

# **Esperti nella gestione dei sistemi informativi e tecnologie informatiche**

---

## **Analisi del rischio e Sicurezza delle attività**

**Docente:** Eduard Roccatello  
**Email:** eduard@roccatello.it  
**Sito:** <http://www.roccatello.it/teaching/rsa/>

# La sicurezza informatica

---

- **La Sicurezza informatica è quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati.**
- Risorsa online sulla definizione di sicurezza:  
[http://it.wikipedia.org/wiki/Sicurezza\\_informatica](http://it.wikipedia.org/wiki/Sicurezza_informatica)

# La sicurezza informatica

---

## □ Sicurezza attiva

- Le tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri.

## □ Sicurezza passiva

- Le tecniche e gli strumenti di tipo *difensivo*, ossia quel complesso di soluzioni il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata

## □ Sono **COMPLEMENTARI**

# Attacchi alla sicurezza informatica

---

## □ Attacchi virus

- Più dell'80% ha riportato almeno un incidente
  - Dato particolarmente allarmante se si pensa che il 98% dei sistemi avevano installato software antivirus
- Un'e-mail su 200 contiene un virus
  - Se il trend continua nel 2007 avremmo 1 e-mail su 10 contenente virus
- 40 nuovi virus e worm vengono creati ogni giorno (ma solo 3 o 4 sono prevalenti)
  - Code Red nel 2001 2.5 miliardi di \$ di danni
  - Melissa 6.7 miliardi di \$ di danni

# Attacchi alla sicurezza informatica

---

## Penetrazione nel sistema (hacking)

- Sono leggermente diminuiti, ma sono quasi il doppio di qualche anno fa'
  - Dato particolarmente allarmante se si pensa che il 98% dei sistemi avevano installato firewall

# Attacchi alla sicurezza informatica

---

## Denial-of-service (DoS)

- Alcuni soggetti, quando non riescono a penetrare un sistema, rendono inservibile il sistema
- Un crescente numero di attaccanti non cercano neanche di penetrare il sistema
- Primo caso nel 1998
- Nel febbraio 2000
  - CNN.com, eBay.com, Yahoo.com, Amazon.com, Dell.com
  - Da un giovane pirata canadese di 15 anni

# Attacchi alla sicurezza informatica

---

- Una piccola compagnia di servizi di provider per Internet fu attaccata da attaccanti anonimi con DoS continui
- L'azienda cessò l'attività perché il costo del ripristino avrebbe causato la bancarotta

# Attacchi alla sicurezza informatica

---

## □ Accessi non autorizzati interni

- Rappresenta uno spettro vario ed eterogeneo di trasgressioni, dalle più piccole alle più devastanti
- È piuttosto comune

# Attacchi a bassa prevalenza ma alto impatto

---

## Frode finanziaria

- Il danno è generalmente alto
- Frode di 8 milioni nel 2001 alla Cisco

## Furto di segreti commerciali

- Danno notevole del furto di informazioni proprietarie
- I piani sono copiati e rivenduti alla controparte
  - Danni per diversi milioni di dollari

# Attacchi a bassa prevalenza ma alto impatto

---

## □ Sabotaggio

- L'attaccante cancella o modifica dei file o fa danni hardware
- Nel 2001 un impiegato ha forzato il database della sua precedente azienda cancellando centinaia di file e alterando record di fatture

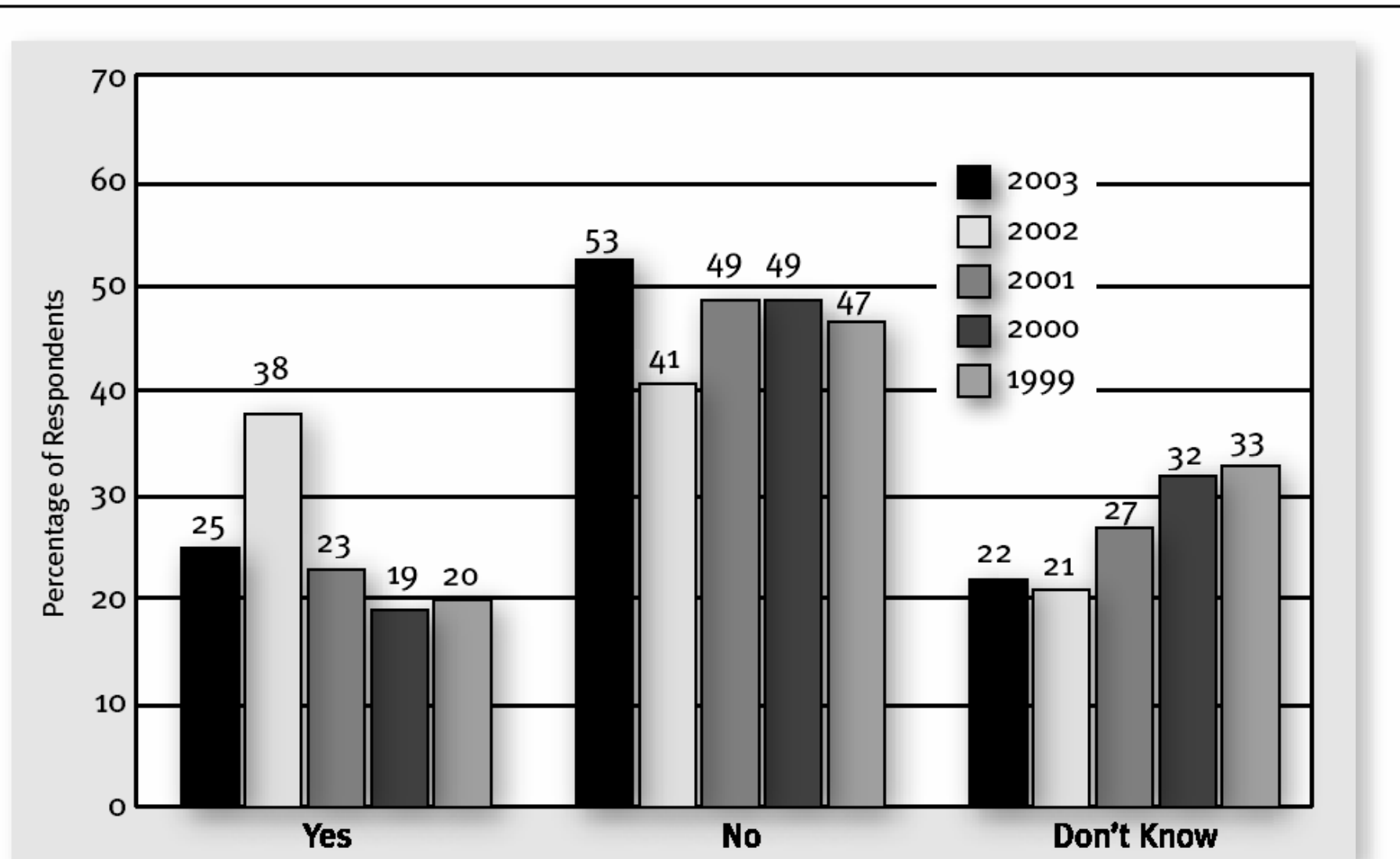
# Attacchi non comuni e basso impatto

---

- Eavesdropping (l'atto di origliare) e interposizione
  - Intercettazione su rete
  - Nonostante la loro forte carica scenica sono molto rari
  - Ci sono metodi di prevenzione efficaci
    - Si fa piuttosto uso delle altre metodologie di attacco più semplici

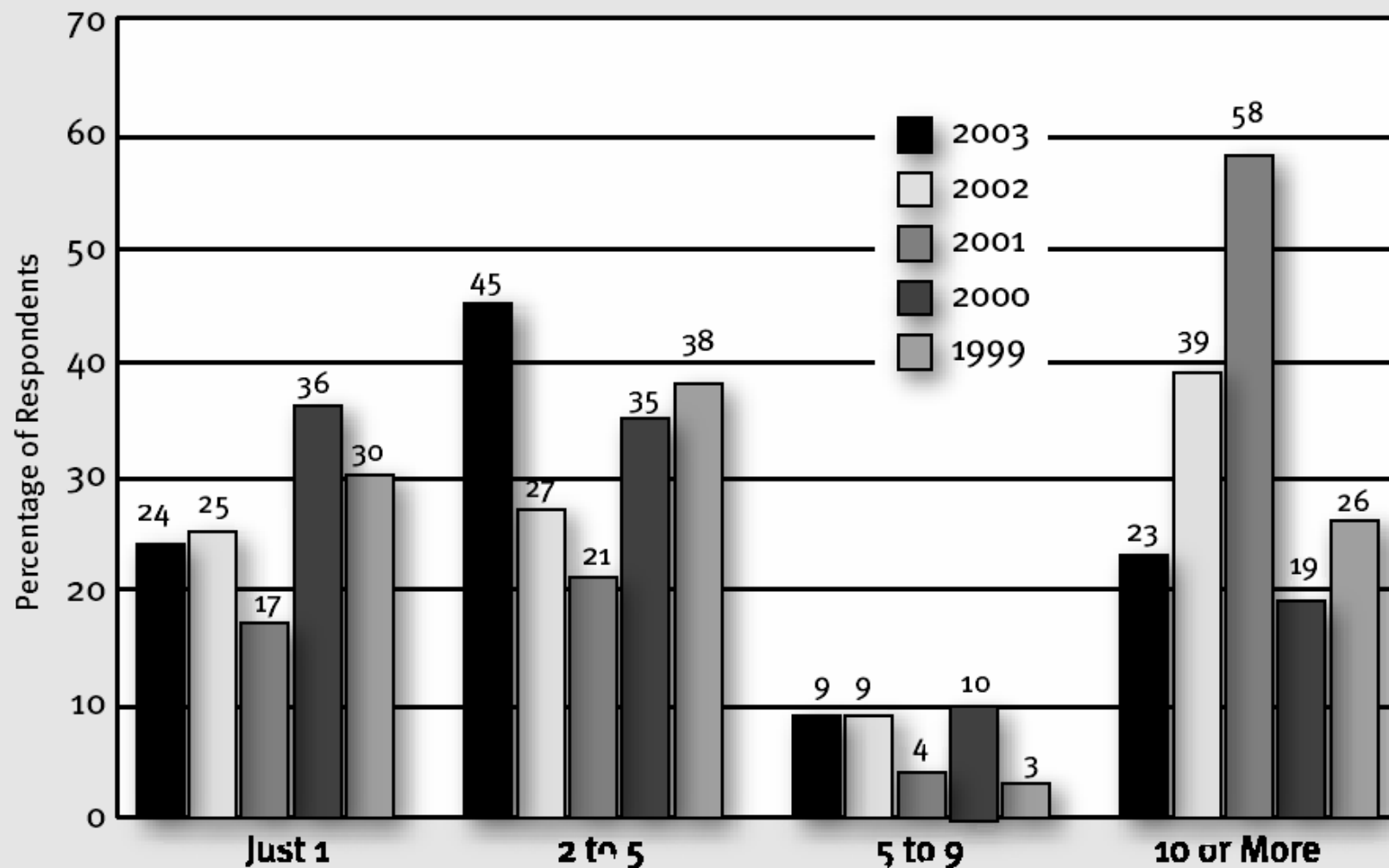
# Attacchi ai siti WEB

Has Your WWW Site Suffered Unauthorized Access or Misuse Within the Last 12 Months?



