



# Sicurezza dell'Informazione M

Alma Mater Studiorum - Università di Bologna  
CdS Laurea Magistrale in Ingegneria Informatica  
II Ciclo - A.A. 2024/2025

## Corso di Sicurezza dell'Informazione M

Docente: Rebecca Montanari  
[rebecca.montanari@unibo.it](mailto:rebecca.montanari@unibo.it)



# Sicurezza dell'Informazione M in una slide

Propedeuticità: per trarre maggior profitto dal corso è importante aver chiari i concetti e gli strumenti forniti dai corsi di reti di calcolatori, sistemi operativi e laboratorio di sicurezza informatica T

Modalità d'esame: prova scritta e prova pratica (anche possibilità di Attività Progettuale da 3 cfu)

- **Orari di ricevimento del docente:**  
c/o studi DISI – edificio aule nuove (di fianco aula 5.7)

- **Concordare l'appuntamento inviando email a:  
[rebecca.montanari@unibo.it](mailto: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. Servono come traccia**

**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](http://www.cacr.math.uwaterloo.ca/hac))
- 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) forniti sul sito del corso
- David F. Ferraiolo: “Role-Based Access Control”



# Orario delle lezioni

Normalmente:

- martedì ore 12-14**
- giovedi' ore 9-12**

Sono previste esercitazioni in aula nelle date che verranno comunicate

***Eventuali variazioni verranno comunicate  
prontamente tramite sito Web del corso***

***Controllare sempre il sito degli orari dei corsi***



# Indicazioni Uso IA Generativa

Leggere attentamente la Policy di Ateneo e il materiale di approfondimento sul portale dell'Ateneo.

**Attenersi alle seguenti indicazioni:**

- I'uso di strumenti di GenAI è ammesso secondo le indicazioni fornite dalla Policy di Ateneo tranne durante gli esami scritti**
- occorre citare sempre l'uso degli strumenti di GenAI nella preparazione delle prove finali (tesi, elaborati delle attività progettuali e prove pratiche). Se non si cita l'uso, le prove finali potrebbero essere respinte .**
- seguire il suggerimento di citazione fornito sul portale (disclaimer ragionato e dettagliato)**
- non è assolutamente ammesso il «copia e incolla»**
- essere sempre pronti ad argomentare gli output prodotti da strumenti di GenAI**

**In caso di dubbi scrivere al docente**



# Cyber Attack Maps

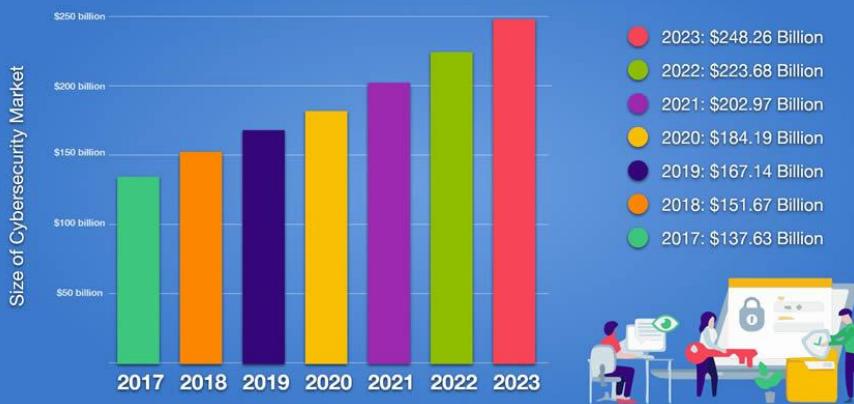
[MAP | Kaspersky Cyberthreat live map](#)



# Un po' di statistiche ....



Cybersecurity Industry Size by Year



Cybersecurity professionals are highly sought-after.

In reality, it's believed that there will be **3.5 million** cybersecurity jobs unfilled in 2025.

The market for jobs is expected to increase by **33% between** 2021 to 2031 According to the Bureau of Labor Statistics.

The median wage for a cybersecurity professional is **\$102,600**, as per the BLS.

(Source: BLS)



# Nuove Figure Professionali

## Alcune figure professionali rilevanti:

- Cyber Risk Manager
- Security Administrator
- Security Engineer
- Security Architect
- Security Analyst
- Security Developer
- Ethical Hacker
- Machine Learning Specialist
- .....



