**Computer security**

From Wikipedia, the free encyclopedia

Jump to: [navigation](http://en.wikipedia.org/wiki/Computer_security#mw-head), [search](http://en.wikipedia.org/wiki/Computer_security#p-search)

This article is about computer security through design and engineering. For computer security exploits and defenses, see [computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity).

|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/en/thumb/9/99/Question_book-new.svg/50px-Question_book-new.svg.png | This article **needs additional citations for verification**. Please help [improve this article](http://en.wikipedia.org/w/index.php?title=Computer_security&action=edit) by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help:Introduction_to_referencing/1). Unsourced material may be [challenged](http://en.wikipedia.org/wiki/Template:Citation_needed) and [removed](http://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(September 2010)* |

|  |
| --- |
| **Computer security** |
| * [Secure operating systems](http://en.wikipedia.org/wiki/Security-focused_operating_system) * [Security by design](http://en.wikipedia.org/wiki/Security_by_design) * [Secure coding](http://en.wikipedia.org/wiki/Secure_coding) |
| [**Computer insecurity**](http://en.wikipedia.org/wiki/Computer_insecurity) |
| * [Vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)   + [Eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping) * [Exploits](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29)   + [Trojans](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29)   + [Viruses](http://en.wikipedia.org/wiki/Computer_virus) and [worms](http://en.wikipedia.org/wiki/Computer_worm)   + [Denial of service](http://en.wikipedia.org/wiki/Denial_of_service) * [Payloads](http://en.wikipedia.org/wiki/Payload_%28computing%29)   + [Rootkits](http://en.wikipedia.org/wiki/Rootkit)   + [Keyloggers](http://en.wikipedia.org/wiki/Keylogger) |
| * [v](http://en.wikipedia.org/wiki/Template:Computer_security) * [t](http://en.wikipedia.org/wiki/Template_talk:Computer_security) * [e](http://en.wikipedia.org/w/index.php?title=Template:Computer_security&action=edit) |

**Computer security** is [information security](http://en.wikipedia.org/wiki/Information_security) as applied to [computers](http://en.wikipedia.org/wiki/Computer) and networks.

The field covers all the processes and mechanisms by which computer-based equipment, information or data and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

|  |
| --- |
| **Contents**   * [1 Security by design](http://en.wikipedia.org/wiki/Computer_security#Security_by_design) * [2 Security architecture](http://en.wikipedia.org/wiki/Computer_security#Security_architecture) * [3 Hardware mechanisms that protect computers and data](http://en.wikipedia.org/wiki/Computer_security#Hardware_mechanisms_that_protect_computers_and_data) * [4 Secure operating systems](http://en.wikipedia.org/wiki/Computer_security#Secure_operating_systems) * [5 Secure coding](http://en.wikipedia.org/wiki/Computer_security#Secure_coding) * [6 Capabilities and access control lists](http://en.wikipedia.org/wiki/Computer_security#Capabilities_and_access_control_lists) * [7 Applications](http://en.wikipedia.org/wiki/Computer_security#Applications)   + [7.1 Cloud computing security](http://en.wikipedia.org/wiki/Computer_security#Cloud_computing_security)   + [7.2 Aviation](http://en.wikipedia.org/wiki/Computer_security#Aviation)     - [7.2.1 Notable system accidents](http://en.wikipedia.org/wiki/Computer_security#Notable_system_accidents) * [8 Cybersecurity breach stories](http://en.wikipedia.org/wiki/Computer_security#Cybersecurity_breach_stories) * [9 Computer security policy](http://en.wikipedia.org/wiki/Computer_security#Computer_security_policy)   + [9.1 United States](http://en.wikipedia.org/wiki/Computer_security#United_States)     - [9.1.1 Cybersecurity Act of 2010](http://en.wikipedia.org/wiki/Computer_security#Cybersecurity_Act_of_2010)     - [9.1.2 International Cybercrime Reporting and Cooperation Act](http://en.wikipedia.org/wiki/Computer_security#International_Cybercrime_Reporting_and_Cooperation_Act)     - [9.1.3 Protecting Cyberspace as a National Asset Act of 2010](http://en.wikipedia.org/wiki/Computer_security#Protecting_Cyberspace_as_a_National_Asset_Act_of_2010)     - [9.1.4 White House proposes cybersecurity legislation](http://en.wikipedia.org/wiki/Computer_security#White_House_proposes_cybersecurity_legislation)   + [9.2 Germany](http://en.wikipedia.org/wiki/Computer_security#Germany)     - [9.2.1 Berlin starts National Cyber Defense Initiative](http://en.wikipedia.org/wiki/Computer_security#Berlin_starts_National_Cyber_Defense_Initiative)   + [9.3 Hacking Back](http://en.wikipedia.org/wiki/Computer_security#Hacking_Back) * [10 Terminology](http://en.wikipedia.org/wiki/Computer_security#Terminology) * [11 Legal issues and global regulation](http://en.wikipedia.org/wiki/Computer_security#Legal_issues_and_global_regulation) * [12 Notes](http://en.wikipedia.org/wiki/Computer_security#Notes) * [13 See also](http://en.wikipedia.org/wiki/Computer_security#See_also) * [14 References](http://en.wikipedia.org/wiki/Computer_security#References) * [15 External links](http://en.wikipedia.org/wiki/Computer_security#External_links) |

**Security by design**

Main article: [Security by design](http://en.wikipedia.org/wiki/Security_by_design)

One way to think of computer security is to reflect security as one of the main features

Some of the techniques in this approach include:

* The [principle of least privilege](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Attacker) gains access to that part, they have only limited access to the whole system.
* [Automated theorem proving](http://en.wikipedia.org/wiki/Automated_theorem_proving) to prove the correctness of crucial software subsystems.
* [Code reviews](http://en.wikipedia.org/wiki/Code_review) and [unit testing](http://en.wikipedia.org/wiki/Unit_testing) are approaches to make modules more secure where formal correctness proofs are not possible
* [Defense in depth](http://en.wikipedia.org/wiki/Defense_in_depth_%28computing%29), 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](http://en.wikipedia.org/wiki/Fail-safe) for the equivalent in [safety engineering](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Audit_trail) tracking 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](http://en.wikipedia.org/wiki/Full_disclosure) to ensure that when bugs are found the "[window of vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)" is kept as short as possible.

