Core Security Concepts	
CIA triad	Confidentiality, Integrity, Availability: the three pillars of security
AAA	Authentication, Authorization, Accounting: who you are, what you can do, what is logged
Zero Trust	Never trust, always verify: verify every user and device explicitly
Least privilege	Users get only the minimum access needed for their job
Defense in depth	Layered controls so one failure does not breach everything

Threats & Attacks	
APT	Advanced Persistent Threat: long-term targeted intrusion, often nation-state
DDoS	Distributed Denial of Service: traffic flood from many sources
MITM	Man-in-the-Middle: attacker intercepts traffic between two parties
SQLi	SQL Injection: malicious SQL via unsanitized input
XSS	Cross-Site Scripting: malicious script injected into web pages
XSRF/CSRF	Cross-Site Request Forgery: forged requests using a victim's session
Phishing / Whaling / Vishing	Email / executive-targeted / voice-call social engineering
Ransomware	Malware that encrypts data and demands payment

Cryptography & PKI	
AES	Advanced Encryption Standard: symmetric cipher (128/192/256-bit)
RSA	Asymmetric cipher used for key exchange and digital signatures
PKI	Public Key Infrastructure: CAs, certificates, trust chains
CA	Certificate Authority: issues and signs digital certificates
CRL / OCSP	Certificate Revocation List / online check for revoked certs
Hashing (SHA-256)	One-way integrity check; hashing is not encryption
Digital signature	Proves authenticity, integrity, and non-repudiation
TLS	Encrypts data in transit (HTTPS); SSL is deprecated

Network Security	
IDS / IPS	Intrusion Detection / Prevention System: detect vs detect-and-block
HIDS / NIDS	Host-based vs network-based IDS
SIEM	Security Information and Event Management: centralized log analysis
SOAR	Security Orchestration, Automation and Response
WAF	Web Application Firewall: filters HTTP attacks like SQLi and XSS
NAC	Network Access Control: enforces device compliance before joining
DMZ	Demilitarized Zone: buffer network between public and private

By **bytebar**
cheatography.com/bytebar/

Not published yet.
Last updated 20th September, 2026.

Network Security (cont)	
VPN / IPsec	Encrypted tunnel; IPsec suite for secure IP communications
VLAN	Virtual LAN: segments broadcast domains logically
SPF / DKIM / DMARC	Email authentication trio against spoofing

Identity & Access	
MFA	Multi-Factor Authentication: two or more proof categories
SSO	Single Sign-On: one login for many apps
SAML / OAuth / OpenID	Federation and delegated authorization standards
RADIUS / TACACS+	AAA protocols (TACACS+ encrypts the full payload)
RBAC / ABAC	Role-Based / Attribute-Based Access Control
Kerberos	Ticket-based auth, port 88; default in Active Directory
LDAP	Directory access protocol, port 389 (LDAPS 636)

Operations & Governance	
BIA	Business Impact Analysis: identifies critical processes and recovery priorities
RTO / RPO	Recovery Time Objective / Recovery Point Objective
SLA	Service Level Agreement: uptime and performance contract
Hardening	Disabling unnecessary services and ports to reduce attack surface
Patching	Applying fixes; one of the highest-ROI controls
Backups (3-2-1)	3 copies, 2 media types, 1 offsite
Incident response	Preparation, Detection, Containment, Eradication, Recovery, Lessons learned

By **bytebar**
cheatography.com/bytebar/

Not published yet.
Last updated 20th September, 2026.