

Approfondimento Reti di Calcolatori e Cybersecurity

INIZIO ORE 9:10

Concetti Fondamentali di Sicurezza

Approfondimento
Cybersecurity

<date>
Location



La Sicurezza

Safety: relativa alla sicurezza fisica, fault tolerance } evitare che fure erranti
Security: insieme a presenza di attore malevolo } vs difendersi da malintenzionati

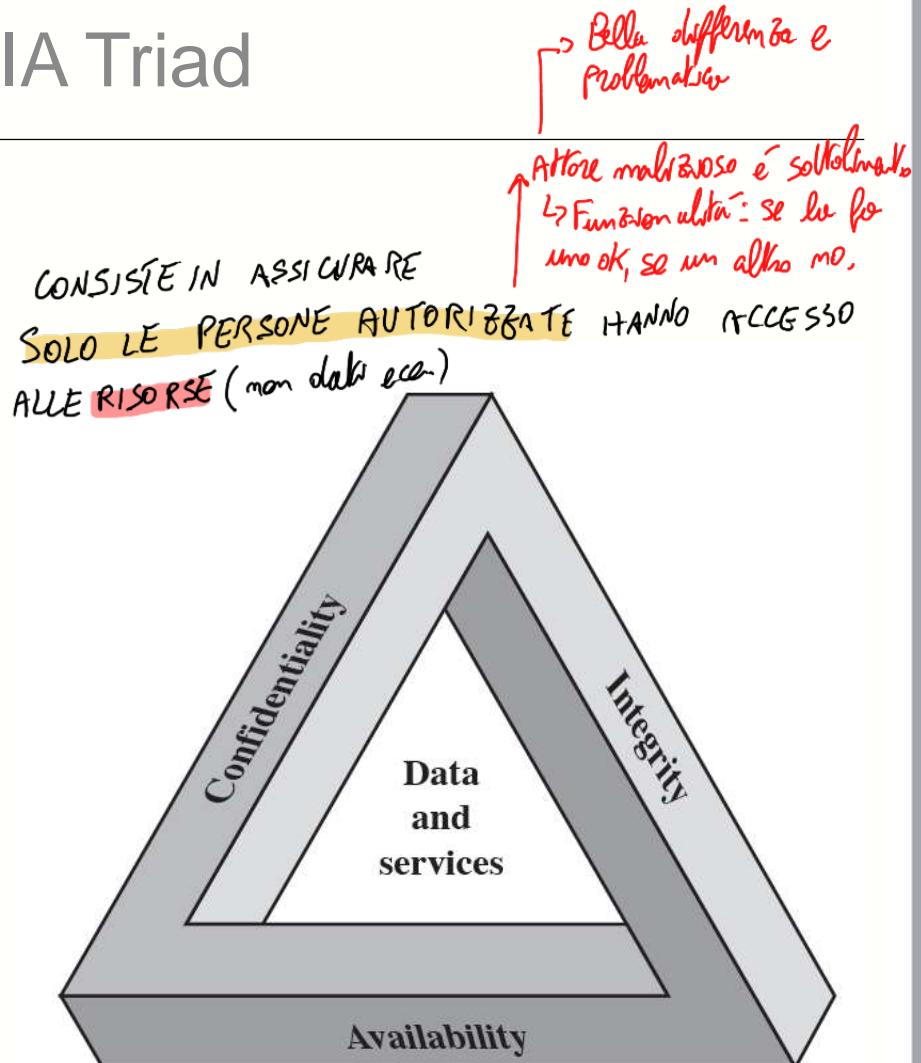
Un termine adottato in contesti differenti con significati differenti, include concetti quali:

- ✓ controllo degli accessi,
- ✓ autenticazione,
- ✓ autorizzazione,
- ✓ profilazione degli utenti,
- ✓ backup,
- ✓ disaster recovery,
- ✓ disponibilità,
- ✓ continuità del servizio,
- ✓ ... E molti altri...