**Security architecture**

Security Architecture can be defined 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 to maintain the system's quality attributes: [confidentiality](http://en.wikipedia.org/wiki/Confidentiality), [integrity](http://en.wikipedia.org/wiki/Integrity), [availability](http://en.wikipedia.org/wiki/Availability), [accountability](http://en.wikipedia.org/wiki/Accountability) and [assurance services](http://en.wikipedia.org/wiki/Assurance_services).[[1]](http://en.wikipedia.org/wiki/Computer_security#cite_note-1)

**Hardware mechanisms that protect computers and data**

See also: [Computer security compromised by hardware failure](http://en.wikipedia.org/wiki/Computer_security_compromised_by_hardware_failure)

Hardware based or assisted computer security offers an alternative to software-only computer security. Devices such as [dongles](http://en.wikipedia.org/wiki/Dongle), case intrusion detection, drive locks, or disabling USB ports, or CD ROM Drives may be considered more secure due to the physical access required in order to be compromised[[*original research?*](http://en.wikipedia.org/wiki/Wikipedia:No_original_research)].

**Secure operating systems**

Main article: [Security-focused operating system](http://en.wikipedia.org/wiki/Security-focused_operating_system)

One use of the term computer security refers to technology to implement a secure [operating system](http://en.wikipedia.org/wiki/Operating_system). Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever. Though still valid, the technology is in limited use today, primarily because it imposes some changes to system management and also because it is not widely understood. Such ultra-strong secure operating systems are based on [operating system kernel](http://en.wikipedia.org/wiki/Operating_system_kernel) technology that can guarantee that certain security policies are absolutely enforced in an operating environment. An example of such a [Computer security policy](http://en.wikipedia.org/wiki/Computer_security_policy) is the [Bell-LaPadula model](http://en.wikipedia.org/wiki/Bell-LaPadula_model). The strategy is based on a coupling of special [microprocessor](http://en.wikipedia.org/wiki/Microprocessor) hardware features, often involving the [memory management unit](http://en.wikipedia.org/wiki/Memory_management_unit), to a special correctly implemented operating system kernel. This forms the foundation for a secure operating system which, if certain critical parts are designed and implemented correctly, can ensure the absolute impossibility of penetration by hostile elements. This capability is enabled because the configuration not only imposes a security policy, but in theory completely protects itself from corruption. Ordinary operating systems, on the other hand, lack the features that assure this maximal level of security. The design methodology to produce such secure systems is precise, deterministic and logical.

Systems designed with such methodology represent the state of the art[[*clarification needed*](http://en.wikipedia.org/wiki/Wikipedia:Please_clarify)] of computer security although products using such security are not widely known. In sharp contrast to most kinds of software, they meet specifications with verifiable certainty comparable to specifications for size, weight and power. Secure operating systems designed this way are used primarily to protect national security information, military secrets, and the data of international financial institutions. These are very powerful security tools and very few secure operating systems have been certified at the highest level ([Orange Book](http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria) A-1) to operate over the range of "Top Secret" to "unclassified" (including Honeywell SCOMP, USAF SACDIN, NSA Blacker and Boeing MLS LAN.) The assurance of security depends not only on the soundness of the design strategy, but also on the assurance of correctness of the implementation, and therefore there are degrees of security strength defined for COMPUSEC. The [Common Criteria](http://en.wikipedia.org/wiki/Common_Criteria) quantifies security strength of products in terms of two components, security functionality and assurance level (such as EAL levels), and these are specified in a [Protection Profile](http://en.wikipedia.org/wiki/Protection_Profile) for requirements and a [Security Target](http://en.wikipedia.org/wiki/Security_Target) for product descriptions. None of these ultra-high assurance secure general purpose operating systems have been produced for decades or certified under Common Criteria.

In USA parlance, the term High Assurance usually suggests the system has the right security functions that are implemented robustly enough to protect DoD and DoE classified information. Medium assurance suggests it can protect less valuable information, such as income tax information. Secure operating systems designed to meet medium robustness levels of security functionality and assurance have seen wider use within both government and commercial markets. Medium robust systems may provide the same security functions as high assurance secure operating systems but do so at a lower assurance level (such as Common Criteria levels EAL4 or EAL5). Lower levels mean we can be less certain that the security functions are implemented flawlessly, and therefore less dependable. These systems are found in use on web servers, guards, database servers, and management hosts and are used not only to protect the data stored on these systems but also to provide a high level of protection for network connections and routing services.

**Secure coding**

Main article: [Secure coding](http://en.wikipedia.org/wiki/Secure_coding)

If the operating environment is not based on a secure operating system capable of maintaining a domain for its own execution, and capable of protecting application code from malicious subversion, and capable of protecting the system from subverted code, then high degrees of security are understandably not possible. While such secure operating systems are possible and have been implemented, most commercial systems fall in a 'low security' category because they rely on features not supported by secure operating systems (like portability, and others). In low security operating environments, applications must be relied on to participate in their own protection. There are 'best effort' secure coding practices that can be followed to make an application more resistant to malicious subversion.

In commercial environments, the majority of software subversion [vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) result from a few known kinds of coding defects. Common software defects include [buffer overflows](http://en.wikipedia.org/wiki/Buffer_overflows), [format string vulnerabilities](http://en.wikipedia.org/wiki/Format_string_vulnerabilities), [integer overflow](http://en.wikipedia.org/wiki/Integer_overflow), and [code/command injection](http://en.wikipedia.org/wiki/Code_injection). These defects can be used to cause the target system to execute putative data. However, the "data" contain executable instructions, allowing the attacker to gain control of the processor.

Some common languages such as C and C++ are vulnerable to all of these defects (see [Seacord, *"Secure Coding in C and C++"*](http://www.cert.org/books/secure-coding)). Other languages, such as Java, are more resistant to some of these defects, but are still prone to code/command injection and other software defects which facilitate subversion.

