450 in 2020. The venture capital sector, which saw deal value rise from \$485 million in 2020 to \$3.23 billion in 2021, was mostly responsible for the increase in investment in Africa. About half of this investment was made in FinTech.

### Technologies

Fintech companies use a variety of technologies, including artificial intelligence (AI), big data, robotic process automation (RPA), and blockchain. AI algorithms can provide insight on customer spending habits, allowing financial institutions to better understand their clients. Chatbots are another AI-driven tool that banks are starting to use to help with customer service.

Big data can predict client investments and market changes in order to create new strategies and portfolios, analyze customer spending habits, improve fraud detection, and create marketing strategies. Robotic Process Automation is an artificial intelligence technology that focuses on automating specific repetitive tasks. RPA helps to process financial information such as accounts

payable and receivable more efficiently than the manual process and often more accurately. Blockchain is an emerging technology in finance which has driven significant investment from many companies. The decentralized nature of blockchain can eliminate the need for a third party to execute transactions.

### Awards and recognition

Financial magazine Forbes created a list of the leading disruptors in financial technology for its Forbes 2021 global Fintech 50. In Europe there is a list called the FinTech 50, which aims to recognise the most innovative companies in fintech. A report published in February 2016 by EY commissioned by the UK Treasury compared seven leading fintech hubs: the United Kingdom, California, New York

City, Singapore, Germany, Australia and Hong Kong. It ranked California first for 'talent' and 'capital', the United Kingdom first for 'government policy' and New York City first for 'demand'. For the past few years, PwC has posted a report called the "Global Fintech Report". The 2019 report covers many topics of the financial technology sector, describing the landscape of the "Fintech" industry, and some of the emerging technologies in the sector. And it provides strategies for financial institutions on how to incorporate more "fintech" technologies into their business.

### Outlook

Finance is seen as one of the industries most vulnerable to disruption by software because financial services, much like publishing, are made of information rather than concrete goods. In particular blockchains have the potential to reduce the cost of transacting in a financial system. While finance has been shielded by regulation until now, and weathered the dot-com boom without major upheaval, a new wave of startups is increasingly "disaggregating" global banks. However, aggressive enforcement of the Bank Secrecy Act and money transmission regulations represents an ongoing threat to fintech companies. In response, the International Monetary Fund (IMF) and the World Bank jointly presented Bali Fintech Agenda on October 11, 2018 which consists of 12 policy elements acting as a guidelines for various governments and central banking institutions to adopt and deploy "rapid advances in financial technology". The New York Venture Capital Association (NYVCA) hosts annual summits to educate those interested in learning more about fintech. In 2018 alone, fintech was responsible for over 1,700 deals worth over 40 billion dollars. In 2021, one in every five dollars invested by venture capital has gone into fintech.



## Challenges and solutions

In addition to established competitors, fintech companies often face doubts from financial regulators like issuing banks and the Federal Government. In July 2018, the Trump Administration issued a policy statement that allowed FinTech companies to apply for special purpose national bank charters from the federal Office of the Comptroller of the Currency. Federal preemption applies to state law regarding federally chartered banks. Data security is another issue regulators are concerned about because of the threat of hacking as well as the need to protect sensitive consumer and corporate financial data. Leading global fintech companies are proactively turning to cloud technology to meet increasingly stringent compliance regulations. The Federal Trade Commission provides free resources for corporations of all sizes to meet their legal obligations of protecting sensitive data. Several private initiatives suggest that multiple layers of defense can help isolate and secure financial data.

