Sicurezza dell'Informazione M

Alma Mater Studiorum - Università di Bologna
CdS Laurea Magistrale in Ingegneria Informatica
I Ciclo - A.A. 2018/2019

Corso di Sicurezza dell'Informazione M

Docente: Rebecca Montanari
rebecca.montanari@unibo.it

http://lia.disi.unibo.it/Courses/SicurezzaM1819/

Sicurezza dell'Informazione M in una slide

Propedeuticità: ***nessuna***
ma i contenuti dei corsi della triennale quali Reti di Calcolatori, Amministrazione di Sistemi possono essere ***sicuramente utili***

Modalità d'esame: prova scritta e orale (con sviluppo di un'applicazione sicura– opzionale; anche possibilità di Attività Progettuale da 4 cfu)

- **Orari di ricevimento del docente:**
  c/o studi DISI – edificio aule nuove (di fianco aula 5.7)
  - **Su appuntamento via email rebecca.montanari@unibo.it**

Materiale Didattico

- **Copia** delle diapositive mostrate a lezione ed esercitazioni guidate di laboratorio (scaricabili mano a mano dalle pagine Web del corso; le slide saranno caricate di settimana in settimana)

ATTENZIONE: le slide NON SONO UN LIBRO DOVE TUTTO è scritto.
A lezione vengono proposti esercizi ed attività non necessariamente presenti sulle slide

- **Testi suggeriti per approfondimento:**
  - B. Schneier: “Applied Cryptography” John Wiley
  - A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone: “Handbook of Applied Cryptography” CRC Press 1997 (www.cacr.math.uwaterloo.ca/hac)
  - H.C.A. van Tilborg: “Fundamentals of Cryptology” Kluver Academic Publishers N. Ferguson, B. Schneier: “Practical Cryptography” Wiley Publishing
  - William Stallings: “Crittografia e sicurezza delle reti. Standard, Tecniche, Applicazioni” McGraw-Hill
  - Capitoli di libro "Sicurezza dell'Informazione" (R. Laschi, R. Montanari, A. Riccioni) (vedi sito Web del corso)

Orario delle lezioni

Normalmente:

- **lunedì ore 09:00-11:30**, aula 5.6
- **mercoledì ore 09:00-11:30**, aula 5.7

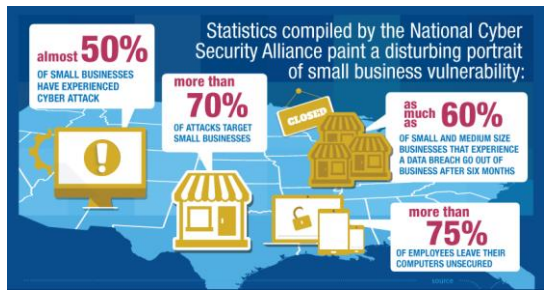
Qualche lezione/esercitazione sarà svolta direttamente in Lab2, previo avviso a lezione in abbondante anticipo

Eventuali variazioni verranno comunicate prontamente tramite sito Web del corso

Cyber Attack Maps

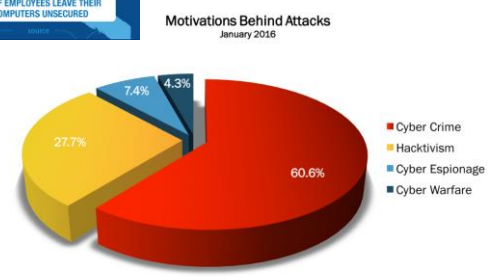
- **http://map.norsecorp.com/**
- **https://www.fireeye.com/cyber-map/threat-map.html**
- **https://cybermap.kaspersky.com/**

Un po' di statistiche ….

