



Sicurezza dell'Informazione M

Alma Mater Studiorum - Università di Bologna
CdS Laurea Magistrale in Ingegneria Informatica
I Ciclo - A.A. 2019/2020

Corso di Sicurezza dell'Informazione M

Docente: Rebecca Montanari
rebecca.montanari@unibo.it

<http://lia.disi.unibo.it/Courses/SicurezzaM1920/>



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 prova di laboratorio (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" Kluwer Academic Publishers N. Ferguson, B. Schneier: "Practical Cryptography" Wiley Publishing
- William Stallings: "Crittografia e sicurezza delle reti. Standard, Tecniche, Applicazioni" McGraw-Hill **CONSIGLIATO**
- Capitoli di libro "Sicurezza dell'Informazione" (R. Laschi, R. Montanari, A. Riccioni) (disponibili sul sito Web del corso)



Orario delle lezioni

Normalmente:

- ❑ **lunedì ore 11:00-13:30**, aula 5.6
- ❑ **venerdì ore 09:00-12**, 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

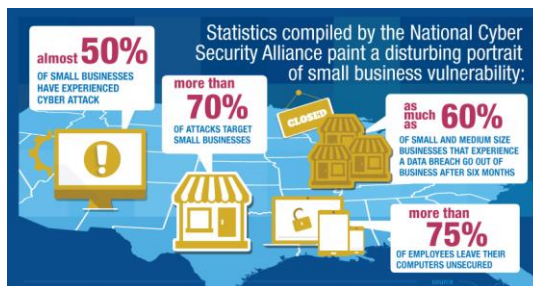
– <https://www.fireeye.com/cyber-map/threat-map.html>

– <https://cybermap.kaspersky.com/>

Intro al Corso – Sicurezza dell'Informazione M



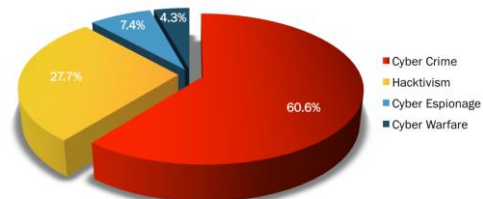
Un po' di statistiche



Studio Gartner:

- 114 miliardi di dollari nel 2018 (12,4% in più rispetto al 2017)
- 124 miliardi di dollari nel 2019 (8,8% in più rispetto al 2018)

Motivations Behind Attacks
January 2016



Intro al Corso – Sicurezza dell'Informazione M



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



Intro al Corso – Sicurezza dell'Informazione M



Primo Attacco Informatico: Morris Worm

Sun Microsystems Sun3,
Vax computers with 4
BSD Unix

**2 novembre
1988**



Robert T. Morris Jr,
studente nel 1988 alla
Cornell University.

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 il Computer System Research
Group 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

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

Intro al Corso – Sicurezza dell'Informazione M



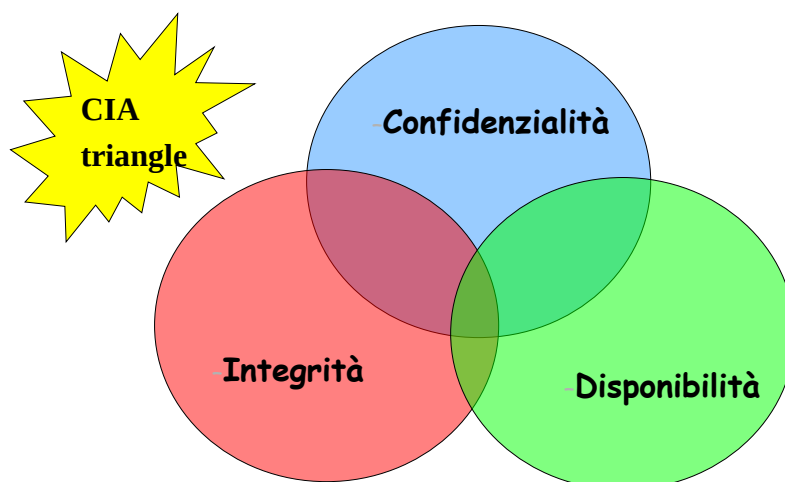
Problemi di Sicurezza

La sicurezza informatica ha uno scope molto ampio di indagine:

- Sicurezza dell'Hardware
- Sicurezza del Software (programmi, sistema operativo)
- Sicurezza dei Dati
- Sicurezza della Rete

