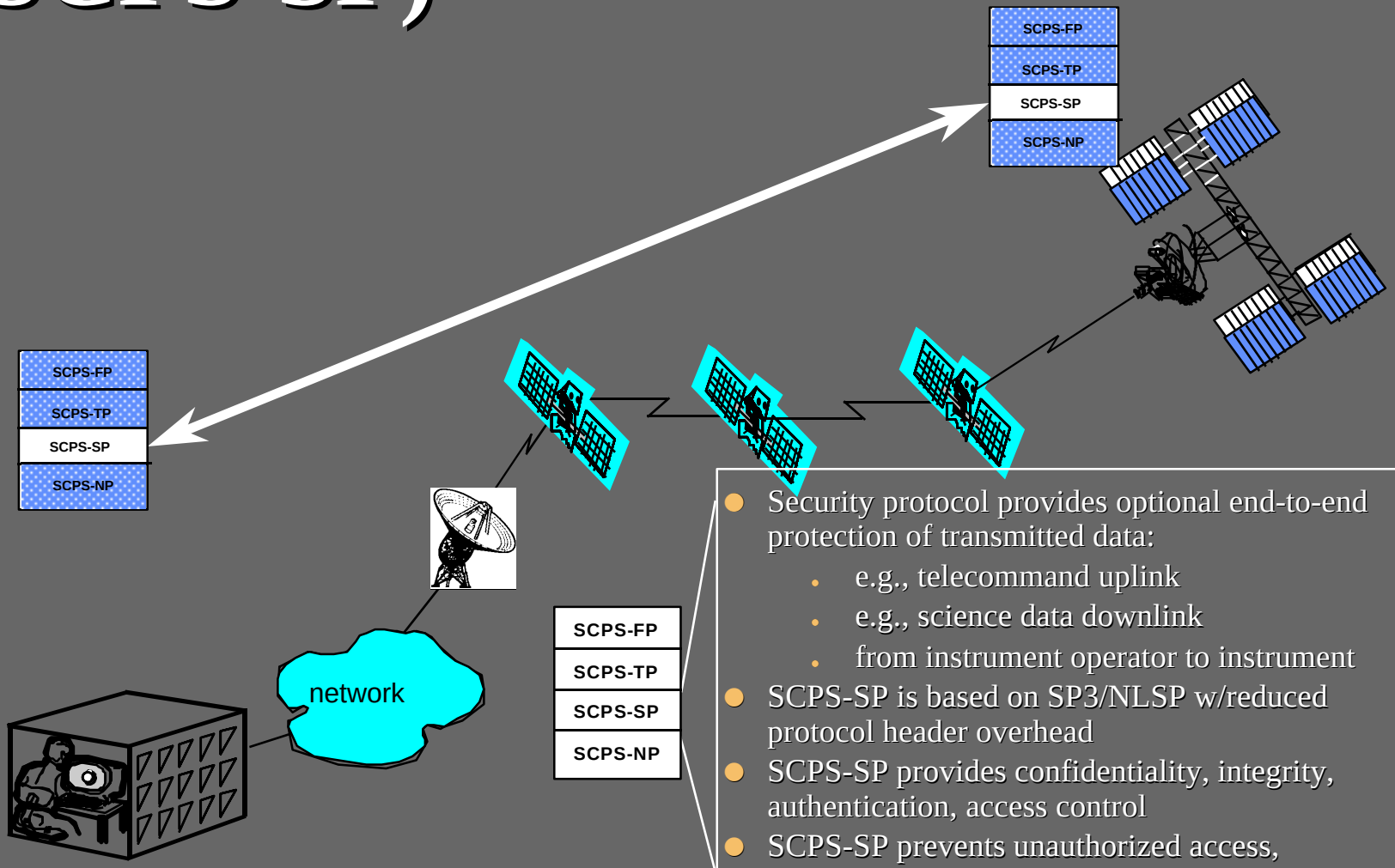
The SCPS Security Protocol (SCPS-SP)



- Security protocol provides optional end-to-end protection of transmitted data:
  - e.g., telecommand uplink
  - e.g., science data downlink
  - from instrument operator to instrument
- SCPS-SP is based on SP3/NLSP w/reduced protocol header overhead
- SCPS-SP provides confidentiality, integrity, authentication, access control
- SCPS-SP prevents unauthorized access, interception, modification, spoofing/masquerading
- SCPS-SP is algorithmic independent