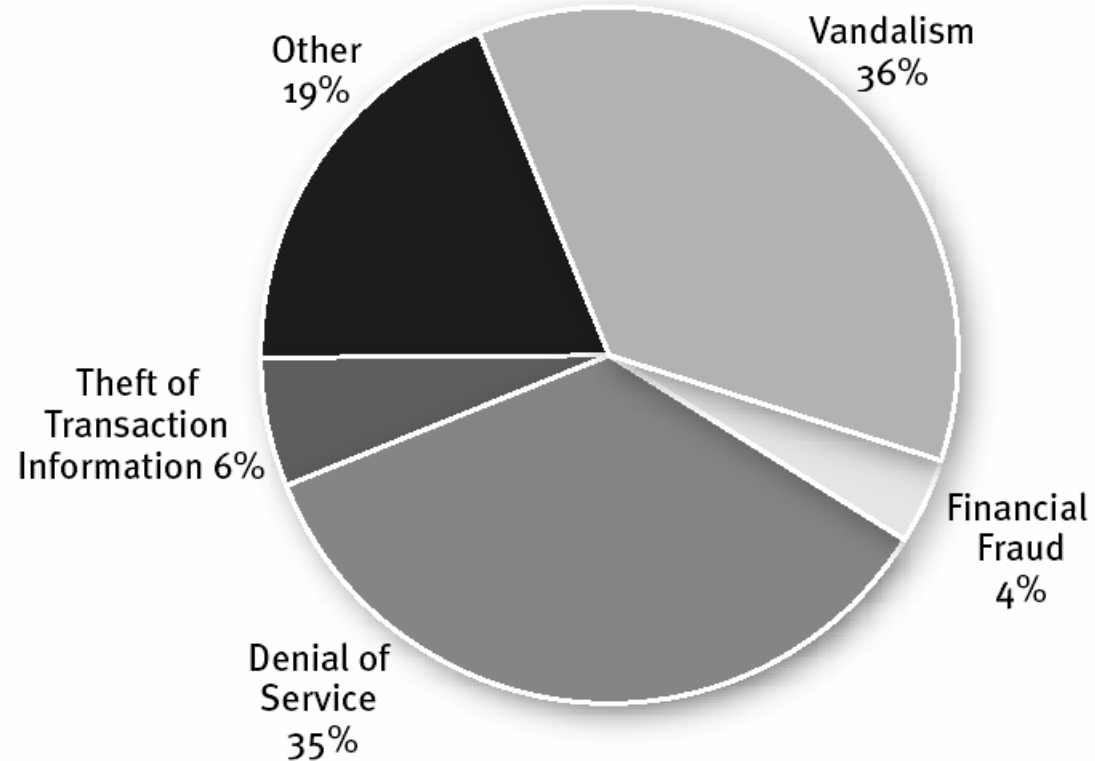
# Attacchi ai siti WEB

## WWW Site Incidents: If Yes, How Many Incidents?



# Attacchi ai siti WEB

## WWW Site Incidents: What Types of Unauthorized Access or Misuse?



CSI/FBI 2003 Computer Crime and Security Survey  
Source: Computer Security Institute  
2003: 185 Respondents/35%

# Miopia dei Media

---

- In generale i media tendono a focalizzarsi sulle minacce più vistose
- **Riportano solo le "nuove" minacce**
  - Quando un attacco diventa comune tipicamente non ne viene più parlato, anche se continua a crescere la minaccia

# Altri dati empirici di attacchi

---

## □ Analisi dei Log dei firewall

- I firewall catturano i pacchetti che appartengono ad un attacco e li annotano in dettaglio in un file di log
- Sono stati analizzati 5.5 miliardi di log in 300 centri per un periodo di 5 mesi
- Sono stati individuati **128,678 attacchi**
  - Tasso annuo di 1000 per centro informatico
- Escludendo i virus/worm, solo il 39% era diretto alla particolare vittima
  - Il resto degli attacchi era random su base IP

## Altri dati empirici di attacchi

---

- ❑ 23% di tutti i centri ha avuto almeno un attacco altamente aggressivo in un periodo di 6 mesi
- ❑ Solo l'1% di tutti gli attacchi erano altamente aggressivi
- ❑ Ma questi erano spesso capaci di fare danni seri

# Altri dati empirici di attacchi

---

## □ SecurityFocus

- Dati di 10,000 utenti nel 2001
- Frequenza degli attacchi
  - 129 milioni di tentativi di network scanning
    - 13,000 per centro
  - 29 milioni di attacchi a siti WEB
    - 3,000 per centro
  - 6 milioni di attacchi di tipo DoS
    - 600 per centro
- Target degli attacchi
  - 31 milioni Windows
  - 22 milioni UNIX/LINUX
  - 7 milioni Cisco IOS
  - Tutti i sistemi operativi sono stati attaccati

# Altri dati empirici di attacchi

---

## □ **U.K. Department of Trade and Industry**

- 2/3 dei centri sorvegliati ha perso meno di 15,000 \$ per i loro peggiori incidenti
- Ma il 4% ha perso più di 725,000 \$

## □ **MessageLabs (antivirus outsourcing)**

- 1 ogni 200 e-mail è infetta
- La percentuale di e-mail infette sono fortemente in crescita

# Altri dati empirici di attacchi

---

## □ **Honeypot project**

- È stato messo in piedi un network per vedere come gli attacchi vengono portati
- Un PC con Windows 98 in rete senza password è stato compromesso 5 volte in 4 giorni
- Un PC con LINUX (con configurazione di default) è stato compromesso 1 volta ogni 3 giorni

## □ **Tranquilli, domani sarà peggio!**

# Prospettive preoccupanti

---

## □ Crescita della frequenza di attacchi

- Gli attacchi cresceranno
  - (e probabilmente anche gli incidenti di sicurezza)
- Negli ultimi anni si è avuto quasi un raddoppio di incidenti ogni anno
  - Fra 5 anni  $2^5$  .....
  - .... speriamo nella saturazione .....
  - .... e nelle protezioni

# Prospettive preoccupanti

---

- Crescita della variabilità nella scelta della vittima**
  - Nel passato c'erano attaccati solo a grossi centri
  - Ora la scelta è molto casuale
  - Non ci si può più fidare della "security through obscurity"
  - Gli attacchi avvengono attraverso la scelta (spesso casuale) dell'IP
    - Casa ..... molto a rischio
    - Piccoli centri ..... abbastanza a rischio
    - Grossi centri ..... ????????

# Prospettive preoccupanti

---

## □ Crescita della malevolenza

- Negli anni scorsi gli attacchi tendenzialmente non erano fatti in modo troppo malevolo
  - Gli hacker cercavano di non fare danni
- Gli attacchi malevoli tendono a diventare la norma
  - I virus e simili spesso creano danni notevoli
  - Sono cresciuti notevolmente i DoS
- Il fatto che l'attacco è remoto porta a una dissociazione tra attaccante e vittima (con i suoi danni)

# Prospettive preoccupanti

---

## □ **Crescita dell'automazione degli attacchi**

- Gli attacchi stanno divenendo sempre più automatici (robot software), piuttosto che diretti individualmente-singolarmente
- Essenzialmente, i virus e simili sono degli attacchi robotizzati che viaggiano attraverso i computer
- Attacco a diversi computer in minuti
- Attacco ad uno stesso centro da molti altri computer nella stessa ora, nello stesso minuto, nello stesso istante

# Attaccanti

---

## Elite Hackers

- **Hacking** è "intenzionalmente accedere o usare un computer senza autorizzazione o al di là dei permessi detenuti"
- Una volta che un hacker è entrato in un computer può
  - Leggere file sensibili
  - Cancellare o modificare file
  - Fare dei cambiamenti al sistema al fine di rendere più facile un attacco in futuro

# Attaccanti

---

## ■ Hacking versus cracking

- Hacking: compiere un lavoro difficile che richiede eccezionale esperienza
- Cracking: accedere in modo illegale

## ■ Eccellenza tecnica e tenacia

- L'hacker non riesce a entrare in un sistema ben protetto velocemente e con facilità
  - ... non è come nei film .....
  - entrare in un sistema ben difeso può richiedere giorni, mesi di duro lavoro

# Attaccanti

---

## ■ White Hat Hackers

- Violano sistemi, ma poi dicono all'amministratore o venditore che il sistema non è sicuro
  - Spesso indicano come prevenire quel tipo di attacco
  - Evitano di fare danni e non estorcono denaro
  - Sostengono di aver lo scopo di aumentare l'affidabilità dei sistemi fornendo notizie sulla vulnerabilità alle compagnie
  - Le compagnie sostengono di non sapere mai cosa essi abbiano fatto realmente nel sistema

# Attaccanti

---

- **Black Hat Hackers**

- Hanno lo scopo di fare danni e non riportano vulnerabilità

- **Gray Hat Hackers**

- Passano da un tipo di hacker all'altro

- **Hacking with a code of ethics**

- Codice di condotta secondo principi etici
  - Motivazione principale: amore per il sapere
  - "non fare danni"
  - Ma vengono cancellati i file di log e disabilitate alcune protezioni