Recently another bad coding practice has come under scrutiny; [dangling pointers](http://en.wikipedia.org/wiki/Dangling_pointer). The first known exploit for this particular problem was presented in July 2007. Before this publication the problem was known but considered to be academic and not practically exploitable.[[2]](http://en.wikipedia.org/wiki/Computer_security#cite_note-2)

Unfortunately, there is no theoretical model of "secure coding" practices, nor is one practically achievable, insofar as the code (ideally, read-only) and data (generally read/write) generally tends to have some form of defect.

**Capabilities and access control lists**

Main articles: [Access control list](http://en.wikipedia.org/wiki/Access_control_list) and [Capability (computers)](http://en.wikipedia.org/wiki/Capability_%28computers%29)

Within computer systems, two security models capable of enforcing privilege separation are [access control lists](http://en.wikipedia.org/wiki/Access_control_list) (ACLs) and [capability-based security](http://en.wikipedia.org/wiki/Capability-based_security). The semantics of ACLs have been proven to be insecure in many situations, for example, the [confused deputy problem](http://en.wikipedia.org/wiki/Confused_deputy_problem). It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Capabilities have been mostly restricted to research [operating systems](http://en.wikipedia.org/wiki/Operating_system) and commercial OSs still use ACLs. 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](http://en.wikipedia.org/wiki/E_programming_language).

The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are [operating systems](http://en.wikipedia.org/wiki/Operating_system) where [security](http://en.wikipedia.org/wiki/Security) is not an add-on.

**Applications**

Computer security is critical in almost any technology-driven industry which operates on computer systems. The issues of computer based systems and addressing their countless vulnerabilities are an integral part of maintaining an operational industry.[[3]](http://en.wikipedia.org/wiki/Computer_security#cite_note-FAA_Computer_Security-3)

**Cloud computing security**

Security in the cloud is challenging[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)], due to varied degrees of security features and management schemes within the cloud entities. In this connection one logical protocol base need to evolve so that the entire gamut of components operates synchronously and securely[[*original research?*](http://en.wikipedia.org/wiki/Wikipedia:No_original_research)].

**Aviation**

The aviation industry is especially important when analyzing computer security because the involved risks include human life, expensive equipment, cargo, and transportation infrastructure. Security can be compromised by hardware and software malpractice, human error, and faulty operating environments. Threats that exploit computer vulnerabilities can stem from sabotage, espionage, industrial competition, terrorist attack, mechanical malfunction, and human error.[[4]](http://en.wikipedia.org/wiki/Computer_security#cite_note-Computer_Security_in_Aviation-4)

The consequences of a successful deliberate or inadvertent misuse of a computer system in the aviation industry range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns such as data theft or loss, network and [air traffic control](http://en.wikipedia.org/wiki/Air_traffic_control) outages, which in turn can lead to airport closures, loss of aircraft, loss of passenger life. [Military](http://en.wikipedia.org/wiki/Military) systems that control munitions can pose an even greater risk.

A proper attack does not need to be very high tech or well funded; for a power outage at an airport alone can cause repercussions worldwide.[[5]](http://en.wikipedia.org/wiki/Computer_security#cite_note-5) One of the easiest and, arguably, the most difficult to trace security vulnerabilities is achievable by transmitting unauthorized communications over specific radio frequencies. These transmissions may spoof air traffic controllers or simply disrupt communications altogether. These incidents are very common, having altered flight courses of commercial aircraft and caused panic and confusion in the past.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. Beyond the radar's sight controllers must rely on periodic radio communications with a third party.

Lightning, power fluctuations, surges, [brownouts](http://en.wikipedia.org/wiki/Brownout_%28electricity%29), blown fuses, and various other power outages instantly disable all computer systems, since they are dependent on an electrical source. Other accidental and intentional faults have caused significant disruption of safety critical systems throughout the last few decades and dependence on reliable communication and electrical power only jeopardizes computer safety.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Notable system accidents**

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using [trojan horse](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) viruses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of [National Aeronautics and Space Administration](http://en.wikipedia.org/wiki/National_Aeronautics_and_Space_Administration)'s Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.[[6]](http://en.wikipedia.org/wiki/Computer_security#cite_note-6)

**Cybersecurity breach stories**

One true story that shows what mainstream [generative](http://en.wikipedia.org/wiki/Generative_programming) technology leads to in terms of online security breaches is the story of the Internet's first [worm](http://en.wikipedia.org/wiki/Computer_worm).

In 1988, 60,000 computers were connected to the Internet, but not all of them were PCs. Most were mainframes, minicomputers and professional workstations. On November 2, 1988, the computers acted strangely. They started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers. The purpose of such software was to transmit a copy to the machines and run in parallel with existing software and repeat all over again. It exploited a flaw in a common e-mail transmission program running on a computer by rewriting it to facilitate its entrance or it guessed users' password, because, at that time, passwords were simple (e.g. username 'harry' with a password '...harry') or were obviously related to a list of 432 common passwords tested at each computer.[[7]](http://en.wikipedia.org/wiki/Computer_security#cite_note-multiple-7)

The software was traced back to 23 year old [Cornell University](http://en.wikipedia.org/wiki/Cornell_University) graduate student [Robert Tappan Morris, Jr.](http://en.wikipedia.org/wiki/Robert_Tappan_Morris,_Jr.). When questioned about the motive for his actions, Morris said 'he wanted to count how many machines were connected to the Internet'.[[7]](http://en.wikipedia.org/wiki/Computer_security#cite_note-multiple-7) His explanation was verified with his code, but it turned out to be buggy, nevertheless.