# 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, balcanizzazione del perimetro





# Primo Attacco Informatico: Morris Worm

**Sun Microsystems  
Sun3, Vax computers  
with 4 BSD Unix**

**2 novembre  
1988**



**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**

**Rober T. Morris Jr,  
studente nel 1988 alla  
Cornell University.**

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



# Sicuro?

## Cosa?

## Da chi?

## Perché?





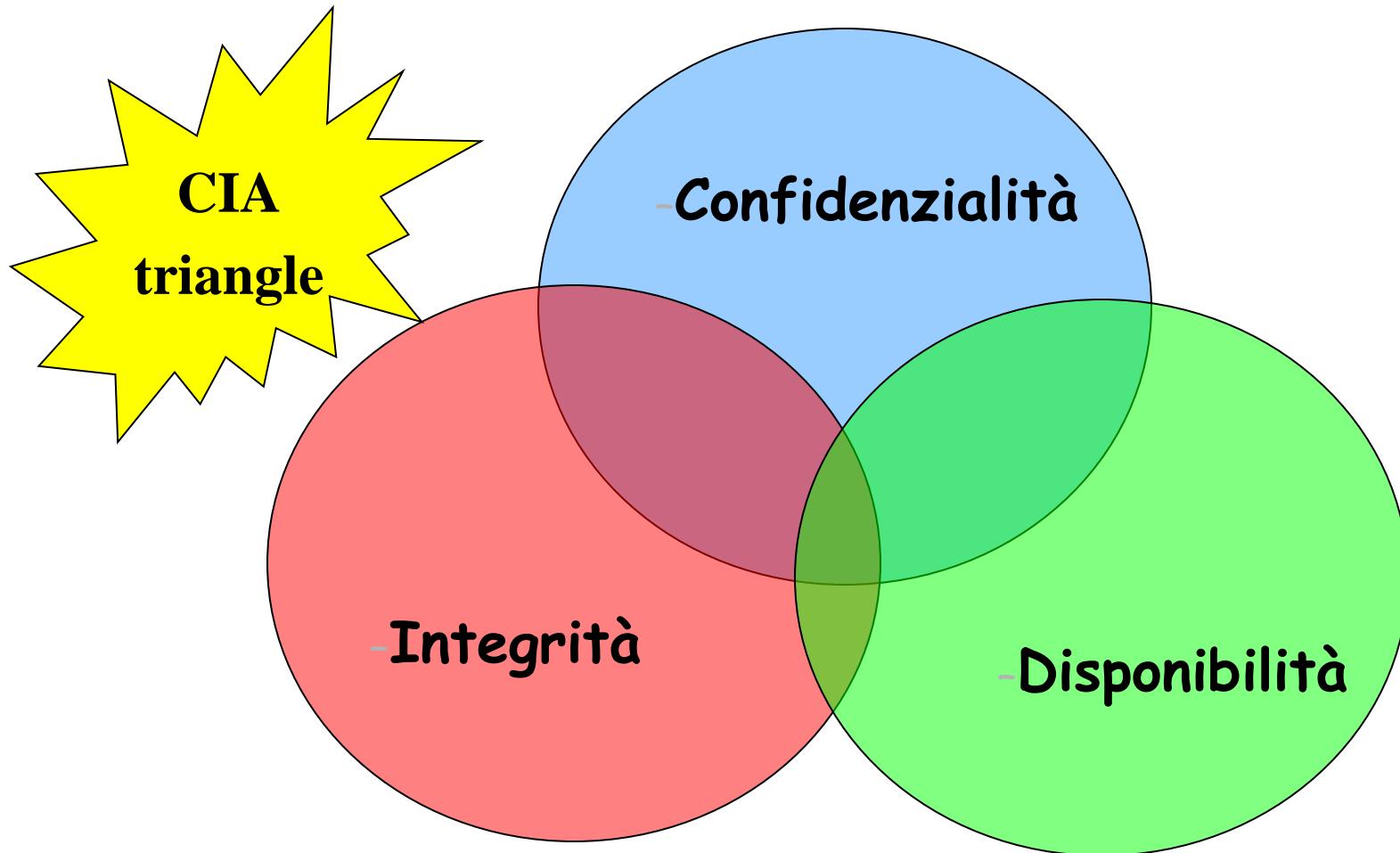
# Problemi di Sicurezza

**La sicurezza informatica ha uno scope molto ampio di indagine:**

- **Sicurezza dell'Hardware**
- **Sicurezza del Firmware**
- **Sicurezza del Software (programmi, sistema operativo)**
- **Sicurezza dei Dati**
- **Sicurezza delle Reti**

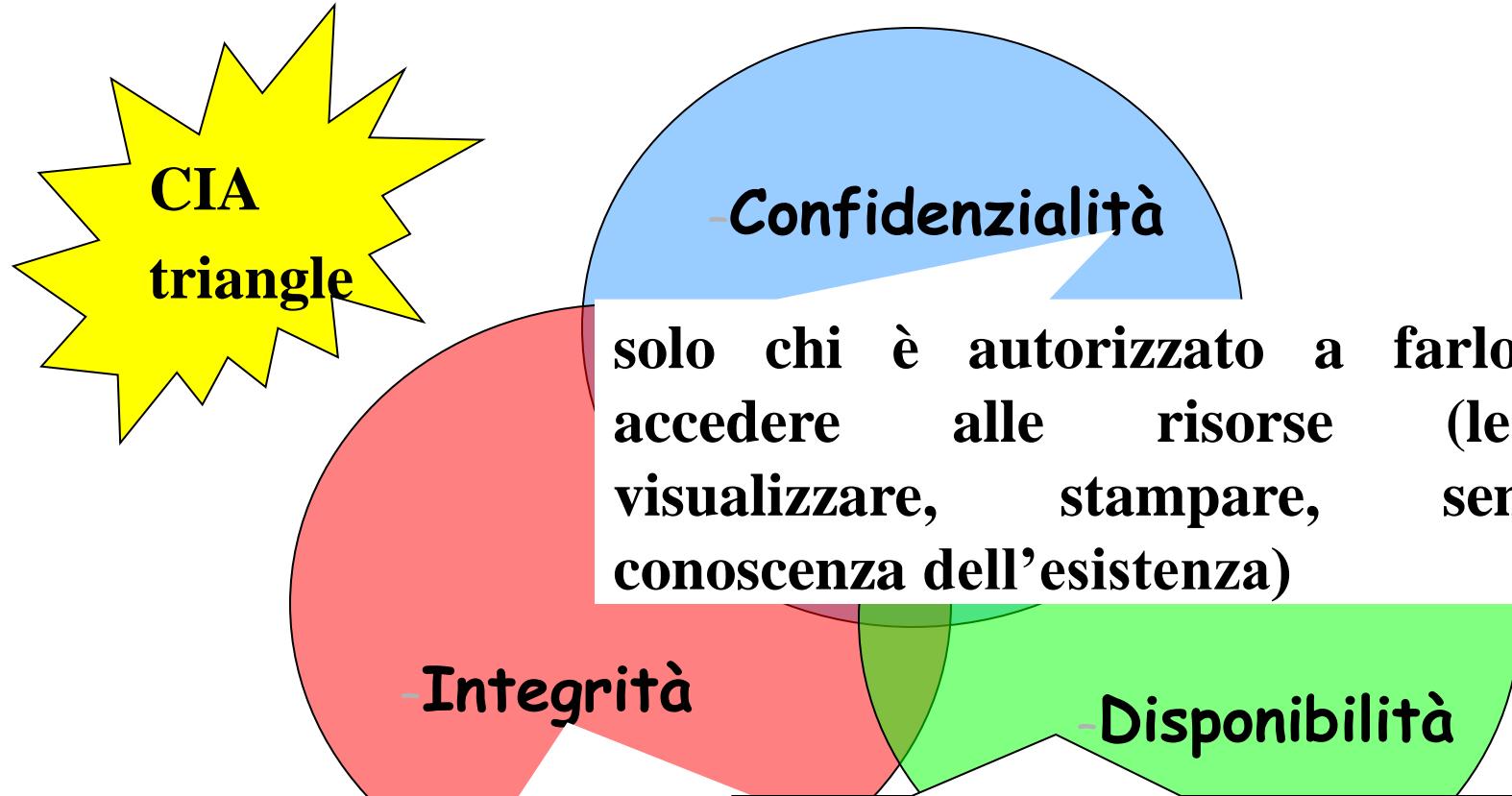


# Le tre proprietà di base per la sicurezza dell'informazione





# Le tre proprietà di base per la sicurezza dell'informazione



so lo chi è autorizzato a farlo può modificare, eliminare, creare risorse

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



# 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.**



# 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

**Vulnerabilità:** punto debole del sistema che può rendere realizzabile una minaccia

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

**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



# Vulnerabilità ed assenza di sicurezza

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



# Vulnerabilità Humanware

One out of every 142 passwords is '123456'

The '123456' password was spotted 7 million times across a data trove of one billion leaked credentials, in one of the biggest password re-use studies of its kind.

By Catalin Cimpanu for Zero Day | July 1, 2020 -- 15:09 GMT (16:09 BST) | Topic: Security

Manage Scripts  
Waiting for ade.googlesyndication.com...

