Programma Corso annuale di Sicurezza Informatica 2020-21
Laurea Ingegneria Medica Magistrale, secondo biennio (60 h).

Motivazione Sicurezza Informatica in Ingegneria Medica

- Gli aspetti dell'ingegneria in medicina legati alla sicurezza informatica.
- Le principali normative italiane di riferimento. Il Regolamento Europeo GDPR.
- Fonti: **pdf 1** e riferimenti in essa citati, testo del regolamento.

Elementi base e terminologia della Sicurezza **[SB]**

- Introduzione alla Terminologia Sicurezza: vulnerabilità, minacce, attacchi, bersagli, vittime, contromisure, robustezza, Ridondanza e resilienza.
- Difesa e Protezione dei sistemi.
- Sicurezza informatica, la triade del NIST: disponibilità, integrità, confidenzialità.
- Descrizione dei principali attacchi informatici: eavedropping, tampering,
- Metodi di Autenticazione Fonte **SB**
- Classificazione delle Informazioni. Struttura a livelli autorizzativi. Nulla Osta sicurezza.

Confidenzialità Generalità

- Criptografia Antica: Scitale; Cifrature di Cesare, atbash , Cifrature Polialfabetica : Vigenere e Bellaso; Steganografia**.**
- Esercizi con Octave Cifratura, decifratura e decrittazione di Cesare con Varianti; Scitale; Cifrature a Blocchi **.**
- Cifratura di Vigenere e Bellaso .
- Algoritmi e complessità: macchine di Touring, scaling delle risorse allocate.
- Cifratura elementari: trasposizionali (permutazioni a blocchi) e sostituzionali
- Cifratura di Augusto.

Elementi di Teoria dei numeri **[PC]**

- I numeri naturali: Assiomi di Peano.
- Le operazioni e le loro proprietà
- Esempi di induzione: tartaglia, serie geometrica e aritmetica.
- La divisione
- Gruppi, Anelli.
- Costruzione Assiomatica di Z_n.
- Equivalenze. Classi di equivalenza. Gruppi quozienti
- Z_n come Gruppi quozienti di classi di equivalenza modulare in Z
- Cardinalità Insiemi
- Anelli primali: Th di Fermat ed Eulero
- Sistemi diofantei
- Th cinese dei resti
- Numeri primi
- Algoritmo di Euclide
- Anelli primi Z_p*
- Sottogruppi ciclici - Generatori
- Ciclicità dei gruppi Z_p*
- Test di primalità e pseudo-primalità

- Potenze gruppi ciclici e generatori
- Teorema di Gauss
- Teorema di Carlmichael
- Anelli di polinomi
- Divisione tra polinomi

Cenni di teoria della probabilità **[Gn]**

- Spazi di probabilità – variabili stocastiche .
- Entropia – Leggi debole dei grandi numeri –
- Analisi dei linguaggi: frequenza dei caratteri.
- La robustezza della cifratura di Augusto
- Generatori di numeri random e pseudo-random.

Cenni di teoria dell'informazione **[FF]**

- Diseguaglianza di Jansen
- Mutua informazione
- Entropia di shannon
- Cifrari ideali - Cifrario trasposizionale a blocchi
- Cifrari Perfetti: One time pad

Confidenzialità - Crittografia moderna **[SB]**

- Elementi di crittografia
- La crittografia a chiavi asimmetriche: chiave pubblica e chiave privata.
- Algoritmo di RSA
- Crittografia a chiave simmetrica
- Le cifrature a blocchi.
- DES, Triplo DES (AES solo citato)
- Scambio di Chiavi Segrete su canali non protetti: Protocollo di Deffie-Helman e di Shamir
- Autenticazione
- Certificati digitali , Authorità certificanti, Non ripudiazione
- PGP

Integrità **[SB]**

- Le funzioni di verifica: hash functions
- Il controllo ciclico di ridondanza CRC
- Esempio di CRC: Ethernet L1 cablato
- MD5 **[Pdf 18-19]**
- Generatori di numeri random e pseudo-random
- Collisioni: Paradosso del compleanno
- Secure Hash Functions: SHA-1, SHA-2 (SHA-512)

Buone Pratiche per la gestione dei sistemi

- Analisi del sistema (cosa proteggere e/o difendere). Non proteggere e difendere tutto allo stesso modo. **[**
- Allocazione esterna della sicurezza informatica: Contratti di Gestione, indici di prestazione, Qualità dei Servizi
- Accordi per i contratti di gestione (SLA).
- Ridondanza delle risorse.