**Computer security policy**

|  |  |
| --- | --- |
| Globe icon. | The examples and perspective in this section **may not represent a** [**worldwide view**](http://en.wikipedia.org/wiki/Wikipedia:WikiProject_Countering_systemic_bias) **of the subject**. Please [improve this article](http://en.wikipedia.org/w/index.php?title=Computer_security&action=edit) and discuss the issue on the [talk page](http://en.wikipedia.org/wiki/Talk:Computer_security). *(December 2010)* |

**United States**

**Cybersecurity Act of 2010**

On April 1, 2009, Senator [Jay Rockefeller](http://en.wikipedia.org/wiki/Jay_Rockefeller) (D-WV) introduced the "Cybersecurity Act of 2009 - S. 773" ([full text](http://www.opencongress.org/bill/111-s773/text)) in the [Senate](http://en.wikipedia.org/wiki/United_States_Senate); the bill, co-written with Senators [Evan Bayh](http://en.wikipedia.org/wiki/Evan_Bayh) (D-IN), [Barbara Mikulski](http://en.wikipedia.org/wiki/Barbara_Mikulski) (D-MD), [Bill Nelson](http://en.wikipedia.org/wiki/Bill_Nelson) (D-FL), and [Olympia Snowe](http://en.wikipedia.org/wiki/Olympia_Snowe) (R-ME), was referred to the [Committee on Commerce, Science, and Transportation](http://en.wikipedia.org/wiki/Committee_on_Commerce,_Science,_and_Transportation), which approved a revised version of the same bill (the "Cybersecurity Act of 2010") on March 24, 2010.[[8]](http://en.wikipedia.org/wiki/Computer_security#cite_note-computerworldapproval-8) The bill seeks to increase collaboration between the public and the private sector on cybersecurity issues, especially those private entities that own infrastructures that are critical to national security interests (the bill quotes [John Brennan](http://en.wikipedia.org/wiki/John_O._Brennan), the Assistant to the President for Homeland Security and Counterterrorism: "our nation’s security and economic prosperity depend on the security, stability, and integrity of communications and [information infrastructure](http://en.wikipedia.org/wiki/Information_infrastructure) that are largely privately owned and globally operated" and talks about the country's response to a "cyber-[Katrina](http://en.wikipedia.org/wiki/Hurricane_Katrina)".[[9]](http://en.wikipedia.org/wiki/Computer_security#cite_note-cybersecurity2010-9)), increase public awareness on cybersecurity issues, and foster and fund cybersecurity research. Some of the most controversial parts of the bill include Paragraph 315, which grants the [President](http://en.wikipedia.org/wiki/President_of_the_United_States) the right to "order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network."[[9]](http://en.wikipedia.org/wiki/Computer_security#cite_note-cybersecurity2010-9) The [Electronic Frontier Foundation](http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation), an international [non-profit](http://en.wikipedia.org/wiki/Non-profit) [digital rights](http://en.wikipedia.org/wiki/Digital_rights) advocacy and legal organization based in the [United States](http://en.wikipedia.org/wiki/United_States), characterized the bill as promoting a "potentially dangerous approach that favors the dramatic over the sober response".[[10]](http://en.wikipedia.org/wiki/Computer_security#cite_note-notsober-10)

**International Cybercrime Reporting and Cooperation Act**

On March 25, 2010, Representative [Yvette Clarke](http://en.wikipedia.org/wiki/Yvette_Clarke) (D-NY) introduced the "International Cybercrime Reporting and Cooperation Act - H.R.4962" ([full text](http://www.opencongress.org/bill/111-h4962/text)) in the [House of Representatives](http://en.wikipedia.org/wiki/United_States_House_of_Representatives); the bill, co-sponsored by seven other representatives (among whom only one [Republican](http://en.wikipedia.org/wiki/Republican_Party_%28United_States%29)), was referred to three [House committees](http://en.wikipedia.org/wiki/United_States_congressional_committee).[[11]](http://en.wikipedia.org/wiki/Computer_security#cite_note-reportingandcooperation-11) The bill seeks to make sure that the administration keeps [Congress](http://en.wikipedia.org/wiki/United_States_Congress) informed on information infrastructure, [cybercrime](http://en.wikipedia.org/wiki/Cybercrime), and end-user protection worldwide. It also "directs the President to give priority for assistance to improve legal, judicial, and enforcement capabilities with respect to cybercrime to countries with low information and communications technology levels of development or utilization in their critical infrastructure, telecommunications systems, and financial industries"[[11]](http://en.wikipedia.org/wiki/Computer_security#cite_note-reportingandcooperation-11) as well as to develop an action plan and an annual compliance assessment for countries of "cyber concern".[[11]](http://en.wikipedia.org/wiki/Computer_security#cite_note-reportingandcooperation-11)

**Protecting Cyberspace as a National Asset Act of 2010**

On June 19, 2010, [United States Senator](http://en.wikipedia.org/wiki/United_States_Senate) [Joe Lieberman](http://en.wikipedia.org/wiki/Joe_Lieberman) (I-CT) introduced a bill called "Protecting Cyberspace as a National Asset Act of 2010 - S.3480" ([full text in pdf](http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123)), which he co-wrote with Senator [Susan Collins](http://en.wikipedia.org/wiki/Susan_Collins) (R-ME) and Senator [Thomas Carper](http://en.wikipedia.org/wiki/Thomas_Carper) (D-DE). If signed into law, this controversial bill, which the American media dubbed the "[*Kill switch bill*](http://en.wikipedia.org/wiki/Kill_switch#Cybersecurity_policy)", would grant the [President](http://en.wikipedia.org/wiki/President_of_the_United_States) emergency powers over the Internet. However, all three co-authors of the bill issued a statement claiming that instead, the bill "[narrowed] existing broad Presidential authority to take over telecommunications networks".[[12]](http://en.wikipedia.org/wiki/Computer_security#cite_note-nokillswitch-12)

**White House proposes cybersecurity legislation**

On May 12, 2011, the White House sent Congress a proposed cybersecurity law designed to force companies to do more to fend off cyberattacks, a threat that has been reinforced by recent reports about vulnerabilities in systems used in power and water utilities.[[13]](http://en.wikipedia.org/wiki/Computer_security#cite_note-13)