IL MASSIMO DELLA RETE  
E IL MASSIMO DELLE



# Mercato delle vulnerabilità

Webinar: Cyber Security, la sicurezza del web | ZERODIUM - How to Sell Your Exploit

<https://zerodium.com/program.html>

## Eligible Research

ZERODIUM is currently acquiring zero-day exploits and innovative security research related to the following products:

**Operating Systems**  
Remote code execution or local privilege escalation, or VM escape:  
  
- Microsoft Windows  
- Linux / BSD  
- Apple macOS  
- VMware ESXi

**Web Browsers**  
Remote code execution, or sandbox bypass/escape, or both:  
  
- Google Chrome  
- Microsoft Edge  
- Mozilla Firefox  
- Apple Safari

**Clients / Files**  
Remote code execution or sensitive information disclosure:  
  
- MS Office (Word/Excel)  
- Adobe Acrobat / Reader  
- Email (Outlook/Thunderbird)  
- Archivers (7-Zip/WinRAR/WinZip/Tar)

**Mobiles / Smartphones**  
Remote code execution, or privilege escalation, or any other exploit type:  
  
- Apple iOS  
- Apple watchOS  
- Android  
- Windows Mobile

**Web Servers**  
Remote code execution or sensitive information disclosure:  
  
- Apache HTTP Server  
- Microsoft IIS Server  
- nginx web server  
- PHP / ASP  
- OpenSSL / mod\_ssl

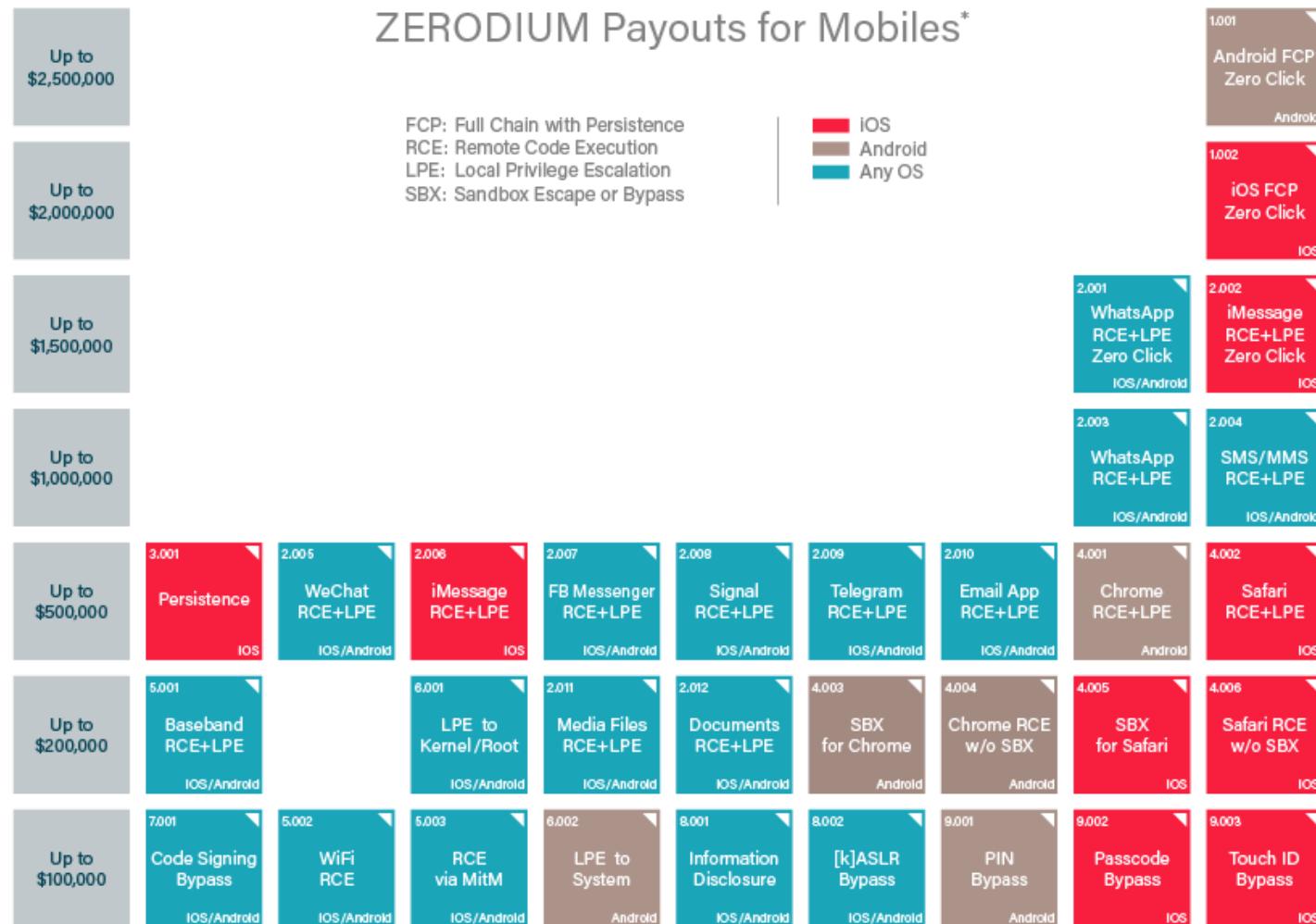
**Email Servers**  
Remote code execution or sensitive information disclosure:  
  
- MS Exchange  
- Dovecot  
- Postfix  
- Exim  
- Sendmail

**WebApps / Panels**  
Remote code execution, or SQL injection, or information disclosure:  
  
- cPanel / Plesk / Webmin  
- WordPress / Joomla / Drupal  
- vBulletin / MyBB / phpBB  
- IPS Suite / IP.Board  
- Roundcube / Horde

**Research / Techniques**  
Any other security research, exploits, or techniques related to:  
  
- WiFi / Baseband RCE  
- Routers / IoT RCE  
- AntiVirus RCE/LPE  
- Tor De-anonymization  
- Mitigations Bypass



