# Authentication Systems:-

Auth's from a third party ~~ab~~ systems

OAuth2 → Open Auth System

SAML
Shibboleth

*Kerberos* in MIDexam
↳ to reduce computational overhead
↓
Diagram from book

# Well-Known Attack Types & Vulnerabilities:-

* SQL Injection
* Buffer Overflow

# DDOS attack → smurf attack

# Laws → bdlaws.minlaw.gov.bd

1) Social Engineering Attack → how to deceive someone

# Hash function requirements:

1) can be ~~ab~~ applied to any sized message M.
2) Produces fixed length output h.
3) is easy to compute ~~any~~ h = H(M) ~~an~~ for any msg M.
4) given h is infeasible to find x s.t. H(x) = h.
   * one way property
5) given x is infeasible to find y s.t. H(y) = H(x)
   * weak collision resistance.
6) is infeasible to find and x, y s.t. H(y) = H(x)
   * strong collision resistance.