
Università degli Studi di Parma
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Corso di Laurea in Informatica

# Sistemi Informativi

# La sicurezza informatica

Giulio Destri

# Dr. Ing. Giulio Destri, Ph.D.

**Professore a contratto di Sistemi Informativi @Università di Parma dal 2003**

**Digital Transformation Advisor, Innovation Manager, Business Coach, Trainer @LINDA**

**Esaminatore ISO27021 e UNI11506-11621 BA (EPBA) @Intertek**

**Membro commissione UNI/CT 526 @UNINFO**

**Blogger @6MEMES di MAPS**

**Certificazioni: ISO27001LA , ISO9001LA, ISO27021, ITILv3 e v4, COBIT-2019, SCRUM Master, EPBA, NLP Coach, NLP AMP**

**https://www.linkedin.com/in/giuliodestri**

**http://www.giuliodestri.it/articoli.shtml**

**giulio.destri@unipr.it**

**twitter.com/GiulioDestri**

# Scopo del modulo

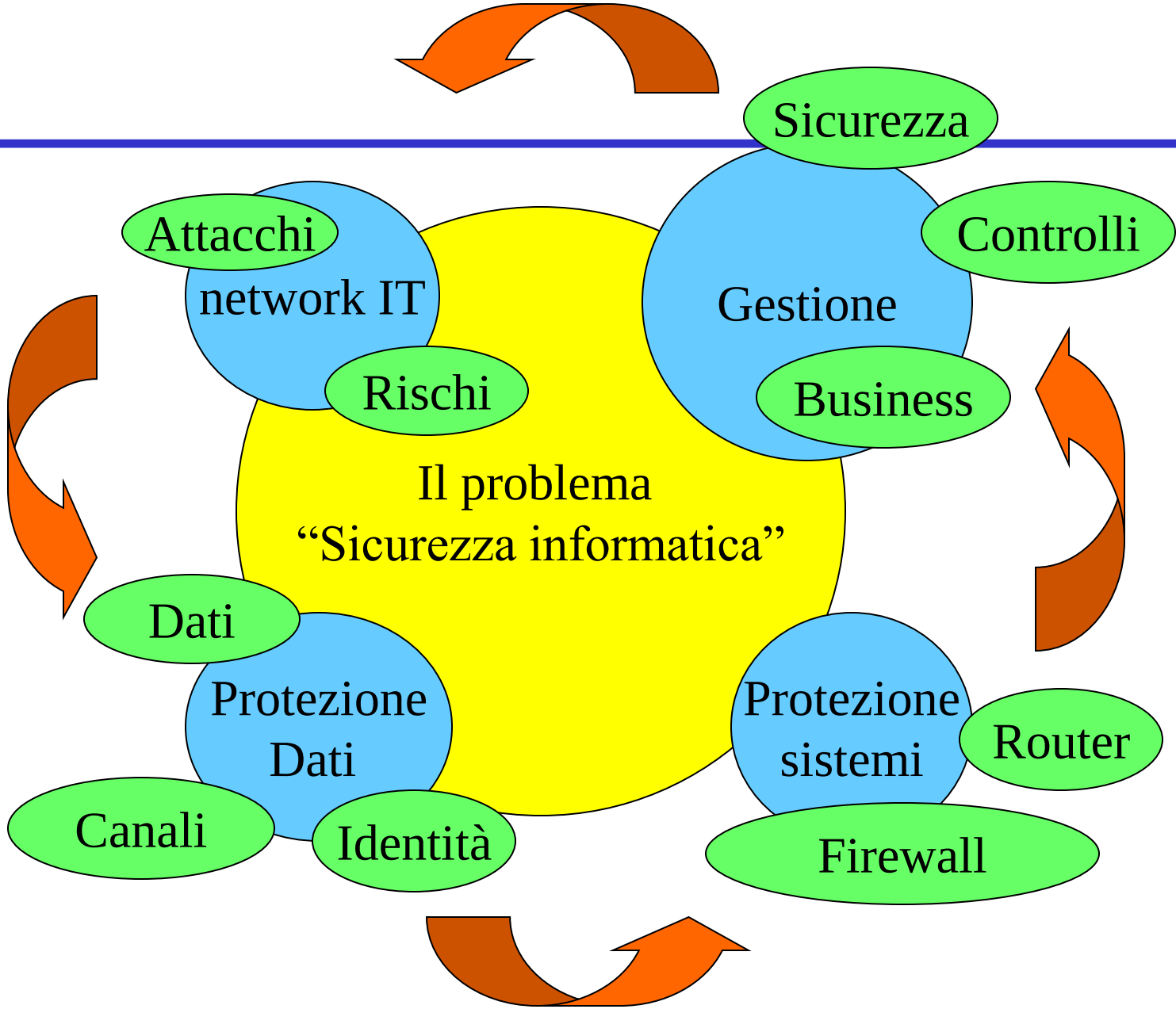
**Definire**

**i concetti base**
**della sicurezza informatica**
**con i più diffusi pericoli**
**e le loro soluzioni**

# Argomenti

- Introduzione alla Sicurezza Informatica
- Problemi da guasti ed eventi naturali
- Le minacce umane alla sicurezza
- La crittografia per la protezione delle informazioni
- L'Identità Elettronica
- La protezione dei dati
- La protezione dei Sistemi
- Gestire la Sicurezza
- ISO 27001 e la legislazione

# Introduzione alla Sicurezza Informatica



# Cronache dall'Aprile 2001

- Furto informatico in Gran Bretagna presso 4 Banche on-line: centinaia di migliaia di steriline il bottino
- Appare un virus completamente multipiattaforma (Windows e Linux)
- Le autorità USA ammettono che hackers si sono introdotti ed hanno ottenuto privilegi di amministratore su sistemi governativi contenenti informazioni riservate

# E’ un mondo difficile…

- Ogni settimana le cronache registrano nuovi attacchi
- Ogni settimana nascono anche nuovi strumenti in ausilio degli attaccanti
- La rapida evoluzione dei sistemi conduce a software non completamente testato in circolazione

# …vita intensa…

- Il problema dell'anno 2000 e l'avvento dell'Euro hanno assorbito la maggior parte delle risorse dei sistemi informatici

- L'avvento di nuove tecnologie (es. Windows2000/XP) pone problemi di aggiornamento

# …e futuro incerto

- Dal 1990 ad oggi la sofisticatezza delle tipologie di attacco non ha fatto che crescere

- Nello stesso tempo, la disponibilità di tool di attacco presso i circuiti degli hacker rende possibile anche a persone con minore competenza di compiere gli attacchi

# Rischi diretti

- Furti
  - Denaro
  - Informazioni
  - Dati sui clienti
- Perdita di produttività
  - Corruzione dei dati
  - Spese e tempo per il ripristino

# Rischi indiretti

- Perdite indirette
  - Potenziali clienti
  - Vantaggi sui propri prodotti
  - Impatto negativo sul proprio brand name
- Esposizioni legali
  - Non rispetto delle clausole di riservatezza
  - Non rispetto delle leggi sulla privacy

# Il ruolo della Sicurezza oggi

- Oggi la sicurezza informatica è una necessità
- Lo sfruttamento delle potenzialità delle reti è anch'esso una necessità per l'Azienda
- Le due esigenze devono convivere attraverso una consapevole politica di gestione

# Servizi e sicurezza

- Sino a poco tempo fa il personale EDP si doveva concentrare solo sui livelli applicativi
- Oggi esso è impegnato a fornire all'azienda tutta una serie di nuove funzionalità
- La conoscenza delle tecnologie di reti e delle basi di sistemi operativi diventa una necessità

# In ogni caso…

- Anche se non «esattamente» sinonimi, CyberSecurity e (IT Security) sicurezza informatica sono legati strettamente fra loro
- Per completezza è bene introdurre i concetti di sicurezza (ICT) diretta e indiretta

# Sicurezza (ICT) diretta

- Tutto ciò che riguarda la prevenzione di attacchi diretti ai sistemi ICT, come ad esempio l'effetto di virus informatici sul nostro PC di casa o sul server aziendale contenente i dati della contabilità.

