CyBOK

The Cyber Security Body of Knowledge

Network Security Knowledge Tree

COPYRIGHT

CHANGE LOG

Version date	Version number	Changes made
July 2021	2.0	Version updated following major revision of KA with re-structuring to place the network protocol discussion in a wider context and mention of a broader range of network architectures.
October 2019	1.0	

Security Goals and Attacker Models
- Security Goals in Networked Systems
- Attacker Models

Networking Applications
- Local Area Networks (LANs)
- Connected Networks and the Internet
- Bus Networks
- Wireless Networks
- Fully Distributed Networks: DHTs and Unstructured P2P Networks
- Software-Defined Networking and Network Function Virtualisation

Security at the Application Layer
- Email and Messaging Security
- Hyper Text Transfer Protocol Secure (HTTPS)
- DNS Security
- Network Time Protocol (NTP) Security
- Distributed Hash Table (DHT) Security
- Anonymous and Censorship-Free Communication

Network Protocols and Their Security

Security at the Transport Layer
- TLS (Transport Layer Security)
- Public Key Infrastructure
- TCP Security
- UDP Security
- QUIC

Security at the Internet Layer
- IPv4 Security
  - IP Spoofing
  - Fragmentation Attacks
  - VPNs and IPsec
  - NAT
- IPv6 Security
- Routing Security
  - Within an Autonomous System (AS)
  - Across ASs
- ICMP Security

Security on Link Layer
- Port-based Network Access Control (IEEE 802.1X)
- WAN Link-Layer Security
- Attacks on Ethernet Switches
- Address Resolution Protocol (ARP) / Neighbor Discovery Protocol (NDP)
- Network Segmentation
- Wireless Security
- Bus Security

Network Security Tools
- Firewalling
  - Application Gateway (AG)
  - Circuit-level Gateway (CG)
  - DMZ
  - Intrusion Prevention System (IPS)
- Intrusion Detection and Prevention Systems
- Network Security Monitoring
- SDN and NFV Security
- Network Access Control
- Zero Trust Networking
- DoS Countermeasures

Other Network Security Topics
- Cloud and Data Center Security
- Delay-Tolerant Networks and Ad-hoc Sensors Networks
- Network Covert Channels
- Payment Networks
- Physical-Layer Security
- Networking Infrastructure Security
- Cross-Border Regulations