# Attaccanti

---

## Virus e distributori

- Scrivere un virus non è un crimine in molte nazioni
- Per commettere un crimine bisogna *release* (distribuire) il virus
- Tracciare la diffusione del virus è normalmente impossibile
  - I distributori sono spesso solo sospettati
- A volte le pene sono piccole
  - L'autore del devastante virus Melissa del 1999 fu condannato a 20 mesi e una ammenda di 5,000 \$

# Attaccanti

---

## □ Script Kiddies (ragazzini)

- Uso di script di attacco (script kiddies)
- Tendono a scambiarsi tra loro questi script
- Tendono a renderli disponibili ad un grande numero di hacker relativamente poco esperti
- Causano danni anche forti
  - I DoS a CNN.com, eBay.com, Yahoo.com, Amazon.com Dell.com fatti da ragazzini di 15 anni
- Il rumore generato dai script kiddies può mascherare attacchi più sofisticati
- Crescono in letalità anche perché, inesperti, tendono a vandalizzare i sistemi

# Attaccanti

---

## □ Criminali

- Alcuni attaccanti sono una variante degli ordinari criminali
- Furti di carte di credito e di identità
- Furti di segreti industriali
- Spie ingaggiate non solo da aziende concorrenti, ma anche da governi nazionali
- Estorsioni

# Attaccanti

---

## Dipendenti di aziende

- Possono rappresentare un largo danno alla sicurezza aziendale
  - Hanno accessi e conoscenza
  - Si possono verificare
    - Furti finanziari
    - Furti di segreti industriali
    - Sabotaggio
      - Soprattutto da parte di quei dipendenti arrabbiati con l'azienda
    - Creazione di bombe logiche
      - Distruzione di grandi quantità di dati ad una certa data

# Attaccanti

---

## □ Dipendenti di aziende

- C'è spesso la necessità di ricorrere a consulenti e appaltatori, a cui occorre delegare la sicurezza
- Il pericolo può nascondersi tra i dipendenti IT e lo staff della sicurezza

# Attaccanti

---

## □ Cyberterrorismo e Cyberwar

- Costituisce un nuovo livello di pericolosità
- Possibilità di distruzione di infrastrutture
  - Da parte di gruppi sia governativi sia non governativi
  - Attacchi a strutture IT
  - Uso di IT per attaccare infrastrutture IT e le loro infrastrutture fisiche
    - Centrali elettriche, banche...

# Attaccanti

---

## **Cyberterrorismo e Cyberwar**

- **Attacchi multi-pronged (a più punte)**
  - Simultaneo uso di attacchi IT
  - Ognuno basato su differenti metodi di attacco
  - Massimizzano la distruzione e confondono le vittime
- **Cyberterrorismo**
  - Gruppi di terroristi (attivisti)
- **Cyberwar**
  - Governi nazionali

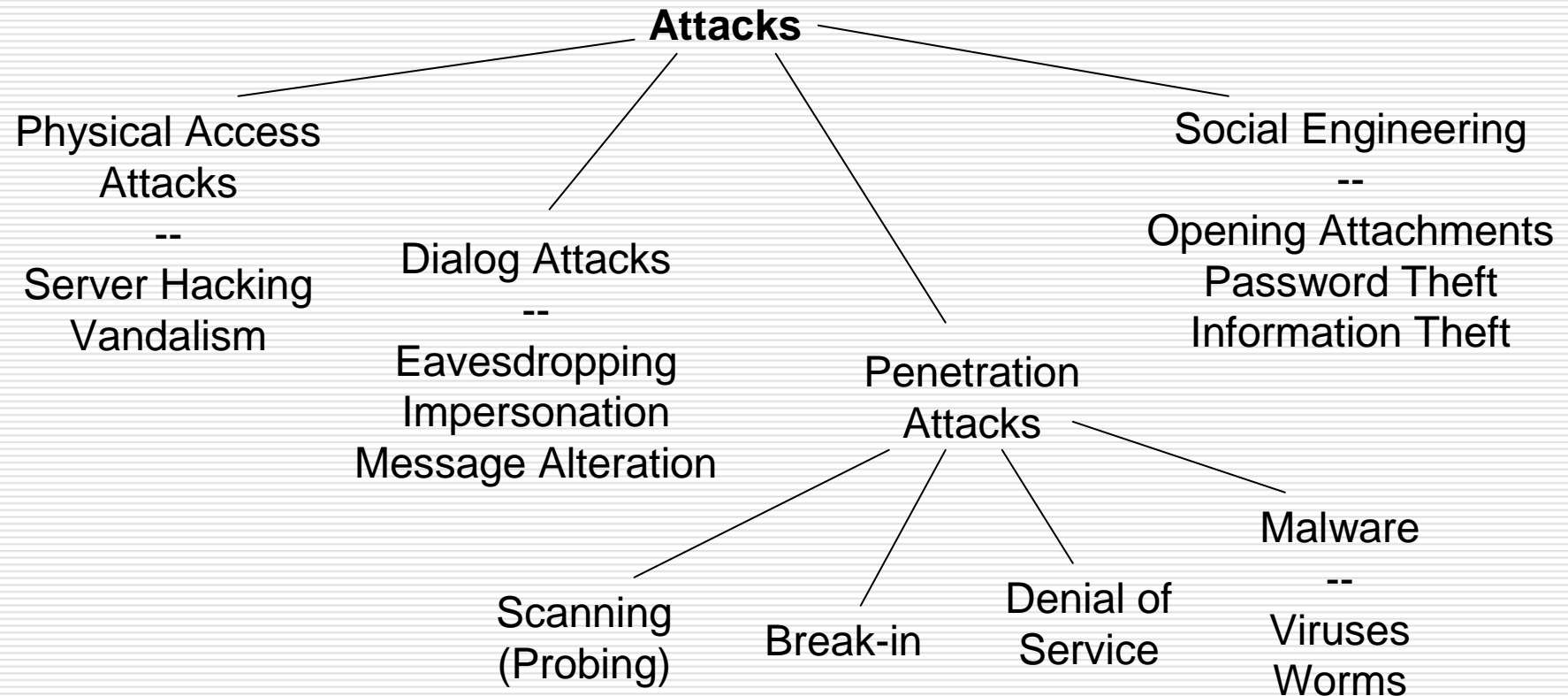
# Attaccanti

---

- Ci sono inoltre dilettanti che fanno una ***information warfare***
  - Dilettanti singoli o a gruppi capaci di provocare gravi danni
  - Rilascio di virus particolarmente dannosi può essere vista come una forma di cyberterrorismo

# Attacchi

---



# Controllo degli accessi

---

- ❑ È la parte essenziale delle strategie e delle pratiche che una compagnia deve usare per prevenire accessi indesiderati
- ❑ Le risorse più sensibili necessitano di un controllo di accesso molto più rigoroso
- ❑ Occorre specificare le tecnologie per il controllo degli accessi e le procedure attivate per ogni risorsa
- ❑ Testare la protezione
  - Senza test sicuri non c'è alcuna protezione
  - È facile commettere errori o tralasciare alcuni aspetti che permettono di aggirare la rete protettiva stesa

# Attacchi non molto diffusi

---

## □ Attacchi di accesso al sito e difesa

- Wiretaps (intercettazioni), in particolare intrusioni in reti LAN wireless
  - Lettura di segnali e inserimento dei propri segnali
- Hacking dei server con accessi fisici
  - Utenti con sufficienti autorità e accesso fisico può installare password cracking software
    - Possibilità di carpire le password

# Attacchi non molto diffusi

---

## Social engineering

- Ingannare un impiegato per ottenere informazioni o compiere un'azione che riduce la sicurezza del sistema o danneggia il sistema stesso
  - Kevin Mitnick
  - È più facile da realizzare di quanto si pensi
- Anche un'e-mail,
  - che promette magari un'antivirus,
  - e invece contiene in attachment un virus
- Chiedere una password spacciandosi per uno che ha il diritto di conoscerla
- Chiedere di inviare un file

