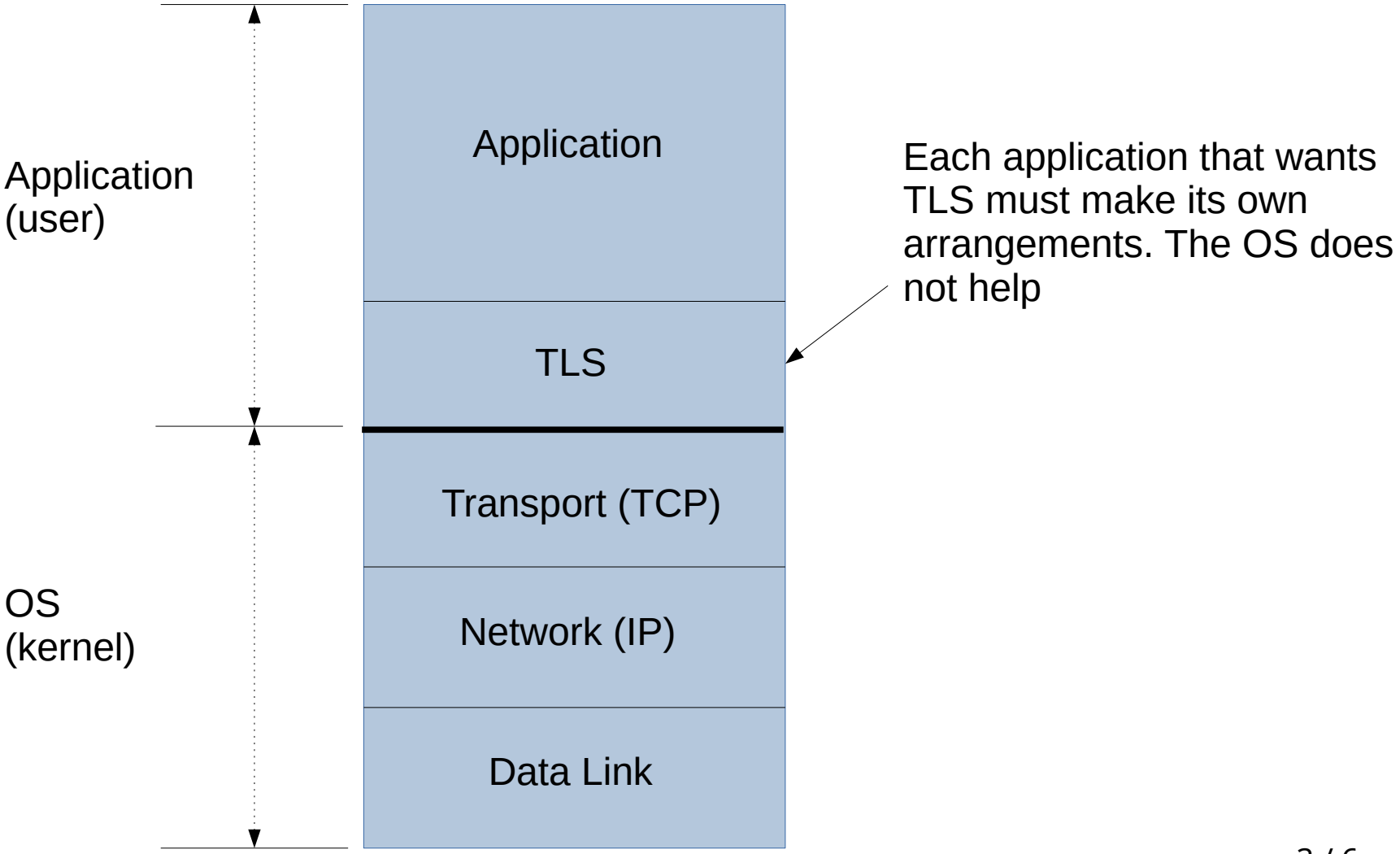
Transport Layer Security

Vermont Technical College
Peter Chapin

History

- Protocol originally called “Secure Sockets Layer” (SSL). All SSL versions are now historic (and flawed).
- Taken over by the IETF and changed to “TLS”
- Current version is TLS 1.3. Earlier versions have minor security flaws.

TLS's Stack Location



Terminology

- Authentication
  - Verifying the identity of your peer
- Authorization
  - Verifying permissions to perform various actions
- Data Integrity
  - Protecting against unauthorized writes
- Confidentiality
  - Protecting against unauthorized reads

TLS Provides

- Confidentiality (encrypted payloads)
  - Passwords sent over TLS connections cannot be read off the network
- Data Integrity (modifications are detected)
  - *However*: Packet/segment headers are not protected
- Authentication (optional)
- Replay Protection

TLS Does Not Provide

- Host security
  - Once the data reaches the other side it is up to the receiving host to protect it
- Various attacks against IP and TCP itself
  - IPsec can be used to protect against this
- However…
  - DNS and IP spoofing can be detected since a malicious host can’t authenticate.