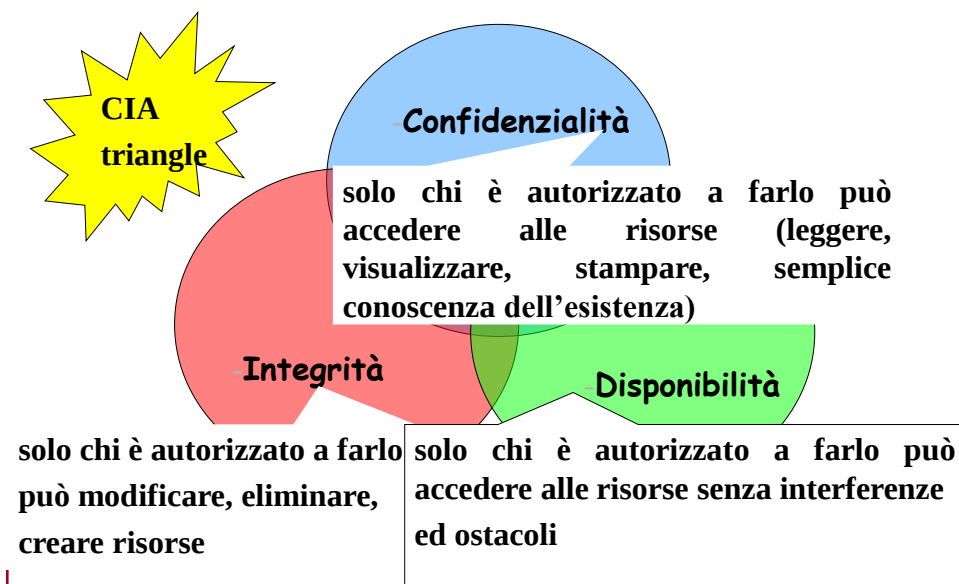


Le tre proprietà di base per la sicurezza dell'informazione





Le tre proprietà di base per la sicurezza dell'informazione



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'**



Vulnerabilità ed assenza di sicurezza

Vulnerabilità	Assenza di		
	confidenzialità	integrità	disponibilità
Hardware	individuazione furto	aggiunta modifica eliminazione	arresto impedimento
Software	individuazione	modifica falsificazione	eliminazione
Dati	lettura	modifica falsificazione	perdita cancellazione

Intro al Corso – Sicurezza dell'Informazione M



Una possibile definizione di sicurezza informatica

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

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

Intro al Corso – Sicurezza dell'Informazione M

14



La sicurezza non è un prodotto ma un processo



Security is a process,
not a product

(Bruce Schneier, Crypto-Gram, May 2005)

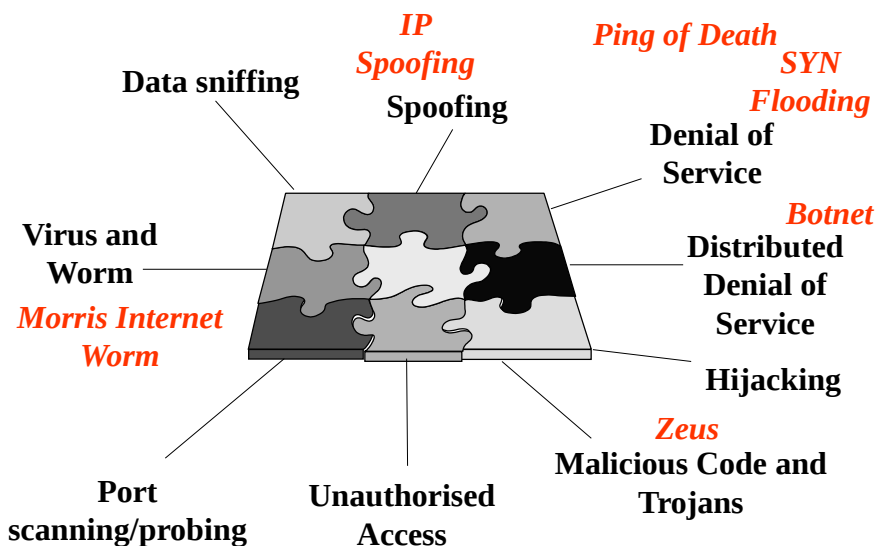
Computer Security: Will We Ever Learn?

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.**



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 ...)