# Sicurezza (ICT) indiretta

- La prevenzione dell'uso di sistemi ICT come strumento ponte per condurre un attacco verso altri apparati che sono connessi a tali sistemi e anche (almeno in parte)
- La prevenzione che problemi nei sistemi ICT, dovuti magari ad eventi casuali, possano estendersi agli altri apparati connessi.

# Sicurezza IT

- Sicurezza dei sistemi IT
- Obiettivi:
  - Proteggere i sistemi
  - Proteggere i dati in essi contenuti

# Sicurezza OT

- Sicurezza dei sistemi OT
- Obiettivo primario:
  - Garantire la continuità di servizio

# I sistemi informatici sono complessi

"L'Informatica non è una scienza esatta
e il Computer non funziona in modo
deterministico"

Antico Proverbio della Facoltà di
Ingegneria di Bologna

# Problemi da guasti ed eventi naturali

# Sicurezza rispetto ad eventi fortuiti

Garantire la sicurezza rispetto ad eventi fortuiti (rotture, guasti, corti circuiti, disastri naturali…) significa descrivere le tecniche di salvaguardia dei dati che li difendono da guasti tecnici accidentali o danneggiamenti fisici subiti dai sistemi

# Vulnerabilità IT: esempi

- Vulnerabilità dovute alla collocazione geografica del sistema informatico (es: terremoti, inondazioni…)
- vulnerabilità dovute a errori sistematici presenti nell'hardware o nel software (errori di progettazione)
- vulnerabilità dovute a possibili malfunzionamenti accidentali dell'hardware,
- vulnerabilità dovute a deficienze nelle procedure di utilizzo da parte degli utenti.

# Vulnerabilità IT: gruppi

- Ambientali e geografiche (eventi naturali)
- Da progettazione
- Da realizzazione
- Da mancato test / mancati controlli
- Da errori / debolezze in componenti software
- Da errori / malfunzionamenti hardware
- Da malfunzionamenti infrastruttura
- Da attacchi deliberati (virus compresi)

# Vulnerabilità IT: le cause

- Le caratteristiche del sistema, la sua collocazione, il livello di competenza degli utenti concorrono a determinare un elenco di vulnerabilità.

# Gli eventi accidentali

- In un contesto di sicurezza informatica è opportuno trattare anche le problematiche legate ad eventi accidentali
- Esistono leggi che regolamentano la protezione dei dati dalle perdite accidentali
- Talvolta queste tecniche sono un'ottima risposta anche a problemi legati ad azioni fraudolente umane

# I punti critici  dei sistemi

- I sistemi operativi non sempre sono sufficientemente robusti rispetto a condizioni operative non infrequenti
- Le macchine hanno parti meccaniche soggette ad usura (ventole, dischi etc…)
- La componentistica elettronica può presentare dei problemi
- Gli utenti non esperti possono commettere errori nell'uso dei sistemi

# Il problema della complessità

- Vecchi e nuovi bug software
- Modularizzazione del software
- Interconnessione dei programmi
- Comprensione da parte dell'utente
- Effetti dell'installazione di nuovi software/release

# I dati: l'anima dei sistemi

Cosa si intende per "dati"?

- Contenuto di DB relazionali
- Archivi documentali/multimediali
- Micro applicativi (es. generatori report)
- DB personali (es. elenco indirizzi)
- Archivi di Directory Service
- Configurazioni dei programmi e delle postazioni di lavoro

# I dati: l'anima dei sistemi - 2

- In un sistema fortemente centralizzato tutti i dati risiedono o nel DB o, comunque, entro file sui dischi del server
- In un sistema distribuito i dati sono ripartiti su più server e hanno una forma molto varia
- Spesso poi ci sono dati importanti "sparsi in giro" per i client

# Salvaguardia dei dati: il backup

- Per la conservazione dei dati è necessario centralizzare la raccolta dei file almeno su server dipartimentali
- Un backup automatico dei dischi dei client (es. sfruttando le condivisioni di dominio) diventa rapidamente ingestibile
- Gli utenti devono procedere alla salvaguardia dei propri dati

# Il backup

- Cosa si deve salvare?
- Quanto è grande la mole di dati?
- Con che frequenza?

# Il backup - 2

- Incrementale o alle differenze
- Totale
- Politica di salvataggio (es. giorno/settimana/mese)

# Il backup: i supporti

- Nastro DAT (8-24 GB)
- Nastro DSS (40 GB)
- Nastro VHS (24 GB)
- Altri nastri
- CD, DVD ROM
- Disco estraibile
- Flash memory Pen
- Dischi distribuiti
- NAS
- Cloud

# Archiviazione dei dati

- Riordino dei dati secondo schemi prestabliti
- Suddivisione su più supporti
- Conservazione dei supporti

# Il backup dell'Immagine

- La fase di installazione e configurazione di un sistema assorbe molto tempo
- Client: installazione OS, MS-Office, Client prog. Contabilità, client tn5250…

- Server: installazione di tutte le parti
- In funzione dello scopo del sistema (es. piattaforma di amministrazione)

# Il backup dell'Immagine - 2

- In funzione dello scopo del sistema (es. piattaforma di amministrazione) si definiscono tutti i componenti software della dotazione base
- Con un programma con Norton Ghost o DiskImage si crea una "immagine" dell'installazione
- In caso di problemi si ripristina la configurazione base

# Il fermo macchina

- In un sistema aziendale, ogni periodo di ferma provoca una perdita economica più o meno grave
- Un certo tempo di fermo macchina può essere fisiologico
- In ogni caso si deve minimizzare tale valore

# Necessità

- Minimizzare i periodi di fermo macchina
- Salvare i dati
- Salvare le configurazioni
- Salvare le installazioni
- Archiviare dati di uso non frequente

# Le minacce umane alla sicurezza

# Gli attacchi: argomenti della sezione

- Scopo degli attacchi
- Il profilo dell'attaccante
- Classificazione degli attacchi
- I punti di vista: sistemi e reti
- I Virus

# Classificazione degli attacchi

- Intrusione
- Impersonificazione
- Intercettazione (es. Sniffing)
- Abuso (es. spamming)
- Denial-of-service (es. sovraccarico)
- Il ruolo dei Virus

- Social Engineering

# Obiettivi di un attacco

- Accedere a dati riservati
- Assumere un'identità
- Effettuare transazioni finanziarie fraudolente
- Usare risorse senza averne diritto
- Mandare fuori servizio un sistema
- Mostrare al mondo quanto si è bravi entrando nei sistemi altrui

# Accesso a dati riservati

- Entrare in un DB
- Entrare in un archivio di posta e/o documenti
- Entrare in un filesystem
- Entrare in un directory service
- Impadronirsi di indirizzi di posta
- Impadronirsi di un archivio di chiavi e/o password

# Assumere un'identità

- Entrare in un sistema con privilegi non propri
- Potere usare a scrocco servizi non propri
- Vedere dati non propri (si ricade nel caso precedente)
- Accedere a risorse finanziarie non proprie
- Fare uno scherzo

# Transazioni finanziarie fraudolente

- Rubare il codice carta di credito
- Rubare codici per l'accesso Home Banking
- Attaccare direttamente sistemi bancari
- Usare codici validi per accedere a un sistema e poi assumere privilegi non propri
- Azioni interne ai sistemi
- Impersonificazione di sistemi

