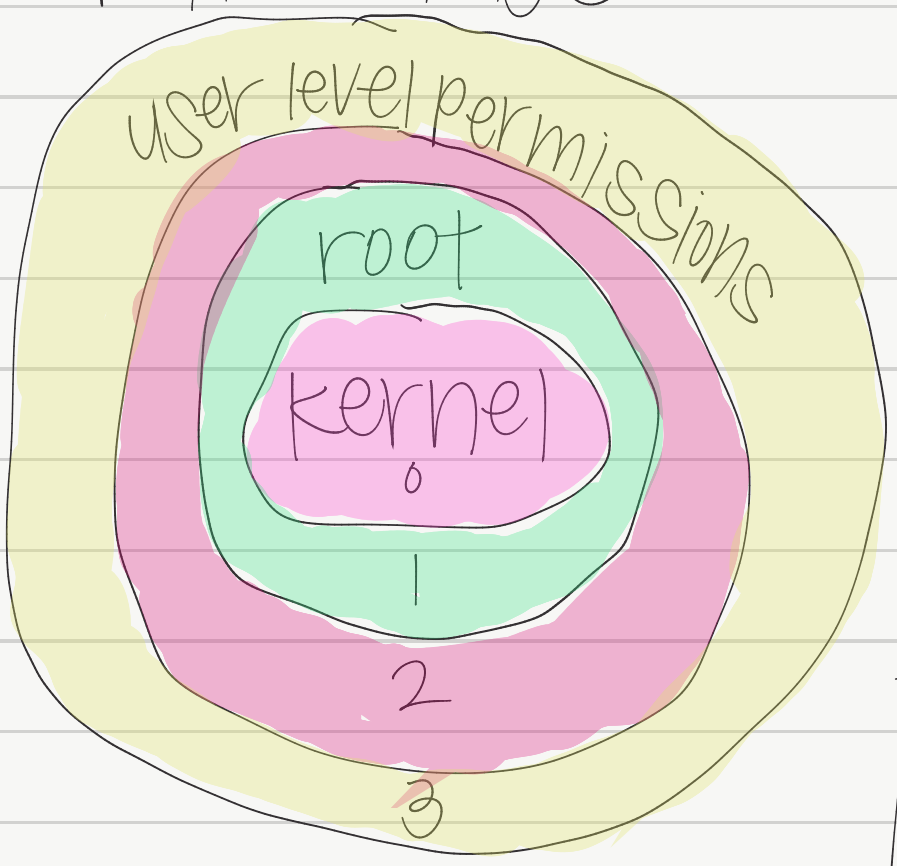
Security+ Vocab Notes

Dec 10, 2024 at 4:02 PM

- TACACS+: Terminal Access Controller Access Control System Plus, network security protocol that provides authentication, authorization, and accounting services for remote access servers
- RADIUS: Remote Authentication Dial-In User Service, a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect to a network
- Zero Trust control plane: policy engine (PE) and policy Administrator (PA)
- PEP (Policy Enforcement Point) ——— PDP (Policy Decision Point)
- Data plane — control plane
- Key Escrow: a method of storing cryptographic keys with a third party
- Self Encrypting Drive (SED): a data storage device equipped with hardware-level encryption functionality
- Full-Disk Encryption (FDE): software technology designed to provide confidentiality for an entire data storage device
- Encrypting File System (EFS): an MS Windows component that enables encryption of individual files
- HTTPS secures web traffic via SSL/TLS encryption
- Simple Mail Transfer Protocol Secure (SMTPS): a deprecated TLS-based method for secure transmission of email messages
- Secure Hypertext Transfer Protocol (SHTTP): an