SPARTA

Security Protocol Protection Services Concept

- **Authentication:**
  - **implicit: key selection based on source/destination pair**
  - **explicit: address info contained in protected header**
- **Integrity:**
  - **integrity check value taken over the PDU + secret key**
- **Confidentiality:**
  - **encipherment of PDU (and check value, if present)**
- **Access Controls:**
  - **implicit access controls based on key management**
    - **distribution of keys between pairs of systems allowed to communicate**
  - **embedded security label option available to check classification level range**

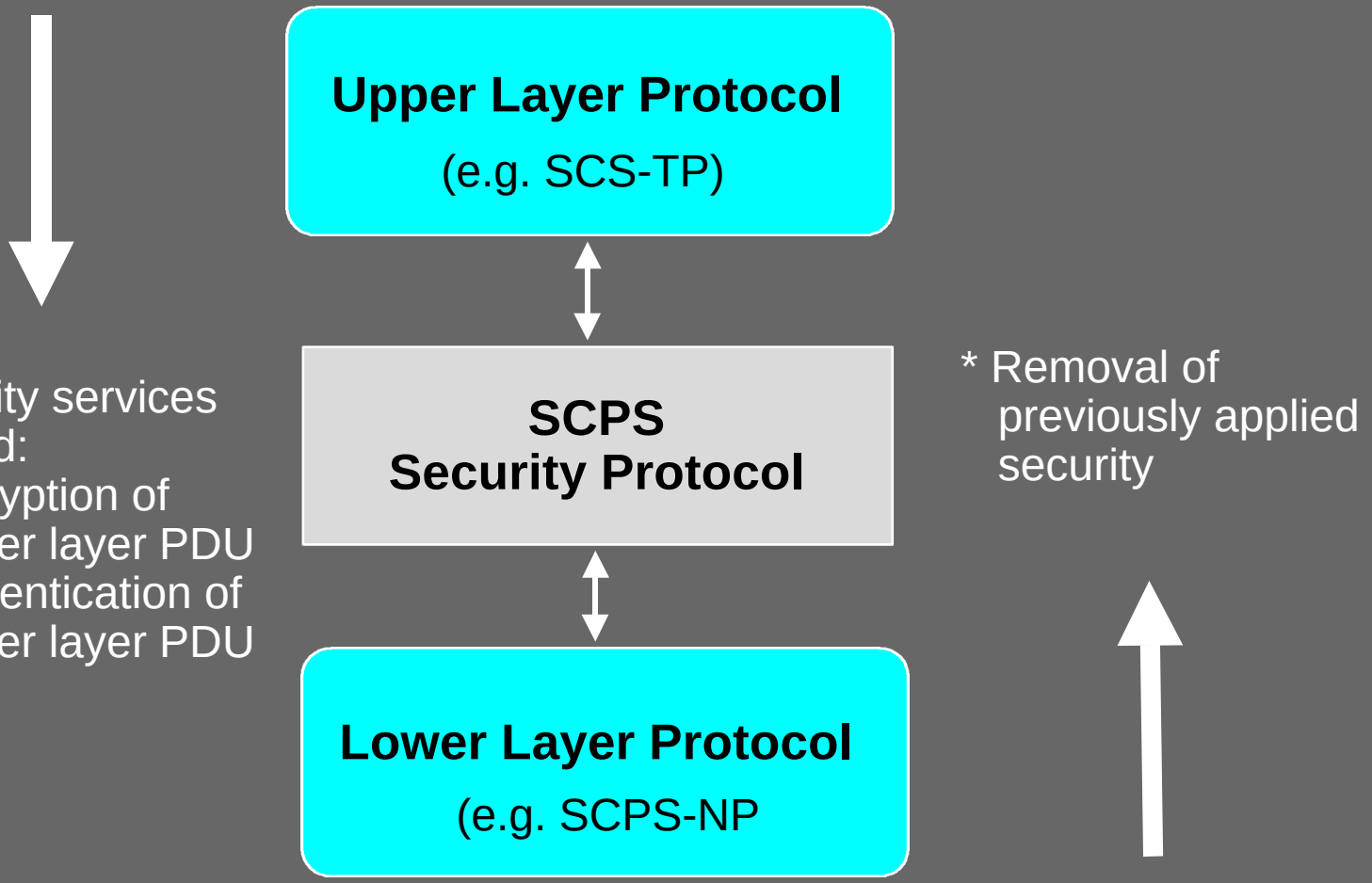
SPARTA

Overview: How Does a Security Protocol Work?