# Abuso di risorse

- Accesso alla rete esterna
- Uso di servizi in modo contrario alle regole
- Spamming
- Uso dei server come ponte per attacchi a terzi

# Denial-of-Service

- Bloccare un servizio (programma server)
- Bloccare un server (computer server)
- Bloccare la rete
- Bloccare/alterare il DNS

# Chi è l'attaccante?

- Hacker
- Cracker
- Spia industriale
- Sabotatore
- Impersonale
- Virus

# Le vulnerabilità dei sistemi

- Vulnerabilità dei dati
- Vulnerabilità dei programmi applicativi
- Vulnerabilità dei programmi server
- Vulnerabilità dei sistemi operativi
- Vulnerabilità dei sistemi fisici
- Vulnerabilità delle trasmissioni

# Intrusione in un sistema

- Accesso non autorizzato ad un servizio disponibile in un server
- Connessione di terminale remoto (tipico UNIX)
- Ingresso sul disco (tipico Windows)

# Classificazione tecnica “tradizionale”

- Attacchi alle password
- Attacchi alla sicurezza di  reti e pacchetti
- Attacchi che sfruttano file di accesso privilegiato
- Attacchi al protocollo IP

# Classificazione tecnica “tradizionale” - 2

- Attacchi all’organizzazione aziendale
- Attacchi basati sulla previsione di sequenze di numeri
- Attacchi per il dirottamento di sessioni
- Attacchi alle librerie condivise
- Attacchi che sfruttano vulnerabilità tecnologiche

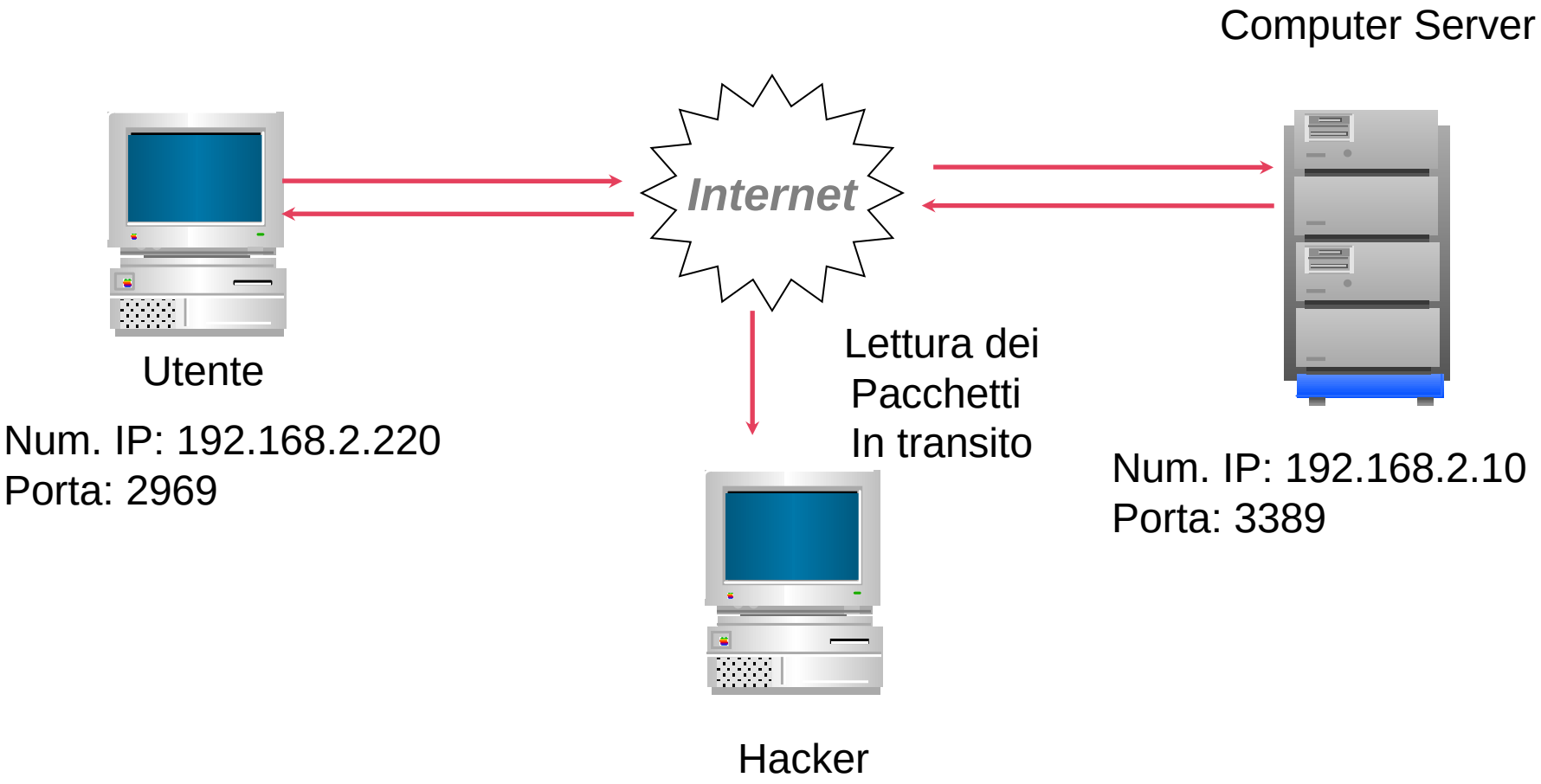
# Attacchi alle password

- Tentativi successivi
- Attacchi a dizionario
- Numero massimo di tentativi
- Tentativo di cattura dei file delle password

# Attacchi alle reti

- Intercettazione dei dati in transito
- Packet Sniffing
- Analisi di quanto intercettato

# Attacchi alle reti



# Attacchi ai file di accesso privilegiato

- Tipici dei sistemi UNIX
- Sfruttano le possibilità di login automatico dei file di privilegio
- Consentono, una volta entrati in un singolo server, un accesso a tutta una rete

# Attacchi al Protocollo IP

- Sfrutta le proprietà di basso livello di IP
- IP Spoofing
- Consiste in pratica nell'assumere l'identità di un computer facente lecitamente parte di una rete
- E' piuttosto facile da prevenire

# Attacchi all'organizzazione aziendale

- Un attaccante, fingendo di essere un responsabile di rete, invia mail o telefona ad un utente
- "Social Engineering"
- Prevenzione con procedure rigorose

