

Vocabulary List

*-Property

Bell-LaPadula Model (BLP)
Biba model/Strict Integrity Policy
Biba's Low Water Mark Policy
Biba's Ring Policy
Caesar Cipher
Chinese Wall Policy
Clark-Wilson policy
Huffman encoding
Kerckhoff's Law
Lempel-Ziv algorithm
Lipner's integrity matrix model
Principle of Easiest Penetration
Principle of Least Privilege
Shared Resource Matrix Methodology
Simple-Security Property
System Z
Vernam Cipher
Vigenère cipher
Vigenère tableau
access control list
access control matrix (ACM)
access control policy
adaptive chosen plaintext attack
annualized loss expectancy
asymmetric cipher/public key algorithm
attack
auditing
authentication
availability
bandwidth/capacity/throughput
basic security theorem
bit (2 meanings)
block cipher
book cipher
breakable
capability-based system
channel
chosen ciphertext attack
chosen plaintext attack
ciphertext-only attack
columnar transposition
conditional commands
confidentiality

confusion
containment problem
countermeasure
covert channels
cryptanalysis
cryptography
cryptosystem
cryptology
diffusion
discrete source/zero-memory source
discretionary access controls (DAC)
dominates relation
downgrading
encoding
encryption/decryption
entropy
equivocation
existence of channel
fabrication
first-order model, etc.
fundamental theorem of the noiseless channel
hierarchical levels
information content
information flow policies
information theory
integrity
integrity levels
integrity policies
interception
interruption
intrusion detection
key distribution
key length
key management
keyed cipher/keyless cipher
keyspace
known plaintext attack
label creep
lattice-based security
leaking permissions
lossless encoding
malleable algorithm
mandatory access controls (MAC)
metapolicy
modification
monoalphabetic cipher

multi-level security (MLS)
need-to-know categories
noisy/noiseless
non-interference
non-repudiation
nth order Markov source
objects
one-time pad
partial order
perfect cipher
plaintext/ciphertext
policy/mechanism/assurance distinction
polyalphabetic substitution
prefix-free
private/public key
product cipher
protection systems
pseudo-random number generator (PRNG)
read/write/execute/create/destroy permissions
risk management
role-based access control (RBAC)
security
security labels/levels
security model
security policy
sender/receiver
separation of duty
separation of function
simple substitution cipher
storage channels
stream cipher
strong cryptosystem
strong tranquility property
subjects
substitution
substitution cipher
symmetric channel
symmetric cipher/secret key algorithm
system attribute
system high
system low
the safety question
threat
timing channels
total order
transposition
trusted subject
trusted subjects
uniquely decodable
unwinding theorem
vulnerability
water mark policy
weak tranquility property
zero-order model