- Provides security services and mechanisms to the SCPS protocol suite to provide information protection
- On transmit, the Security Protocol:
  - receives a PDU from a higher level protocol (e.g., Transport),
  - applies requested (or required, per security policy) security services,
  - hands a PDU to the next lower protocol (e.g., Network) for transmission over the network
- On receive, the Security Protocol:
  - receives a PDU from lower layer protocol (e.g. Network)
  - attempts to un-apply security services
  - if un-application of security *passes*, hands PDU to next upper layer protocol

SPARTA

How Does a Security Protocol Work?

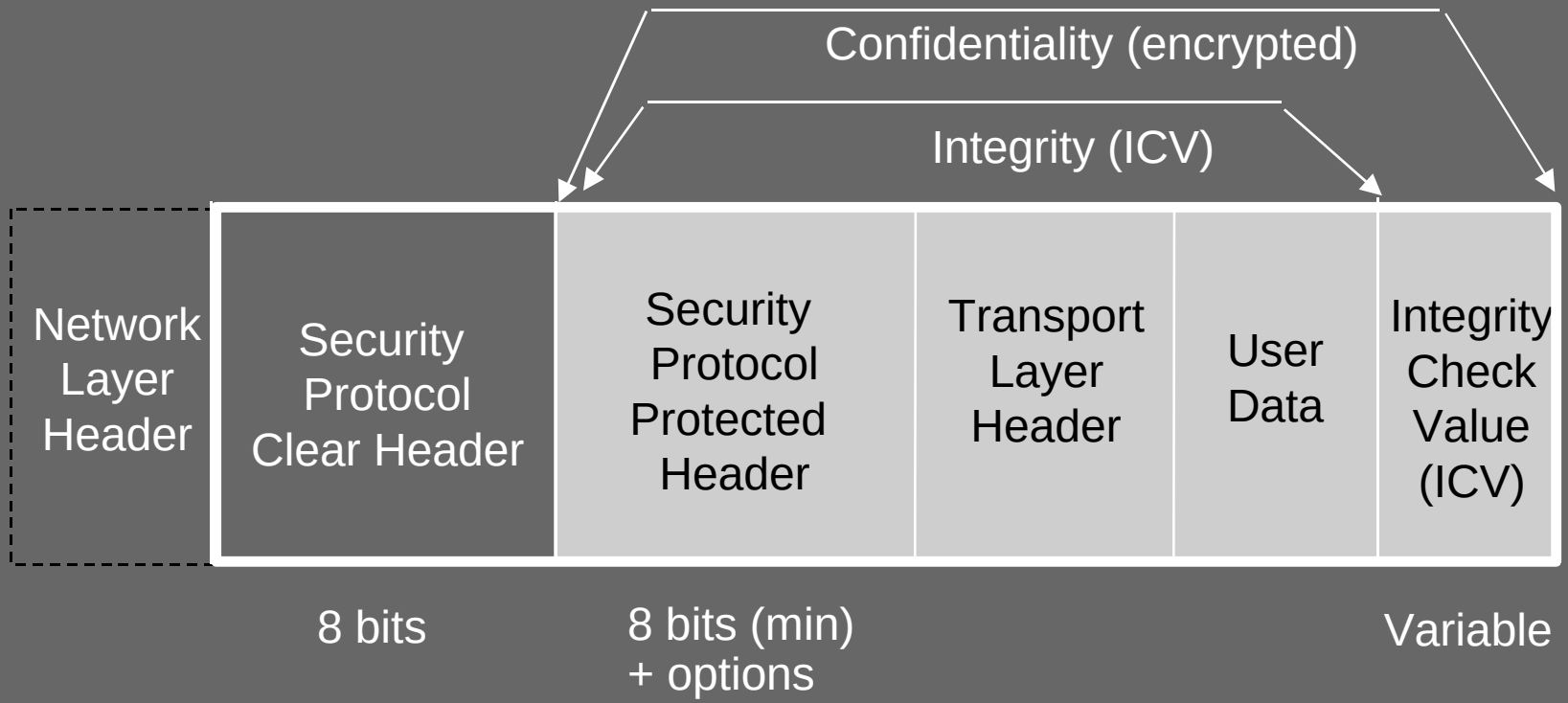


* Security services applied:
  - encryption of upper layer PDU
  - authentication of upper layer PDU