# Attacchi non molto diffusi

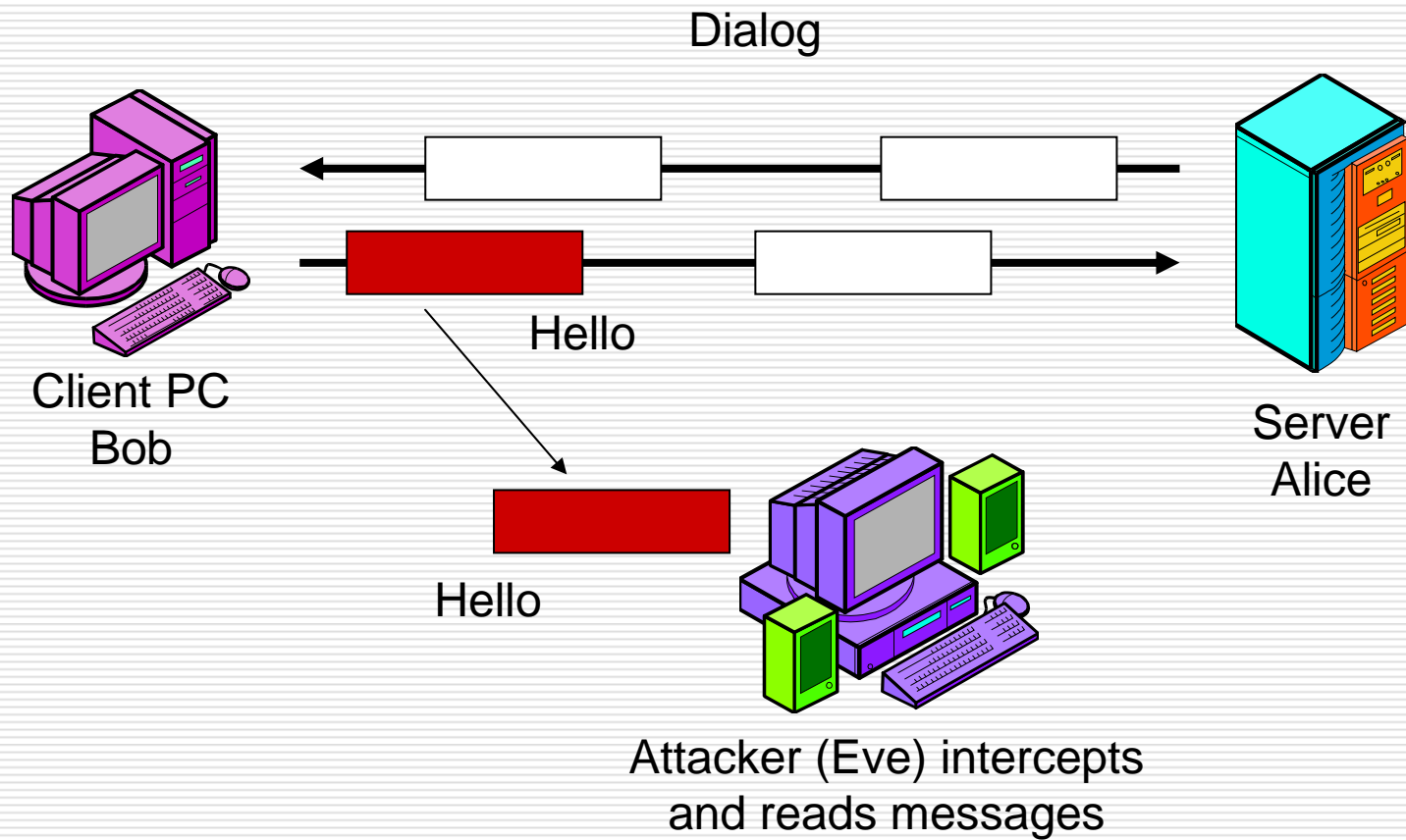
---

## □ Difese contro il social engineering

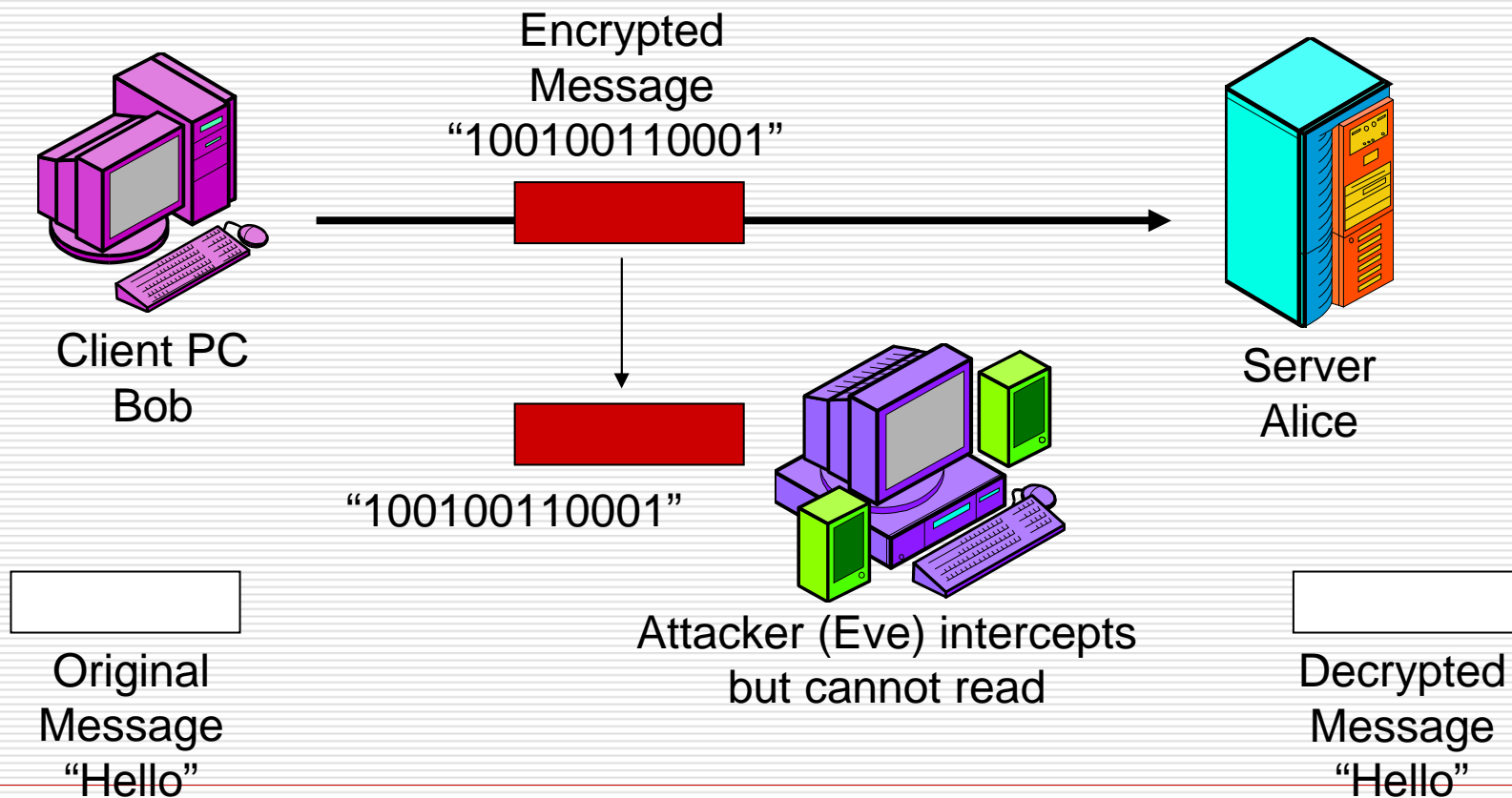
- Training ed educazione
- Rinforzo attraverso sanzioni (punizioni)

# Man in the middle

---

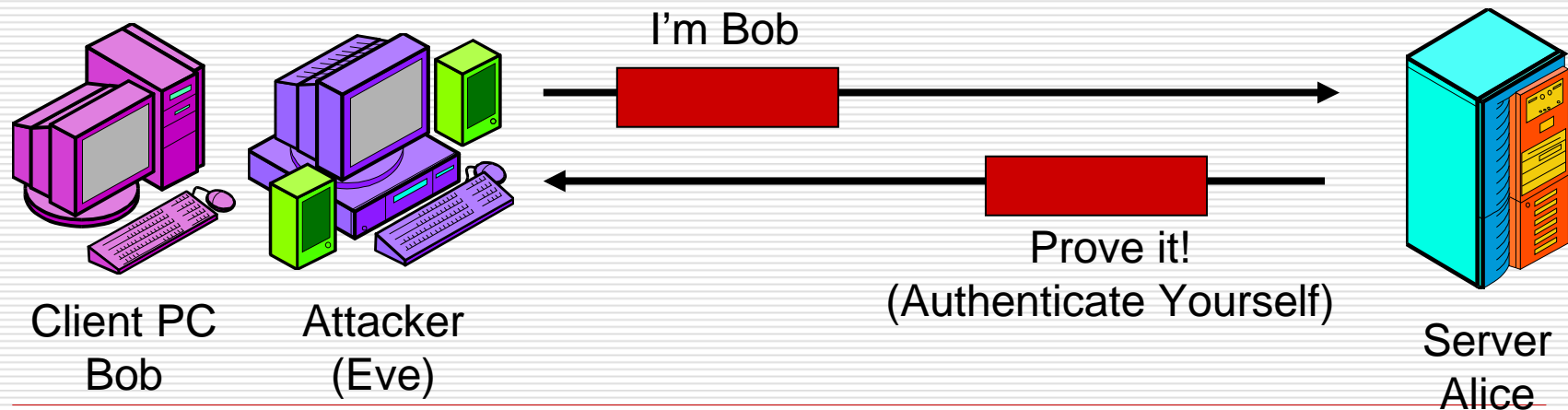


- ❑ **La cifratura è un buona contromisura**
- ❑ **ATTENZIONE:** Catturando e decriptando messaggi cifrati un attaccante può riuscire a ottenere la fiducia incondizionata dei due



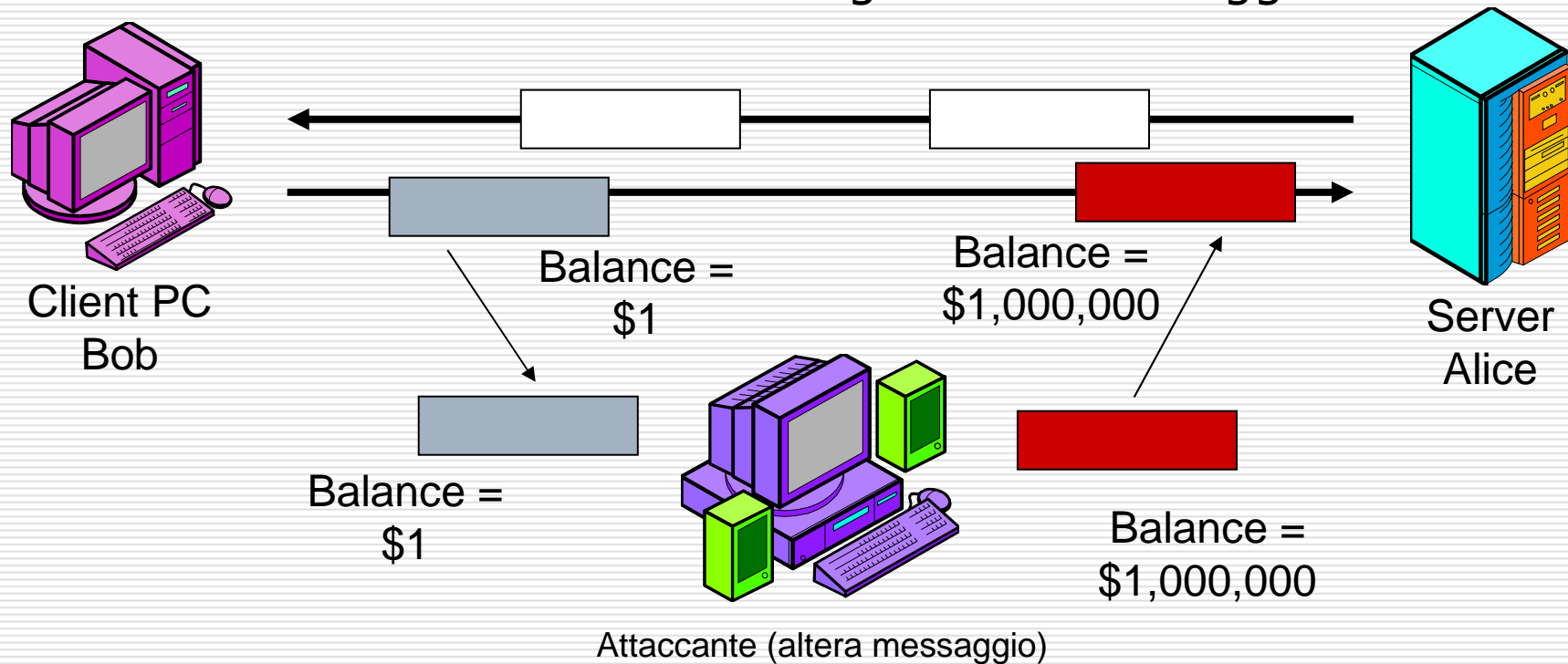
# Impostori e autenticazione

- ❑ Come può Alice essere sicura che la persona che dichiara di essere Bob lo è in realtà
- ❑ Se l'impostore può ingannare Alice, può ottenere da questa informazioni sensibili
- ❑ Alice dovrebbe autenticare le persone che tentano di parlare con lei. Chiedere informazioni che **solo Bob può sapere** o di inserire una particolare smart-card



