**Attack (computing)**

From Wikipedia, the free encyclopedia

Jump to: [navigation](http://en.wikipedia.org/wiki/Attack_%28computing%29" \l "mw-head), [search](http://en.wikipedia.org/wiki/Attack_%28computing%29" \l "p-search)

For other uses, see [Attack](http://en.wikipedia.org/wiki/Attack_%28disambiguation%29).

In [*computer*](http://en.wikipedia.org/wiki/Computer) and [*computer networks*](http://en.wikipedia.org/wiki/Computer_network) an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.[[1]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-1)

|  |
| --- |
| **Contents**   * [1 Definitions](http://en.wikipedia.org/wiki/Attack_%28computing%29#Definitions)   + [1.1 IETF](http://en.wikipedia.org/wiki/Attack_%28computing%29#IETF)   + [1.2 US Government](http://en.wikipedia.org/wiki/Attack_%28computing%29#US_Government) * [2 Phenomenology](http://en.wikipedia.org/wiki/Attack_%28computing%29#Phenomenology) * [3 Types of attacks](http://en.wikipedia.org/wiki/Attack_%28computing%29#Types_of_attacks) * [4 Consequence of a potential attack](http://en.wikipedia.org/wiki/Attack_%28computing%29#Consequence_of_a_potential_attack) * [5 See also](http://en.wikipedia.org/wiki/Attack_%28computing%29#See_also) * [6 References](http://en.wikipedia.org/wiki/Attack_%28computing%29#References) * [7 External links](http://en.wikipedia.org/wiki/Attack_%28computing%29#External_links) |

**Definitions**

**IETF**

[Internet Engineering Task Force](http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) defines attack in [RFC 2828](http://tools.ietf.org/html/rfc2828) as:[[2]](http://en.wikipedia.org/wiki/Attack_%28computing%29" \l "cite_note-rfc2828-2)

*an* [*assault*](http://en.wikipedia.org/wiki/Assault) *on system security that derives from an intelligent* [*threat*](http://en.wikipedia.org/wiki/Threat_%28computer%29)*, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade* [*security services*](http://en.wikipedia.org/wiki/Security_service_%28telecommunication%29) *and violate the* [*security policy*](http://en.wikipedia.org/wiki/Security_policy) *of a system.*

**US Government**

CNSS Instruction No. 4009 dated 26 April 2010 by [Committee on National Security Systems](http://en.wikipedia.org/wiki/Committee_on_National_Security_Systems) of [United States of America](http://en.wikipedia.org/wiki/United_States)[[3]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-CNSSI4009-3) defines an attack as:

*Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.*

The increasing dependencies of modern society on information and computers networks (both in private and public sectors, including military)[[4]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-4) [[5]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-5) [[6]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-6) has led to new terms like cyber attack and [Cyberwarfare](http://en.wikipedia.org/wiki/Cyberwarfare).  
CNSS Instruction No. 4009[[3]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-CNSSI4009-3) define a **cyber attack** as:

*An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.*

**Phenomenology**

An attack can be *active* or *passive*.[[2]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-rfc2828-2)

An "active attack" attempts to alter system resources or affect their operation.

A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: [wiretapping](http://en.wikipedia.org/wiki/Telephone_tapping).)

An attack can be perpetrated by an *insider* or from *outside* the organization;[[2]](http://en.wikipedia.org/wiki/Attack_%28computing%29" \l "cite_note-rfc2828-2)

An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

The term "attack" relates to some other basic security terms as shown in the following diagram:[[2]](http://en.wikipedia.org/wiki/Attack_%28computing%29" \l "cite_note-rfc2828-2)

+ - - - - - - - - - - - - + + - - - - + + - - - - - - - - - - -+

| An Attack: | |Counter- | | A System Resource: |

| i.e., A Threat Action | | measure | | Target of the Attack |

| +----------+ | | | | +-----------------+ |

| | Attacker |<==================||<========= | |

| | i.e., | Passive | | | | | Vulnerability | |

| | A Threat |<=================>||<========> | |

| | Agent | or Active | | | | +-------|||-------+ |

| +----------+ Attack | | | | VVV |

| | | | | Threat Consequences |

+ - - - - - - - - - - - - + + - - - - + + - - - - - - - - - - -+

A resource (both physical or logical), called an [asset](http://en.wikipedia.org/wiki/Asset_%28computing%29), can have one or more [vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) that can be [exploited](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) by a [threat](http://en.wikipedia.org/wiki/Threat_%28computer%29) agent in a threat action. The result can potentially compromises the [Confidentiality](http://en.wikipedia.org/wiki/Confidentiality), [Integrity](http://en.wikipedia.org/wiki/Integrity) or [Availability](http://en.wikipedia.org/wiki/Availability) properties of resources (potentially different that the vulnerable one) of the organization and others involved parties (customers, suppliers).  
The so-called [CIA triad](http://en.wikipedia.org/wiki/CIA_triad) is the basis of [Information Security](http://en.wikipedia.org/wiki/Information_Security).