Concetti Fondamentali: CIA Triad

DEF

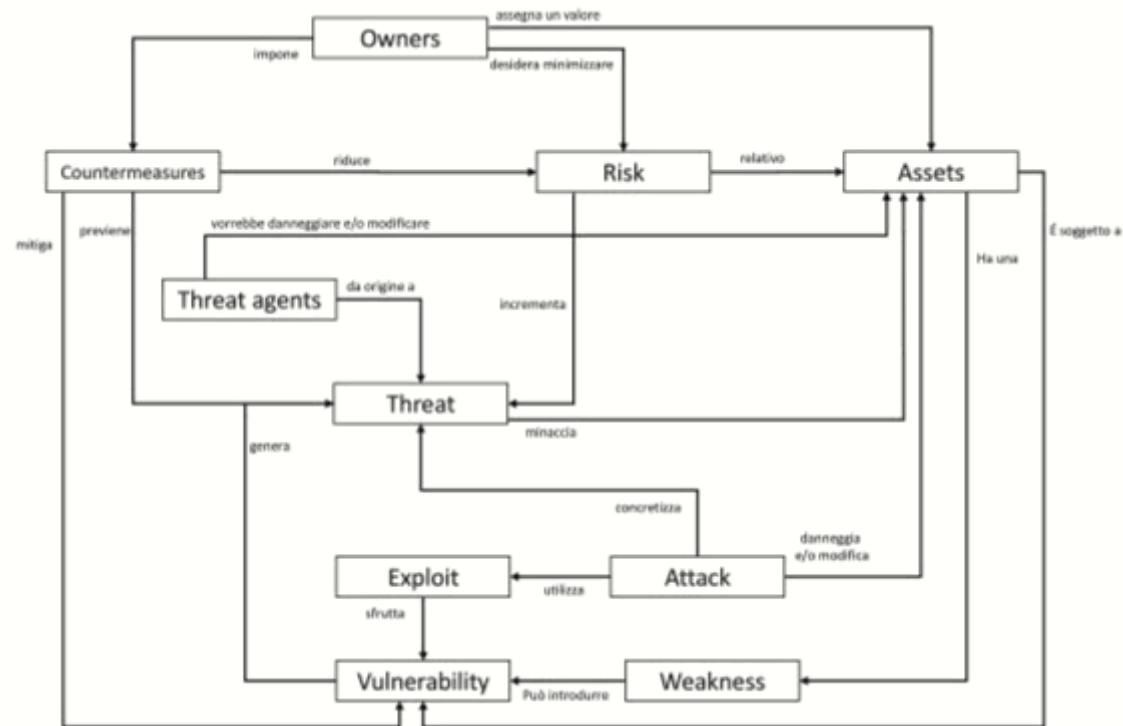
- **Confidenzialità (Confidentiality):** consists in ensuring that only authorized persons have access to resources
- **Integrità (Integrity):** consists in ensuring that a resource can only be modified by authorized people and only in authorized ways
- **Disponibilità (Availability):** consists in ensuring that a resource is available to authorized individuals at the appropriate time



↓
tempo appropriato: devo trovare risorsa nel momento in cui serve;
esempio del tipo: attacco con obiettivo di DoS per rendere servizio non disponibile quando serve

Terminologia

- **Threat:**
 - La minaccia che possa avvenire un evento dannoso come un attacco
- **Threat agents:**
 - Entità maliziosa che da origine alla minaccia
- **Asset :**
 - Ogni Entità cui il proprietario del sistema assegna un valore *
- **Risk :**
 - La probabilità che una minaccia possa concretizzarsi
- **Countermeasures :**
 - Azioni utili a prevenire di una minaccia/riduce il rischio



* La sicurezza ha forte valore soggettivo; debi avere un chiaro sviluppo in gioco: in genere metterei preferenze che costano meno per proteggere al sistema.

