Name: Abdullatif Bumkidan IS4 Enroll.no: 2220[illegible]69

Lab Qs: (Answer in handwriting)

A1) Iot: every day objects equipped with sensors, connectivity and embedded Processing to exchange data over the internet.
Ex: (1) smart thermostat. (2) Smart cameras.

A2) A system where computational algorithms and physical components are tightly integrated and coordinated via a network (e.g. Smart grid)

A3) Iot emphasizes ubiquitous connectivity of devices; CPS stresses feedback control between cyber and physical domains. All CPS may use Iot, but not every Iot device perform closed-loop physical control.

A4) botnet = network of compromised devices controlled by an attacker. Mirai (2016) infected cam's/routers and launched 1 Tbps DDoS against Dyn DNS.

A5) A boot-time process that verifies cryptographic signature of firmware before execution; if invalid, device halts or rolls back.

A6) 1. Threat modeling (STRIDE).
2. Secure boot initialization (trust anchor).
3. Key injection (unique device ID & keys).
4. OTA update check (signed firmware).
5. Secure decommission (Erase secrets, revoke certificate)

~~A7)~~

A7) Weak default passwords. unpatched firmware. open Ports. unencrypted traffic.
Attacks: (1) Mirai DDoS. (2) Stuxnet PLC Worm.

A8) Over-The-Air Update = remote delivery of signed firmware patched to IoT devices using encrypted channel.

A9) Symmetric or asymmetric ciphers designed for constrained devices (small code, low power, 64-128 bit keys) Essential because standard AES/RSA drains battery.

A10) Scans Telnet/SSH with defaults, disable unused services Firmware updates, Telnet filtering, rate-limiting.

A11) ~~Sign~~ Signed firmware ensures integrity, hardware root-of-trust (ROM + unique keys) stores immutable boot code and keys. Preventing rollback and tampering.

A12) Provides certificate hierarchy to authenticate devices establish TLS tunnels, and distribute Public keys ~~Secu~~ Security.

A13) Processing data near sensors reduces latency and ~~fast~~ ~~Anomaly~~ exposure, enables local filtering, encryption, and faster anomaly detection without cloud dependency.

A14) Field devices (RTU/PLC) → Communication (Modbus, DNP3) → HMI/SCADA server.
Vulnerabilities: default credentials, no encryption, outdated OS, exposed ports.

A15.) Systmatic identification of threats (STRIDE) assignment of risk scores, and selection of mitigations before coding starts, reduces cost of fixes.

A16) Isolated hardware area (e.g. ARM TrustZone) that runs secure code, stores keys, and resist physical tampering; ensures confidentiality even if OS is compromised.

A17) Provides immutable audit trail for sensor readings, device identity, and firmware hashes, enables decentralized trust without a single CA.

A18) Sensors secret-share readings, cloud computes aggregates statistics (sum, avg) without learning individual values; only final result is revealed.

A19) Block ciphers: ~~Present~~ PRESENTS, SPECK, SIMON; Stream, Trivium, Hash; PHOTON; ECC curves; Curve25519; all optimized for < 10 KB ROM and < 1 mW power.

A20) Scanned Telnet defaults, enslaved 600k cameras/routers, launched 1 Tbps DDoS on Dyn, disrupting Twitter, Netflix. Clean-up required firmware updates and ISP filtering.

A21) Use device certificates + TLS mutual auth; sign readings with ECDSA; timestamp on blockchain; choose ECC-p256 for speed/low bandwidth.

A22) Attacker scans public IP, exploits unpatched HMI (~~e.g. Stuxnet~~ e.g. SCADA), pivots to PLC, alters ~~set~~ set-points. prevention; VPN VPN-only access, DMZ, patch management, ICS protocol whitelisting anomaly detection.

A16) Isolated hardware area (e.g. ARM TrustZone) that runs secure code, stores keys, and resist physical tampering; ensures confidentiality even if OS is compromised.

A17) Provides immutable audit trail for sensor readings, device identity, and firmware hashes, enables decentralized trust without a single CA.

A18) Sensors secret-share readings, cloud computers aggregates statistics (sum, avg) without learning individual values; only final result is revealed.

A19) Block ciphers; ~~RECENTS~~ PRESENTS; SPECK, SIMON; Stream, Trivium, hash; PHOTON; ECC curves; Curve25519; all optimized for < 10 KB ROM and < 1 mW power.

A20) Scanned Telnet defaults, enslaved 600k cameras/routers, launched 1 Tbps DDoS on Dyn, disrupting Twitter. Netflix. clean-up required firmware updates and ISP filtering.

A21) Use device certificates + TLS mutual auth; sign readings with ECDSA; timestamp on blockchain; choose ECC-p256 for speed/low bandwidth.

A22) Attacker scans public IP, exploits unpatched HMI (~~e.g. SQLi~~ (e.g., SQLi), pivots to PLC, alters ~~set~~ set-points. prevention; VPN VPN-only access, DMZ, patch management, ICS protocol whitelisting anomaly detection.

A23) Threats: firmware replay, network eavesdropping, unauthorized control. Mitigations: AES-CCM for confidentiality/integrity. ECDH key exchange, signed OTA, role-based access.

A24) Embedded: resource-constrained, real-time, physical exposure, Custom RTOS. Traditional: rich OS, user apps, standard crypto, easier patching.

A25) Trade-off between security level & resources, sid-channel resistance, key management, standardization, interoperability with legacy systems.