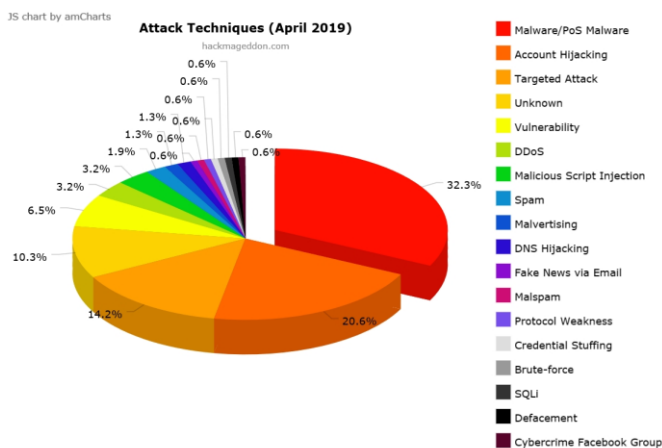


Virus e Worm

- **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, contiene funzionalità aggiuntive impreviste
- **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)

Intro al Corso – Sicurezza dell'Informazione M



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 che può rendere realizzabile una 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

Intro al Corso – Sicurezza dell'Informazione M



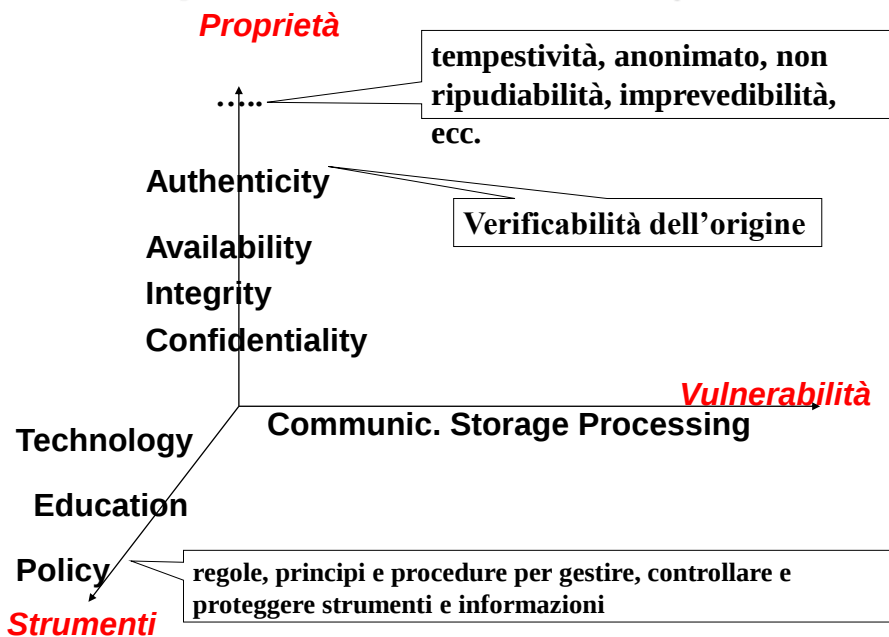
Minacce, vulnerabilità e contromisure



Intro al Corso – Sicurezza dell'Informazione M



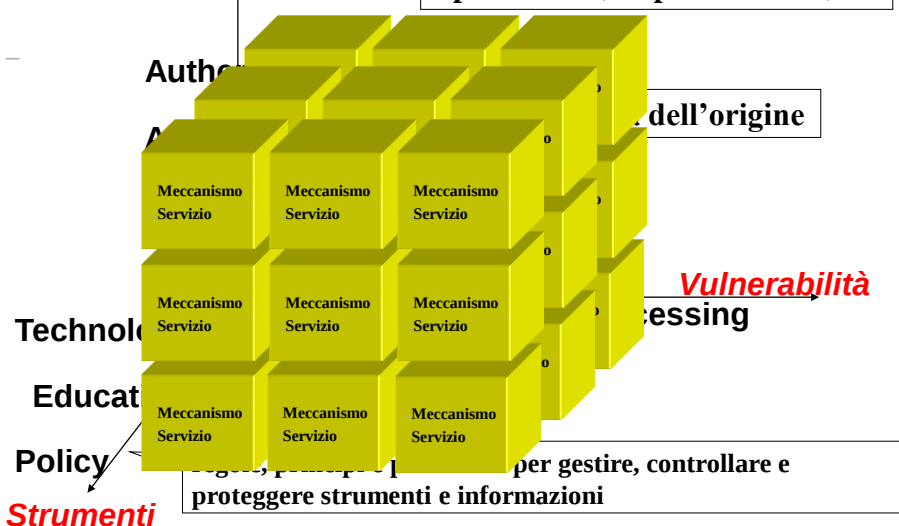
Lo spazio della sicurezza (NSTISSC)



Intro al Corso – Sicurezza dell'Informazione M



**tempestività, anonimato, non
ripudiabilità, imprevedibilità,**



Intro al Corso – Sicurezza dell'Informazione M



- **Modelli, tecnologie e infrastrutture per garantire la sicurezza dei dati**

Non ci occuperemo in modo approfondito (per motivi di mancanza di ore) di penetration testing, di sistemi operativi sicuri, di progettazione di programmi sicuri, di rilevamento di malware e di hardware sicuro, di analisi del rischio!!!!!! Solo cenni!!!