**Germany**

**Berlin starts National Cyber Defense Initiative**

On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) [de:Nationales Cyber-Abwehrzentrum](http://de.wikipedia.org/wiki/Nationales_Cyber-Abwehrzentrum), which is located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) [de:Bundesamt für Sicherheit in der Informationstechnik](http://de.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Sicherheit_in_der_Informationstechnik), BKA (Federal Police Organisation) [de:Bundeskriminalamt (Deutschland)](http://de.wikipedia.org/wiki/Bundeskriminalamt_%28Deutschland%29), BND (Federal Intelligence Service) [de:Bundesnachrichtendienst](http://de.wikipedia.org/wiki/Bundesnachrichtendienst), MAD (Military Intelligence Service) [de:Amt für den Militärischen Abschirmdienst](http://de.wikipedia.org/wiki/Amt_f%C3%BCr_den_Milit%C3%A4rischen_Abschirmdienst) and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on Feb. 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like [Stuxnet](http://en.wikipedia.org/wiki/Stuxnet) [de:Stuxnet](http://de.wikipedia.org/wiki/Stuxnet)

**Hacking Back**

There has been a significant debate regarding the legality of hacking back against digital attackers (who attempt to or successfully breach an individual's, entity's, or nation's computer). The arguments for such counter-attacks are based on notions of equity, active defense, vigilantism, and the minutiae of the [Computer Fraud and Abuse Act](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act) (CFAA). The arguments against it are majorly based on the legal definition of intrusion and unauthorized access, as defined by the CFAA. The debate is ongoing.[[14]](http://en.wikipedia.org/wiki/Computer_security#cite_note-14)

**Terminology**

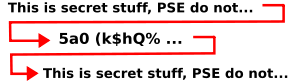
|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/en/thumb/f/f2/Edit-clear.svg/40px-Edit-clear.svg.png | This section **may require** [**cleanup**](http://en.wikipedia.org/wiki/Wikipedia:Cleanup) **to meet Wikipedia's** [**quality standards**](http://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style). No [cleanup reason](http://en.wikipedia.org/wiki/Template:Cleanup/doc) has been specified. Please help [improve this section](http://en.wikipedia.org/w/index.php?title=Computer_security&action=edit) if you can. *(November 2010)* |

The following terms used in engineering secure systems are explained below.

* [Authentication](http://en.wikipedia.org/wiki/Authentication) techniques can be used to ensure that communication end-points are who they say they are.
* [Automated theorem proving](http://en.wikipedia.org/wiki/Automated_theorem_proving) and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.
* [Capability](http://en.wikipedia.org/wiki/Capability_%28computers%29) and [access control list](http://en.wikipedia.org/wiki/Access_control_list) techniques can be used to ensure privilege separation and mandatory access control. [This section](http://en.wikipedia.org/wiki/Computer_security#Capabilities_vs._ACLs) discusses their use.
* [Chain of trust](http://en.wikipedia.org/wiki/Chain_of_trust) techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.
* [Cryptographic](http://en.wikipedia.org/wiki/Cryptography) techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.
* [Firewalls](http://en.wikipedia.org/wiki/Firewall_%28computing%29) can provide some protection from online intrusion.
* A [microkernel](http://en.wikipedia.org/wiki/Microkernel#Microkernel) is a carefully crafted, deliberately small corpus of software that underlies the operating system *per se* and is used solely to provide very low-level, very precisely defined primitives upon which an operating system can be developed. A simple example with considerable didactic value is the early '90s GEMSOS (Gemini Computers), which provided extremely low-level primitives, such as "segment" management, atop which an operating system could be built. The theory (in the case of "segments") was that—rather than have the operating system itself worry about mandatory access separation by means of military-style labeling—it is safer if a low-level, independently scrutinized module can be charged **solely** with the management of individually labeled segments, be they memory "segments" or file system "segments" or executable text "segments." If software below the visibility of the operating system is (as in this case) charged with labeling, there is no theoretically viable means for a clever hacker to subvert the labeling scheme, since the operating system *per se* does **not** provide mechanisms for interfering with labeling: the operating system is, essentially, a client (an "application," arguably) atop the microkernel and, as such, subject to its restrictions.
* [Endpoint Security](http://en.wikipedia.org/w/index.php?title=End_point_security&action=edit&redlink=1) software helps networks to prevent data theft and virus infection through portable storage devices, such as USB drives.
* Confidentiality is the nondisclosure of information except to another authorized person.[[15]](http://en.wikipedia.org/wiki/Computer_security#cite_note-15)
* Data Integrity is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.[[16]](http://en.wikipedia.org/wiki/Computer_security#cite_note-16)

*Some of the following items may belong to the* [*computer insecurity*](http://en.wikipedia.org/wiki/Computer_insecurity) *article:*