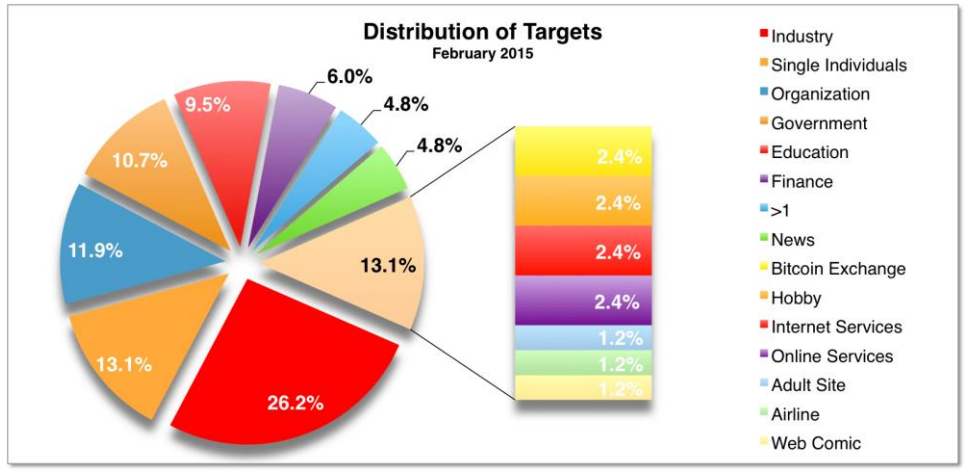


Costi globali del cyber-crime previsti per il 2019:

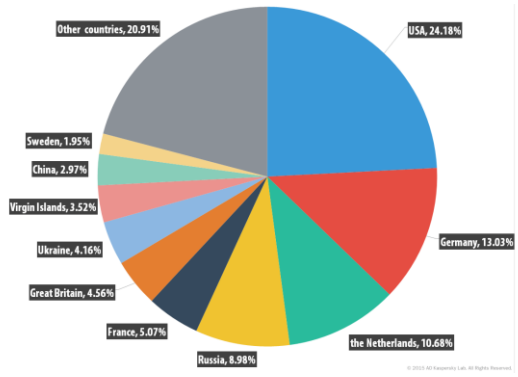
2.000 miliardi di dollari (il triplo del 2015)



Un po' di statistiche ….



Un po' di statistiche ….



Paesi di provenienza di spam

Perché è esploso il problema della sicurezza informatica a livello globale?

VECCHI PARADIGMI

- informazioni ed elaborazione centralizzate
- accesso tramite terminali
- comunicazione “unicast” tramite linee dedicate

NUOVI PARADIGMI

- informazioni ed elaborazione distribuite
- accesso tramite postazioni distribuite intelligenti
- comunicazioni “broadcast” e/o linee condivise
- comunicazioni wireless
- nuovi paradigmi applicativi (web, P2P, SMS, …)
- Internet of Things

Primo Attacco Informatico: Morris Worm

2 novembre 1988

Sun Microsystems Sun3, Vax computers with 4 BSD Unix

Effetti su circa 10% degli host di Internet:

File inusuali su /usr/tmp, messaggi strani sui log file ad es. di sendmail, carico della CPU, tentativi di access al file delle password

Dopo meno di 12 ore CSRG di Berkeley individua una serie di passi per bloccare la diffusione, due ore all’università di Purdue si trova la contromisura efficace per bloccare il worm

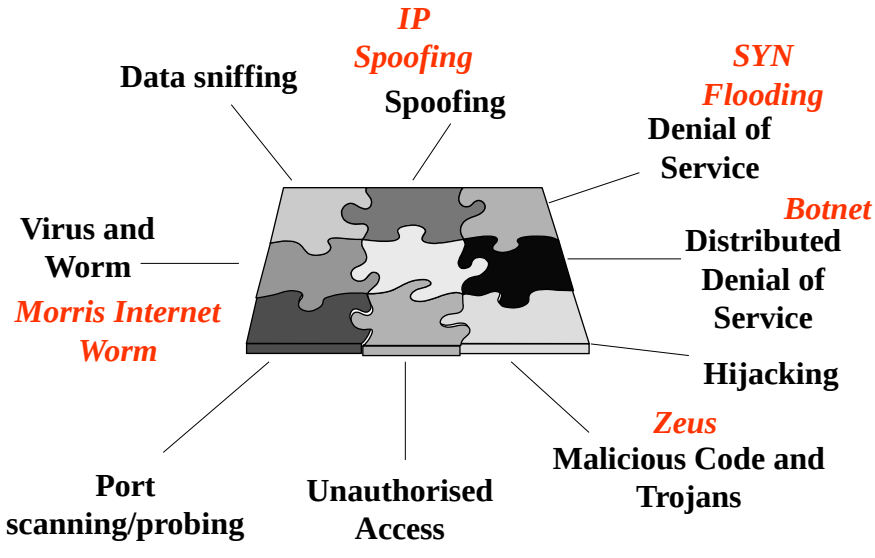
Rober T. Morris Jr, studente laureato alla Cornell University.

