Vivian Do 12/08/2022

Final Exam Cheat Sheet:

Confidentiality: assures that confidential or private information is not made available or disclosed to authorized individuals; privacy ≠ confidentiality
- can be preserved by using encryption (symmetric (DES, AES) & asymmetric encryptions)

Integrity: guarding against improper information modification or destruction
- data integrity can be achieved by using message authentication code (MAC), or message integrity code (MIC)
  - MAC & MIC can come from hash functions (MD5, SHA) or block ciphers

Availability: assures timely & reliable access to and use of information; loss of this is the disruption of access to or use of info.
- firewall, intrusion detection system (IDS), anti virus software can be used to achieve this

Authenticity = being genuine & able to be verified & trusted; confidence in validity of message (message originator)
- overlaps w/ integrity; can be achieved by digital signatures (DSA)

Accountability = security goal that generates requirements for actions of entity to be traced uniquely to that entity
- can be achieved by logging and auditing, digital signatures

Symmetric Cryptography: Alice (good) → Encryption $e()$ (key k) → Decryption $d()$ (key k) → Bob (good); key generator — secure channel

x = plaintext, k = key, y = ciphertext

Encryption = $y = e_k(x)$

Decryption = $x = d_k(y)$

- private-key / single-key cryptography
- Encryption w/ symmetric cipher!
- key must be transmitted via secured channel between sender & reciever!

Public-Key Cryptography: plaintext message m → encryption algorithm → ciphertext $k_B^+(m)$ → decryption algorithm → plaintext message $m = k_B^-(k_B^+(m))$

k_B^+ = public key; k_B^- = private key

- need $k_B^+()$ and $k_B^-()$ such that $k_B^-(k_B^+(m)) = m$
- given public key, it should be impossible to compute private key (RSA)

Digital Signature = verifiable & nonforgeable; reciever can prove that sender & no one else have signed document
- can be signed & encrypted with private key

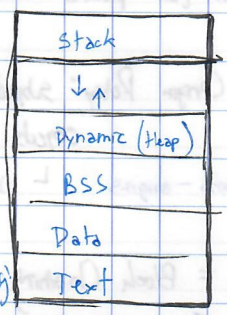
Hash functions = Message Digest (MD); SHA series

Greatest Common Divisor = gcd
- gcd(a, b) is relatively prime when a and b's gcd(a, b) = 1
- can find gcd by factorization & Euclidean Algorithm

Booting/Bootstrapping: loading an OS into memory from powered-off state

BIOS: basic input/output system; code stored in firmware component
- loads memory w/ second-stage boot loader

Memory Organization



- can use crypto hashes for proof of work in bitcoin blockchain (prevents double-spending)

Password Salt: associating a random number with each userid
- hash is compared w/ salt associated w/ userid & password stored in salt

1) User types userid X and password P
2) system looks up S and H, where S is the random salt for userid X and H is stored hash of S and X & password
3) System tests whether $h(S||P) = H$

Buffer Overflow: input in running process extends length of buffer; causes apps to behave improperly & unexpectedly
- Effects: process can operate on malicious data or execute malicious code passed by attacker
- buffer w/ shellcode (injected directly into buffer) is a "payload"

Propagation Malware:
- virus = human-assisted propagation
- worm = automatic propagation w/o human help

Concealment Malware:
- rootkit = modifies OS to hide its existence
- Trojan = provides desirable functionality; hides malicious operation

Insider Attack: security breach caused by someone part of organization that controls asset should be protected

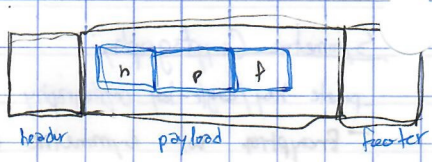
Packet Switching Pros/Cons: no wasted bandwidth; multiplexing; service adaptation

Internet Protocol Stack:

application	1
transport	2
network	3
link	4
physical	5

1) supporting network applications (FTP, SMTP, HTTP)
2) process-process data transfer (TCP, UDP)
3) routing of datagrams from source to destination
   - IP, routing protocols (PPP, Ethernet)
4) data transfer between neighboring network elements
5) bits "on the wire"

Encapsulation:



Data Link frame → IP packet → TCP/UDP packet

Session Hijacking: TCP hijacking; security attack over a protected network; attempt to take control of network session
IP Spoofing: an attempt to send packets from one IP address that appears to originate at another
Packet Sniffers: Read information traversing on a network

DNS Cache Poisoning - give DNS false records & get it cached
- always check identifiers! - deploy DNSSEC!

Tunnels can prevent eavesdropping; VPNs are safe!

Same Origin Policy: subjects from one origin cannot access objects from another origin
- domains - origins
- cookies - subjects

Firewall = integrated collection of security measures designed to prevent unauthorized electronic access to networked PC system
- accepted, rejected, dropped @ TCP or UDP
- packet filters, stateful filters, & app-layer

(RU8ER) Key stream - can be generated on-line one bit/byte at the time
stream Cipher - XOR pt w/ key stream

CBC - ✓ fast & simple; no shows patterns in pt
✗ not suitable for apps allowing packet losses

AES = Block Chaining
ECB - ✓ very simple; can tolerate loss/damage of block
✗ documents & images are unsuitable; patterns = repeated

Binary Numbs for S-Box

0	0000	8	1000
1	0001	9	1001
2	0010	10	1010
3	0011	11	1011
4	0100	12	1100
5	0101	13	1101
6	0110	14	1110
7	0111	15	1111