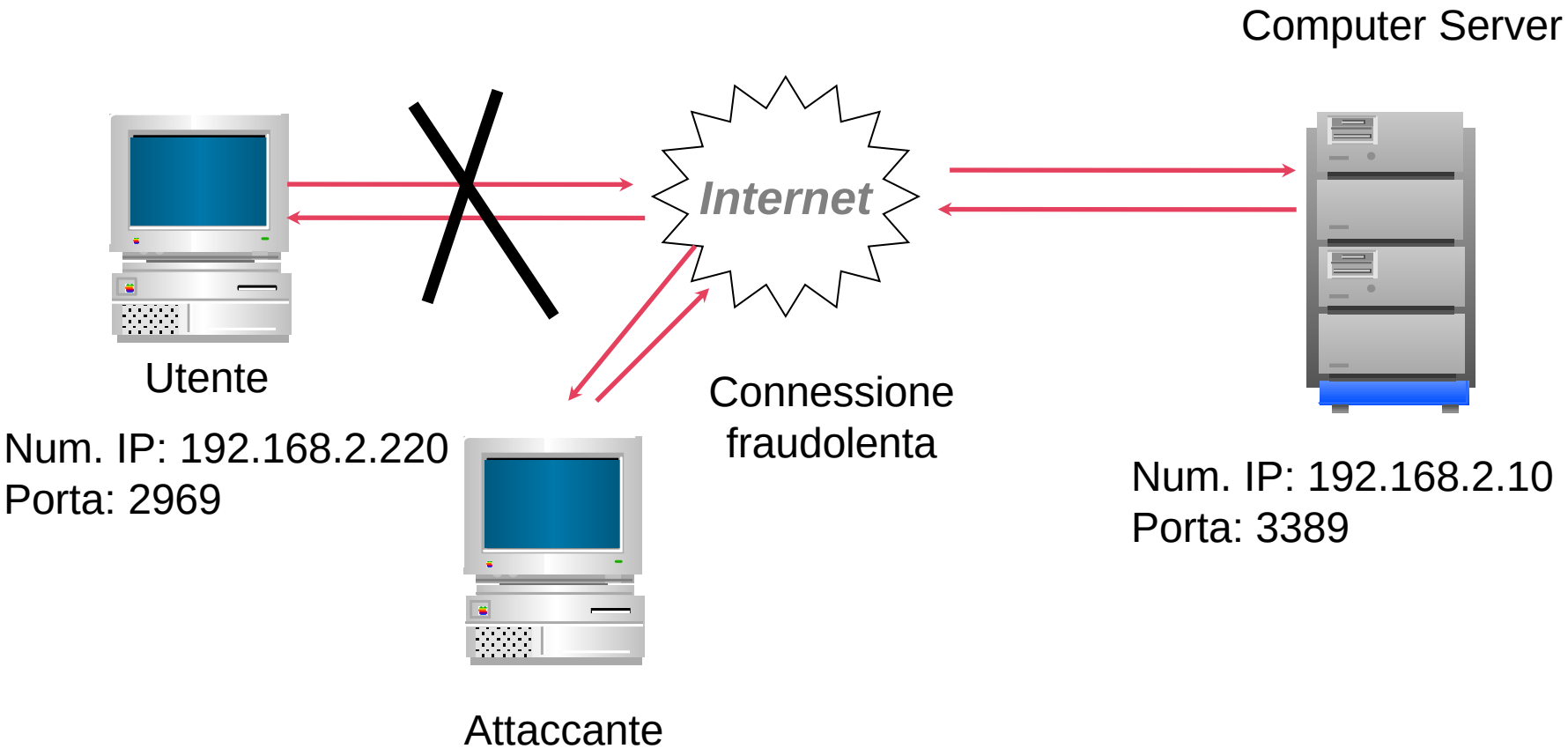
# Previsione di sequenze di numeri

- Tipica del mondo UNIX
- Studio della fase di connessione di sessioni legittime entro la rete
- Individuazione dell'algoritmo di generazione dei codici
- Riproduzione ed ottenimento di una sessione non lecita

# Dirottamento di sessioni

- Prevede lo sniffing della rete
- Individuazione dei dati di una connessione legittima
- Sostituzione dell'attaccante all'utente connesso

# Dirottamento di sessioni



# Attacchi alle librerie

- Una libreria condivisa è un gruppo di funzioni comuni a uno o più programmi
- Nel mondo Windows sono le DLL, nel mondo UNIX i file .so
- Sostituzione di una libreria con un file "arricchito" da istruzioni relative agli scopi dell'attaccante

# Vulnerabilità tecnologiche

- Quasi tutti i sistemi operativi e gli applicativi presentano delle vulerabilità
- I casi più frequenti verranno esaminati in seguito

# Attacchi tipici

- Attacchi ai programmi server TCP/IP
- Attacchi alla Posta Elettronica
- Attacchi al mondo Web
- Attacchi diretti ai sistemi operativi
- Attacchi ad una rete

# Attacchi diretti a programmi server TCP/IP

- Un programma server TCP/IP è un applicativo che apre un server socket su una data porta IP e si pone in attesa di connessioni IP (ascolto)
- Una volta stabilita la connessione il client invia un certo numero di byte al server (richiesta), che risponderà con una stringa di byte e così via

# Attacchi diretti a programmi server TCP/IP

- Sia i protocolli tipici di Internet (HTTP, FTP, SMTP ecc…) sia quelli proprietari si basano per il loro funzionamento su scambio di stringhe di byte fra client e server
- In alcuni casi sullo stesso socket passano sia comandi sia dati, in altri casi (es. FTP) i dati e i comandi viaggiano su canali separati

# Attacchi diretti a programmi server TCP/IP

- Ma cosa accade se da parte del client vengono inviati più byte di quanti preveda il protocollo o sequenze non corrispondenti a comandi previsti?
- In alternativa, se apro 1000 o 10000 connessioni contemporanee con un servizio, il computer server che lo ospita è in grado di sopportarle?

# Il Buffer Overflow

- Invio ad un server TCP/IP di un numero di byte superiore al previsto
- I byte ricevuti in più "sfondano" i confini dell'area di memoria riservata e "passano" in altre parti del programma o addirittura oltre il programma stesso
- Nella parte "in più" vengono inseriti comandi binari che il programma server interpreta o "passa" al sistema operativo

# Esempi di Buffer Overflow

- Il programma SendMail (il primo server SMTP) è stato nominato “il più bacato della storia” per i buffer overflow
- Inviando comandi opportuni ai primi server di questo tipo era possibile ottenere una sessione di root su macchine UNIX

# Esempi di Buffer Overflow

- La prima versione del modulo TCPBios delle macchine Windows95 era molto vulnerabile al buffer overflow
- Inviando un pacchetto di dimensioni opportune sulla porta 139 di un PC Windows95 era possibile provocarne il blocco immediato
- Il problema è stato corretto rapidamente in uno dei primi SP

# Invio di comandi non previsti

- Questo tipo di attacco è tipico nel mondo Web
- Consiste nell'inviare pacchetti di lunghezza lecita, ma contenenti comandi/stringhe non previste dal protocollo
- Può condurre al blocco del servizio o del sistema (es. ping of death)

# Attacchi alla Posta Elettronica

- La posta elettronica di Internet (o delle Intranet) usa il protocollo SMTP o il suo successore ESMTP

- Un server E-mail, oltre agli attacchi dei tipi visti prima, è esposto a una serie di attacchi tipici

# Attacchi alla Posta Elettronica - 2

- Overflow
- Spamming
- Impersonificazione e-mail

# Mail Overflow

- La capacità delle caselle di posta è, di solito, limitata
- Inviando alcuni messaggi particolarmente voluminosi si può arrivare a saturare tale capacità
- Il sistema risulta incapace di accettare nuove mail sinchè non viene vuotata la casella

# Spamming

- Ogni server di posta può comportarsi da relay, ossia da instradatore per posta non a lui direttamente destinata, come un ufficio postale
- Se non vengono inseriti adeguati controlli un server di posta può venire usato per invio di posta non autorizzata (spamming)

# Mail anonime o impersonificate

- Nella versione base il protocollo dell'e-mail non verifica l'indirizzo del mittente
- Connettendosi a un server e-mail e dando i comandi opportuni si possono inviare mail anonime o a nome del mittente voluto
- Esistono programmi in grado di rendere facilissima questa operazione