In the European Union, fintech companies must adhere to data protection laws, such as GDPR. Companies need to proactively protect users and companies data or face fines of 20 million euros, or in the case of an undertaking, up to 4% of their total global turnover. In addition to GDPR, European financial institutions including fintech firms have to update their regulatory affairs departments with the Payment Services Directive (PSD2), meaning they must organise their revenue structure around a central goal of privacy. Any data breach, no matter how small, can result in direct liability to a company (see the Gramm–Leach–Bliley Act) and ruin a fintech company's reputation. The online financial sector is also an increasing target of distributed denial of service extortion attacks. This security challenge is also faced by historical bank companies since they do offer Internet-connected customer services. Many FinTech technologies have very high start-up costs but very low marginal costs for adding additional customers, effectively necessitating many FinTechs to act as natural monopolies

## REFERENCES

- [1]. "#Cybercrime— what are the costs to victims - North Denver News". North Denver News. 17 January 2015. Retrieved 16 May 2015.
- [2]. "Bitcoin not a currency says Japan government". BBC News. 7 March 2014. Retrieved 25 January 2022.
- [3]. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Retrieved 5 September 2021.
- [4]. "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2021.
- [5]. "Chapter 3: Computer Forensic Fundamentals - Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives [Book]". www.oreilly.com. Retrieved 2022-03-04.
- [6]. "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.
- [7]. "computer security | Definition & Facts | Britannica". www.britannica.com. Retrieved 12 July 2022.
- [8]. "Computer Security and Mobile Security Challenges". researchgate.net. 3 December 2015. Archived from the original on 12 October 2016. Retrieved 4 August 2016.
- [9]. "Cryptocurrencies: What Are They?". Schwab Brokerage.
- [10]. "Cyber crime costs global economy \$445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.
- [11]. "cybercrime | Definition". Encyclopedia Britannica. Retrieved 25 May 2021.
- [12]. "cybercrime | Definition, Statistics, & Examples | Britannica". www.britannica.com. Retrieved 14 December 2021.
- [13]. "Email Security | Trellix". www.trellix.com. Retrieved 24 October 2022.
- [14]. "EXP-SA: Prediction and Detection of Network Membership through Automated Hard Drive Analysis".
- [15]. "Ghidra". Archived from the original on 15 August 2020. Retrieved 17 August 2020.
- [16]. "How To Make A Mint: The Cryptography of Anonymous Electronic Cash". groups.csail.mit.edu. Archived from the original on 26 October 2017. Retrieved 11 January 2018.
- [17]. "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015. Retrieved 4 July 2016.
- [18]. "Insurtech startups are leveraging rapid growth to raise big money". TechCrunch. April 20, 2021. Retrieved October 13, 2021.