OWNER assegna valore. Minaccia di toccare una delle 3 CIA del threat agent

Terminologia (continua)

→ Può portare a vulnerabilità. Se c'è vulnerabilità c'è una weakness

- **Weakness:** Puoi vederlo come problema negativo, che può portare a vulnerabilità
 - Una mancanza strutturale di progettazione e /o di programmazione che può rendere un obiettivo suscettibile di attacco
- **Vulnerability:** es: bug che possono essere utilizzate per minacciare una delle 3 info della CIA
 - Una debolezza inserita intenzionalmente o accidentalmente del sistema che può essere sfruttata in maniera maliziosa
- **Attack:** Processo che sfrutta l'exploit per usare la vulnerabilità (Attack → Processo / Exploit → Costru)
 - Un'azione intrapresa contro un obiettivo con l'intenzione di arrecare danno o compiere una azione non permessa dalla policy di sicurezza
- **Exploit:** Soluzione tecnica che sfrutta vulnerabilità: codice
 - Utilizzo di una vulnerabilità per effettuare un attacco che concretizzi una minaccia (threat)

Alcuni Concetti di Sicurezza Fondamentali

Se un'utente ha fatto sì, se un altro no,

- Autenticazione e Identità:
 - *L'autenticazione è il processo utilizzato per garantire l'identità di chi accede ad un sistema*
 - I processi di autenticazione sono indispensabili per la realizzazione dei requisiti di **Confidenzialità** e **Integrità**: questi infatti assumono la capacità di distinguere tra diverse persone...
- Non ripudiabilità:
 - La possibilità di dimostrare in modo inequivocabile che una certa persona ha svolto una certa azione. È collegato soprattutto al concetto di integrità: se non posso dimostrare chi ha modificato una risorsa, non posso garantire che solo chi è autorizzato lo ha fatto

Concetti Fondamentali: Policy

- Un amministratore della sicurezza ha il compito di definire le “politiche di sicurezza” da adottare per rispettare simili requisiti
- Una “Politica di Sicurezza” è un insieme di regole che definiscono "gli stati ammissibili" di un sistema (*chi è autorizzato e chi no! Cosa è letto e cosa non*)
- L'obiettivo di una “Politica di sicurezza” è identificare le risorse critiche e definire le regole ed i criteri di accesso ad esse.
- Un “Meccanismo di sicurezza” è composto da un insieme di strumenti, metodi e procedure che mettono in pratica una politica di sicurezza

Problemi di Sicurezza

Esempio:

La Firma di un Contratto

Requisito: Garantire che il documento, una volta firmato non possa essere più cambiato nel suo contenuto ed è dimostrabile l'identità di chi lo ha firmato e è vincolato

Concetto di Sicurezza: Non Ripudiabilità (chi ha apposto la firma sa chi dichiara di esserlo)

Requisiti CIA: Integrità

Esempio di Meccanismo di Sicurezza: Firma Digitale

↳ Garantisce entrambe.
Ma non garantisce Confidenzialità

Problemi di Sicurezza

La Firma di un Contratto

Re **Requisito:** Una Pagina Web per vedere i risultati di una analisi medica
po
di **Requisito:** la ‘Pagina Web’ dovrà garantire che la persona che
Co accede alla pagina sia chi dichiara di essere
Re **Concetto di Sicurezza:** Autenticazione
Es **Requisiti CIA:** Confidenzialità
Esempio di Meccanismo di Sicurezza: Login con Username e
Password