Intro al Corso – Sicurezza dell'Informazione M



Programma



Intro al Corso – Sicurezza dell'Informazione M



Servizi e Meccanismi

- **Meccanismo di Sicurezza:** meccanismo progettato per rilevare, prevenire un attacco, risanare il sistema a seguito di un attacco.
- **Servizio di Sicurezza:** servizio che migliora la sicurezza dell'elaborazione dei dati e del trasferimento delle informazioni. Un servizio di sicurezza utilizza uno o più meccanismi.

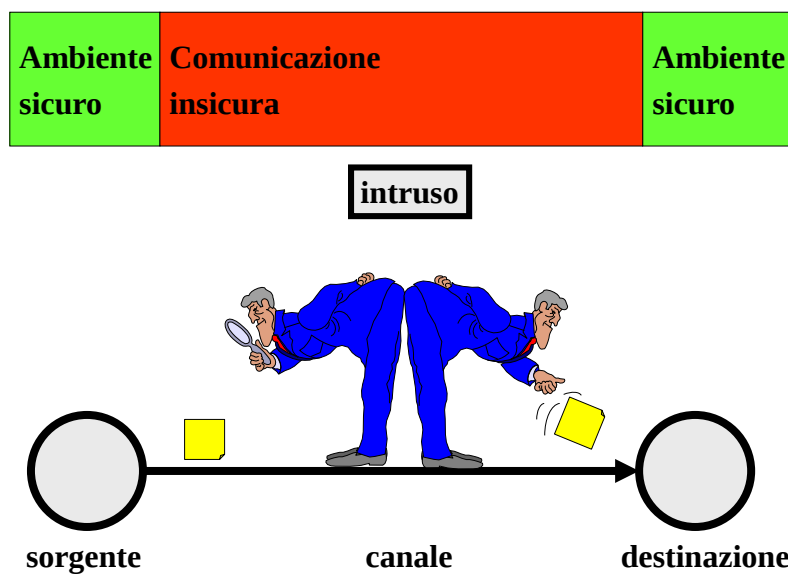
Intro al Corso – Sicurezza dell'Informazione M



Intro al Corso – Sicurezza dell'Informazione M



Il modello del canale insicuro



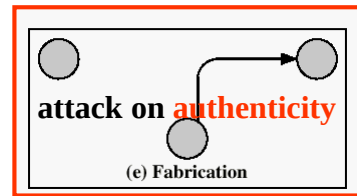
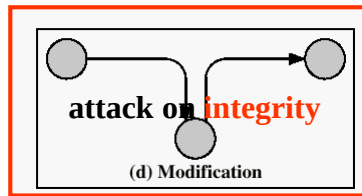
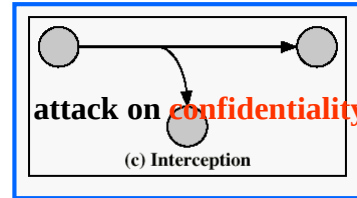
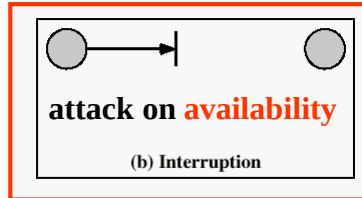
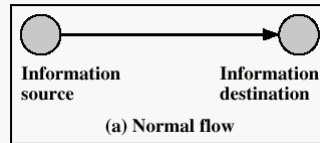
Intro al Corso – Sicurezza dell'Informazione M



Attacchi alla Sicurezza

☐ Attacco passivo

☐ Attacco attivo



Intro al Corso – Sicurezza dell'Informazione M

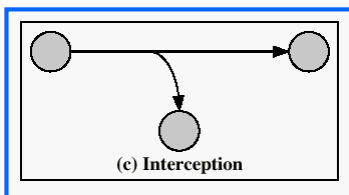


Attacchi passivi: contromisure

- **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

Intro al Corso – Sicurezza dell'Informazione M

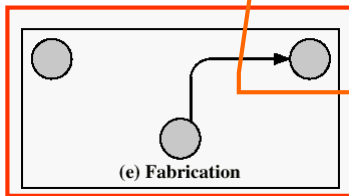
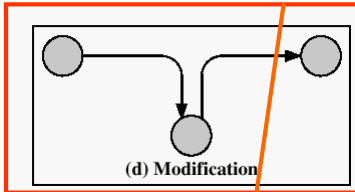