obsolete protocol used for secure data transfer over the web
honeypots and honeynets attract and observe
honeyfiles and honeytokens (data) alert
· detect rootkits by booting the hard drive from an external device
· logic bombs: when x=1 do
· keyloggers can be software or hardware with a plugged in device
· shellcode executes the exploit
· IPSEC secures packets
· DES old, 3DES encrypt decrypt encrypt
· AES replaced DES and 3DES
· block ciphers: DES, 3DES, AES, IDEA, Blowfish, Twofish, RC5, RC6 (DES replacement)
· Stream ciphers: RC4
· SHA-1: 160 bit digest
· SHA-2: 24-512 bit digest
· SHA-3: 224-512 bit digest
· post-quantum cryptography: increased key size, lattice-based cryptography
· RTO time to recover, RPO up to what point is recovered
· qualitative likelihood and impact, quantitative probability and potential impact
· risk transfer insurance, risk acceptance do nothing, risk avoidance eliminate hazards, risk mitigation reduce the impact
· Single Loss Expectancy (SLE) = asset value x Exposure factor (EF) (proportion lost)

computer rings



malware

↓

dropper to initiate
or run other malware

↓

maybe downloader
to get additional
tools post infection

---

stream ciphers — block ciphers
faster, more efficient higher security

confidentiality
encryption

availibility
redundancy

integrity
hashing

RM

governance

performance measurement

resource management

alignment

RM

↓

identification

↓

analysis

↓

treatment

↓

monitoring

↓

reporting

policies
↓
standards
↓
procedures

governance

GRC

risk

compliance

BYOD — CYOD — COPE

BYOD
user
control

COPE
company
control

- internal vs. external compliance monitoring is over compliance to internal or external policies
- procurement is end to end and includes acquisition
- MIME enables email messages beyond text, S/MIME provides encryption, authentication, message integrity, and other services
- SFTP: enables secure file transfer over SSH
- SSH: a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers
- IPSEC: a suite of protocols and technologies that provide encryption, authentication, and data integrity for network traffic
- ESP: the part of IPSEC that provides authentication, confidentiality, and integrity
- SRTP: a protocol that enables secure, real-time delivery of audio and video over an IP network
- CCMP: an encryption protocol primarily used in Wi-Fi networks implementing the WPA2 security standard
- TKIP was designed to improve the security of WEP implementations
- Deprecated encryption protocols and cryptographic hash functions: DES, MD5, SHA-1, SSL, RC4
- TLS: a cryptographic protocol designed to provide secure communications over a computer network and is the successor to SSL

assignment and accounting

asset management

classification and categorization

monitoring and tracking

Layer 2: Datalink, switches, frames, MAC addresses

Layer 3: Internet, IPSEC, routers, packets, IP addresses

ECC(public key hash)

asymmetric

Diffie-Hellman, RSA

stream — block

RC4

DES, IDEA, Twofish, Blowfish, 3DES, AES, RC5, RC6

symmetric

- Asymmetric ciphers: DHE, ECC, RSA
- Symmetric ciphers: AES, DES, IDEA, RC4
- KEK: a cryptographic key usually used in key management systems to add security when encrypting and decrypting other keys
- PSK: a shared secret authentication method used in WPA, WPA2, and EAP
- IKE: a protocol used to set up secure connections and exchange cryptographic keys in IPSEC VPNS
- DHE: generates temporary keys for each session, providing secrecy to past and future communications
- ECDHE: a key exchange protocol that uses ECC for enhanced security and efficiency
- PFS: a solution designed to strengthen the security of session keys
- RSA: a public-key cryptosystem used for digital signatures, secure key exchange, and encryption
- ECC is best-suited for low-power devices, embedded systems, and mobile devices
- RC4 is a deprecated stream cipher used in legacy applications like WEP
- IDEA is a symmetric block cipher encryption algorithm largely replaced by AES
- Most are BS, Diffie-Hellman and RSA are AB, and RC4 is SS ★★★★
- IV: random value to ensure the same plaintext input does not produce the same ciphertext

output, even if the same encryption key is used, usually used with block ciphers
- XOR: commonly used in cybersecurity, typically for encryption and obfuscation, exclusive or
- CBC: block cipher mode that chains ciphertext blocks together
- CFB: a block mode that transforms a block cipher into a stream cipher
- CTM: a block cipher mode that combines a unique counter with encryption key to generate a stream of pseudorandom data blocks used for encrypting data
- ECB: the simplest and weakest block cipher mode that is not recommended for use