The attack can be *active* when it attempts to alter system resources or affect their operation: so it compromises Integrity or Availability. A "*passive attack*" attempts to learn or make use of information from the system but does not affect system resources: so it compromises Confidentiality.

A Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).[[2]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-rfc2828-2)

A set of policies concerned with information security management, the [information security management systems](http://en.wikipedia.org/wiki/Information_security_management_system) (ISMS), has been developed to manage, according to [Risk management](http://en.wikipedia.org/wiki/Risk_management) principles, the [countermeasures](http://en.wikipedia.org/wiki/Countermeasure_%28computer%29) in order to accomplish to a security strategy set up following rules and regulations applicable in a country.[[7]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-Vacca-7)

An attack should led to a *security incident* i.e. a *security event* that involves a *security violation*. In other words, a security-relevant system event in which the system's security policy is disobeyed or otherwise breached.

The overall picture represents the [risk factors](http://en.wikipedia.org/wiki/Risk_factor_%28computing%29) of the risk scenario.[[8]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-8)

An organization should make steps to detect, classify and manage security incidents. The first logical step is to set up an [Incident response plan](http://en.wikipedia.org/w/index.php?title=Incident_response_plan&action=edit&redlink=1) and eventually a [Computer emergency response team](http://en.wikipedia.org/wiki/Computer_emergency_response_team).

In order to detect attacks, a number of [countermeasures](http://en.wikipedia.org/wiki/Countermeasure_%28computer%29) can be set up at organizational, procedural and technical levels. [Computer emergency response team](http://en.wikipedia.org/wiki/Computer_emergency_response_team), [Information technology security audit](http://en.wikipedia.org/wiki/Information_technology_security_audit) and [Intrusion detection system](http://en.wikipedia.org/wiki/Intrusion_detection_system) are example of these.[[9]](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_note-Vacca1-9)

**Types of attacks**

An attack usually is perpetrated by someone with bad intentions: [Black hatted](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29) attacks falls in this category, while other perform [Penetration testing](http://en.wikipedia.org/wiki/Penetration_test) on an organization information system to find out if all foreseen controls are in place.  
The attacks can be classified according to their origin: i.e. if it is conducted using one or more computers: in the last case is called a distributed attack. [Botnet](http://en.wikipedia.org/wiki/Botnet) are used to conduct distributed attacks.  
Other classifications are according to the procedures used or the type of vulnerabilities exploited: attacks can be concentrated on network mechanisms or host features.  
Some attacks are physical: i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is called [malware](http://en.wikipedia.org/wiki/Malware).

The following is a partial short list of attacks:

* Passive
  + Network
    - [wiretapping](http://en.wikipedia.org/wiki/Telephone_tapping)
    - [Port scanner](http://en.wikipedia.org/wiki/Port_scanner)
    - [Idle scan](http://en.wikipedia.org/wiki/Idle_scan)
* Active
  + [Denial-of-service attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
  + [Spoofing](http://en.wikipedia.org/wiki/Spoofing_attack)
  + Network
    - [Man in the middle](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)
    - [ARP poisoning](http://en.wikipedia.org/wiki/ARP_poisoning)
    - [Ping flood](http://en.wikipedia.org/wiki/Ping_flood)
    - [Ping of death](http://en.wikipedia.org/wiki/Ping_of_death)
    - [Smurf attack](http://en.wikipedia.org/wiki/Smurf_attack)
  + Host
    - [Buffer overflow](http://en.wikipedia.org/wiki/Buffer_overflow)
    - [Heap overflow](http://en.wikipedia.org/wiki/Heap_overflow)
    - [Format string attack](http://en.wikipedia.org/wiki/Format_string_attack)

**Consequence of a potential attack**

A whole industry is working trying to minimize the likelihood and the consequence of an information attack.

For a partial list look at [Category:Computer security software companies](http://en.wikipedia.org/wiki/Category:Computer_security_software_companies)

They offer different products and services, aimed at:

* study all possible attacks category
* publish books and articles about the subject
* discovering vulnerabilities
* evaluating the risks
* fixing vulnerabilities
* invent, design and deploy countermeasures
* set up [contingency plan](http://en.wikipedia.org/wiki/Contingency_plan) in order to be ready to respond

Many organization are trying to classify vulnerability and their consequence: the most famous vulnerability database is the [Common Vulnerabilities and Exposures](http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

The [Computer emergency response teams](http://en.wikipedia.org/wiki/Computer_emergency_response_team) were set up by government and large organization to handle computer security incidents.