Condannato nel 1990 ad ammenda di 10000 dollari, reclusione per 3 anni con la condizionale e 400 ore di servizio sociale

Problemi di base

- **le reti sono insicure:**
  - le comunicazioni avvengono in chiaro
  - le reti locali funzionano in broadcast
  - le connessioni geografiche non avvengono tramite linee punto-punto ma:
    - attraverso linee condivise
    - tramite router di terzi
- **il software contiene molti bachi!**

Esempi di Attacchi Informatici



Alcune Tipologie di Attacchi di Rete

- **IP spoofing / shadow server:** qualcuno si sostituisce ad un host
- **packet sniffing:** si leggono password di accesso e/o dati riservati
- **connection hijacking / data spoofing:** si inseriscono/ modificano dati durante il loro transito in rete
- **denial-of-service (DoS) e distributed DoS (DDoS):** si impedisce il funzionamento di un servizio (es.SYN o PING flooding)

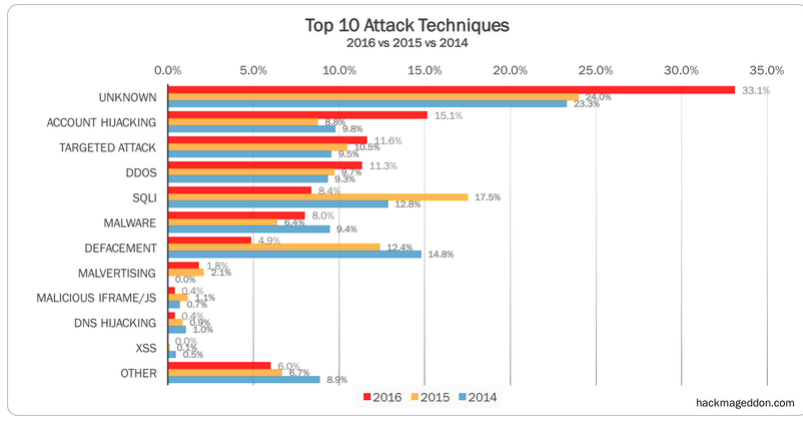
Alcune Tipici Problemi Applicativi

- **buffer overflow:** permette l'esecuzione di codice arbitrario iniettato tramite un input appropriatamente manipolato
- **memorizzare nei cookie informazioni sensibili** leggibili da terzi (in transito o localmente sul client)
- **memorizzare le password in chiaro in un DB** leggibili da terzi (es. l'operatore del backup)
- **"inventare" un sistema di protezione:** rischio di protezione inadeguata (se sbagliano i grandi figuriamoci cosa combinano i non esperti ...)

Virus e Worm

- **Virus** provoca danni e si replica propagato dagli umani (involontariamente)
- **worm** provoca danni perché si autoreplica (satura risorse) propagazione automatica
- **trojan (horse)** = vettore di malware
- **backdoor** = punto di accesso non autorizzato
- **rootkit** = strumenti per accesso privilegiato, nascosti (modifica di un programma, libreria,driver, modulo kernel, hypervisor) ed invisibili

Top Ten Tecniche di Attacco



Top Ten Tecniche di Attacco a livello Applicativo

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Una possibile definizione di sicurezza informatica

E' l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'azienda.

