Security

Overview

Security is protection from or resilience against potential harm (or other unwanted coercion). Beneficiaries (technically referents) of security may be persons and social groups, objects and institutions, businesses and corporations or any other entity or phenomenon vulnerable to unwanted change.

Security mostly refers to protection from hostile forces, but it has a wide range of other senses:

absence of harm
presence of an essential good
resilience against potential damage
secrecy
containment
state of mind
unconstrained degrees of freedom[i]

Security can be both physical and virtual.

A security referent is the focus of a security policy or discourse. A referent may be a potential beneficiary or victim of a security policy or system. Security referents may be persons or social groups, objects, institutions, ecosystems or any other phenomenon vulnerable to unwanted change by the forces of its environment.

The security context is the relationship between a security referent and its environment. From this perspective, security and insecurity depend first on whether the environment is beneficial or hostile to the referent and also on how capable the referent is of responding to their environment in order to survive and thrive.

Capabilities are the means by which a referent provides for security (or is provided for) and vary widely, including:

- coercive capabilities, including the capacity to project coercive power into the environment
- protective systems (firewall, antivirus software, ...)
- warning systems
- negotiated action intended to prevent insecurity from developing
- policy intended to develop lasting economic, physical and digital conditions of security

Terms

Certain concepts recur throughout different fields of security.

- access control; the selective restriction of access to a place or other resource
- assurance; an expression of confidence that a security measure will perform as expected
- authorization; the function of specifying access rights or privileges to resources related to information security and computer security in general and to access control in particular
- cipher; an algorithm that defines a set of steps to encrypt or decrypt information so that it is incomprehensible
- countermeasure; a means of preventing an act or system from having its intended effect

- defense in depth; a school of thought holding that a wider range of security measures will enhance security
- exploit (noun); a means of capitalizing on a vulnerability in a security system (usually a cyber security system)
- identity management; enables the right individuals to access the right resources at the right times and for the right reasons
- password; secret data, typically a string of characters, usually used to confirm a user's identity
- resilience; the degree to which a person, community, nation or system is able to resist adverse external forces
- risk; a possible event which could lead to damage, harm or loss
- security management; identification of an organization's assets (including people, buildings, machines, systems and information assets), followed by the development, documentation and implementation of policies and procedures for protecting these assets
- threat; a potential source of harm
- vulnerability; the degree to which something may be changed (usually in an unwanted manner) by external forces

SHIPS Security

Computer Security

> Computer security refers to the security of computing devices such as computers and smartphones, as well as computer networks, such as private and public networks, and the internet. The field has growing importance due to the increasing reliance on computational systems. It concerns the protection of hardware, software, data, people and the procedures by which systems are accessed. The means of computer security include the physical security of systems and the security of information held on them.

Internet Security

> Internet security encompasses the internet, browser security, web site security and network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the internet. The internet is an inherently insecure channel for information exchange, with high risk of intrusion or fraud, such as phishing, online viruses, trojans, ransomware and worms. Many methods are used to combat these threats, including encryption and ground-up engineering.

Network Security

> Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs: conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises and other types of institutions. It does as its title explains: it secures the network, as well as protecting and

overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Data Security

Data security means protecting digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyber attack or a data breach.

i An unconstrained system in a domain disposes of all the degrees of freedom (orientations) inherent to its nature. The orientation of a system is part of the description of how it is embedded in the domain. More specifically, it refers to the imaginary morphism that is needed to move the system (model) from a current placement to a reference placement. A single morphism may not be enough to reach the current placement, in which case it may be necessary to add another imaginary morphism to change the model's position. Typically, the orientation is given relative to a frame of reference, usually specified by a Cartesian coordinate system. It can essentially morph free along every ax. Degrees of freedom can be removed by adding constraints, such as taking away an orientation (dimension) or restricting the domain or co-domain. This also decreases uncertainty. Orientation of a system is part of the description of how it is embedded in its domain. It refers to the imaginary transformation that is needed to move the system from its current placement to a reference placement. One arrow may not be enough to reach the reference placement, in which case it may be necessary to add imaginary translations to change the system's position (or linear position). The position and orientation together fully describe how the object is embedded in the domain. Morphisms may be thought to occur in any order, as the orientation of a model does not change when it morphs, nor does its embedding changes. Typically, an orientation is given relative to a frame of reference, usually specified by a Cartesian coordinate system. The degrees of freedom of a system is the number of parameters of the system that may vary independently. This notion is formalized as the dimension of a manifold or an algebraic variety.