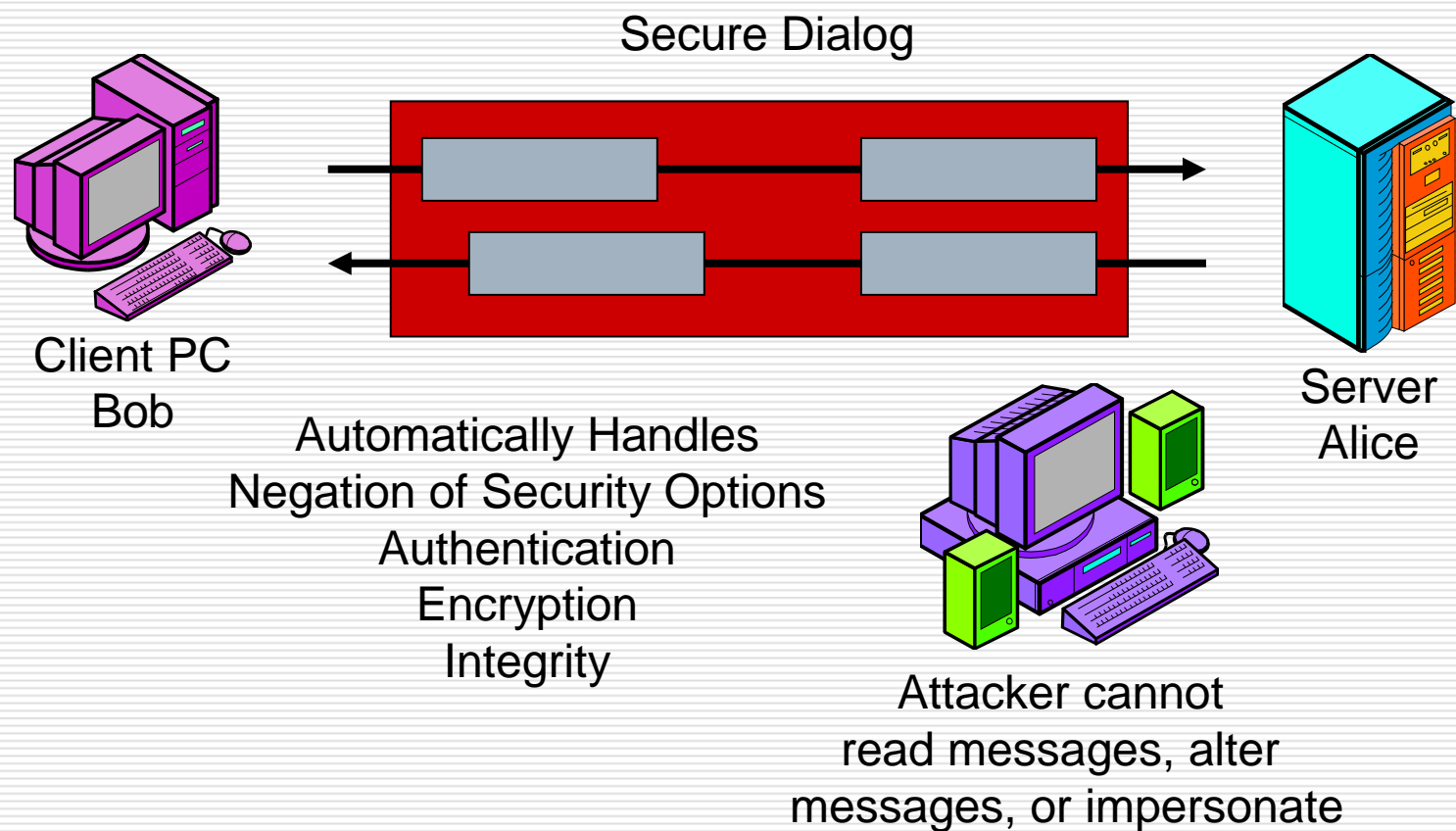
# Alterazione dei messaggi

- Attacco man-in-the-middle
  - Alterazione del messaggio durante il cammino
- Occorre assicurarsi dell'integrità del messaggio



# ■ Sistemi crittografici

□ SSL/TSL, IPsec



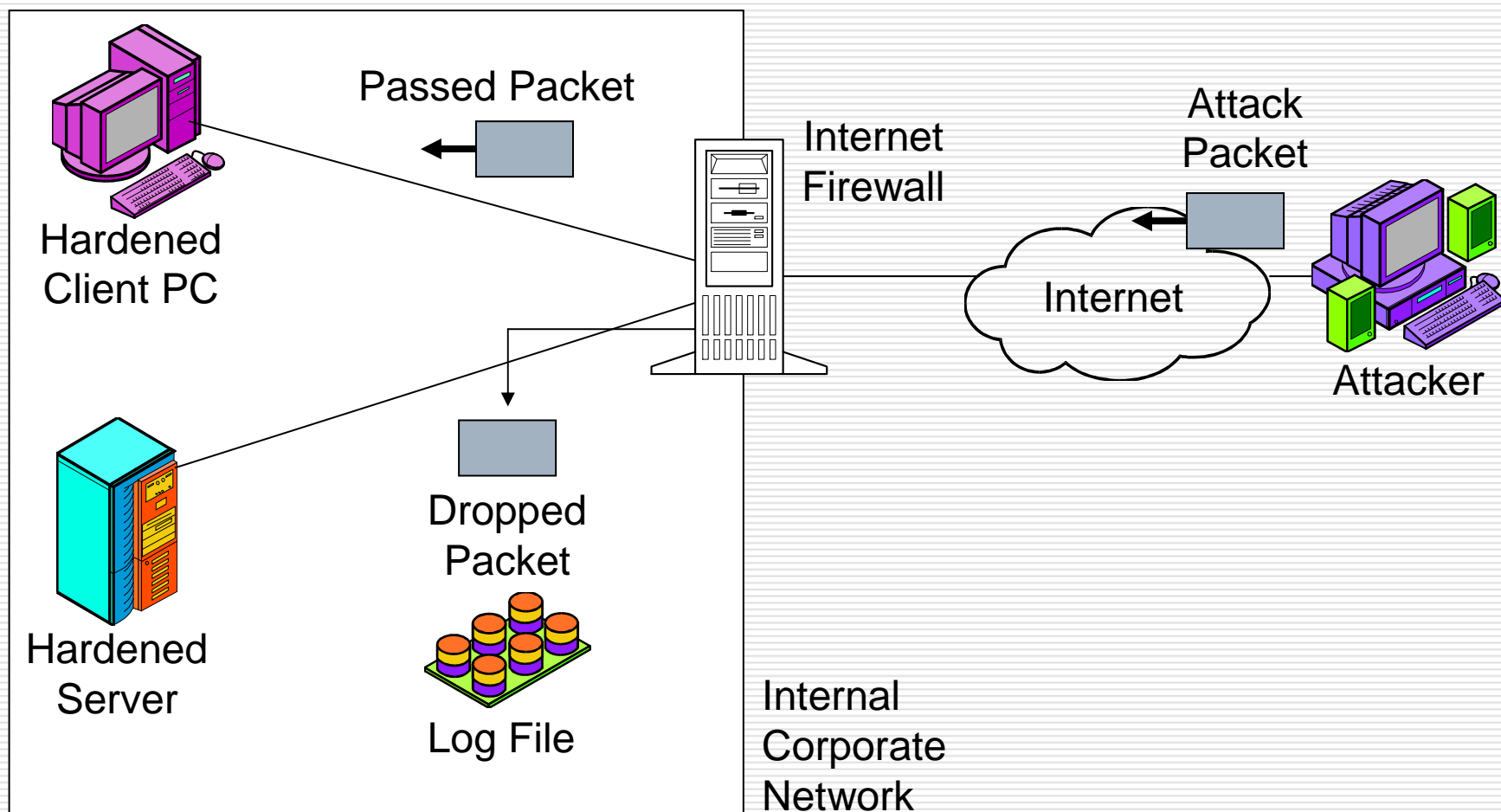
# Accesso non autorizzato e difese

---

## Pericoli di penetrazione

- Attacchi
  - Scanning (sondare)
  - Break-in (irrompere - forzare)
  - DoS
  - Malware (virus e worm)