# Zerodium

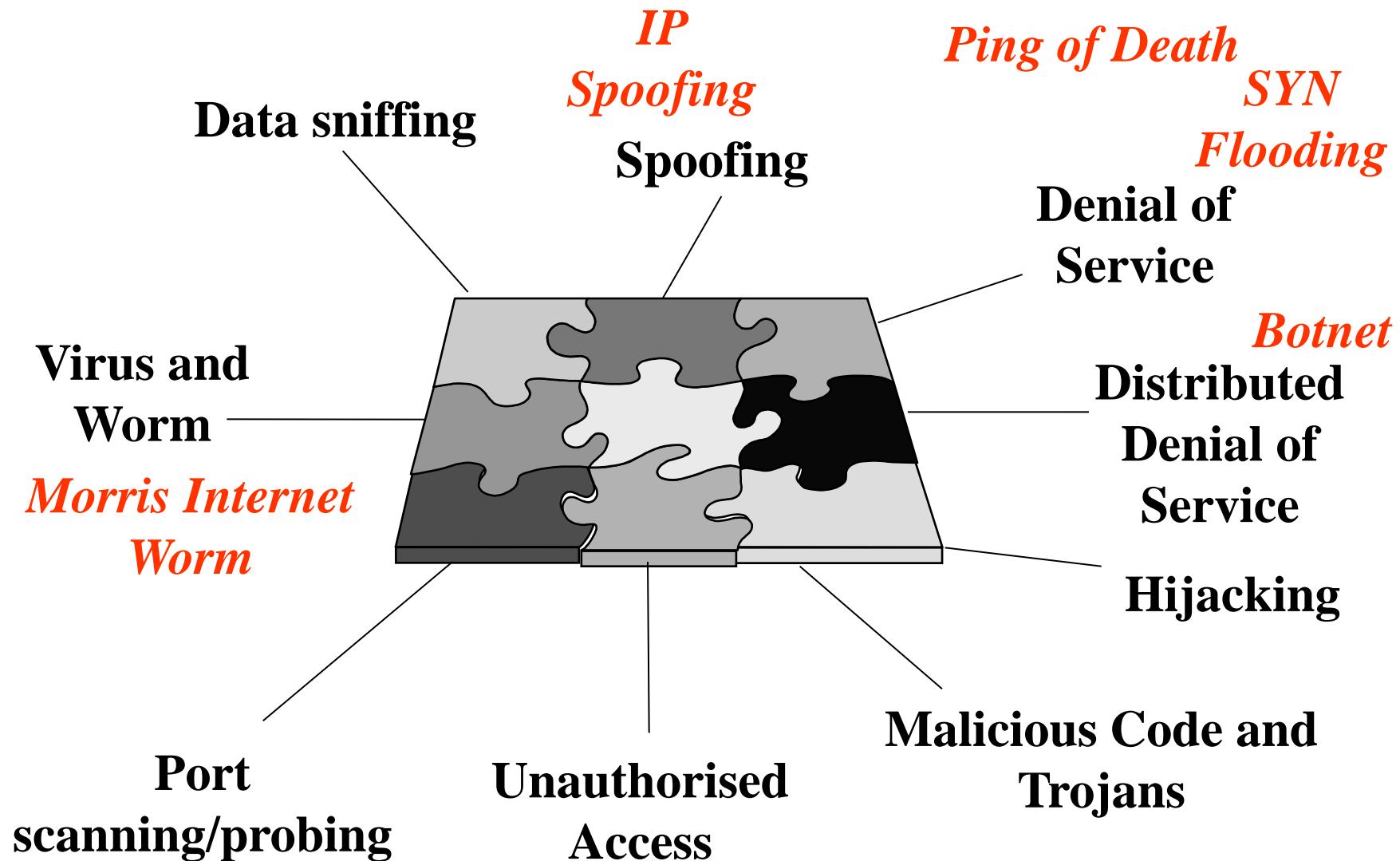


\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com



# Esempi di Attacchi Informatici





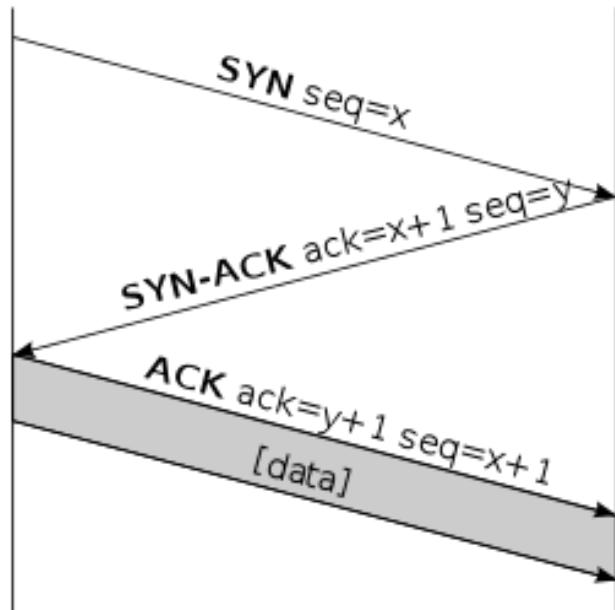
# Alcune Tipologie di Attacchi di Rete

- **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)

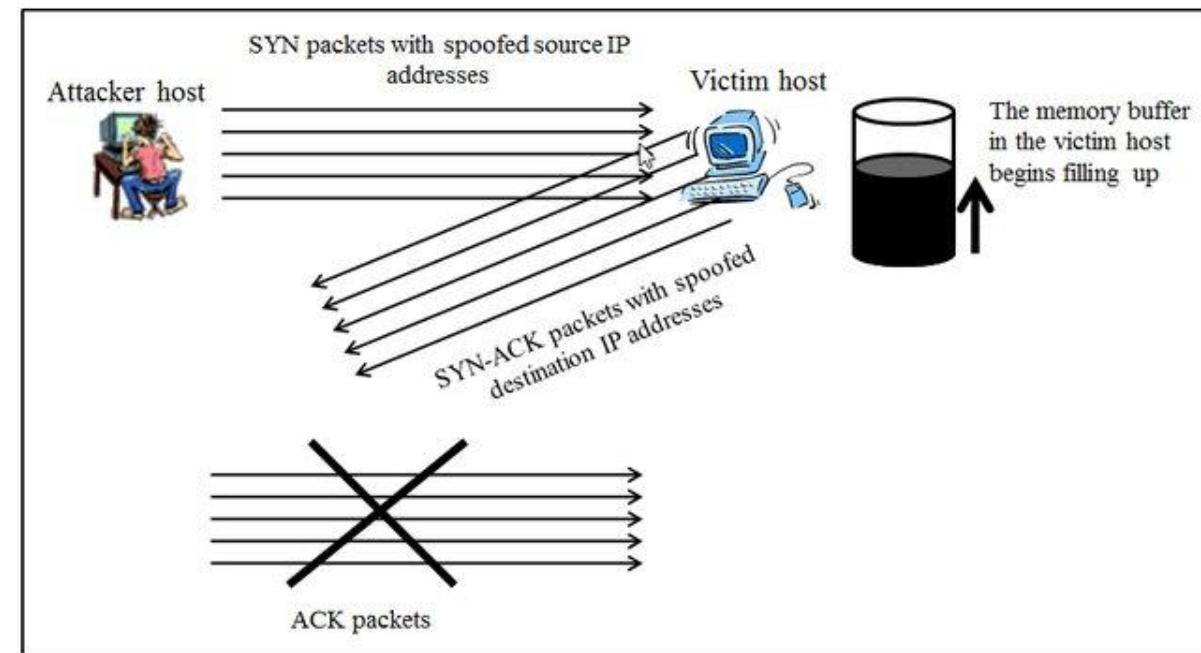


# SYN Flooding

Client



Server





# 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 OWASP delle Vulnerabilità 2025

## OWASP Top 10 : 2021 vs 2025

2021

A01: Broken Access Control

A02: Cryptographic Failures

A03: Injection

A04: Insecure Design

A05: Security Misconfiguration

A06: Vulnerable and Outdated Components

A07: Identification and Authentication Failures

A08: Software and Data Integrity Failures

A09: Security Logging and Monitoring Failures

A10: Server-Side Request Forgery

2025

A01: Broken Access Control

A02: Cryptographic Failures

A03: Injection

A04: Security Misconfiguration

A05: Identification and Authentication Failures

A06: Exposed Sensitive Data

A07: Server Side Request Forgery

A08: Supply Chain Failure(A08+A06 from 2021)

A09: Security Logging and Monitoring Failures

A10: ?

