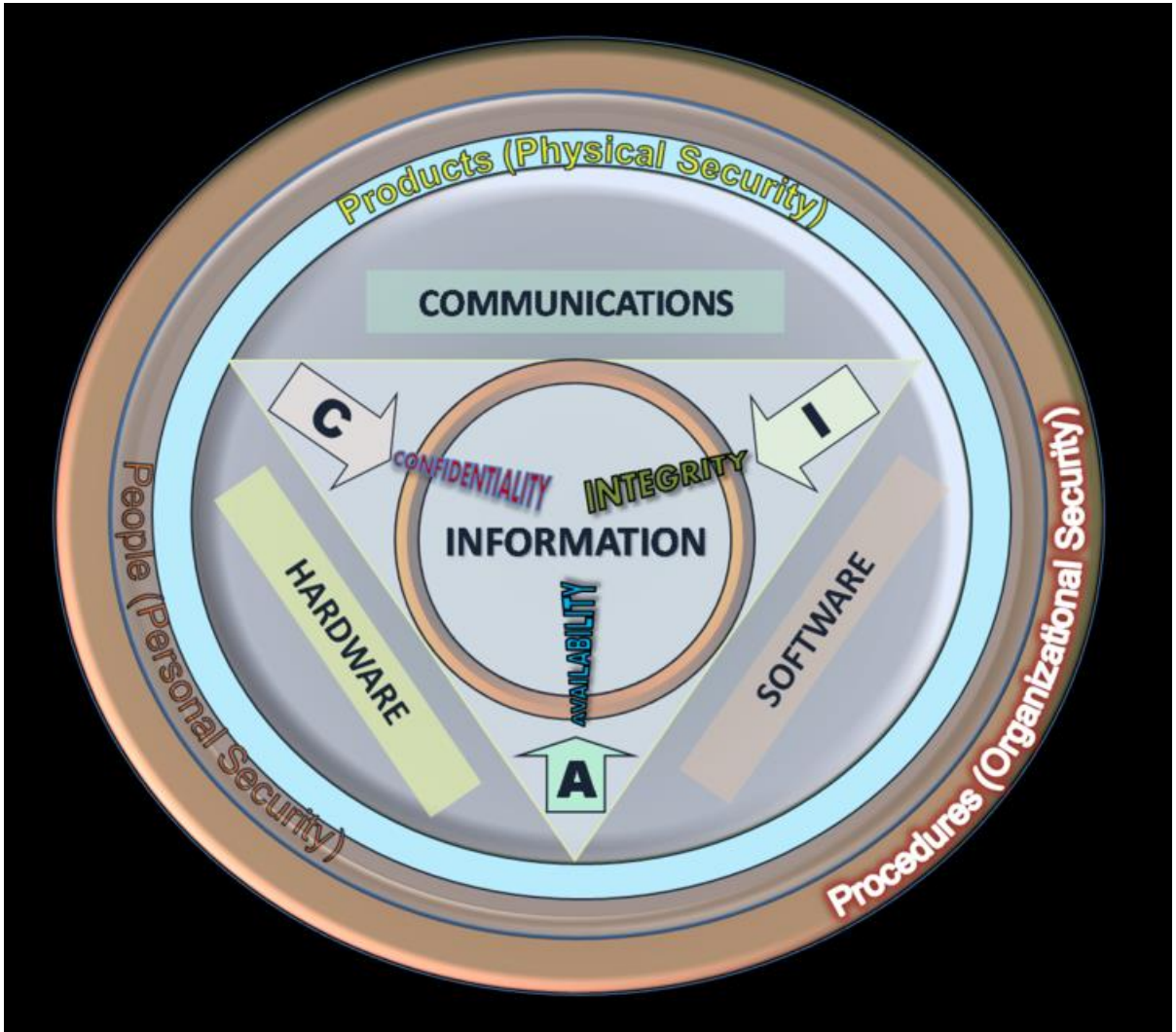
Security Services
vs
Mechanisms

Outline

- Security services
  - Security components/goals/features/properties
- Security mechanisms:
  - Symmetric Cryptography
  - Asymmetric Cryptography
  - Cryptographic Checksums
  - Digital Signatures
  - Digital Certificates
  - Kerboros
  - …

Security Service

- The CIA Triad (https://en.wikipedia.org/wiki/Information_security)



Security services

- **Confidentiality**: Data is only for the authorized.
- **Data integrity**: Data is correct.
- **Origin integrity**: Origin of the data is correct.
- **Availability**: Data is available to the authorized.
- **Non-repudiability**: There exists a mechanism to prove that the actor (sender, receiver, writer, retrieval, …) indeed performed that action.
- Message authentication
- Entity authentication
- Anonymity
- etc.

Security services

Note: What services to implement depend on the application's security policy/requirements.

- Example application

  You are part of a project team, which is developing an information system for command, communication and control (3C) between a command center and nuclear submarines. Of course, the communication between the command center and the submarine must be secured from potential faults and attacks.

  Explain how each of the following goals could be achieved by providing detailed protocols (showing the actors and their respective actions).

Security service: Exercise

- **Goal #1:** The communication must remain secret. That is, only the targeted recipient of a message should have access to the content of the message.
- **Goal #2:** The correctness of the messages/commands must be verifiable. That is, if the message ever gets altered, the change should be detected.
- **Goal #3:** The recipient of a message should be able to verify the true identity of the sender. That is, an unauthentic sender should be detected.
- **Goal #4:** A command issued by A cannot later be denied by A. That is, A cannot later deny either the content or the action of sending that message.
- **Goal #5:** The communication between the command center and the submarines must remain working all the time.

Security Mechanisms

- Common security mechanisms:
  - Symmetric Cryptography
  - Asymmetric Cryptography
  - Cryptographic Checksums
  - Digital Signatures
  - Digital Certificates
  - Firewalls
  - IDS
  - Kerberos
  - 802.11i
  - WEP
  - IPSec
  - SSL
  - …

Security services vs mechanisms vs policies

- A security **service** is provided by implementing one or more **mechanisms**.
- A security mechanism may be used to enforce one or more security services.

Q: What is the relationship between the security policy and security services / mechanisms?

Security services vs mechanisms vs policies

- **Exercise:**

Write a security policy concerning the protection of computers in a public lab.

Q: What security services?

Q: How would each of those services be provided?