* Access [authorization](http://en.wikipedia.org/wiki/Authorization) restricts access to a computer to group of users through the use of [authentication](http://en.wikipedia.org/wiki/Authentication) systems. These systems can protect either the whole computer – such as through an interactive [login](http://en.wikipedia.org/wiki/Login) screen – or individual services, such as an [FTP](http://en.wikipedia.org/wiki/File_Transfer_Protocol) server. There are many methods for identifying and authenticating users, such as [passwords](http://en.wikipedia.org/wiki/Password), [identification cards](http://en.wikipedia.org/wiki/Identification_card), and, more recently, [smart cards](http://en.wikipedia.org/wiki/Smart_card) and [biometric](http://en.wikipedia.org/wiki/Biometric) systems.
* [Anti-virus software](http://en.wikipedia.org/wiki/Anti-virus_software) consists of computer programs that attempt to identify, thwart and eliminate [computer viruses](http://en.wikipedia.org/wiki/Computer_viruses) and other malicious software ([malware](http://en.wikipedia.org/wiki/Malware)).
* [Applications](http://en.wikipedia.org/wiki/Application_software) with known security flaws should not be run. Either leave it turned off until it can be patched or otherwise fixed, or delete it and replace it with some other application. Publicly known flaws are the main entry used by [worms](http://en.wikipedia.org/wiki/Computer_worm) to automatically break into a system and then spread to other systems connected to it. The security website [Secunia](http://en.wikipedia.org/wiki/Secunia) provides a search tool for unpatched known flaws in popular products.
* [Backups](http://en.wikipedia.org/wiki/Backup) are a way of securing information; they are another copy of all the important computer files kept in another location. These files are kept on hard disks, [CD-Rs](http://en.wikipedia.org/wiki/CD-R), [CD-RWs](http://en.wikipedia.org/wiki/CD-RW), and [tapes](http://en.wikipedia.org/wiki/Magnetic_tape_data_storage). Suggested locations for backups are a fireproof, waterproof, and heat proof safe, or in a separate, offsite location than that in which the original files are contained. Some individuals and companies also keep their backups in [safe deposit boxes](http://en.wikipedia.org/wiki/Safe_deposit_box) inside [bank vaults](http://en.wikipedia.org/wiki/Bank_vault). There is also a fourth option, which involves using one of the [file hosting services](http://en.wikipedia.org/wiki/File_hosting_service) that backs up files over the [Internet](http://en.wikipedia.org/wiki/Internet) for both business and individuals.
  + Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, may strike the building where the computer is located. The building can be on fire, or an explosion may occur. There needs to be a recent backup at an alternate secure location, in case of such kind of disaster. Further, it is recommended that the alternate location be placed where the same disaster would not affect both locations. Examples of alternate disaster recovery sites being compromised by the same disaster that affected the primary site include having had a primary site in [World Trade Center](http://en.wikipedia.org/wiki/World_Trade_Center) I and the recovery site in [7 World Trade Center](http://en.wikipedia.org/wiki/7_World_Trade_Center), both of which were destroyed in the [9/11](http://en.wikipedia.org/wiki/9/11) attack, and having one's primary site and recovery site in the same coastal region, which leads to both being vulnerable to hurricane damage (for example, primary site in New Orleans and recovery site in [Jefferson Parish](http://en.wikipedia.org/wiki/Jefferson_Parish), both of which were hit by [Hurricane Katrina](http://en.wikipedia.org/wiki/Hurricane_Katrina) in 2005). The backup media should be moved between the geographic sites in a secure manner, in order to prevent them from being stolen.

[](http://en.wikipedia.org/wiki/File:Encryption_-_decryption.svg)

[http://bits.wikimedia.org/static-1.21wmf11/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Encryption_-_decryption.svg)

[Cryptographic](http://en.wikipedia.org/wiki/Cryptography) techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message, but eavesdroppers cannot, ideally.

* [Encryption](http://en.wikipedia.org/wiki/Encryption) is used to protect the message from the eyes of others. [Cryptographically](http://en.wikipedia.org/wiki/Cryptography) secure [ciphers](http://en.wikipedia.org/wiki/Cipher) are designed to make any practical attempt of [breaking](http://en.wikipedia.org/wiki/Cryptanalysis) infeasible. [Symmetric-key](http://en.wikipedia.org/wiki/Symmetric-key_algorithm) ciphers are suitable for bulk encryption using [shared keys](http://en.wikipedia.org/wiki/Shared_key), and [public-key encryption](http://en.wikipedia.org/wiki/Public-key_encryption) using [digital certificates](http://en.wikipedia.org/wiki/Digital_certificate) can provide a practical solution for the problem of securely communicating when no key is shared in advance.
* [Firewalls](http://en.wikipedia.org/wiki/Firewall_%28networking%29) are systems that help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic that can pass through them, based on a set of system administrator-defined rules.
* [Honey pots](http://en.wikipedia.org/wiki/Honeypot_%28computing%29) are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.
* [Intrusion-detection systems](http://en.wikipedia.org/wiki/Intrusion-detection_system) can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.
* [Pinging](http://en.wikipedia.org/wiki/Ping_%28networking_utility%29) The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.
* [Social engineering](http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29) awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

**Legal issues and global regulation**

One of the main challenges to and main complaints about the antivirus industry is the lack of global web regulations, a global base of common rules to judge, and eventually punish, [cyber crimes](http://en.wikipedia.org/wiki/Cyber_crimes) and [cyber criminals](http://en.wikipedia.org/wiki/Cyber_criminals). In fact, nowadays, even if an antivirus firm locates the cyber criminal behind the creation of a particular [virus](http://en.wikipedia.org/wiki/Virus_%28computer%29) or piece of [malware](http://en.wikipedia.org/wiki/Malware) or again one form of [cyber attack](http://en.wikipedia.org/wiki/Cyber-Attacks), often the local authorities cannot take action due to lack of laws under which to prosecute.[[17]](http://en.wikipedia.org/wiki/Computer_security#cite_note-ted.com-17)[[18]](http://en.wikipedia.org/wiki/Computer_security#cite_note-18) This is mainly caused by the fact that mostly every country has an own regulation about [cyber crimes](http://en.wikipedia.org/wiki/Cyber_crimes).

"[Computer viruses] switch from one country to another, from one jurisdiction to another — moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."[[17]](http://en.wikipedia.org/wiki/Computer_security#cite_note-ted.com-17) ([Mikko Hyppönen](http://en.wikipedia.org/wiki/Mikko_Hypp%C3%B6nen))

Due to some of the [European](http://en.wikipedia.org/wiki/European_Union)'s antivirus firms (e.g. [Avira](http://en.wikipedia.org/wiki/Avira), [BullGuard](http://en.wikipedia.org/wiki/BullGuard), [F-Secure](http://en.wikipedia.org/wiki/F-Secure), [Frisk](http://en.wikipedia.org/wiki/FRISK_Software_International), [Panda](http://en.wikipedia.org/wiki/Panda_Security), [TG Soft](http://en.wikipedia.org/wiki/TG_Soft), [...](http://en.wikipedia.org/wiki/Comparison_of_antivirus_software)) to solve this problem, the [European Commission](http://en.wikipedia.org/wiki/European_Commission) has decided to establish the [European Cybercrime Centre](http://en.wikipedia.org/wiki/European_Cybercrime_Centre)(EC3).[[19]](http://en.wikipedia.org/wiki/Computer_security#cite_note-19) The EC3 effectively opened on 1 January 2013 and will be the focal point in the EU's fight against cyber crime, contributing to faster reaction to online crimes. It will support member states and the EU's institutions in building an operational and analytical capacity for investigations, as well as cooperation with international partners.[[20]](http://en.wikipedia.org/wiki/Computer_security#cite_note-20)

