COPYRIGHT

© Crown Copyright, The National Cyber Security Centre 2019. This information is licensed under the Open Government Licence v3.0. To view this licence, visit:

https://www.nationalarchives.gov.uk/doc/open-government-licence/ OGL

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK Version 1.0 © Crown Copyright, The National Cyber Security Centre 2019, licensed under the Open Government Licence: https://www.nationalarchives.gov.uk/doc/open-government-licence/.

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.
The Cyber Security Body Of Knowledge

www.cybok.org

Classes of distributed systems
Classes of vulnerabilities & threats
Decentralized P2P models
Attacking P2P systems
Coordinated resources clustering
Coordination classes and attackability

Decentralized point-to-point interactions across distributed entities without a centralized coordination service
Coordinated clustering across distributed resources and services

Wireless sensor networks
Online gaming systems

Coordination of resources vs coordination of resources
Client-server models
N-tier multi-tenancy models
Clouds
Databases
Ledgers
Storage systems

Public
Private
Hybrid
Multi-cloud

Big data services
High performance computing
Access/admission control & ID management
Data transportation
Resource management and coordination services
Data security
Confidentiality, integrity, and availability
Side channel attacks
Data consistency

Unstructured P2P protocols
Structured P2P protocols
Hybrid P2P protocols
Hierarchical P2P protocols

Symmetry of interfaces
Resilience to perturbations
Survivability through replication
Peer resources at the network’s edge
Address variance
Message passing
Distributed hash table

Principles

Mitigations
Denial of service (DoS)
Collusion attacks
Pollution attacks
White washing
Routing attacks
Buffer map cheating attacks
Sybil attacks
Eclipse attacks
Routing table poisoning
Localised eclipse attacks
Outgoing eclipse attacks

Systems coordination styles
Multi-tenant service management
Consistency principles
Concurrency principles
Group membership and consistency

Dependable and secure global coordination

Data management and coordination services

Whole system failures
Nodal failures
Entity failures
Service failures
Component failures

Dependability management services
Reliability technologies
Availability technologies
Security technologies
Dependability technologies

Fault tolerant computing
Dependable computer systems
Dependable computer networks
Dependable hardware
Dependable software

Reliability and quality of service
Dependability engineering
Dependability management
Dependability in computer systems