# Una rete tipica è sicura?

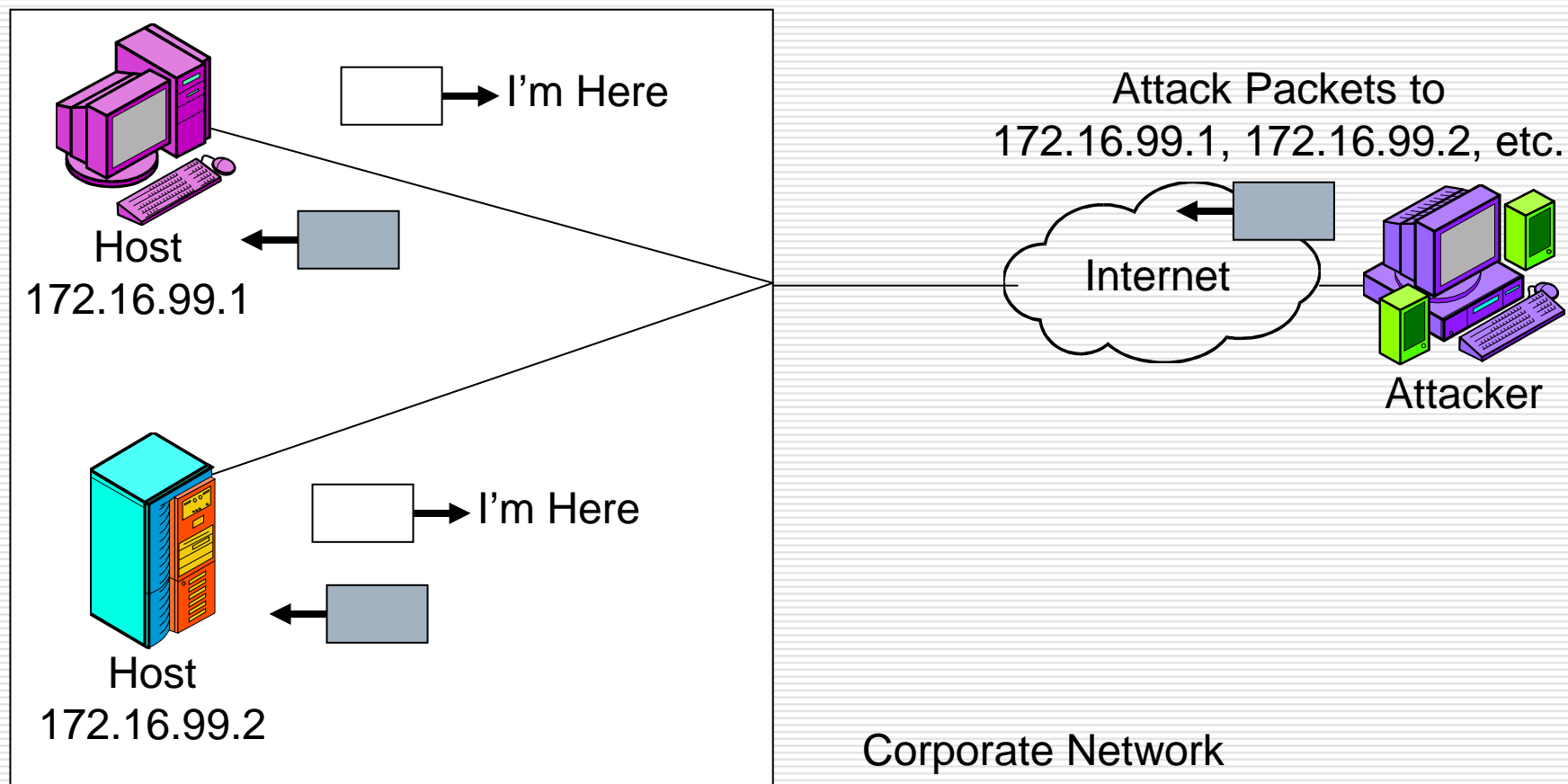


# Security Scanners

---

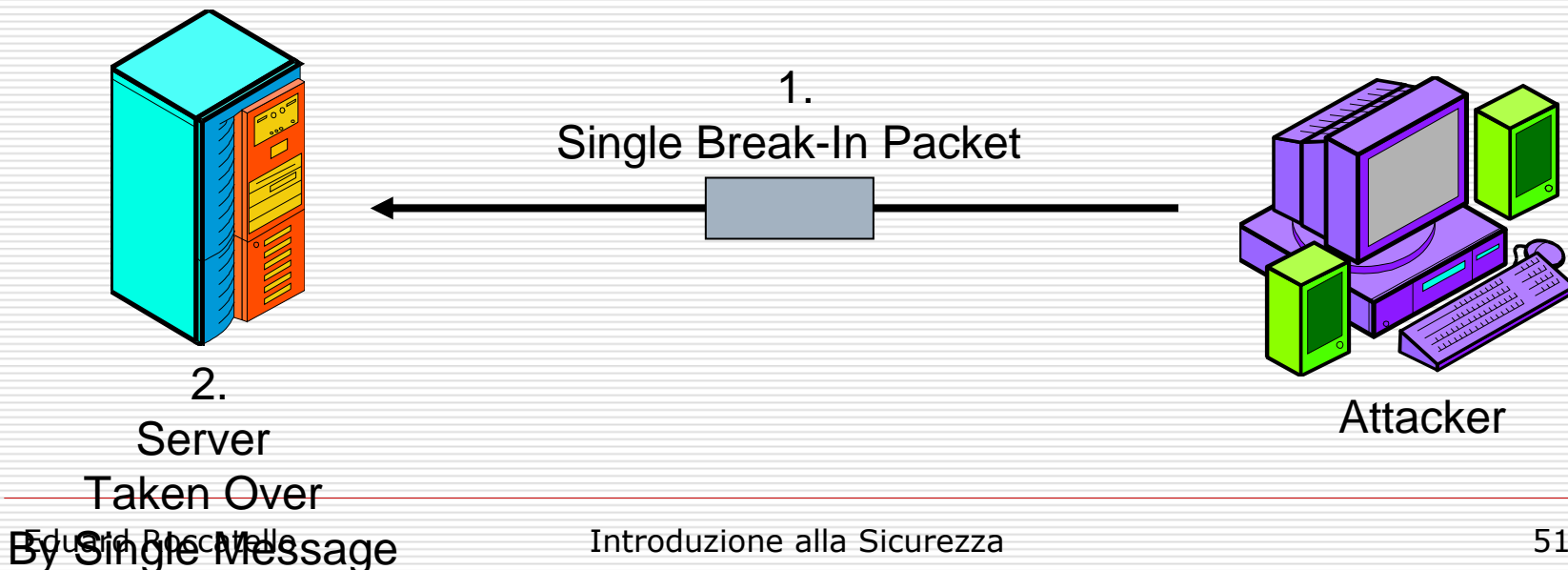
- Costruiti per testare la debolezza dei sistemi
  - Vengono inviati un gran numero di pacchetti di sonda ad una rete aziendale per identificare
    - Indirizzo dei computer
    - Quali servizi sono attivi
    - Vari fingerprints di potenziali vulnerabilità

# Enumerazione delle risorse della rete



# Attacchi Break-in

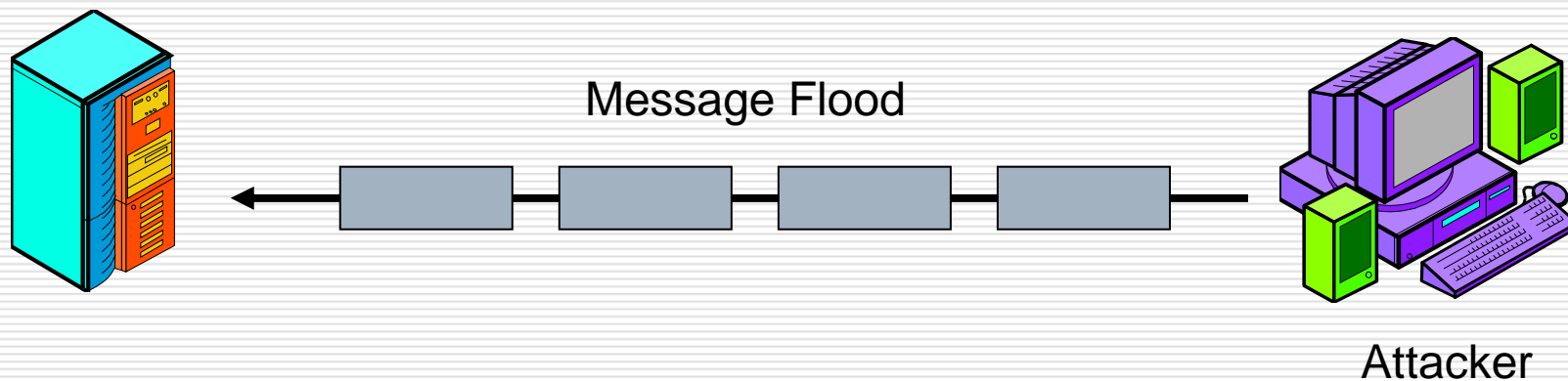
- ❑ Un attaccante può inviare un singolo messaggio che dovrebbe prendere il controllo del computer o fargli eseguire un particolare comando
- ❑ Sono resi possibili dalle debolezze dei sistemi operativi o delle applicativi in esecuzione
- ❑ Può richiedere diverse azioni



# Attacchi Denial of Service

---

- L'attaccante invia un lungo stream di pacchetti di attacco al target
  - Sommergendo il target
  - Annullando la capacità del target di reagire al sovraccarico
- I sistemi non riescono più a servire i clienti



## Malware: virus e worms

---

- Sono armi "*spara e dimentica*"
- L'attaccante semplicemente li invia e questi si propagano attraverso le vittime,
  - senza ulteriori interventi da parte dell'attaccante