**Notes**

* 1. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-1) [Definitions: IT Security Architecture](http://opensecurityarchitecture.com). SecurityArchitecture.org, Jan, 2006
  2. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-2) [New hacking technique exploits common programming error](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1265116,00.html). SearchSecurity.com, July 2007
  3. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-FAA_Computer_Security_3-0) J. C. Willemssen, "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives, 2000.
  4. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-Computer_Security_in_Aviation_4-0) P. G. Neumann, "Computer Security in Aviation," presented at International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, 1997.
  5. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-5) J. Zellan, Aviation Security. Hauppauge, NY: Nova Science, 2003, pp. 65–70.
  6. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-6) [Information Security](http://www.fas.org/irp/gao/aim96084.htm). United States Department of Defense, 1986
  7. ^ [***a***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-multiple_7-0) [***b***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-multiple_7-1) Jonathan Zittrain, 'The Future of The Internet', Penguin Books, 2008
  8. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-computerworldapproval_8-0) [Cybersecurity bill passes first hurdle](http://www.computerworld.com/s/article/9174065/Cybersecurity_bill_passes_first_hurdle), Computer World, March 24, 2010. Retrieved on June 26, 2010.
  9. ^ [***a***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-cybersecurity2010_9-0) [***b***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-cybersecurity2010_9-1) [Cybersecurity Act of 2009](http://www.opencongress.org/bill/111-s773/text), OpenCongress.org, April 1, 2009. Retrieved on June 26, 2010.
  10. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-notsober_10-0) [Federal Authority Over the Internet? The Cybersecurity Act of 2009](http://www.eff.org/deeplinks/2009/04/cybersecurity-act), eff.org, April 10, 2009. Retrieved on June 26, 2010.
  11. ^ [***a***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-reportingandcooperation_11-0) [***b***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-reportingandcooperation_11-1) [***c***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-reportingandcooperation_11-2) [H.R.4962 - International Cybercrime Reporting and Cooperation Act](http://www.opencongress.org/bill/111-h4962/show), OpenCongress.org. Retrieved on June 26, 2010.
  12. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-nokillswitch_12-0) [Senators Say Cybersecurity Bill Has No 'Kill Switch'](http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225701368&subSection=News), informationweek.com, June 24, 2010. Retrieved on June 25, 2010.
  13. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-13) Declan McCullagh, CNET. "[White House proposes cybersecurity legislation](http://news.cnet.com/8301-31921_3-20062277-281.html?part=rss&subj=news&tag=2547-1_3-0-20)." May 12, 2011. Retrieved May 12, 2011.
  14. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-14) Justin P. Webb, Cybercrime Review. "[Hacking Back - are you authorized? A discussion of whether it's an invitation to federal prison or a justified reaction/strategy?](http://www.cybercrimereview.com/2012/10/hacking-back-are-you-authorized.html)." October 16, 2012. Retrieved January 5, 2013.
  15. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-15) ["Confidentiality"](http://medical-dictionary.thefreedictionary.com/confidentiality). Retrieved 2011-10-31.
  16. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-16) ["Data Integrity"](http://www.businessdictionary.com/definition/data-integrity.html). Retrieved 2011-10-31.
  17. ^ [***a***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-ted.com_17-0) [***b***](http://en.wikipedia.org/wiki/Computer_security#cite_ref-ted.com_17-1) ["Mikko Hypponen: Fighting viruses, defending the net"](http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html). TED.
  18. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-18) ["Mikko Hypponen - Behind Enemy Lines"](http://www.youtube.com/watch?v=0TMFRO66Wv4). Hack In The Box Security Conference.
  19. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-19) ["European Cybercrime Centre set for launch"](http://www.virusbtn.com/news/2013/01_09.xml?rss). VirusBulletin.
  20. [**^**](http://en.wikipedia.org/wiki/Computer_security#cite_ref-20) ["European Cybercrime Centre (EC3)"](https://www.europol.europa.eu/ec3). Europol.

**See also**

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | [Portal icon](http://en.wikipedia.org/wiki/File:Monitor_padlock.svg) | [***Computer security portal***](http://en.wikipedia.org/wiki/Portal:Computer_security) |  * [Attack tree](http://en.wikipedia.org/wiki/Attack_tree) * [Authentication](http://en.wikipedia.org/wiki/Authentication) * [Authorization](http://en.wikipedia.org/wiki/Authorization) * [CAPTCHA](http://en.wikipedia.org/wiki/CAPTCHA) * [CERT](http://en.wikipedia.org/wiki/CERT_Coordination_Center) * [Cloud computing security](http://en.wikipedia.org/wiki/Cloud_computing_security) * [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity) * [Computer security model](http://en.wikipedia.org/wiki/Computer_security_model) * [Computer security compromised by hardware failure](http://en.wikipedia.org/wiki/Computer_security_compromised_by_hardware_failure) * [Content security](http://en.wikipedia.org/wiki/Content_security) * [Countermeasure (computer)](http://en.wikipedia.org/wiki/Countermeasure_%28computer%29) * [Cryptography](http://en.wikipedia.org/wiki/Cryptography) * [Cyber security standards](http://en.wikipedia.org/wiki/Cyber_security_standards) * [Dancing pigs](http://en.wikipedia.org/wiki/Dancing_pigs) * [Data loss prevention products](http://en.wikipedia.org/wiki/Data_loss_prevention_products) * [Data security](http://en.wikipedia.org/wiki/Data_security) * [Differentiated security](http://en.wikipedia.org/wiki/Differentiated_security) * [Disk encryption](http://en.wikipedia.org/wiki/Disk_encryption) * [Exploit (computer security)](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) * [Fault tolerance](http://en.wikipedia.org/wiki/Fault_tolerance) * [Firewalls](http://en.wikipedia.org/wiki/Firewall_%28networking%29) * [Full disclosure](http://en.wikipedia.org/wiki/Full_disclosure) * [Human-computer interaction (security)](http://en.wikipedia.org/wiki/Human-computer_interaction_%28security%29) | * [Identity management](http://en.wikipedia.org/wiki/Identity_management) * [Information Leak Prevention](http://en.wikipedia.org/wiki/Information_Leak_Prevention) * [Information security](http://en.wikipedia.org/wiki/Information_security) * [Internet privacy](http://en.wikipedia.org/wiki/Internet_privacy) * [ISO/IEC 15408](http://en.wikipedia.org/wiki/ISO/IEC_15408) * [IT risk](http://en.wikipedia.org/wiki/IT_risk) * [Kish cypher](http://en.wikipedia.org/wiki/Kish_cypher) * [Mobile security](http://en.wikipedia.org/wiki/Mobile_security) * [Network Security Toolkit](http://en.wikipedia.org/wiki/Network_Security_Toolkit) * [Network security](http://en.wikipedia.org/wiki/Network_security) * [Open security](http://en.wikipedia.org/wiki/Open_security) * [OWASP](http://en.wikipedia.org/wiki/OWASP) * [Penetration test](http://en.wikipedia.org/wiki/Penetration_test) * [Physical information security](http://en.wikipedia.org/wiki/Physical_information_security) * [Physical security](http://en.wikipedia.org/wiki/Physical_security) * [Presumed security](http://en.wikipedia.org/wiki/Presumed_security) * [Privacy software](http://en.wikipedia.org/wiki/Privacy_software) * [Proactive Cyber Defence](http://en.wikipedia.org/wiki/Proactive_Cyber_Defence) * [Sandbox (computer security)](http://en.wikipedia.org/wiki/Sandbox_%28computer_security%29) * [Security Architecture](http://en.wikipedia.org/wiki/Security_Architecture) * [Separation of protection and security](http://en.wikipedia.org/wiki/Separation_of_protection_and_security) * [Threat (computer)](http://en.wikipedia.org/wiki/Threat_%28computer%29) * [Vulnerability (computing)](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) |

