Programma Corso annuale di Sicurezza Informatica 2019-20
Laurea Ingegneria Medica Magistrale, secondo biennio. (90 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.

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.

Fonti: **Pdf 2** e riferimenti in essa citati.

- 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. **Pdf**

Confidenzialità Generalità

- Criptografia Antica: Scitale; Cifrature di Cesare, atbash , Cifrature Polialfabetica : Vigenere e Bellaso; Steganografia**. [Pdf 3-4]**
- Esercizi con Octave Cifratura, decifratura e decrittazione di Cesare con Varianti; Scitale; Cifrature a Blocchi **. [Pdf 4]**
- Cifratura di Vigenere e Bellaso . **[Pdf 5]**
- Algoritmi e complessità: macchine di Touring, scaling delle risorse allocate. . **[Pdf 6]**
- Cifratura elementari: trasposizionali (permutazioni a blocchi) e sostituzionali
- Cifratura di Augusto. **[Pdf 6]**

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

- I numeri naturali: Assiomi di Peano.
- Le operazioni e le loro proprietà . **[Pdf 7]**
- Induzione: fibonacci, tartaglia, serie geometrica e aritmetica.
- La divisione **[Pdf 8]**
- Gruppi, Anelli.
- Costruzione Assiomatica di Z_n. **[Pdf 9]**
- 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 **[Pdf 10]**
- Numeri primi
- Algoritmo di Euclide
- Anelli primi Z_p^* **[Pdf 11]**
- Sottogruppi ciclici - Generatori

- Ciclicità dei gruppi Z_p^* **[Pdf 12]**
- Test di primalità e pseudo-primalità **[Pdf 14]**
- Classi laterali: th di Lagrange **[Pdf 15]**
- Potenze gruppi ciclici e generatori **[Pdf 16]**
- Teorema di Gauss **[Pdf 16]**
- Teorema di Carlmichael **[Pdf 17]**
- Anelli di polinomi [**Pdf 22]**
- Divisione tra polinomi **[Pdf 22]**

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

- Spazi di probabilità – variabili stocastiche . **[Pdf 21]**
- catene stocastiche
- Entropia – Leggi debole e forte dei grandi numeri – **[Pdf 22]**
- Analisi dei linguaggi: frequenza dei caratteri. **[Pdf 22-23]**
- La robustezza della cifratura di Augusto **[Pdf 23]**
- Generatori di numeri random e pseudo-random (fonti Pdf,) . **[Pdf 22]**
- Generatori moderni di numeri random: Mersenne Twiste**r [Pdf 25]**

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

- Diseguaglianza di Jansen **[Pdf 23]**
- Mutua informazione **[Pdf 23]**
- Entropia di shannon **[Pdf 23]**
- Catene stocastiche e loro entropia **[Pdf 24]**
- Cifrari ideali - Cifrario trasposizionale a blocchi **[Pdf 24]**
- Cifrari Perfetti: One time pad **[Pdf 25]**

Confidenzialità - Crittografia moderna **[SB]**

- Elementi di crittografia
- La crittografia a chiavi asimmetriche: chiave pubblica e chiave privata.
- Algoritmo di RSA **[Pdf 13]**
- Crittografia a chiave simmetrica **[Pdf 12]**
- Le cifrature a blocchi.
- DES, Triplo DES (AES solo citato) **[Pdf 26]**
- Scambio di Chiavi Segrete su canali non protetti: Protocollo di Deffie-Helman e di Shamir **[Pdf 33-34]**
- Autenticazione **[Pdf 30]**
- Certificati digitali , Authorità certificanti, Non ripudiazione
- PGP **[Pdf 33-34]**

Integrità **[SB]**

- Le funzioni di verifica: hash functions **[Pdf 18]**
- Il controllo ciclico di ridondanza CRC **[Pdf 19]**
- Esempio di CRC: Ethernet L1 cablato **[GMN-Pdf 19]**
- MD5 **[Pdf 18-19]**
- Generatori di numeri random e pseudo-random
- Paradosso del compleanno **[Pdf]**
- Secure Hash Functions: SHA-1, SHA-2 (SHA-512) **[Pdf 30-39]**