Problemi di Sicurezza

La Firma di un Contratto

Requisito: Una Pagina Web per vedere i risultati di una analisi medica

po

di Re

Co acc

Re Co

Ese Re

Ese

Pas

Una Pagina Web per prenotare un servizio al comune

Requisito: la ‘Pagina Web’ dovrà essere sempre a

disposizione, la sua mancanza si può configurare come una

interruzione di pubblico servizio

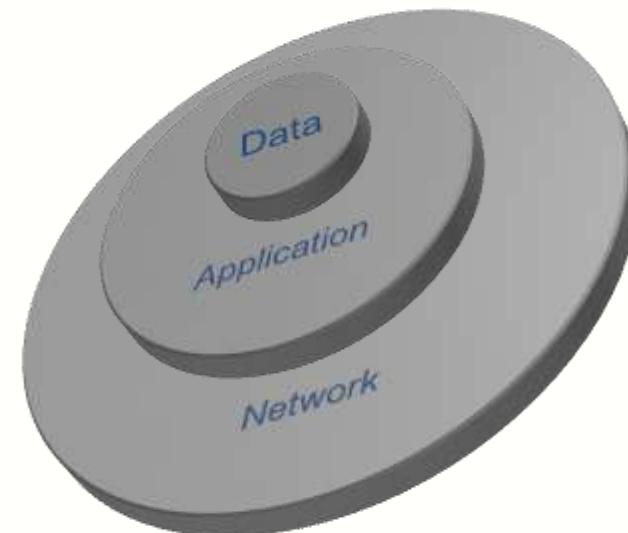
Requisiti CIA: **Disponibilità**

Esempio di Meccanismo di Sicurezza: Meccanismi di controllo
del traffico per garantire che il sistema sia sempre attivo

Sicurezza: Cosa Proteggere

Quali sono i nostri asset

- Le Risorse di un sistema *da proteggere rispetto a CIA*
 - i dati
 - Le applicazioni
 - la rete