- [19]. "Is it a currency? A commodity? Bitcoin has an identity crisis". Reuters. 3 March 2020. Retrieved 25 January 2022.
- [20]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. 2021. Retrieved December 28, 2021.
- [21]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. 2021. Retrieved December 28, 2021.
- [22]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. Retrieved December 28, 2021.
- [23]. "KPMG Pulse of FinTech H1 2021 Global". KPMG. 2021. Retrieved December 28, 2021.
- [24]. "Reliance spells end of road for ICT amateurs". The Australian. 7 May 2013.
- [25]. "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.
- [26]. "The Surprising Way Startups Are Disrupting the Life-Insurance Business". Wall Street Journal. June 10, 2019. Retrieved October 13, 2021.
- [27]. "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. Retrieved 17 May 2021.
- [28]. "What Is Computer Forensics?". Western Governors University. Retrieved 2022-03-04.
- [29]. "What is FinTech and why does it matter to all entrepreneurs?". Hot Topics. July 2014. Retrieved December 9, 2014.
- [30]. A. J. Neumann, N. Statland and R. D. Webb (1977). "Post-processing audit tools and techniques" (PDF). nist.gov. US Department of Commerce, National Bureau of Standards. pp. 11-3–11-4. Retrieved 19 June 2020.
- [31]. Aaron Phillip; David Cowen; Chris Davis (2009). Hacking Exposed: Computer Forensics. McGraw Hill Professional. p. 544. ISBN 978-0-07-162677-4. Retrieved 27 August 2010.
- [32]. Adams, R. (2012). "The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice".
- [33]. Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless". International Business Times. Archived from the original on 12 September 2015. Retrieved 15 September 2015.
- [34]. Arcos Sergio. "Social Engineering" (PDF). upc.edu. Archived (PDF) from the original on 3 December 2013. Retrieved 16 April 2019.
- [35]. Bezek, Ian (14 July 2021). "What Is Proof-of-Stake, and Why Is Ethereum Adopting It?".
- [36]. Bossler, Adam M.; Berenblum, Tamar (20 October 2019). "Introduction: new directions in cybercrime research". Journal of Crime and Justice. **42** (5): 495–499. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.
- [37]. Brown, Aaron (7 November 2017). . www.bloomberg.com. Retrieved 25 January 2022.
- [38]. Chaum, David. "Blind Signatures for Untraceable Payments" (PDF). www.hit.bme.hu. Archived from the original (PDF) on 18 December 2014. Retrieved 26 October 2014.
- [39]. Chaum, David. "Untraceable Electronic Cash" (PDF). blog.koehntopp.de. Archived (PDF) from the original on 3 September 2011. Retrieved 10 October 2012.
- [40]. Chen, Chiu-Chin; Liao, Chia-Chun (September 15, 2021). "Research on the development of Fintech combined with AIoT". 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). IEEE. pp. 1–2. doi:10.1109/icce-tw52618.2021.9602952. ISBN 978-1-6654-3328-0. Fintech is an industry that uses a series of technological innovations such as cloud computing and big data to allow technology to serve finance and greatly improve financial efficiency.
- [41]. Dunbar, B (January 2001). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment".
- [42]. Eilam, Eldad (2005). Reversing: secrets of reverseengineering. John Wiley & Sons. ISBN 978-0-7645-7481-8.
- [43]. Garfinkel, S. (August 2006). "Forensic Feature Extraction and Cross-Drive Analysis".
- [44]. Geiger, M (March 2005). "Evaluating Commercial Counter-Forensic Tools" (PDF). Archived from the original (PDF) on 2014-12-30. Retrieved 2012-04-02.
- [45]. Gordon, Sarah (25 July 2006). "On the definition and classification of