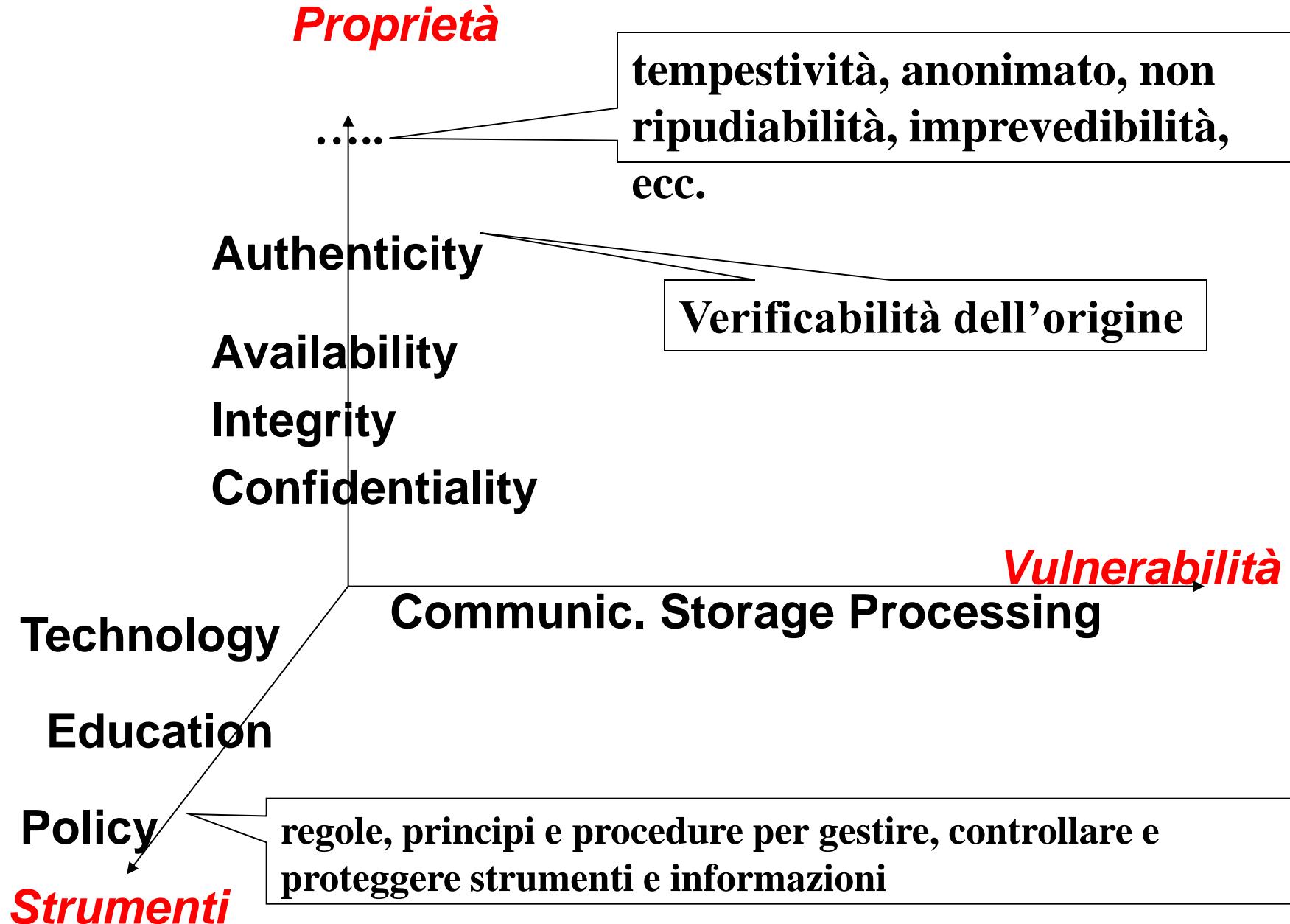


# Minacce, vulnerabilità e contromisure





# Lo spazio della sicurezza (NSTISSC)





# Lo spazio della sicurezza (NSTISSL)

**Proprietà**

tempestività, anonimato, non ripudiabilità, imprevedibilità,

—  
Autenticazione

Accesso

Meccanismo  
Servizio

Meccanismo  
Servizio

Meccanismo  
Servizio

Meccanismo  
Servizio

dell'origine

Technologia

Vulnerabilità  
Processing

Educazione

Policy

Meccanismo  
Servizio

Meccanismo  
Servizio

Meccanismo  
Servizio

Meccanismo  
Servizio

Strumenti

Regole, protocolli per gestire, controllare e proteggere strumenti e informazioni