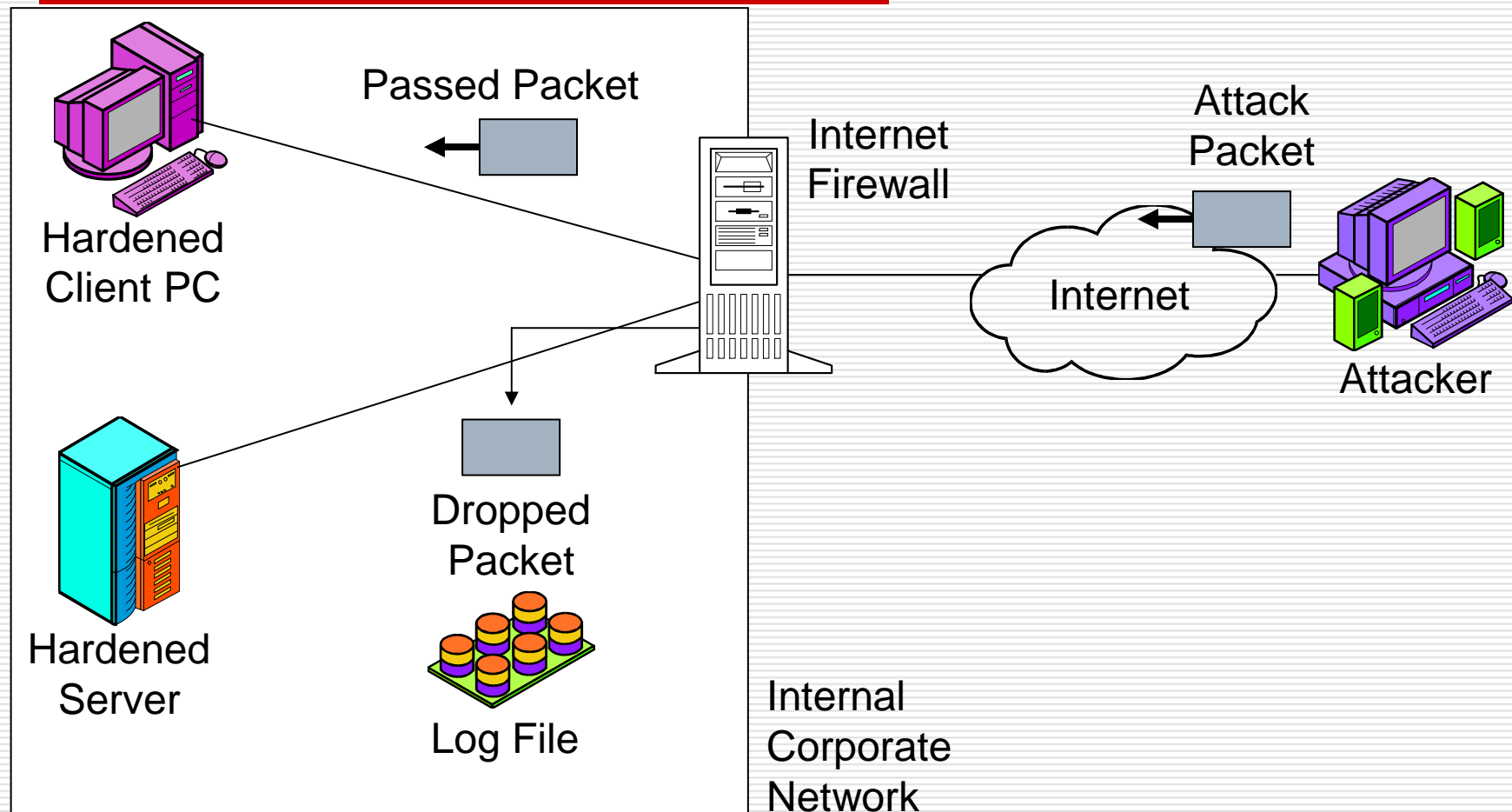
# Difese contro l'accesso non autorizzato

---

## Firewalls

- Sono la prima linea di difesa contro la penetrazione
- Sono particolari computer progettati per
  - tenere i messaggi dell'attaccante fuori della LAN privata
  - permettere ai messaggi di utenti autorizzati di passare all'interno della LAN
- Esaminano ogni pacchetto in arrivo o in partenza
  - Se il firewall riconosce la signature (o pattern, o definizione) di messaggi ritenuti pericolosi elimina il messaggio
  - altrimenti lo immette nella LAN

# Sistemi di protezione: Firewall

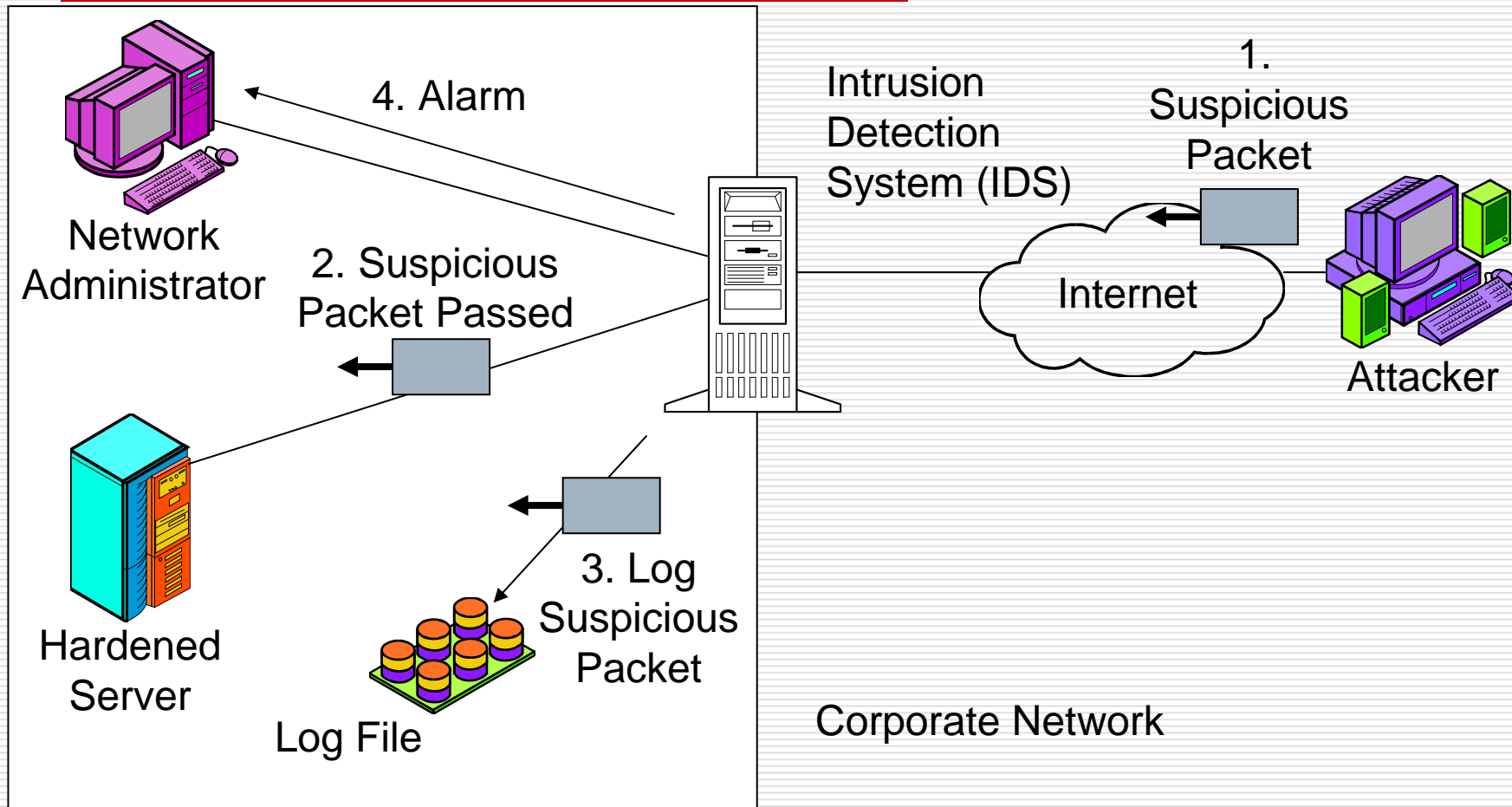


# Intrusion Detection System (IDS)

---

- Un IDS è come un campanello di allarme
- Avverte l'amministratore se riscontra un possibile attacco nascosto nei pacchetti in arrivo
- L'amministratore può prendere dei provvedimenti in modo da rendere inutili i vari tentativi di attacco
- Come un firewall controlla tutti i pacchetti in arrivo o in partenza
  - Ma non compie azioni sui pacchetti
    - Immagazzina i pacchetti per il forensics o per l'analisi dell'amministratore

# Intrusion Detection System (IDS)

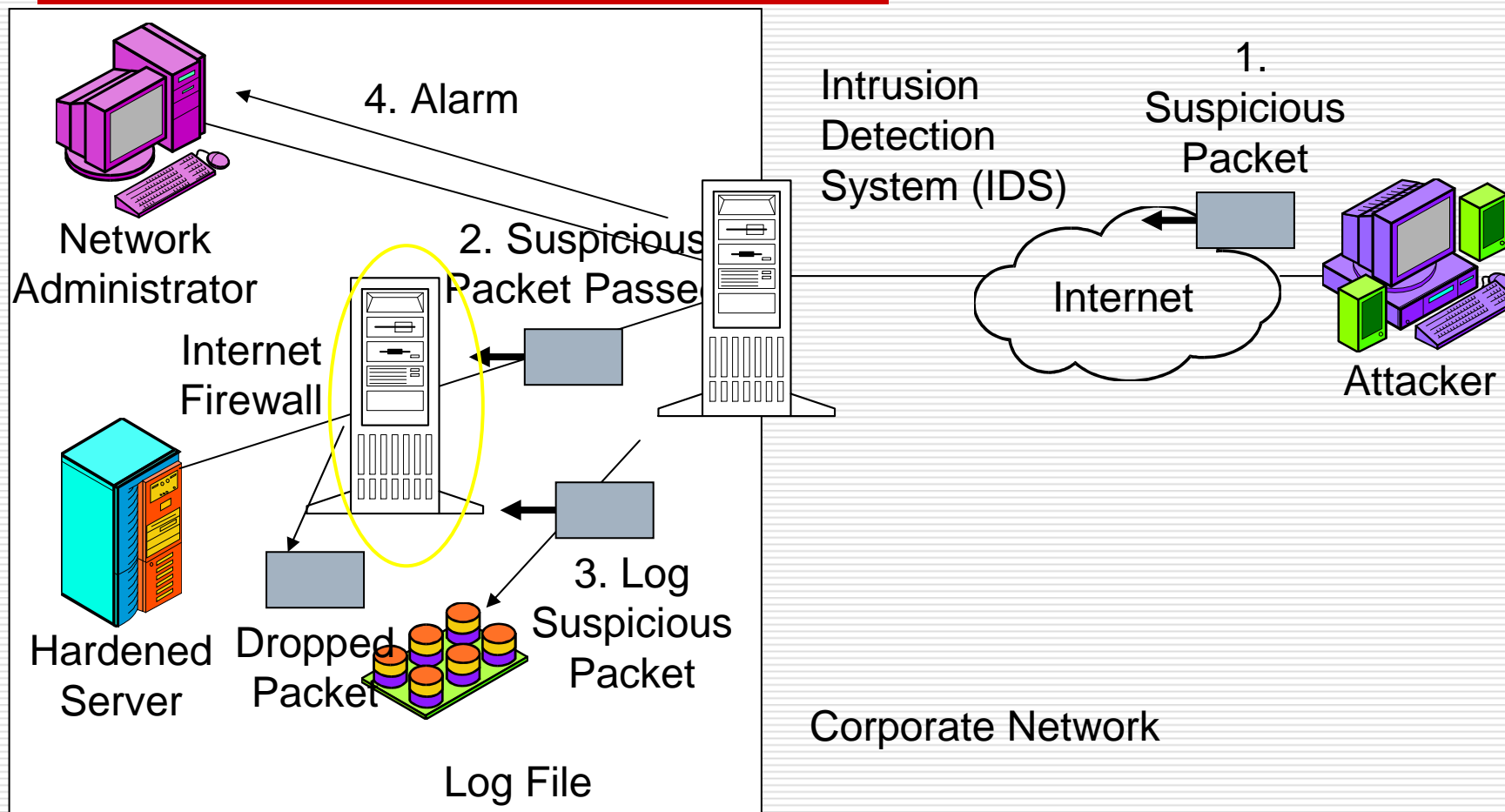


# Firewall contro IDS

---

- ❑ Il dropping dei pacchetti nei firewall viene effettuato solo se si è avuta la violazione di specifiche regole
- ❑ Anche nei IDS c'è l'identificazione dei pacchetti, ma sulla base di semplici sospetti, e che, quindi non possono essere eliminati arbitrariamente
- ❑ La differenza tra i firewall e gli IDS si fa sempre più sottile
  - I firewall cominciano ora a somigliare sempre più agli IDS
  - Gli IDS usano regole euristiche per riconoscere certi tipi di attacchi di penetrazione e prendono iniziative sul dropping dei pacchetti
  - Gli IDS identificano una maggiore varietà (spesso troppo grande) di attività sospetta
- ❑ I firewall e gli IDS sono complementari, e non identici