Buone Pratiche per la gestione dei sistemi

- Analisi del sistema (cosa proteggere e/o difendere). Non proteggere e difendere tutto allo stesso modo. **[Pdf 35]**
- Allocazione esterna della sicurezza informatica: Contratti di Gestione, indici di prestazione, Qualità dei Servizi
- Accordi per i contratti di gestine (SLA). **[Pdf 35]**
- Ridondanza delle risorse. **[Pdf 21]**
- Backup e Raid come tutela della disponibilità dei dati. . **[Pdf 21]**
- Valutazione del rischio, rapporto costi-benefici. . **[Pdf 27]**
- Quallità del servizio: indici di prestazione **[Pdf 32]**
- Cancellazione dei Dati
- Malware: classificazione e principali malware noti. La svolta di stuxnet e gli attacchi alle infrastrutture fisiche (SCADA). Ricatti informatici (Cryptolocker)**[Pdf 31]**
- Gli antivirus come strumenti minimali di difesa. L'importanza della tempestività del patching. **[Pdf 31]**
- Informazioni Classificate **[Pdf 35]**
- SLA, Policy Sicurezza, Livelli sicurezza
- Nulla Osta Sicurezza **[Pdf 35]**

Elementi di Teoria delle Reti [Ta]

- Elementi di teoria dei Grafi **[Pdf 27]**
- Reti tecnologiche
- Reti di distribuzione
- Reti informatiche . **[Pdf 27]**
- Impilatura (Stacking) delle reti informatiche: Livello Fisico; Datalink; Internet e livelli superiori
- Livello fisico: topologia delle reti, raggiungibilità robustezza. **[Pdf 28]**
- Instradamento
- MAC adress, MAC spooffing
- Protocollo Ethernet 802.3 MAC adress; switch. **[Pdf 28]**
- IP gateway, routers (ARP).**[Pdf 29]**.
- Authonomous Systems **[Pdf 29]**.
- Livello trasporto: TCP **[Pdf 32]**
- Livello name. DNS e Name Servers. Autorità di dominio. Deep Web, Dark Web **[Pdf 32]**
- URL **[Pdf 35]**
- Autorità di certificazione, certificati digitali **[Pdf 33]**
- Nat, Tunneling, VPN**: [Pdf 34]**
- Proxy: open proxy, proxy inversi etc **[Pdf 35]**
- https. **[Pdf 35]**

Sicurezza in rete [SB]

- Collocazione dei dispositivi di sicurezza . **[Pdf 33]**
- Protocollo IKE di IPSEC: Scambio di chiavi . **[Pdf 33]**
- Secure Shell SSH SFTP Definizioni - Esempi pratici **[Pdf 34]**
- Firewall **[Pdf 34]**
- Paradosso del compleanno **[Pdf 34]**
- Collisioni, Secure hash function **[Pdf 34]**
- SHA-512, Block-chain, Bit coin **[Pdf 35]**
- TLS **[Pdf 35]**

- Https **[Pdf 36]**
- Gestione centralizzata dell'autenticazione: Il protocollo kerberos **[Pdf 35]**
- Protocolli di certificazione: X.509 **[Pdf 36-38]**

Attacchi **[SB]**

- Deny of service DOS e DOS distribuiti . Contromisure (cenni) **[Pdf 28]**.
- Attacchi alle credenziali e contromisure **[Pdf 30]**
- Man in The middle. Contromisure **[Pdf 33-35]**
- Replay. Contromisure (certificati e ticket a tempo)
- Metodi non informatici: ingegneria sociale, minacce fisiche, phishing etc **[Pdf 33-35]**
- Sniffing : reti ad Hub e reti istradate. Contromisure
- Spooffing e contromisure **[Pdf 36-37]**

Dimostrazioni pratiche

- Funzionamento di un hub e di uno switch, la configurazione dei loro dispositivi di sicurezza per le connesioni 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.
- Shell locali **[Pdf 34]**
- Connessioni ssh (sftp): il blocco da parte di un firewall ed il relativo aggiramento tramite l'autenticazione su una VPN. Verifica delle chiavi pubbliche.

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; gli attacchi ai protocolli (bgp) dei gateway; gli attacchi ai DNS server e le relative contromisure. Sono stati trascurati gli strumenti automatizzati per la scansione delle vulnerabilità sulla rete e gli strumenti per 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 confidenzialit\`a.

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 trascurati. 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 (numerati cronologicamente)

Note

I pdf delle lezioni contengono molte degli argomenti trattati, ma non coprono tutto quanto discusso a lezione e le spiegazioni alla lavagna. In particolare in teoria dei numeri, alcune parti non sono coperte dai pdf. 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.

Alcune 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 disponibili al sito: http://gordion.casaccia.enea.it/SicurezzaInformatica/