La sicurezza informatica ha lo scopo di proteggere le risorse da accessi indesiderati, garantire la riservatezza delle informazioni, assicurare il funzionamento e la disponibilità dei servizi a fronte di eventi imprevedibili

La sicurezza non è un prodotto ma un processo

Security is a process, not a product

(Bruce Schneier, Crypto-Gram, May 2005)

Computer Security: Will We Ever Learn?

If we've learned anything from the past couple of years, it's that **computer security flaws are inevitable**. Systems break, vulnerabilities are reported in the press, and still many people put their faith in the next product, or the next upgrade, or the next patch. "This time it's secure," they say. So far, it hasn't been.

Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. **The trick is to reduce your risk of exposure regardless of the products or patches**.

Minaccia, Vulnerabilità, Attacco e Contromisura

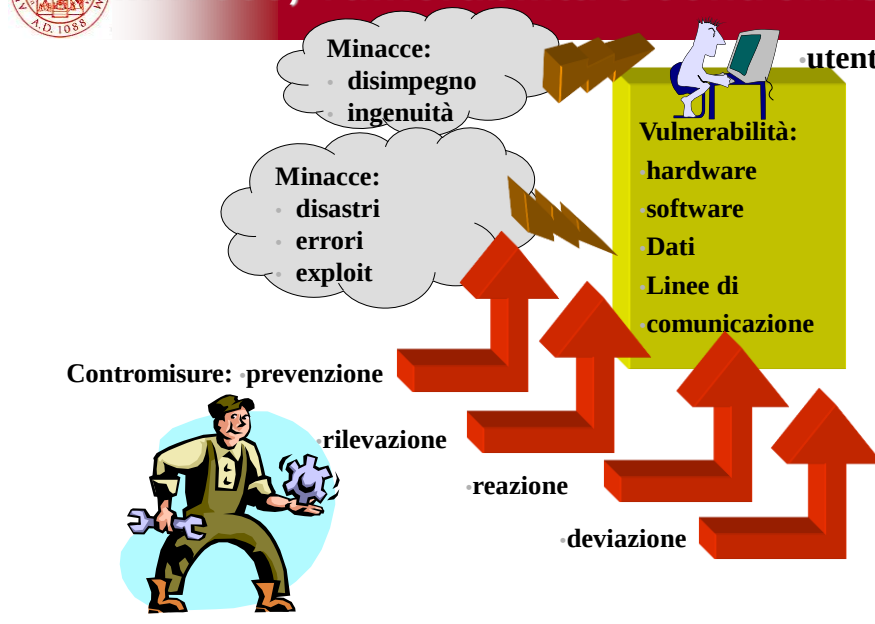
Minaccia: un atto ostile intenzionale o meno che ha un qualsiasi effetto negativo sulle risorse o sugli utenti del sistema

Vulnerabilità: punto debole del sistema a fronte di una certa minaccia

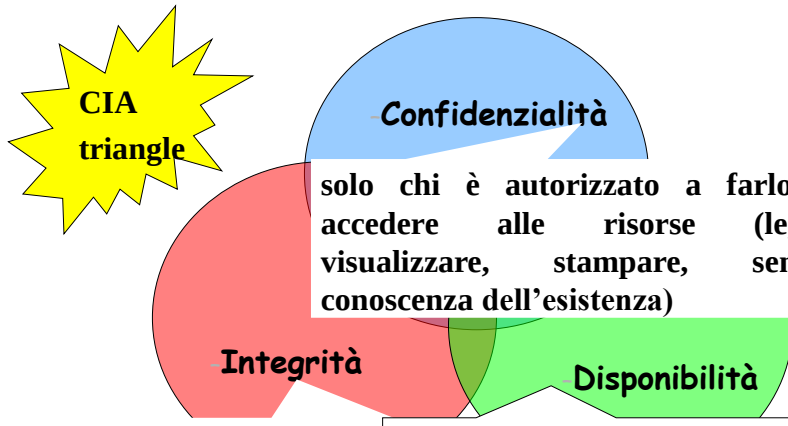
Attacco: qualsiasi azione che usa una vulnerabilità per concretizzare una minaccia