# Gli Attacchi ai server Web

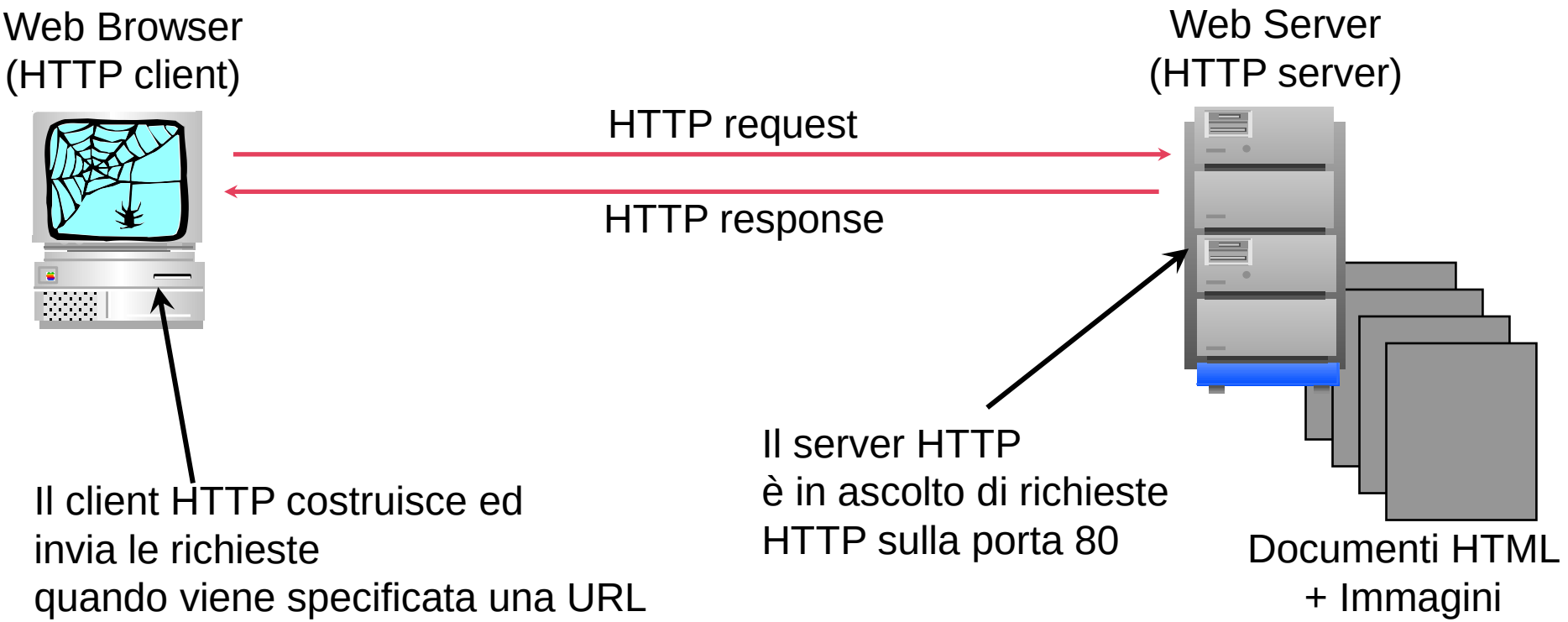
- Il servizio Web è forse il più diffuso su Internet
- L'avvento del Web dinamico e delle applicazioni Web ha reso ancora più grave il problema degli attacchi a server Web

# Il protocollo HTTP

- HyperText Transport Protocol
- Protocollo applicativo, orientato al trasferimento di file/dati
- E' stateless (senza stato)
- Rigidamente client-server
- Ogni richiesta del client apre una connessione, che viene chiusa dal server a richiesta esaudita o su errore

# Il protocollo HTTP - 2

HTTP è un protocollo request/response



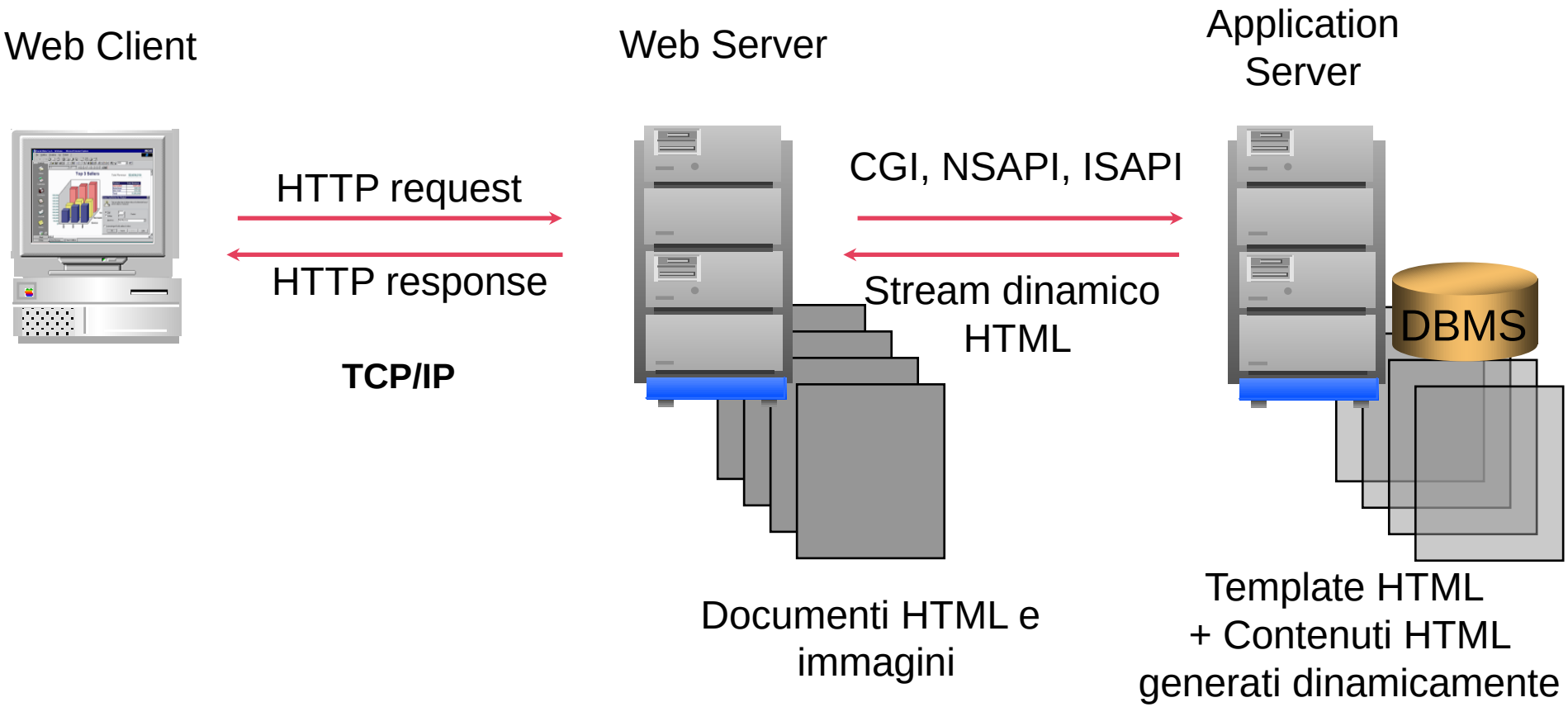
# Attaccare il server Web

- Il server Web usa una parte del filesystem del computer server per le informazioni che mette a disposizione
- La maggior parte degli attacchi tende a accedere all'esterno di tale "area riservata", ovvero a costringere il server Web a fornire dati "riservati"

# Stratificazione logica di un sistema Web

- Web Client
- Connessione HTTP
- Web Server
- Logica di azione o di presentazione
- Logica funzionale
- Server di applicazione
- Database server