# Combinazione tra IDS e Firewall



# Irrobustimento dei server: patches

---

- La maggior parte dei server e client vengono installati con configurazione di default che soffrono di vulnerabilità conosciute
  - Note agli attaccanti che li usano per realizzare exploit
- Nuove vulnerabilità vengono trovate ogni giorno
  - È veramente critico installare le patches di sicurezza del venditore
  - Non è la sola cosa da fare, ma se non viene fatta subito sono guai

# Gestione della sicurezza

---

- La sicurezza è prima di tutto un **fatto gestionale**
- Incarico con una gestione dall'alto verso il basso
  - Deve essere presa in carico dalla dirigenza
  - Necessario per ottenere le risorse e le direttive
- **Esecuzione delle operazioni**
  - È critico che tutto lo staff IT esegua il proprio compito bene e **fedelmente**
  - Molti attacchi si avvantaggiano del fatto che si possono formare bolle di vulnerabilità con una **non perfetta** configurazione o con una **non solerte** gestione delle patches
- **Rinforzo**
  - Uso di sanzioni

# Sicurezza globale

---

- ❑ Chiudere **tutte** le vie di possibili attacchi
- ❑ Warfare asimmetrico
  - Vantaggio dell'attaccante
    - ❑ Mentre la compagnia che si difende deve chiudere tutte le vulnerabilità
    - ❑ All'attaccante basta trovare anche una sola debolezza
- ❑ Difesa in profondità
  - Costringere l'attaccante a superare diverse protezioni prima di avere successo
- ❑ Security audit
  - Ingaggiare un team specifico per provare ad attaccare il sistema e verificarne l'effettiva sicurezza

# Raggiungere la sicurezza

---

## **Confidenzialità**

- L'informazione non dovrebbe essere leggibile ad altre persone
- Gli attaccanti non possono leggere messaggi se non riescono ad intercettarli o se non sono intelligibili (ad esempio se sono crittografati)

# Raggiungere la sicurezza

---

## Integrità

- Se l'attaccante cambia il messaggio nel suo viaggio nella rete questo deve essere rilevato

## Disponibilità

- Il sistema deve essere pronto a servire gli utenti
  - Se si ha un attacco DoS contro il sistema non si riesce ad accedere alle informazioni del database,
  - anche se questo è funzionante normalmente

# Plan-Protect-Response (PPR)

---

## Il ciclo Planning

- Necessità di una sicurezza comprensiva
  - Che chiude **tutte** le porte agli attaccanti
  - Basta **una sola debolezza** per mettere in crisi tutto il sistema
- Analisi dei rischi
  - Enumerazione delle minacce (threat)
  - Severità della minaccia
    - Stima del costo del successo nell'attacco
    - Per la probabilità di successo dell'attacco
  - Valore della protezione
    - Severità della minaccia
    - Meno costo delle contromisure
  - Priorizzazione delle contromisure

# Security Planning

---

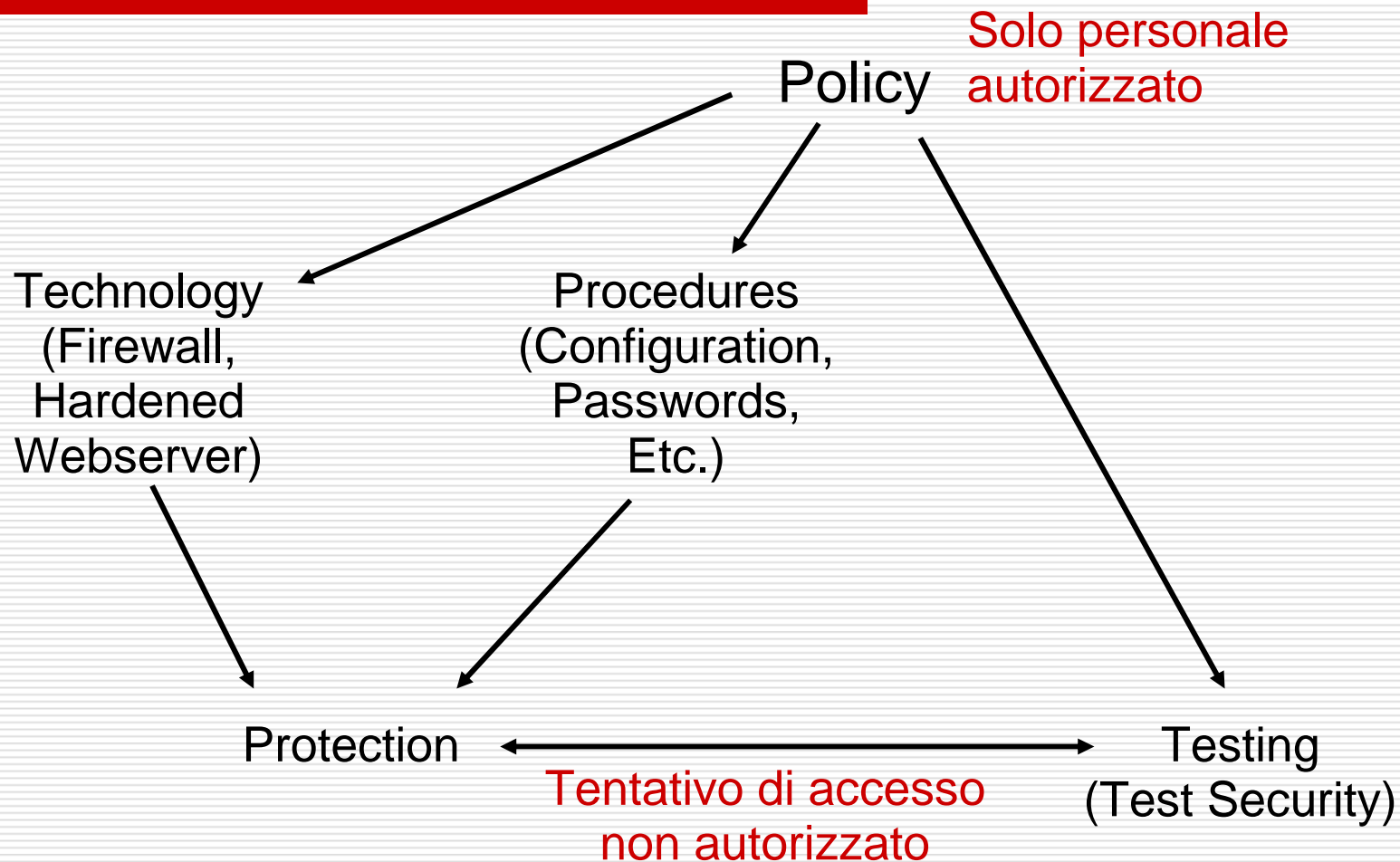
Step	Threat	A	B	C	D
1	Cost if attack succeeds	\$500,000	\$10,000	\$100,000	\$10,000
2	Probability of occurrence	80%	20%	5%	70%
3	Threat severity	\$400,000	\$2,000	\$5,000	\$7,000
4	Countermeasure cost	\$100,000	\$3,000	\$2,000	\$20,000
5	Value of protection	\$300,000	(\$1,000)	\$3,000	(\$13,000)
6	Apply countermeasure?	Yes	No	Yes	No
7	Priority	1	NA	2	NA

# Politiche di sicurezza

---

- Le politiche devono guidare la scelta delle tecnologie
- Le politiche guidano le procedure per rendere le tecnologie efficaci
- Le politiche devono inoltre guidare i test
  - La completa risposta in tutti test è la sola garanzia che le procedure sono state applicate correttamente

# Pianificare una politica di protezione



# Ciclo di Protezione

---

- Installare tutte le protezioni: firewall, IDS, patches
  - L'installazione e la configurazione sono critiche
  - Usare personale specializzato
- Aggiornare continuamente le protezioni
- Testare le protezioni: security audit

# Ciclo di risposta

---

- Pianificare la risposta
  - Una risposta appropriata e rapida non è possibile nella concitazione del momento se non è stata pianificata preventivamente
  - Uso dei CERT (computer emergency response team)

# Ciclo di risposta

---

- Individuazione e determinazione delle cause dell'incidente
  - Procedure per riportare situazioni sospette
  - Determinazione se realmente sia in corso un attacco o qualche applicazione che non va
  - Comprensione dell'attacco per guidare le azioni da intraprendere

# Ciclo di risposta

---

- Contenimento dell'attacco e recovery
  - Contenere (o meglio fermare) l'attacco e provvedere al recovery (riparo del danno)
    - Devono essere fatti in maniera estremamente veloce
    - È estremamente importante aver provato più volte e in pratica le procedure

# Ciclo di risposta

---

## Punizione

### ■ Forensics

- Per determinare eventuali colpe interne

### ■ Perseguire i colpevoli

### ■ Punizione degli impiegati

## Fixing delle vulnerabilità

- Che hanno permesso il successo dell'attacco