- Backup e Raid come tutela della disponibilità dei dati.
- Valutazione del rischio, rapporto costi-benefici. .
- Quallità del servizio: indici di prestazione
- Cancellazione dei Dati
- Malware: classificazione e principali malware noti. La svolta di stuxnet e gli attacchi alle infrastrutture fisiche (SCADA). Ricatti informatici (Cryptolocker)
- Gli antivirus come strumenti minimali di difesa. L'importanza della tempestività del patching. **[**
- Informazioni Classificate
- SLA, Policy Sicurezza, Livelli sicurezza
- Nulla Osta Sicurezza

Elementi di Teoria delle Reti **[Ta]**

- Elementi di teoria dei Grafi
- Reti tecnologiche
- Reti di distribuzione
- Reti informatiche .
- Impilatura (Stacking) delle reti informatiche: Livello Fisico; Datalink; Internet e livelli superiori
- Livello fisico: topologia delle reti, raggiungibilità robustezza
- Instradamento
- MAC adress, MAC spooffing
- Protocollo Ethernet 802.3 MAC adress; switch.
- IP gateway, routers (ARP)
- Authonomous Systems
- Livello trasporto: TCP **[**
- Livello name. DNS e Name Servers. Autorità di dominio. Deep Web, Dark Web
- URL
- Autorità di certificazione, certificati digitali
- Nat, Tunneling, VPN**:**
- Proxy: open proxy, proxy inversi etc
- http.

Sicurezza in rete **[SB]**

- Collocazione dei dispositivi di sicurezza .
- Protocollo IKE di IPSEC: Scambio di chiavi .
- Secure Shell SSH SFTP Definizioni - Esempi pratici
- Firewall
- SHA-512, Block-chain, Bit coin
- TLS
- Https

Attacchi **[SB]**

- Deny of service DOS e DOS distribuiti . Contromisure (cenni).
- Attacchi alle credenziali e contromisure
- Man in The middle. Contromisure
- Replay. Contromisure (certificati e ticket a tempo)
- Metodi non informatici: ingegneria sociale, minacce fisiche, phishing etc

Dimostrazioni pratiche

- Funzionamento di un router wirelss, la configurazione del dispositivi di sicurezza per l'accesso wireless (filtri al livello data-link MAC address).
- Tabelle di autorizzazione agli accessi e protocollo di autenticazione wireless.
- Configurazione IP di uno switch come router gataway e come DHCP server.
- Connessioni ssh (sftp): il blocco da parte di un firewall ed il relativo aggiramento tramite l'autenticazione su una VPN. Verifica delle chiavi pubbliche.
- Uso di nmap e dell'interfaccia grafica zenmap per scandire le porte.