# Stratificazione fisica di un sistema Web



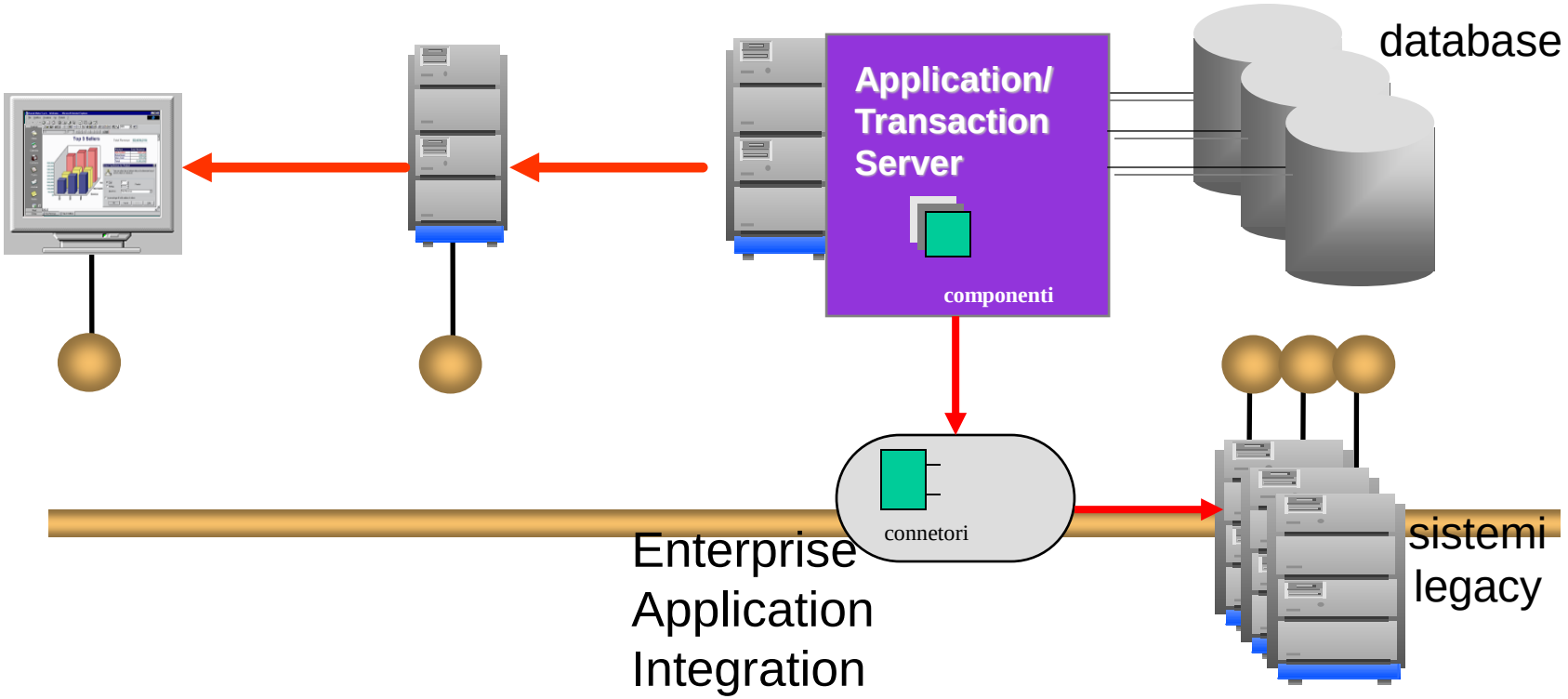
# Stratificazione fisica di un sistema Web - estensioni

Primo livello
Web Browser

Secondo livello
Web Server

Terzo livello
Regole business

Quarto livello
Sorgenti di dati



# Gli Hacking del Web

- Pilfering per cercare informazioni
- Azione diretta sul Web server
- Azione sui CGI script
- Azione sugli ASP script
- Azione sugli application server

- DoS del server

# Esempio di Hacking del Web

- Translate:f
- Esempio di input inatteso di IIS5
- Permette di visualizzare file nascosti di configurazione (es. Global.asa)
- Si possono avere informazioni di accesso al backend

# Attacchi diretti ai sistemi operativi

E’ necessario distinguere fra sistemi:

- WindowsXP home
- WindowsXP/Vista/7/8/10 e Windows2003/2008/2012/2016
- Unix/Linux

# Attacchi diretti a WindowsNT/2000 +

- Crack delle password
- Ricerca dell'utente Administrator
- Attacco al registry
- Attacco al SAM
- Intercettazione dei tasti
- Esecuzione comandi da remoto
- DoS

# Crack delle password

- Quest'azione si può effettuare intercettando la rete e usando un programma con L0phtCrack

- Alternativamente è possibile con comandi **net** cercare un utente valido di risorsa condivisa e tentare di trovarne la password

# Diventare Administrator

- Usare utility di crack
- Agire sui file (es. Sostituendo una utility di sistema)
- Installare qualcosa nel sistema

# Attacchi a registry e SAM

- Agendo in modo opportuno sulle chiavi del registry si può fare qualsiasi cosa
- Il Security Account Manager è il file crittato delle password

# Intercettazione dei tasti

- Esistono programmi che consentono di registrare tutto ciò che viene digitato in tastiera (keystroke logging)

- Installare un siffatto programma nell'avvio automatico significa disporre di tutte le informazioni possibili

# Attacchi specifici per Windows2000+

- Analisi delle Active Directories
- DoS delle Active Directories
- Ingresso diretto via Telnet
- Attacco al Terminal Server
- Salto di privilegi: runas

# Analisi delle Active Directories

- Le AD sono il deposito centrale di informazioni di un dominio
- Un programma VB (e quindi anche un virus) può facilmente aprire una connessione con le AD e leggerne il contenuto

# DoS delle Active Directories

- Se si accede alle AD in scrittura è possibile danneggiare in modo irreparabile un dominio
- Si deve ripartire dai backup

# Telnet e Terminal Server

L’accesso da remoto rende vulnerabili le macchine Win2000 ai tipi di intrusione di UNIX, ossia di apertura di una sessione comandi (GUI o shell) non autorizzata

# RunAs

- Il comando runas rende possibile eseguire un comando a nome di qualcun altro

- Se si entra in un sistema e ci si impadronisce della password di Administrator diviene possibile fare tutto senza nemmeno loggarsi come Administrator

# Attacchi alle reti WindowsNT/2000+

- Uso di una workstation come base
- Sniffing
- DoS
- Conflitti di dominio
- Il problema delle condivisioni

# Attacchi specifici per UNIX

- Attacchi “interni” al sistema (via shell)
- Attacchi “esterni” al sistem (via rete)

# Attacchi "interni" per UNIX

- Forza bruta
- Buffer overflow
- Server X
- Canale di ritorno
- FTP e TFTP
- RPC
- NFS