- cybercrime". Journal in Computer Virology. **2**: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
- [46]. G0safeonline (12 November 2014). "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.
- [47]. Gunsch, G (August 2002). "An Examination of Digital Forensic Models" (PDF).
- [48]. Hennessy, John L., & Patterson, David A. (2019). Computer Architecture: A Quantitative Approach, 6th Edition. Cambridge, Massachusetts: Morgan Kaufmann Publishers
- [49]. Infinite Financial Intermediation, 50 Wake Forest Law Review 643 (2015)
- [50]. Irwin, Luke (5 April 2018). "How NIST can protect the CIA triad, including the often overlooked 'I' – integrity". www.itgovernanceusa.com. Retrieved 16 January 2021.
- [51]. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten (2008-02-21). "Lest We Remember: Cold Boot Attacks on Encryption Keys". Princeton University. Retrieved 2009-11-20.
- [52]. Jump up to:<sup>a b</sup> "Vietnam closes in on Singapore as fintech funding booms". Nikkei Asian Review. Retrieved December 4, 2019.
- [53]. Jump up to:<sup>a b</sup> Andy Greenberg (20 April 2011). "Crypto Currency". Forbes. Archived from the original on 31 August 2014. Retrieved 8 August 2014.
- [54]. Jump up to:<sup>a b c</sup> Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 978-0-12-163104-8.
- [55]. Jump up to:<sup>a b c d e</sup> Pollard, Carol (2008). Computer Forensics for Dummies. John Wiley & Sons, Incorporated. pp. 219–230. ISBN 9780470434956.
- [56]. Jump up to:<sup>a b c d e</sup> Rajesh, K.V.N; Ramesh, K.V.N. (2016). "Computer Forensics: An Overview". I-manager's Journal on Software Engineering. **10** (4): 1–5. doi:10.26634/jse.10.4.6056. ProQuest 181 6335831.
- [57]. Jump up to:<sup>a b c</sup> Nicole Perlroth (7 February 2021). "How the U.S. Lost to Hackers". The New York Times. Archived from the original on 28 December 2021. Retrieved 9 February 2021.
- [58]. Jump up to:<sup>a b</sup> Misa, Thomas J. (2016). "Computer Security Discourse at RAND, SDC, and NSA (1958-1970)". IEEE Annals of the History of Computing. **38** (4): 12–25. doi:10.1109/MAHC.2016.48. S2CID 17 609542.
- [59]. Jump up to:<sup>a b</sup> Richet, Jean-Loup (1 January 2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change. **174** (121282): 121282. doi:10.1016/j.techfore.2021.121282 . ISSN 0040-1625. S2CID 239962449.
- [60]. Jump up to:<sup>a b</sup> Various (2009). Eoghan Casey (ed.). Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 978-0-12-374267-4. Retrieved 27 August 2010.
- [61]. Justice, Matthew. (2021). How Computers Really Work. San Francisco, California: No Starch Press.
- [62]. Kianpour, Mazaher; Kowalski, Stewart; Øverby, Harald (2021). "Systematically Understanding Cybersecurity Economics: A Survey". Sustainability. **13** (24): 13677. doi:10.3390/su132413677.
- [63]. Lai, T. L.; Liao, S.-W.; Wong, S. P. S.; Xu, H. (2020). "Statistical models and stochastic optimization in financial technology and investment science" (PDF). Annals of Mathematical Sciences and Applications. **5** (2): 317–345. doi:10.4310/AMSA.2020.v5.n2.a5. S2 CID 240302839.
- [64]. Lai, T. L.; Liao, S.-W.; Wong, S. P. S.; Xu, H. (2020). "Statistical models and stochastic optimization in financial technology and investment science" (PDF). Annals of Mathematical Sciences and Applications. **5** (2): 317–345. doi:10.4310/AMSA.2020.v5.n2.a5. S2 CID 240302839.
- [65]. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53. ISBN 9781438110196.
- [66]. Larabel, Michael (28 December 2017). "Syzbot: Google Continuously Fuzzing The Linux