# Programma

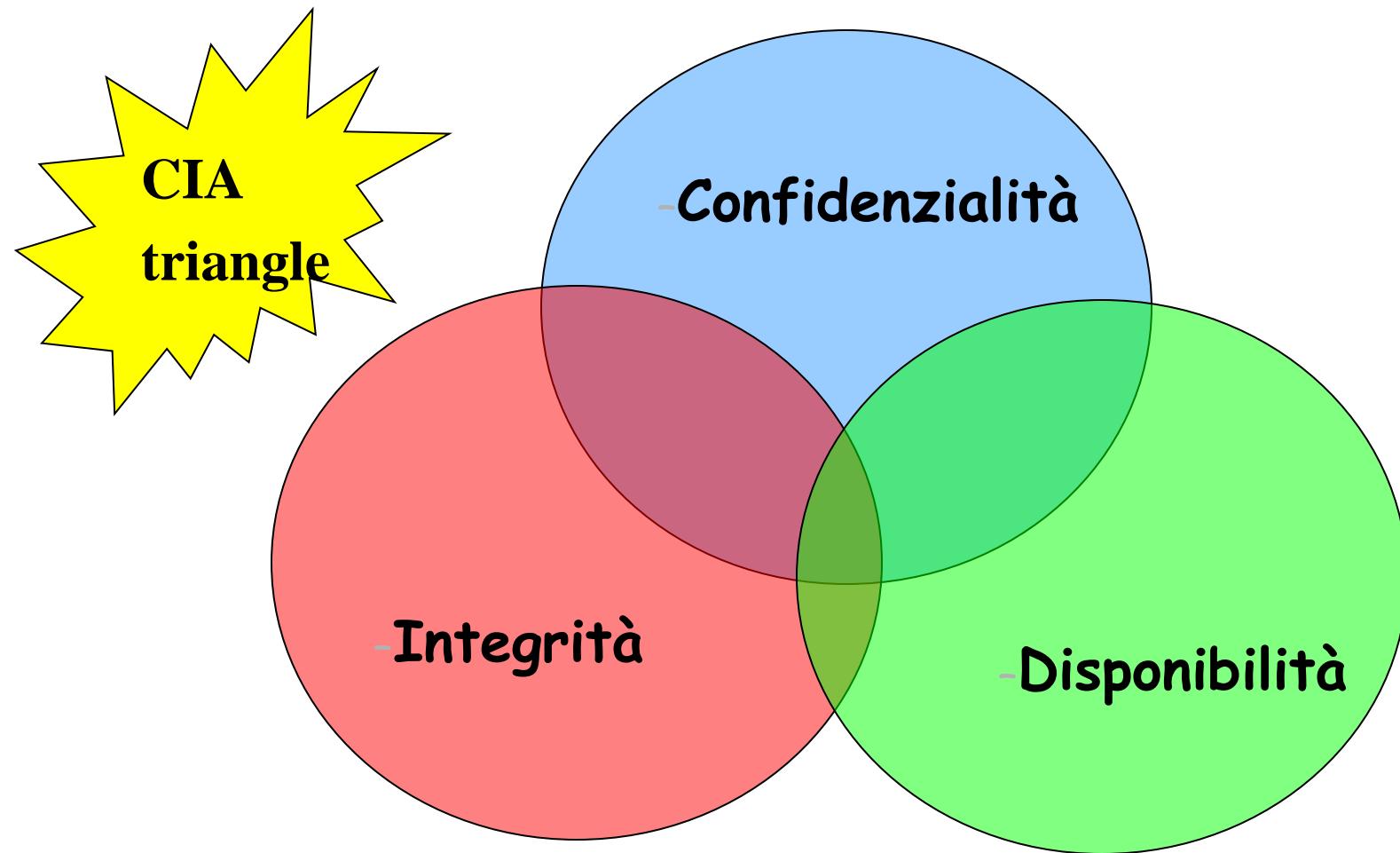
## Focus del corso:

- **Modelli, tecnologie e infrastrutture per garantire la sicurezza dei dati (memorizzazione sicura, trasmissione sicura su rete, accesso autenticato e autorizzato, ...)**

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!!!