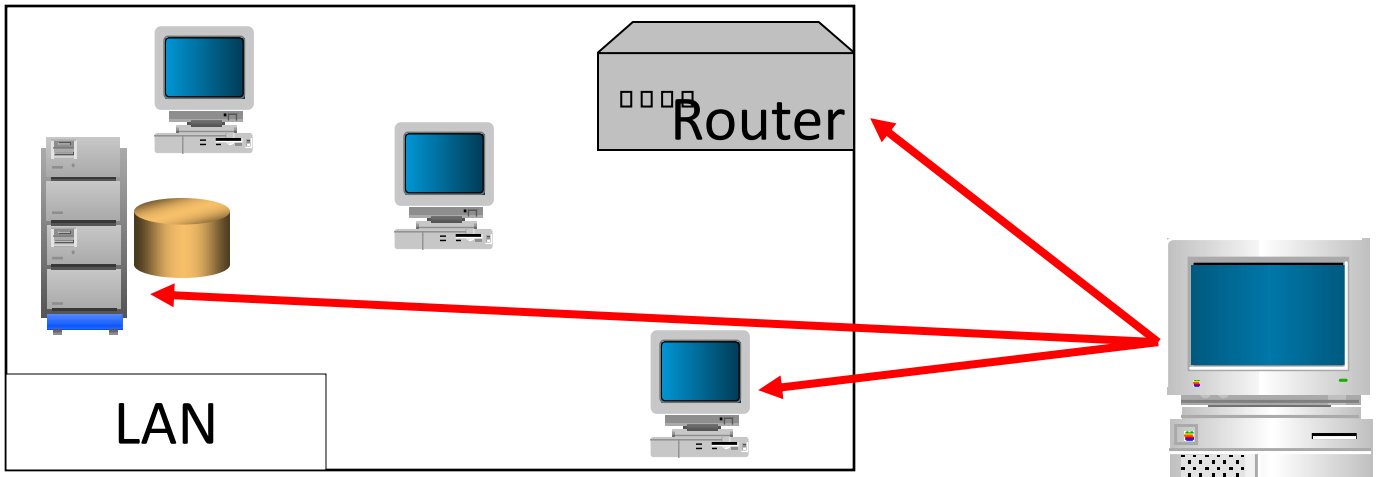
# Attacchi “esterni” per UNIX

- Lettura del file delle password
- Cambio delle configurazioni
- Intercettazione dei tasti
- SUID dei file locali
- Attacchi alla shell
- Uso improprio dei segnali
- Attacchi al kernel

# Attacchi alle reti

- Footprinting e ricostruzione
- Ricerca di punti critici
- Portscan di router e server
- Attacco a un nodo
- Sniffing

# Attacchi alle reti - 2




Hacker

# Anche i router piangono

- I router ospitano un sistema operativo
- Nel caso CISCO è lo IOS
- Esiste la possibilità di accedere in modo fraudolento ad un router

# I Virus

- Un virus è un insieme di istruzioni comprensibili dal computer che svolgono un'attività dannosa e/o fraudolenta
- Il Virus si "mimetizza" entro programmi e/o documenti che ne risultano "infettati"
- Nei comuni PC, una volta lanciato un programma, è praticamente impossibile verificarne l'esecuzione

# Una prima classificazione dei Virus

- Virus degli eseguibili
- Virus dei Boot Sector
- Virus del BIOS
- Virus scripting
- MacroVirus
- Virus del terminale
- Web Virus
- Virus misti

# Virus degli eseguibili

- Sono i Virus più antichi (mondo DOS)
- Infettano i file eseguibili (EXE, COM) o le loro librerie (OVL, DLL)
- Sostituiscono il proprio codice a parte del codice del programma
- Quasi sempre non aumentano la dimensione o modificano la data del programma infettato

# Virus degli eseguibili - 2

- Il contagio può interessare solo i file dei programmi mandati in esecuzione durante l'attività del virus o, indiscriminatamente, tutti i file dei programmi presenti sul disco fisso o sui dischetti non protetti in scrittura inseriti nel computer

# Virus dei Boot Sector

- Infettano il boot sector
- Il Virus viene sicuramente caricato in memoria insieme al sistema operativo
- Per eliminarli serve effettuare un avviamento del computer infettato con una copia non infetta del sistema operativo

# Virus del BIOS

- Attaccano il BIOS, ossia la EPROM dove sono scritte le istruzioni di avviamento e la configurazione del computer
- Possono provocare il blocco hardware
- Per riparare i danni occorre sostituire la EPROM

# Virus Scripting

- Infestano i file .BAT o i file di scripting del sistema operativo (.WSH, .JS, .VB)
- Sono comandi scritti in chiaro o no, contenuti come testo entro tali file

# MacroVirus

- Sono la famiglia più in espansione di tutte
- Sono costituiti da istruzioni fraudolente scritte nei linguaggi di macro di programmi applicativi, e poste entro documenti
- Si attivano all'apertura del documento infetto con la applicazione ad esso collegata

# MacroVirus - 2

- Infestano tutti i documenti di MS-Office
- Ma anche file PDF, PostScript e file di dati di altri programmi dotati di macro (es. StarOffice)
- Non sempre sono tipici di un'applicazione ma possono estendersi anche ad altre

# MacroVirus - 3

- Possono agire anche all'esterno dei documenti infestati (es. chiamate a sistema operativo o ad applicazioni)
- La loro azione può essere qualsiasi
- In particolare temibile è la loro combinazione con posta elettronica e Web o reti in genere

# MacroVirus - 4

- Nel caso più frequente sono attaccati i file .DOC di Word
- Il modello Normal.DOT contiene anche le macro globali di Word
- I MacroVirus infettano quasi sempre tale file

# Virus del terminale

- Sono tipici del mondo delle Shell UNIX
- Sono costituiti da sequenze di comandi (caratteri di escape) per il terminale
- Sono contenuti entro file di testo (soprattutto entro messaggi e-mail)
- Per attivarli basta visualizzare il file

# Web Virus

- Sono contenuti entro pagine Web o HTML in genere (trasmissibili anche via posta elettronica)

- Si dividono in gruppi
  - Web Scripting Virus
  - Virus Java
  - Virus ActiveX
  - Cookie ostile

# Web Scripting Virus

- Sono costituiti da pagine HTML contenenti istruzioni fraudolente (tipicamente VBScript o JavaScript)
- Si attivano alla visualizzazione della pagina grazie all'interprete contenuto nel browser
- Sono fra i più pericolosi

# Virus Java

- Sono contenuti entro gli Applet Java
- Nonostante la macchina virtuale Java del browser sia "isolata" esistono delle falle, che tali virus sfruttano
- Possono come minimo causare il crash del browser

# Virus ActiveX

- Sono contenuti entro i controlli ActiveX lato client
- Interagendo con il sistema operativo locale possono svolgere qualisasi azione
- Es. il virus “spegnimento remoto” del ComputerCaos Club di Amburgo

# Cookie ostile (o Cookie Virus)

- I cookie sono file di testo inviati insieme ai messaggi HTTP
- Sono conservati dal browser fino alla scadenza
- Un cookie ostile può leggere gli altri e le informazioni del browser (es. identità)

# Virus Misti

- E’ purtroppo comune vedere Virus appartenenti a più di una categoria
- Es. MacroVirus che apre il browser, dirigendolo verso una pagina con un WebVirus

# Classificazione dei Virus per azione

- Ficcanaso
- Devastator
- Propagator
- Subdolo
- Worm

# Classificazione dei Virus per azione –2

- Batterio
- Trojan
- TimeBomb o LogicBomb
- Virus Combinato
- Virus Mutante

# Virus Ficcanaso

- Ha lo scopo di reperire informazioni entro il sistema infettato
- Le informazioni vengono ritrasmesse indietro di solito via rete (conn. Diretta o e-mail)
- Ma esistono anche Virus che propagano "al mondo" quanto hanno "trovato"

# Virus “Devastator”

- Ha lo scopo di procurare più danni possibili ad un sistema

- Tutti i danni sono possibili, dalla distruzione selettiva di tutti i file .doc sino alla distruzione dei BIOS delle macchine

# Virus Propagator

- Si deve riprodurre nel massimo numero di esemplari possibili
- A tal fine sfrutta tutti i meccanismi disponibili (es. E-mail, condivisioni di rete, Web…)
- Non necessariamente produce danni

# Virus Subdolo

- Si introduce nei sistemi in modo difficile da scoprire
- Anche i suoi effetti sono difficili da scoprire
- Es. Lo scambio random di righe e parole nei file .DOC

# Virus Worm

- Si propaga solo attraverso la rete
- Spesso prende il controllo dei sistemi
- I suoi effetti possono essere i più vari

# Batterio

- Ha lo scopo di provocare un temporaneo DoS del sistema attaccato
- A tal scopo ne satura le risorse (CPU, RAM, spazio disco) sino a provocarne il crash