Contromisura: azione, dispositivo, procedura o tecnica che consente di rimuovere o di ridurre una vulnerabilità

Minacce, vulnerabilità e contromisure



Le tre proprietà di base per la sicurezza dell'informazione



solo chi è autorizzato a farlo può accedere alle risorse (leggere, visualizzare, stampare, semplice conoscenza dell'esistenza)

solo chi è autorizzato a farlo può modificare, eliminare, creare risorse

solo chi è autorizzato a farlo può accedere alle risorse senza interferenze ed ostacoli

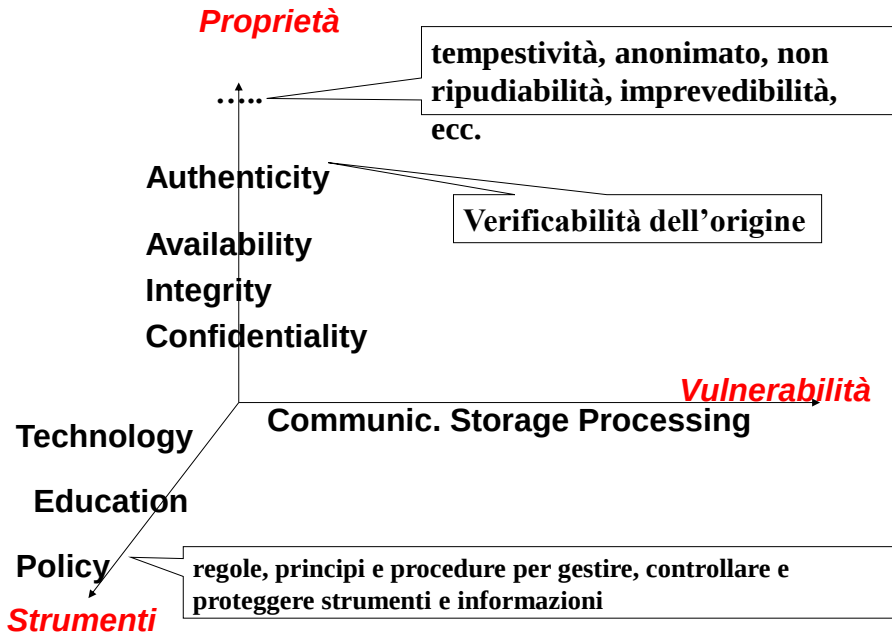
Altri Requisiti di Sicurezza

- **AUTENTICAZIONE della CONTROPARTE**
  (utente nell'accesso ad un sistema e peer durante la comunicazione attraverso reti pubbliche)
  "E' possibile garantire che chi accede a un sistema è chi dice di essere? E' possibile garantire a ciascun comunicante che l'altro è proprio quello che dice di essere?"

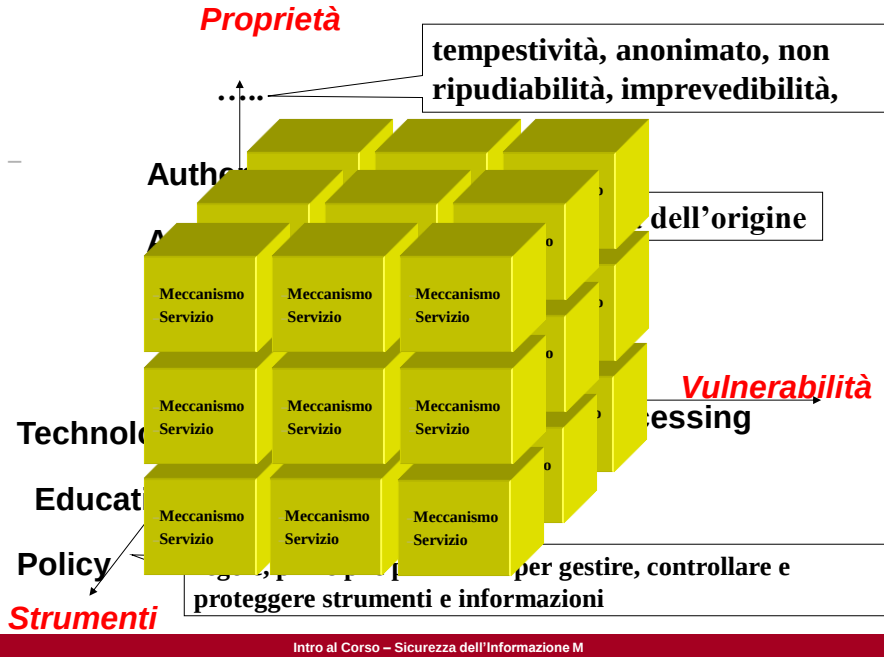
- **NON RIPUDIO**
  "E' possibile garantire che l'autore di un messaggio non potrà disconoscerne la paternità e a chi trasmette un messaggio che non gli venga attribuita la paternità di un messaggio che in realtà non ha mai spedito?"