Cosa specificare in una Security Policy (NIST Families)



I Domini di Sicurezza per NIST: Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	MA Maintenance	PM	Program Management

Tutte le famiglie del set di controlli

Le Funzioni di Sicurezza (*Types of operations*)

avere buona conoscenza di quali sono i componenti del sistema

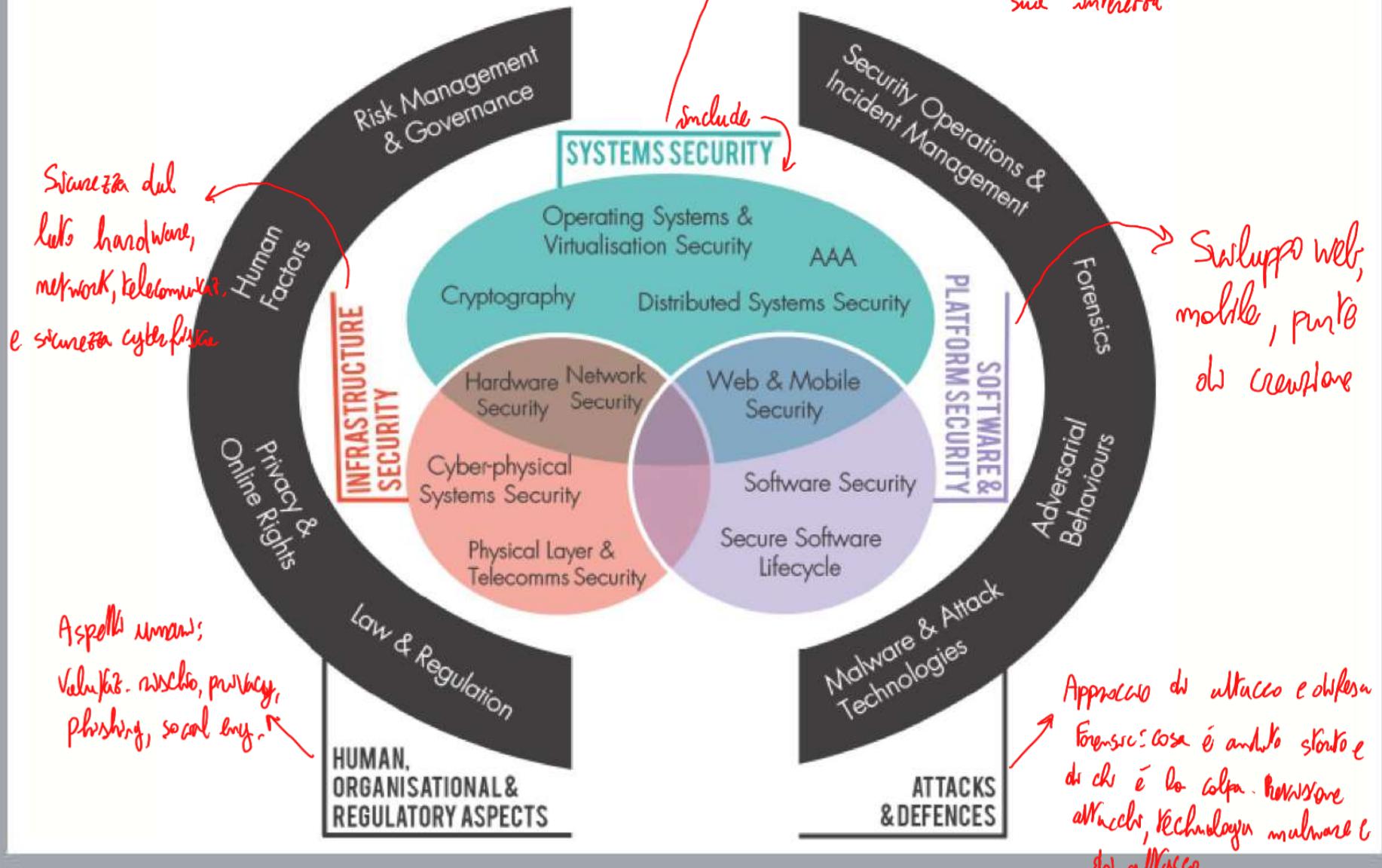
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services. <i>Proteggere tutti gli asset</i> <i>Identificare tutti i possibili attacchi, vulnerabilità ecc.</i>
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident <i>Rispondere ad attacchi</i>
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. <i>Recuperare ciò che succede dopo</i>