# Ci occuperemo di tecnologie per:





# E per 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**
- **TRACCIABILITÀ**



# 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



# 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

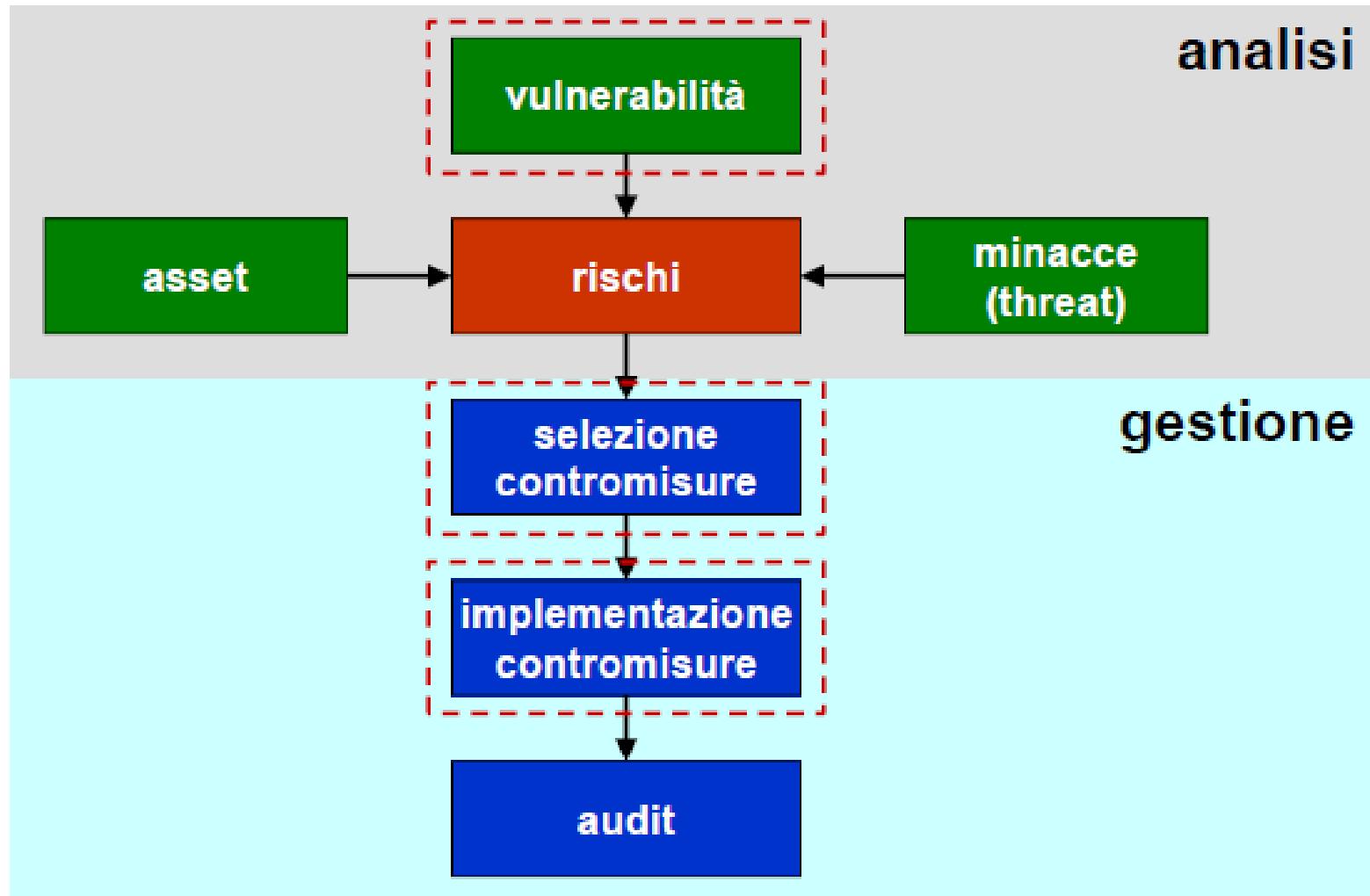


# Fasi Metodologiche (2.)

- **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

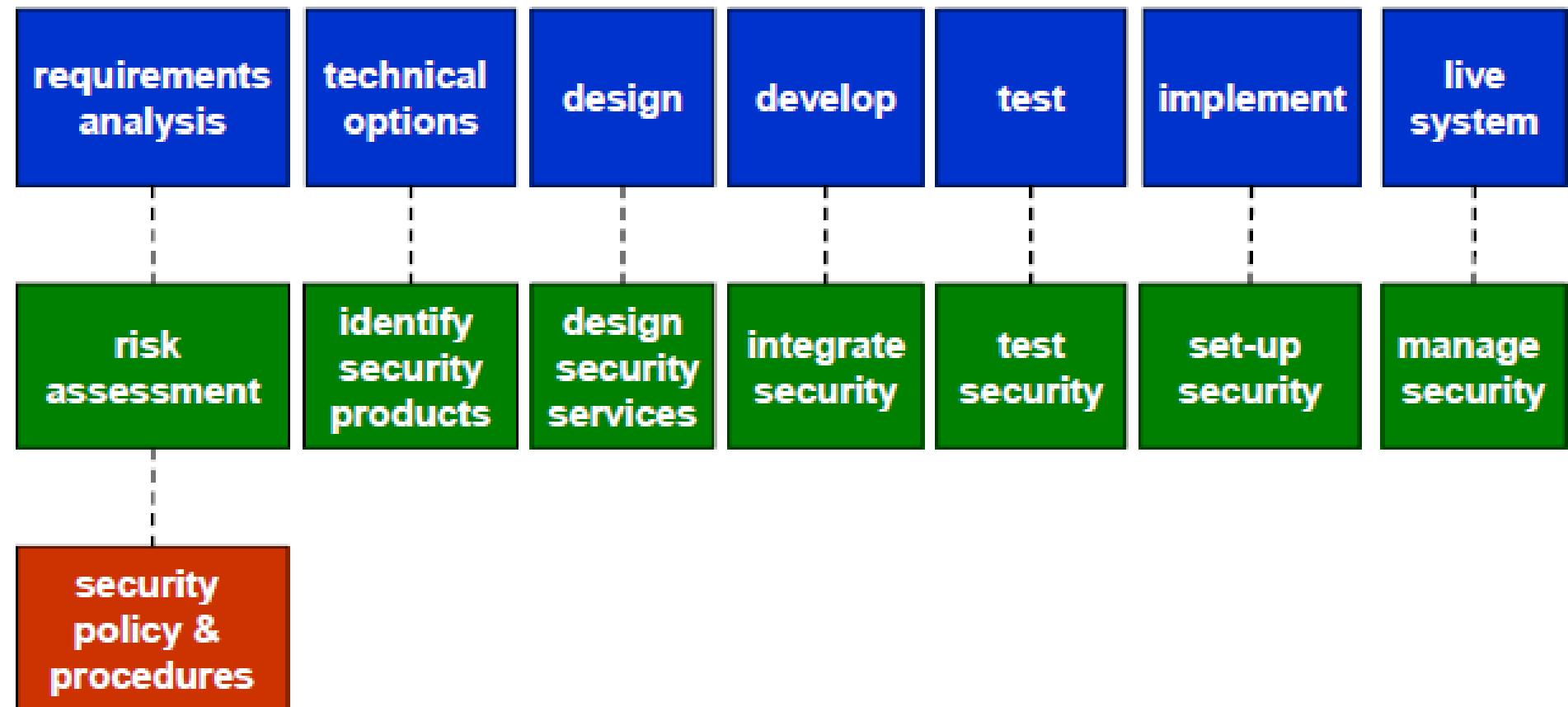


# Analisi e Gestione della Sicurezza





# La sicurezza nel ciclo di vita di un sistema





# Il calcolatore sicuro



# 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)».**



# 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**

**Clusit**

**CINI Cyber Security Lab**

**E la sicurezza del  
firmware?**



# 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.



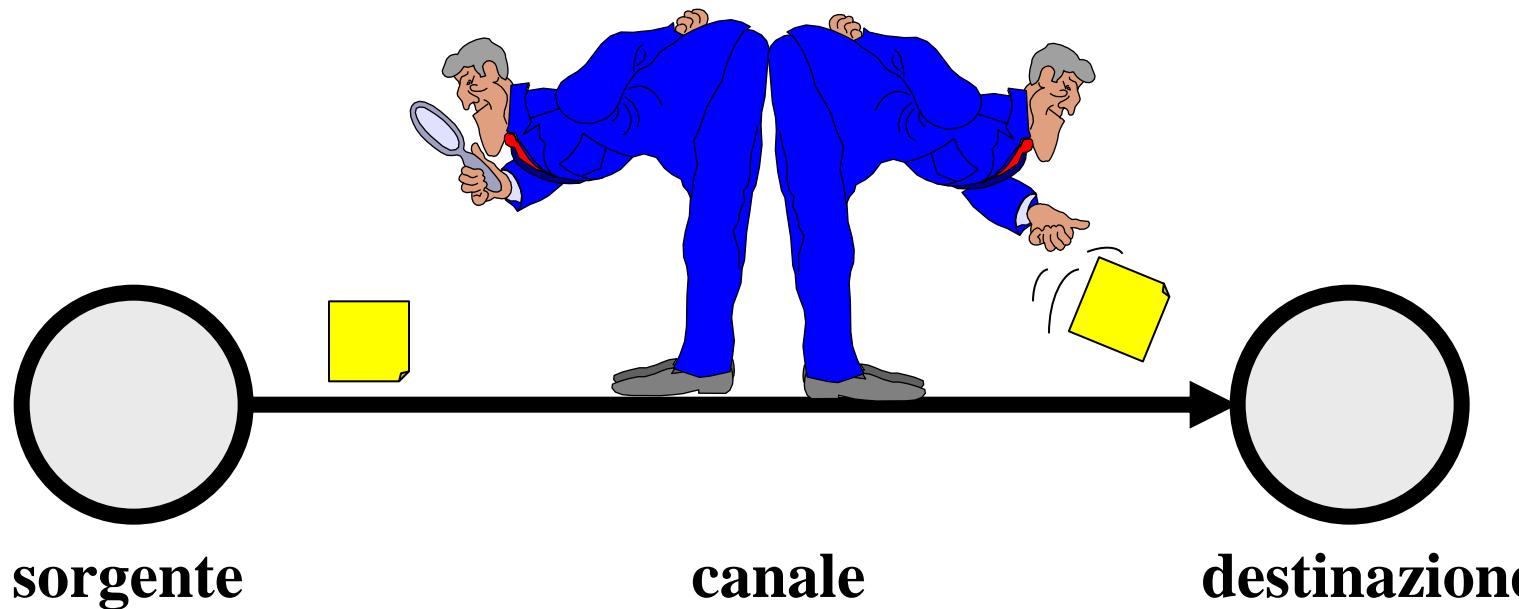
**Attacco intenzionale:  
“ogni azione mirante  
a compromettere una  
proprietà critica della  
informazione”**