Attacchi attivi: contromisure

- **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

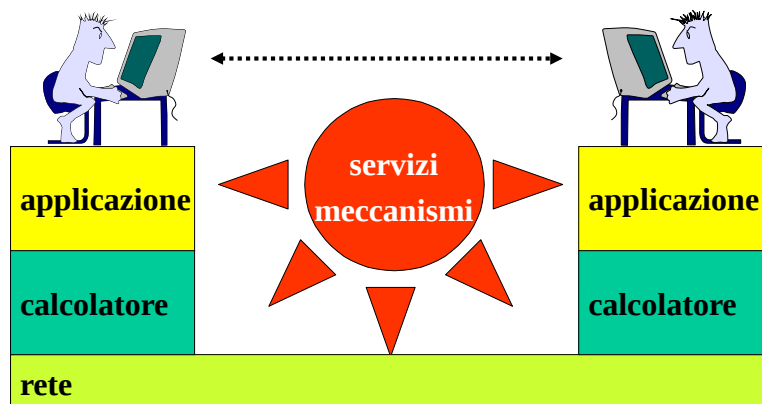


1. controllo d'accesso al canale
2. attestato d'integrità e d'origine

Intro al Corso – Sicurezza dell'Informazione M



Collocazione dei meccanismi e dei servizi per la sicurezza



Intro al Corso – Sicurezza dell'Informazione M



Il calcolatore sicuro

Intro al Corso – Sicurezza dell'Informazione M



Calcolatori sicuri

Obiettivo: rilevazione tempestiva degli errori HW e SW

Tre approcci:

1.

**Progetto integrato
HW&SW**

**Trusted Computer
Platform (Fritz+Nexus)**

2.

**Funzioni e regole
di sicurezza**

**Estensioni
del S.O.
(Unix, SeLinux)**

3.

**Coprocessore
per la sicurezza**

«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. discretionary access control)».

Intro al Corso – Sicurezza dell'Informazione M



La rete sicura

Intro al Corso – Sicurezza dell'Informazione M



Rete sicura

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

Intro al Corso – Sicurezza dell'Informazione M



Valutazione, Certificazione, Enti

**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

...

CERT

CINI Cyber Security Lab

Intro al Corso – Sicurezza dell'Informazione M



Cosa Occorre Conoscere? Brevi Cenni di Analisi del Rischio

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

Intro al Corso – Sicurezza dell'Informazione M



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

Intro al Corso – Sicurezza dell'Informazione M



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

Intro al Corso – Sicurezza dell'Informazione M



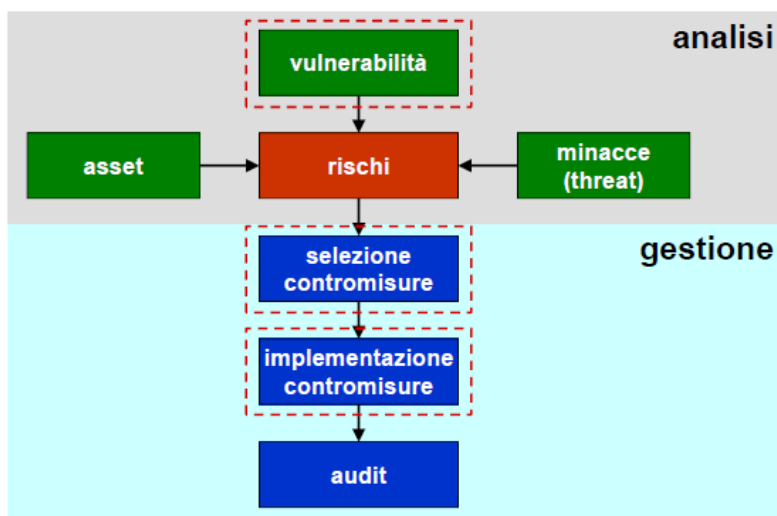
Fasi Metodologiche (2.)

- ❑ **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

Intro al Corso – Sicurezza dell'Informazione M



Analisi e Gestione della Sicurezza



Intro al Corso – Sicurezza dell'Informazione M



La sicurezza nel ciclo di vita di un sistema