The Cyber Security Body of Knowledge (CyBOK)

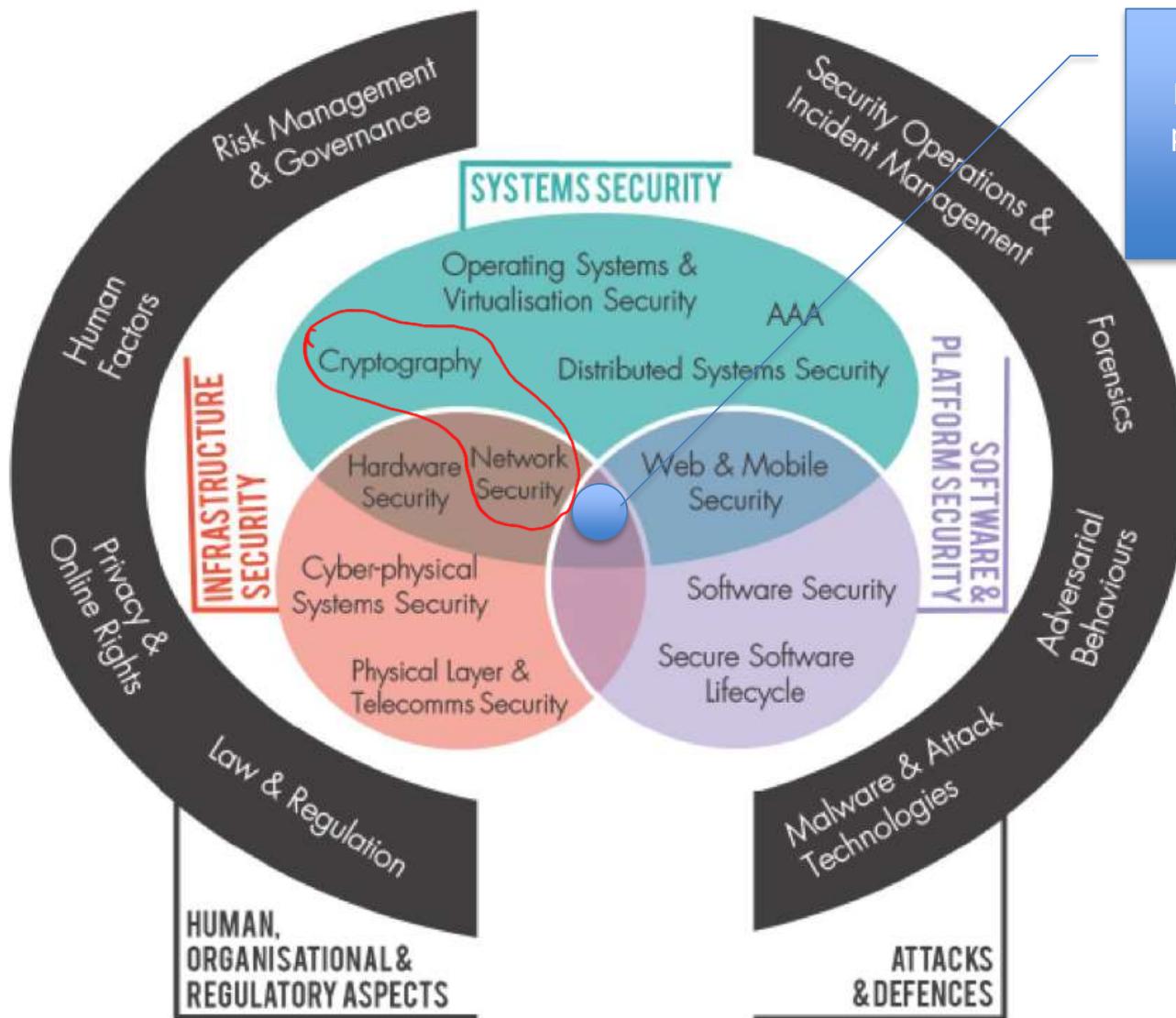
Body of Knowledge

- The CyBOK is divided into 19 top-level Knowledge Areas (KAs), grouped into 5 broad categories:
 - *Human, Organisational, and Regulatory Aspects*
 - *Attacks and Defences*
 - *Systems Security*
 - *Software and Platform Security*
 - *Infrastructure Security*

CyBOK categories



CyBOK categories



Organizzazione del Corso

Teoria

- Concetti Fondamentali
 - Terminologia
 - Cenni di Crittografia
- Network Security
 - Sniffing,
 - Traffic Monitoring
 - Firewall e DMZ
- Web Security
 - HTTP, Servlet
 - OWASP Top Threats

Esercizi Pratici

- Strumenti di rete
- Emulazione di rete
- Utilizzo di strumenti di traffic monitoring
- Emulazione di Attacchi DoS
- Sviluppo di applicazioni web
- Analisi di attacchi Web

Modalità di Esame

- Esame si svolge sull'analisi di un attacco scelto dallo studente e deve includere
 - Analisi teorica dell'attacco
 - Simulazione dell'attacco in ambiente controllato
 - Riscontro del comportamento teorico dell'attacco
- Modalità di esercizio:
 - Presentazione powerpoint
 - Demo dell'attacco
- Durante la presentazione verrano richiesti i temi teorici presentati durante il corso per capirne l'applicabilità nel contesto proposto

Esercitazione Unix e rete

- Esercitazione in aula *→ Online platform di CTF*
- <https://overthewire.org/wargames/bandit/>
- Utilizzo di SSH
 - Windows: putty
 - Unix/Mac: linea di comando e comando ssh
- Accedere a :
 - **bandit.labs.overthewire.org**, on port 2220
 - Username: **bandit0** pwd: **bandit0**
- Imparare a usare i comandi Unix base per operare su un sistema di rete...