**See also**

|  |  |
| --- | --- |
| [Portal icon](http://en.wikipedia.org/wiki/File:Monitor_padlock.svg) | [***Computer Security portal***](http://en.wikipedia.org/wiki/Portal:Computer_Security) |

* [Asset (computing)](http://en.wikipedia.org/wiki/Asset_%28computing%29)
* [Common Vulnerabilities and Exposures](http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)
* [Computer emergency response team](http://en.wikipedia.org/wiki/Computer_emergency_response_team)
* [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity)
* [Computer security](http://en.wikipedia.org/wiki/Computer_security)
* [Contingency plan](http://en.wikipedia.org/wiki/Contingency_plan)
* [Countermeasure (computer)](http://en.wikipedia.org/wiki/Countermeasure_%28computer%29)
* [Exploit (computer security)](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29)
* [Factor Analysis of Information Risk](http://en.wikipedia.org/wiki/Factor_Analysis_of_Information_Risk)
* [Hacking: The Art of Exploitation Second Edition](http://en.wikipedia.org/wiki/Hacking:_The_Art_of_Exploitation_Second_Edition)
* [Internet Engineering Task Force](http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)
* [Information technology security audit](http://en.wikipedia.org/wiki/Information_technology_security_audit)
* [Information Security](http://en.wikipedia.org/wiki/Information_Security)
* [Intrusion detection system](http://en.wikipedia.org/wiki/Intrusion_detection_system)
* [IT risk](http://en.wikipedia.org/wiki/IT_risk)
* [Metasploit](http://en.wikipedia.org/wiki/Metasploit)
* [Month of Bugs](http://en.wikipedia.org/wiki/Month_of_Bugs)
* [National Information Assurance Glossary](http://en.wikipedia.org/wiki/National_Information_Assurance_Glossary)
* [Penetration test](http://en.wikipedia.org/wiki/Penetration_test)
* [Risk factor](http://en.wikipedia.org/wiki/Risk_factor_%28computing%29)
* [Security control](http://en.wikipedia.org/wiki/Security_controls)
* [Security service (telecommunication)](http://en.wikipedia.org/wiki/Security_service_%28telecommunication%29)
* [Threat](http://en.wikipedia.org/wiki/Threat_%28computer%29)
* [Vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)
* [Vulnerability management](http://en.wikipedia.org/wiki/Vulnerability_management)
* [w3af](http://en.wikipedia.org/wiki/W3af)

**References**

1. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-1) [Free download of ISO/IEC 27000:2009 from ISO, via their ITTF web site.](http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip)
2. ^ [***a***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-rfc2828_2-0) [***b***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-rfc2828_2-1) [***c***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-rfc2828_2-2) [***d***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-rfc2828_2-3) [***e***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-rfc2828_2-4) Internet Engineering Task Force [RFC 2828](http://tools.ietf.org/html/rfc2828) Internet Security Glossary
3. ^ [***a***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-CNSSI4009_3-0) [***b***](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-CNSSI4009_3-1) [CNSS Instruction No. 4009](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) dated 26 April 2010
4. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-4) Cortada, James W. (2003-12-04) *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries* USA: Oxford University Press pp. 512 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-19-516588-8](http://en.wikipedia.org/wiki/Special:BookSources/0-19-516588-8)
5. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-5) Cortada, James W. (2005-11-03) *The Digital Hand: Volume II: How Computers Changed the Work of American Financial, Telecommunications, Media, and Entertainment Industries* USA: Oxford University Press [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-19-516587-6](http://en.wikipedia.org/wiki/Special:BookSources/978-0-19-516587-6)
6. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-6) Cortada, James W. (2007-11-06) *The Digital Hand, Vol 3: How Computers Changed the Work of American Public Sector Industries* USA: Oxford University Press pp. 496 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-19-516586-9](http://en.wikipedia.org/wiki/Special:BookSources/978-0-19-516586-9)
7. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-Vacca_7-0) Wright, Joe; Jim Harmening (2009) "15" *Computer and Information Security Handbook* Morgan Kaufmann Publications Elsevier Inc p. 257 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-12-374354-1](http://en.wikipedia.org/wiki/Special:BookSources/978-0-12-374354-1)
8. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-8) [ISACA THE RISK IT FRAMEWORK (registration required)](http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf)
9. [**^**](http://en.wikipedia.org/wiki/Attack_%28computing%29#cite_ref-Vacca1_9-0) Caballero, Albert (2009) "14" *Computer and Information Security Handbook* Morgan Kaufmann Publications Elsevier Inc p. 225 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-12-374354-1](http://en.wikipedia.org/wiki/Special:BookSources/978-0-12-374354-1)