- **CONTROLLO degli ACCESSI**
- **TRACCIABILITA'**

Lo spazio della sicurezza (NSTISSC)



Lo spazio della sicurezza (NSTISSC)



Cosa Occorre Conoscere?

Fondamentale per il responsabile della sicurezza di un'organizzazione è la conoscenza di quali sono:

- attacchi alla sicurezza
- modelli e tecnologie di sicurezza

Occorrono metodi sistematici per la definizione dei requisiti di sicurezza e per l'analisi e la scelta degli approcci da adottare per il soddisfacimento di tali requisiti

Proteggere le Informazioni: Quali Domande?

Quanto valgono le informazioni?

Come si può quantificare il rischio di subire un attacco?

Come si può valutare il danno subito da perdite di informazioni rispetto al costo da sostenere per evitare tali perdite?

metodologia di progettazione, realizzazione e manutenzione della sicurezza che a partire dalle politiche e dai vincoli di un'organizzazione metta in atto un piano per la sicurezza

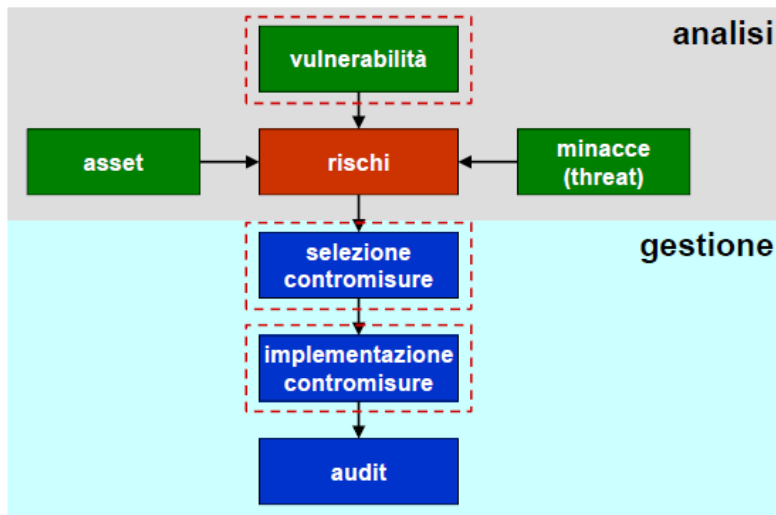
Fasi Metodologiche (1.)

- **analisi del contesto** => struttura dell'organizzazione e finalità (distribuzione geografica delle sedi, unità organizzative, ruoli, competenze, responsabilità)
- **analisi del sistema informatico** => analisi risorse fisiche, logiche, dipendenze tra risorse
- **classificazione degli utenti** => assegnazione di una classe di appartenenza
- **definizione dei diritti di accesso** => a quali servizi e informazioni può accedere una tipologia di utenti