Parti significative non coperte

La sicurezza informatica è una disciplina molto vasta. Nella definizione del corso sono state operate scelte di priorità in base alle conoscenze pregresse degli studenti, i limiti di tempo e l'estensione dei contenuti. La parte più deficitaria riguarda diversi aspetti: la descrizione dei possibili attacchi ad una singola piattaforma (ad esempio il buffer overflow); la ricerca delle vulnerabilità sistematica delle reti; la difesa contro gli attacchi replay e i protocolli di autenticazione simmetrica in rete; gli attacchi ai protocolli (bgp) dei gateway; gli attacchi ai DNS server e le relative contromisure; i sistemi per la gestione dell'interoperabilità tra server come kerberos. Sono stati trascurati i test di penetrazione (pen test) e le analisi di vulnerabilità (ad esempio con openvas o con i software commerciali). Le tipologie di malware sono state solo descritte. La sicurezza dei database e la cancellazione dei dati sono due temi che necessitano approfondimento per la gestione dei dati nel rispetto delle leggi e della confidenzialità.
Un campo molto importante che merita attenzione da parte di chi intenda applicarsi alla sicurezza informatica è il rilevamento delle anomalie (anomaly detection) sia a livello di singola macchina che al livello di rete. L'analisi ex post (ed in tempo reale) dei log-file ed in generale la tracciabilità degli eventi e l'accountability dei sistemi sono stati tappena accennati. Le tecniche di protezione e difesa moderna si basano sull'analisi complessiva delle macchine e del traffico di rete.
Un altro campo molto ampio è legato alle metodologie comportamentali umane e la loro differenza con i bot. In particolare i test di Turing e gli attacchi per violarli. Queste ed altre tematiche sono in continua evoluzione e qualora si dovesse predisporre la sicurezza informatica di un sistema è opportuno verificare le recenti tecniche di attacco e le relative contromisure. Un'altra importante potenzialità da studiare è l'allocazione delle risorse sulle piattaforme cloud. Questa sarà probabilimente la scelta per la futura gestione centralizzata della sanità. I legami con le attività forensi e con la giurisdizione in genere rappresentano dei vincoli importanti in continua evoluzione. Nel corso si è cercato di dare le basi per affrontare consapevolmente la pianificazione di una infrastruttura informatica sicura.

Principali Fonti bibliografiche

- **SB**: W. Stalling & L. Brown *"Computer Security"* (2011) (2° Ed Pearson **ISBN-13:** 978-0132775069 **ISBN-10:** 0132775069)
- **Ta:** A Tanenbaum "*Computer Networks*" Pearson 2011 8-th Ed ISBN 978-81-7758-165-2
- GMN: S. Gai, P Montessori, P Nicoletti "*Dal Cablaggio all'internet Working*" Scuola Superiore G. reiss Romoli ISBN 88 85280 22 6 (**Reti** – Qualunque libro di reti va bene).
- **PC:** G.M. Piacentini Cattaneo "*Algebra"* Zanichelli 2012 (**Th. dei numeri** anche qui va bene un qualunque libro base)
- **Gn:** Gnedenko "*Teoria della Probabilità"* Ed. Riuniti 1979 (**Probabilità**) [esiste anche della MIR]

- **FF:** Francesco Fabris *"Teoria dell'informazione, codici, cifrari"* Bollati Boringhieri
- **Pdf**: i documenti pdf delle lezioni

Note

I pdf delle lezioni contengono molte degli argomenti trattati, ma non coprono tutto quanto discusso a lezione e le esercitazioni. L'esposizione temporale degli argomenti trattati a lezione differisce notevolmente dall'organizzazione tematica del programma.

Per gli esercizi al computer, si è scelto il linguaggio di programmazione "Octave" le cui implementazioni sono disponibili in formato open source su tutte le piattaforme. Inoltre la sua compatibilità con Mathlab ne consente un porting immediato in quel linguaggio. I calcoli in precisione arbitraria sono stati evitati vista la difficile realizzazione su Octave.

Molte dimostrazioni in teoria dei numeri sono state semplificate (mantenendone il rigore) specificatamente per il corso e non sono disponibili in letteratura. Tali dimostrazioni sono descritte nei loro elementi fondamentali nei pdf delle lezioni. Per chi volesse approfondire la tematica si consiglia il testo di M.F. Atiyah e I.G. Macdonald "Introduzione all'algebra commutativa" Feltrinelli.

I pdf delle lezioni, questo programma ed alcuni esercizi svolti con Octave sono stati caricati sulla piattaforma Teams e saranno disponibili al sito:
http://gordion.casaccia.enea.it/SicurezzaInformatica/

L'esame si svolgerà in presenza e prevede uno scritto da un'ora e l'orale subito dopo.