**References**

|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/commons/thumb/a/a4/Text_document_with_red_question_mark.svg/40px-Text_document_with_red_question_mark.svg.png | This section includes a [list of references](http://en.wikipedia.org/wiki/Wikipedia:Citing_sources), but **its sources remain unclear because it has insufficient** [**inline citations**](http://en.wikipedia.org/wiki/Wikipedia:INCITE). Please help to [improve](http://en.wikipedia.org/wiki/Wikipedia:WikiProject_Fact_and_Reference_Check) this article by [introducing](http://en.wikipedia.org/wiki/Wikipedia:When_to_cite) more precise citations. *(September 2010)* |

* [Ross J. Anderson](http://en.wikipedia.org/wiki/Ross_J._Anderson): [*Security Engineering: A Guide to Building Dependable Distributed Systems*](http://www.cl.cam.ac.uk/%7Erja14/book.html), [ISBN 0-471-38922-6](http://en.wikipedia.org/wiki/Special:BookSources/0471389226)
* [Morrie Gasser](http://en.wikipedia.org/w/index.php?title=Morrie_Gasser&action=edit&redlink=1): [*Building a secure computer system*](http://cs.unomaha.edu/%7Estanw/gasserbook.pdf) [ISBN 0-442-23022-2](http://en.wikipedia.org/wiki/Special:BookSources/0442230222), 1988
* Stephen Haag, Maeve Cummings, Donald McCubbrey, Alain Pinsonneault, Richard Donovan: *Management Information Systems for the information age*, [ISBN 0-07-091120-7](http://en.wikipedia.org/wiki/Special:BookSources/0070911207)
* [E. Stewart Lee](http://en.wikipedia.org/w/index.php?title=E._Stewart_Lee&action=edit&redlink=1): [*Essays about Computer Security*](http://www.cl.cam.ac.uk/%7Emgk25/lee-essays.pdf) Cambridge, 1999
* [Peter G. Neumann](http://en.wikipedia.org/wiki/Peter_G._Neumann): [*Principled Assuredly Trustworthy Composable Architectures*](http://www.csl.sri.com/neumann/chats4.pdf) 2004
* [Paul A. Karger](http://en.wikipedia.org/w/index.php?title=Paul_A._Karger&action=edit&redlink=1), [Roger R. Schell](http://en.wikipedia.org/wiki/Roger_R._Schell): [*Thirty Years Later: Lessons from the Multics Security Evaluation*](http://www.acsac.org/2002/papers/classic-multics.pdf), IBM white paper.
* [Bruce Schneier](http://en.wikipedia.org/wiki/Bruce_Schneier): *Secrets & Lies: Digital Security in a Networked World*, [ISBN 0-471-25311-1](http://en.wikipedia.org/wiki/Special:BookSources/0471253111)
* [Robert C. Seacord](http://en.wikipedia.org/wiki/Robert_C._Seacord): *Secure Coding in C and C++*. Addison Wesley, September, 2005. [ISBN 0-321-33572-4](http://en.wikipedia.org/wiki/Special:BookSources/0321335724)
* [Clifford Stoll](http://en.wikipedia.org/wiki/Clifford_Stoll): *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, [ISBN 0-7434-1146-3](http://en.wikipedia.org/wiki/Special:BookSources/0743411463)
* [*Network Infrastructure Security*](http://www.springer.com/computer/communications/book/978-1-4419-0165-1), Angus Wong and Alan Yeung, Springer, 2009.
* [John R. Vacca](http://en.wikipedia.org/w/index.php?title=John_R._Vacca&action=edit&redlink=1) (ed.): *Computer and information security handbook*, Morgan Kaufmann Publishers, 2009
* [Maj. Dawood Fateh - Cyber Intelligence 2012](http://en.wikipedia.org/w/index.php?title=Maj._Dawood_Fateh_-_Cyber_Intelligence_2012&action=edit&redlink=1)

**External links**

* [Security advisories links](http://www.dmoz.org/Computers/Security/Advisories_and_Patches/) from the [Open Directory Project](http://en.wikipedia.org/wiki/Open_Directory_Project)
* [The Repository of Industrial Security Incidents](http://www.securityincidents.org/)