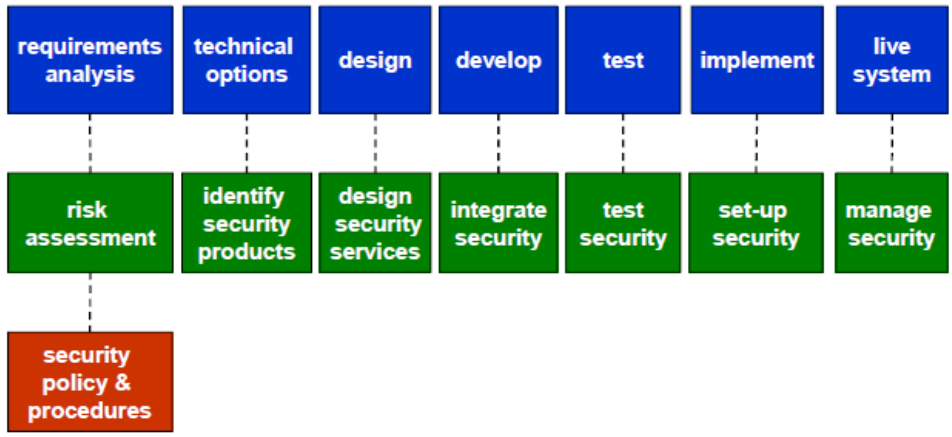
Fasi Metodologiche (2.)

- **catalogazione degli eventi indesiderati** (attacchi indesiderati, eventi)
- **valutazione del rischio** =>associare un rischio a ciascuno degli eventi indesiderati individuati. Rischio esprime la probabilità che un evento accada e il danno che arreca al sistema se accade
- **individuazione delle contromisure** =>analisi di standard e modelli, valutazione del rapporto costo/efficacia, contromisure di carattere sia organizzativo sia tecnico
- **integrazione delle contromisure** => individuare sottoinsieme di costo minimo che soddisfi vincoli di completezza, omogeneità, ridondanza controllata, effettiva attuabilità

Analisi e Gestione della Sicurezza



La sicurezza nel ciclo di vita di un sistema



Programma

Servizi e Meccanismi

- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Valutazione e Certificazione

Standard internazionali per la valutazione e la certificazione della sicurezza:
Orange book del NCSC,
ISO 17799,
ITSEC,
Common Criteria

Direttive europee
....

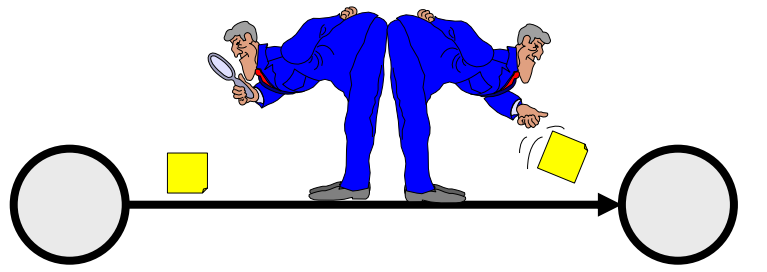
Standard nazionali
cnipa
legge 196/2003 sulla privacy
...

Attacco intenzionale:
"ogni azione mirante a compromettere una proprietà critica della informazione"