# Il modello del canale insicuro



intruso

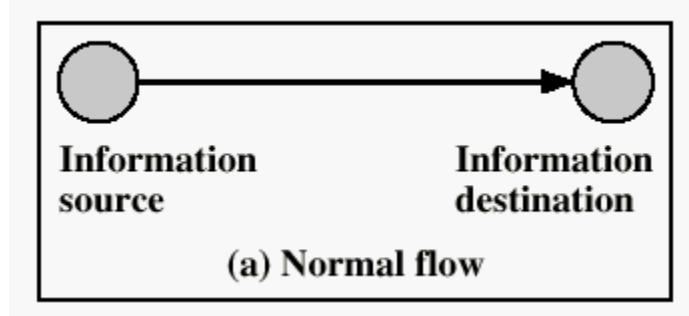




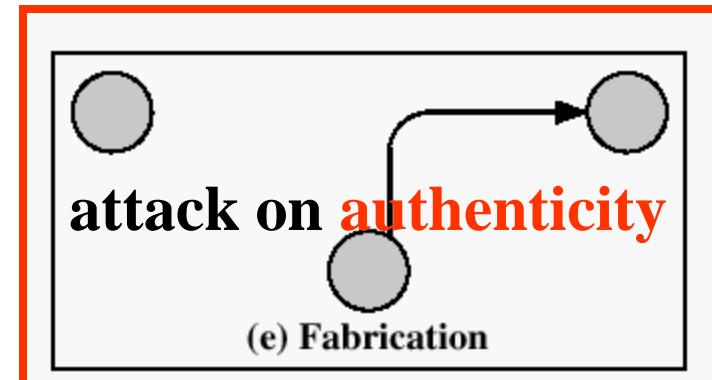
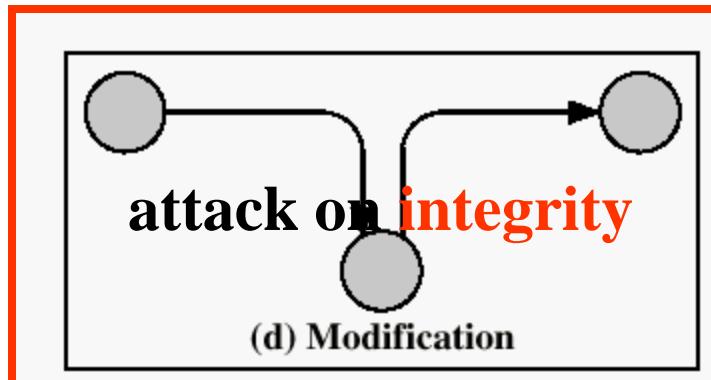
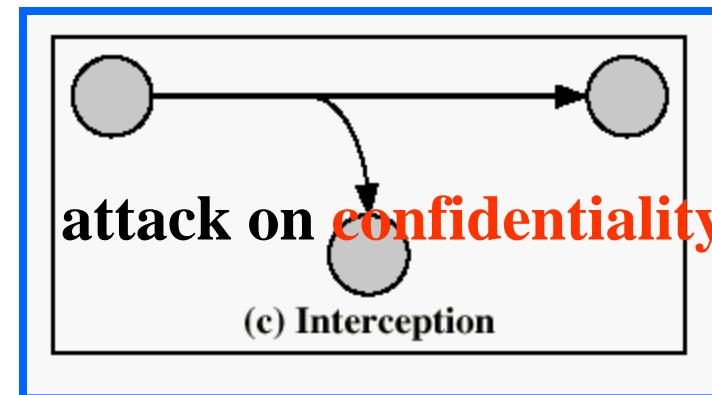
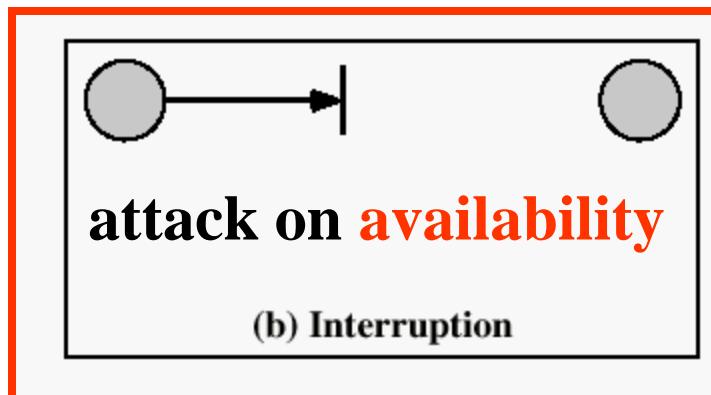
# Attacchi alla Sicurezza



Attacco passivo



Attacco attivo



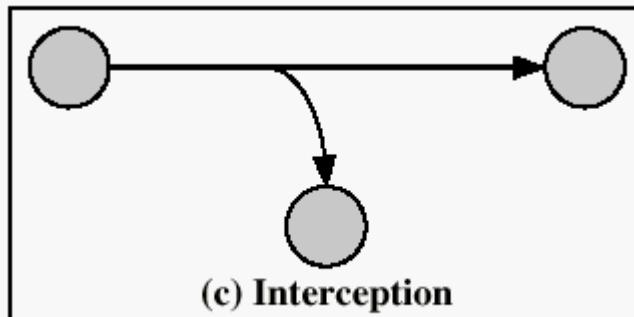


# Attacchi passivi: contromisure

- 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 incomprendibile

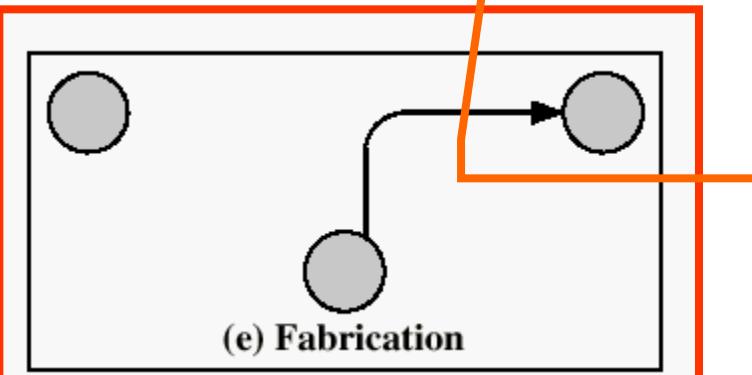
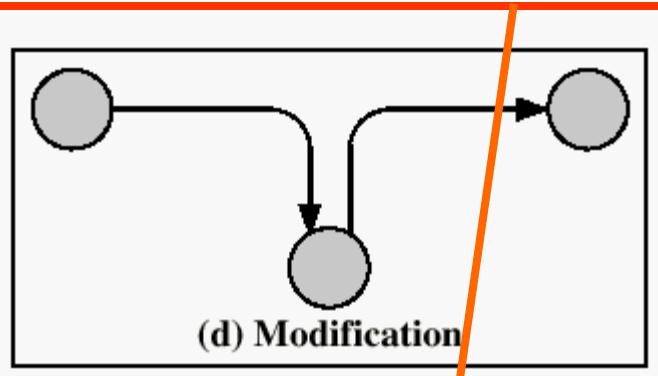


# Attacchi attivi: contromisure

- 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