* Removal of previously applied security

SPARTA

SCPS-SP Header Structure



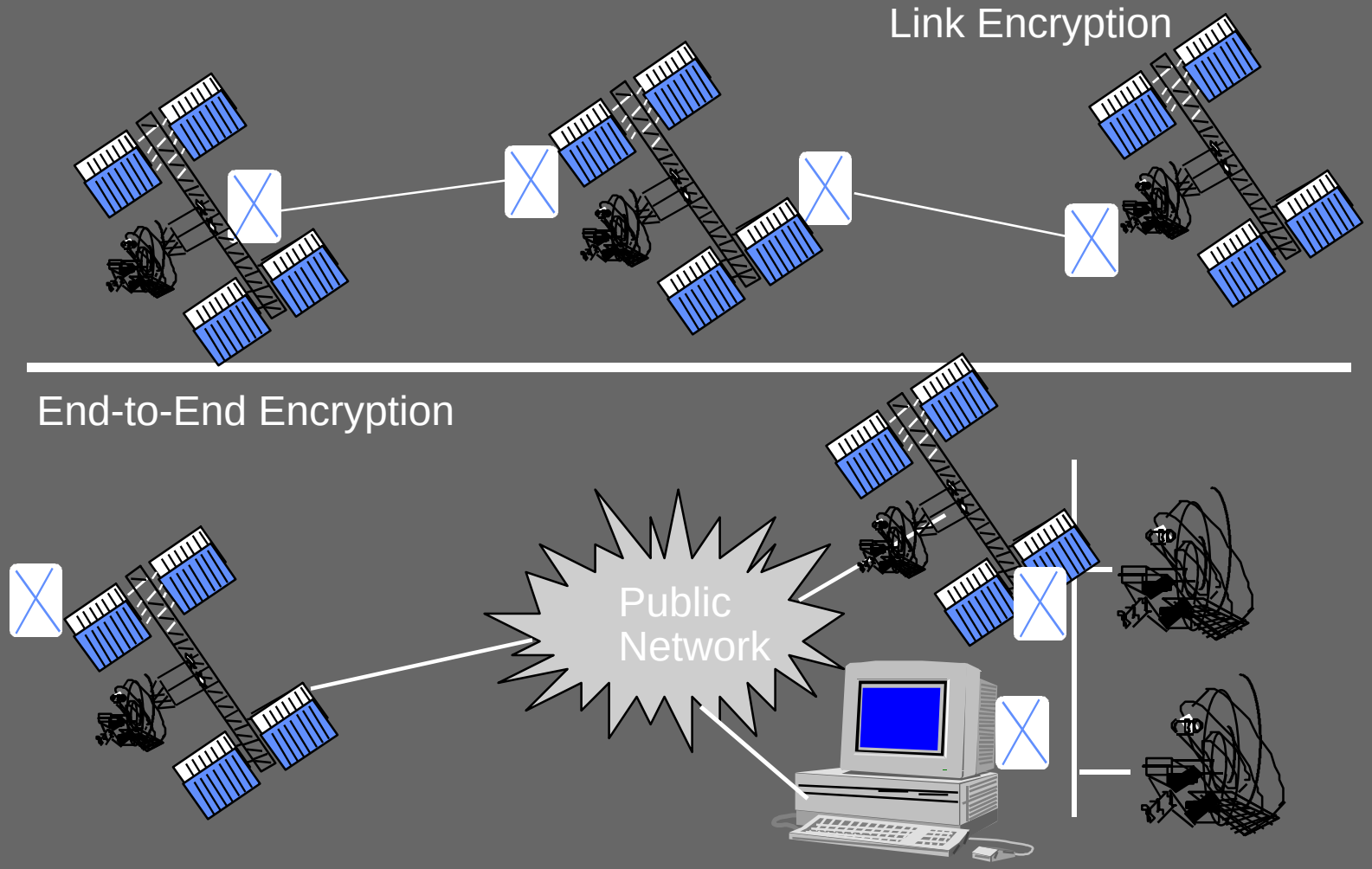
SPARTA

Types of Cryptography

- **Link Encryption**
  - **“traditional” cryptographic implementations for both ground and space applications**
  - **point-to-point**
    - **many cryptographic devices involved**
    - **many encrypt/decrypt operations on a hop-by-hop basis - data is *exposed* and therefore vulnerable**
- **End-to-End Encryption**
  - **protection from the data’s origin to the data’s destination**
  - **data is encrypted at the source and decrypted only at the destination - no data exposure at intermediate systems**
  - **much fewer cryptographic devices involved than link**

SPARTA

Types of Cryptography - Illustration



SPARTA

SP Status

- A CCSDS Red Book (version III) has been completed (CCSDS 713.5-R-3)
- A military standard version of the specification has been completed (MIL-STD-2045-43001).
- An ISO draft international standard is out for ballet (ISO/DIS 15892).
- Reference implementation code has been written and tested.

SPARTA