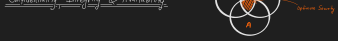


Confidentiality	Integrity	Availability
<p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p>	<p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p>	<p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p> <p>Information that is not intended to be known by unauthorized individuals.</p>

Top (orig) 1/20/21

Security Goals



Confidentiality

Preventing authorized operations on information assets and disclosing, including those for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Threats to Confidentiality: Interception, Spoofing, Man-in-the-Middle



A person, process, or program is (or is not) authorized to access a data asset in a particular way, and if the person, process, or program accesses the data (or not), the fact of doing (not) so is (not) visible, or (not) recorded, or (not) accessible, and the authorization is public.

Integrity

Guarding against incorrect information modification or destruction, which includes information misrepresentation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Threats to Integrity: Fabrication, Modification, Denial of Service

Examples of integrity failures are ones to fail. A number of years ago a medical center in a word document received the word "no" after each cancer screening of the word "no" you can imagine the havoc that could ensue.

Steps to ensure Integrity: Integrity can be inferred to make the best use of an confidentiality, by rigorous control of who or what can access which resources in a system.

Availability

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Threats to Availability: Denial of Service, Data Destruction, Hardware Failure

A computer user's worst nightmare: the hard on the wall and the computer does nothing, their data and program are inaccessible. What can you do to prevent this? Turnaround, time of an operation that failure.

Steps to ensure Availability: There is a timely response to our request. Resources are allocated fairly so that some resources are not hoarded over others. Consistency is maintained that is, avoid resource access, avoid fragmentation and consistent access and operational on failure. The service or system involved follows a philosophy of fault tolerance, wherein hardware or software faults lead to graceful degradation of service or to workarounds rather than to crashes and system loss of information. The service or system can be used easily and in the way it was intended to be used.

Top (orig) 1/20/21

Vulnerability, Threat & Control

Vulnerability

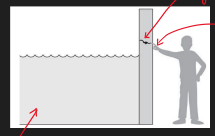
A vulnerability is a weakness in the system, for example in procedure, design, or implementation, that might be exploited to disrupt loss of harm. The existence of a particular system and its vulnerability to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

Threat

A threat to a computing system is a set of circumstances that has the potential to cause loss of harm.

Control

Controls prevent threats from causing vulnerabilities.



Threat

Threat vs Vulnerability vs Control

here, a wall is holding water back. The water to the left of the wall is a threat to the man on the right of the wall. The water could rise, overflowing onto the man, or it could stay beneath the height of the wall, causing the wall to collapse.

So the threat of harm is the potential for the man to get wet or get hurt or be drowned. For now, the wall is acting as the threat to the man is neutralized.

however, we can see a small crack in the wall—a vulnerability that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.

(Pg 17 Snippets)

Security Services

- 1. Authentication
- 2. Access Control
- * 3. Data Confidentiality

- * 4. Data Integrity
- 5. Non Repudiation
- * 6. Availability

(Pg 20 Snippets)

Security Mechanisms

- 1. Encipherment
- 2. Digital Signature
- 3. Access Control
- 4. Data Integrity

- 5. Authentication Exchange
- 6. Traffic Padding
- 7. Routing Control
- 8. Notarization