Il modello del canale insicuro

Ambiente sicuro	Comunicazione insicura	Ambiente sicuro

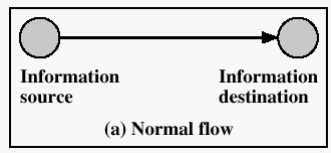
intruso



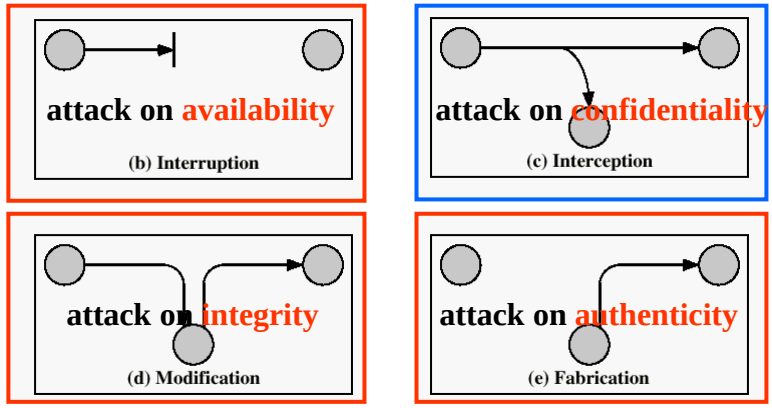
sorgente **canale** **destinazione**

Attacchi alla Sicurezza

Attacco passivo



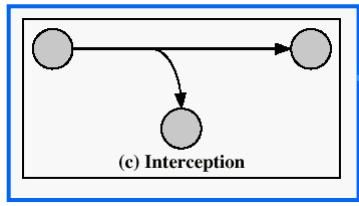
Attacco attivo



Attacchi passivi: contromisure

- Prevenzione: azioni atte a minimizzare la probabilità di successo dell'attacco
- Rilevazione: azioni atte ad individuare che l'attacco è in corso
- Reazione: azioni atte ad annullare, o almeno a delimitare, gli effetti dell'attacco

Attacco passivo Proprietà a rischio: riservatezza

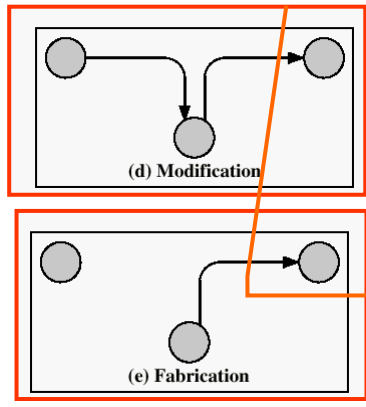


1. controllo d'accesso al canale
2. rappresentazione incomprensibile

Attacchi attivi: contromisure

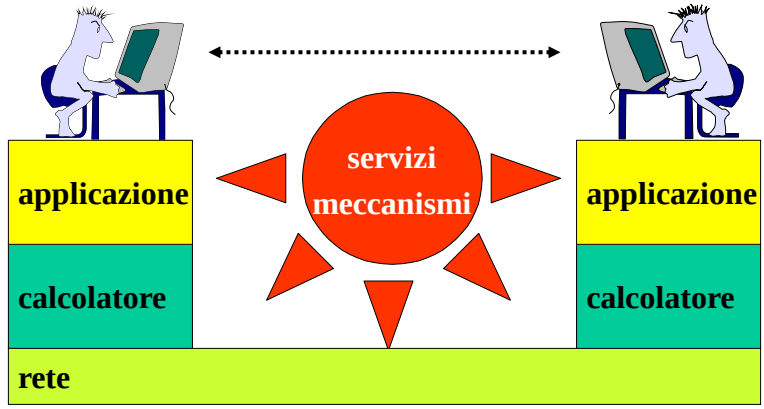
- Prevenzione: azioni atte a minimizzare la probabilità di successo dell'attacco
- Rilevazione: azioni atte ad individuare che l'attacco è in corso
- Reazione: azioni atte ad annullare, o almeno a delimitare, gli effetti dell'attacco

Attacco attivo Proprietà a rischio: integrità, autenticità



1. controllo d'accesso al canale
2. attestato d'integrità e d'origine

Collocazione dei meccanismi e dei servizi per la sicurezza



Il calcolatore sicuro

Calcolatori sicuri

1: Rilevazione tempestiva degli errori HW e SW

2: HW&SW progettato per la sicurezza

Progetto integrato HW&SW (A,B di O.B.) (E3,HIGH di I.)

Trusted Computer Platform (Fritz+Nexus)

Funzioni e regole di sicurezza

Estensioni del S.O. (Unix, SeLinux)

Coprocessore per la sicurezza

R1:"l'accesso ad ogni risorsa HW e SW di un sistema informatico e la sua modalità d'uso devono essere regolamentati; le autorizzazioni concesse ad un utente non devono poter essere usate da altri (mandatory vs. discretional access control)".

La rete sicura

Rete sicura

- Autenticazione dei corrispondenti
- Autenticazione dei messaggi
- Riservatezza delle comunicazioni