- Kernel". [www.phoronix.com/](http://www.phoronix.com/). Retrieved 25 March 2021.
- [67]. Law, Laurie; Sabett, Susan; Solinas, Jerry (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash". *American University Law Review*. **46** (4). Archived from the original on 12 January 2018. Retrieved 11 January 2018
- [68]. Lazarus, Ari (23 February 2018). "Phishers send fake invoices". *Consumer Information*. Retrieved 17 February 2020.
- [69]. Lehman, Jeffrey; Phelps, Shirelle (2005). *West's Encyclopedia of American Law*, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.
- [70]. Leigland, R (September 2004). "A Formalization of Digital Forensics" (PDF).
- [71]. Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (PDF).
- [72]. Lieber, Ron (April 11, 2014). "Financial Advice for People Who Aren't Rich". *The New York Times*. (subscription required)
- [73]. Liu, Jinan; Rahman, Sajjadur; Serletis, Apostolos (2020). "Cryptocurrency Shocks". *SSRN Electronic Journal*. doi:10.2139/ssrn.3744260. ISSN 1556-5068. S2CID 233751995.
- [74]. Malvino, Albert P., & Brown, Jerald A. (1993). *Digital Computer Electronics*, 3rd Edition. New York, New York: Glencoe McGraw-Hill
- [75]. Matteo D'Agnolo. "All you need to know about Bitcoin". *timesofindia-economictimes*. Archived from the original on 26 October 2015.
- [76]. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence". Retrieved 26 July 2010.
- [77]. Millman, Renee (15 December 2017). "New polymorphic malware evades three-quarters of AV scanners". *SC Magazine UK*.
- [78]. Milutinović, Monia (2018). "Cryptocurrency". *Ekonomika*. **64** (1): 105–122. doi:10.5937/ekonomika1801105M. ISSN N 0350-137X.
- [79]. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
- [80]. Nakashima, Ellen (26 January 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions". *The Washington Post*. Retrieved 8 February 2021.
- [81]. Null, Linda, & Lobur, Julia. (2019). *The Essentials of Computer Organization and Architecture*. 5th Edition. Burlington, Massachusetts: Jones and Bartlett Learning.
- [82]. Pagliery, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. ISBN 978-1629370361. Archived from the original on 21 January 2018. Retrieved 20 January 2018.
- [83]. Parker D (1983) *Fighting Computer Crime*, U.S.: Charles Scribner's Sons.
- [84]. Patt, Yale N., & Patel, Sanjay J. (2020). *Introduction to Computing Systems: From Bits and Gates to C and Beyond*, 3rd Edition. New York, New York: McGraw Hill Education.
- [85]. Pernice, Ingolf G. A.; Scott, Brett (20 May 2021). "Cryptocurrency". *Internet Policy Review*. **10** (2). doi:10.14763/2021.2.1561. I SSN 2197-6775.
- [86]. Perrin, Chad (30 June 2008). "The CIA Triad". *techrepublic.com*. Retrieved 31 May 2012.
- [87]. Petzold, Charles. (2009). *Code: The Hidden Language of Computer Hardware and Software*. Redmond, Washington: Microsoft Press.
- [88]. Pitta, Julie. "Requiem for a Bright Idea". *Forbes*. Archived from the original on 30 August 2017. Retrieved 11 January 2018.
- [89]. Polansek, Tom (2 May 2016). "CME, ICE prepare pricing data that could boost bitcoin". *Reuters*. Retrieved 3 May 2016.
- [90]. Ruddenklau, Ian Pollari, Anton (August 9, 2021). "Pulse of Fintech H1 2021 – Global - KPMG Global". *KPMG*. Retrieved January 3, 2022.
- [91]. Sanicola, Lenny (February 13, 2017). "What is FinTech?". *Huffington Post*. Retrieved August 20, 2017.
- [92]. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law*. **12** (2). ISSN 1558-7215.

- [93]. Schueffel, Patrick (March 9, 2017). "Taming the Beast: A Scientific Definition of Fintech". *Journal of Innovation Management*. **4** (4): 32–54. doi:10.24840/2183-0606\_004.004\_0004.
- [94]. Scott, John Clark. (2009). *But How Do It Know? The Basic Principles of Computers for Everyone*. Oldsmar, Florida: John C. Scott.
- [95]. Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). *Politics and Governance*. **6** (2): 1–4. doi:10.17645/pag.v6i2.1569.
- [96]. Stoneburner, G.; Hayden, C.; Feringa, A. (2004). "Engineering Principles for Information Technology Security" (PDF). *csrc.nist.gov*. doi:10.6028/NIST.SP.800-27rA.
- [97]. Van Loo, Rory (February 1, 2018). "Making Innovation More Competitive: The Case of Fintech". *UCLA Law Review*. **65** (1): 232.
- [98]. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
- [99]. Warren G. Kruse; Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9. Retrieved 6 December 2010.
- [100]. Webroot (24 July 2018). "Multi-Vector Attacks Demand Multi-Vector Protection". *MSSP Alert*. Retrieved 11 May 2022.
- [101]. Yaffe-Bellany, David (15 September 2022). "Crypto's Long-Awaited 'Merge' Reaches the Finish Line". *The New York Times*. Retrieved 16 September 2022.
- [102]. Yasinsac, A.; Erbacher, R.F.; Marks, D.G.; Pollitt, M.M.; Sommer, P.M. (July 2003). "Computer forensics education". *IEEE Security & Privacy*. **1** (4): 15–23. doi:10.1109/MSECP.2003.1219052.
- [103]. Yost, Jeffrey R. (April 2015). "The Origin and Early History of the Computer Security Software Products Industry". *IEEE Annals of the History of Computing*. **37** (2): 46–58. doi:10.1109/MAHC.2015.21. ISSN 1934-1547. S2CID 18929482.