# Virus Trojan (Horse)

- E’ un cavallo di Troia
- Ha lo scopo di fare entrare qualcos’altro nel sistema attaccato o di aprire la strada a qualcuno
- Sfrutta la rete

# Time Bomb e Logic Bomb

- Sono Virus "silenti" ossia infettano un sistema senza compiere alcuna altra azione immediatamente
- I Time Bomb si attivano in occasione di dati particolari (es. Michelangelo)
- Le Logic Bomb si attivano in occasione di eventi particolari (es. Licenziamento)

# Virus Mutante

- Quasi esclusivamente tipico dei MacroVirus
- Durante la sua azione, il codice del Virus cambia
- In taluni casi si è verificato anche il “crossover”, ossia la fusione di Virus diversi in documenti a infezione multipla

# Virus Combinato

- Comprende in sè più di una delle caratteristiche suddette e dei corrispondenti modi di agire
- E quindi è estremamente pericoloso
- Purtroppo tutti i nuovi Virus stanno evolvendo in questa direzione

# Classificazione “tecnica” dei Virus

- Virus Polimorfici
- Virus Stealth
- Virus Lenti
- Virus Retro
- Virus Multipartite
- Virus Armored
- Virus Companion
- Virus Phage

# Virus Polimorfici

- Il codice fraudolento viene crittato
- La criptazione cambia infezione dopo infezione
- La “firma” del Virus cambia

# Virus Stealth

- Nascondono le modifiche arrecate ai file o al sistema con la loro presenza
- Per esempio non modificano data e ora o dimensioni dei file infettati

# Virus Lenti

- Infettano un solo file per volta
- Si attaccano ad una utility di sistema e infettano i file che vengono aperti da quella utility

# Virus Retro

- Attaccano direttamente i software antivirus
- Ad esempio distruggono gli archivi delle impronte virali
- Esistono anche Virus-anti-Virus che disinfettano da altri Virus

# Virus Multipartite

- Sfrutta attacchi contemporanei con più tecniche (es. Boot, exe)
- Tende a infettare progressivamente tutte le utility di sistema una volta installatosi in memoria

# Virus Armored

- Si nascondono (“corazzano”) entro codice “esterno” fuorviante
- Sono difficili da riconoscere e analizzare

# Virus Companion

- Creano un nuovo file accanto all'eseguibile che intendono infettare (es. .COM rispetto a .EXE)
- Il file .COM viene eseguito prima e infetta il sistema

# Virus Phage

- Sostituiscono il proprio codice a quello del programma infettato invece che attaccarsi semplicemente

- Provocano danni non riparabili ai programmi infettati

# Virus new generation: Ransomware

- Il ransomware rappresenta una nuova categoria di virus
- E' un tipo di malware che limita l'accesso ad un dispositivo IT chiedendo un riscatto per liberarlo
- La forma più diffusa sono i virus cripto-locker, che cifrano i file dei computer invasi chiedendo un riscatto per restituirli nella forma originale

# Virus new generation: La lezione di Stuxnet (2010)

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

The New York Times

**Middle East**

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

AFRICA | AMERICAS | ASIA PACIFIC | EUROPE | MIDDLE EAST



## Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 360 Comments

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
REPRINTS



Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around

Washington e Tel Aviv hanno collaborato allo sviluppo di Stuxnet per disabilitare elementi chiave dei sistemi di purificazione dell'uranio nelle centrali iraniane, senza lasciare tracce.

Il New York Times, dopo 18 mesi di indagini, ha scoperto finalmente la storia del virus più potente del mondo (www.tomshw.it – 4 giugno 2012, Gruppo Editoriale L'Espresso).

# Un problema secondario: gli Hoax

- Con Hoax si indica un messaggio di avvertimento per un nuovo virus inesistente, diffuso via e-mail con l'invito a spedirlo a quante più persone possibili

- Ciò genera panico ingiustificato e, in definitiva, perdita di tempo e risorse

# Un problema secondario: gli Hoax - 2

- Ma può accadere anche l'imprevisto: caso aol4free.com

- In generale diffidare degli hoax, verificare le informazioni presso siti certi

# Come funzionano gli anti-virus

- Il metodo più semplice è la ricerca delle impronte virali
- Vengono fatte valere le regole note contro Stealth e simili
- Esistono anche motori "euristici" che analizzano ed interpretano i codici "insoliti" trovati, ma sono lenti

# Come funzionano gli anti-virus –2

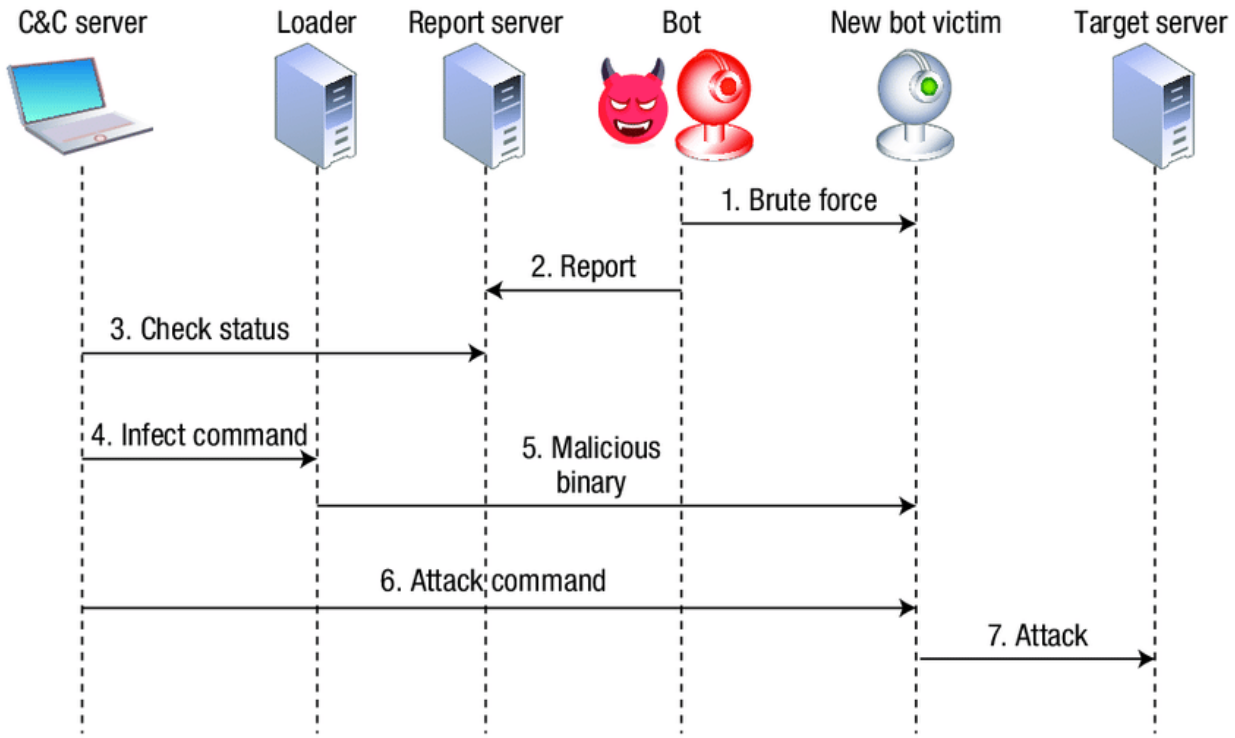
- Durante la fase di disinfezione l'Anti-virus cerca di ripristinare la forma originale del file infettato
- Non sempre ciò è possibile
- Vale quanto detto per le protezioni dei dati

# Un Virus antico potente: Nimda

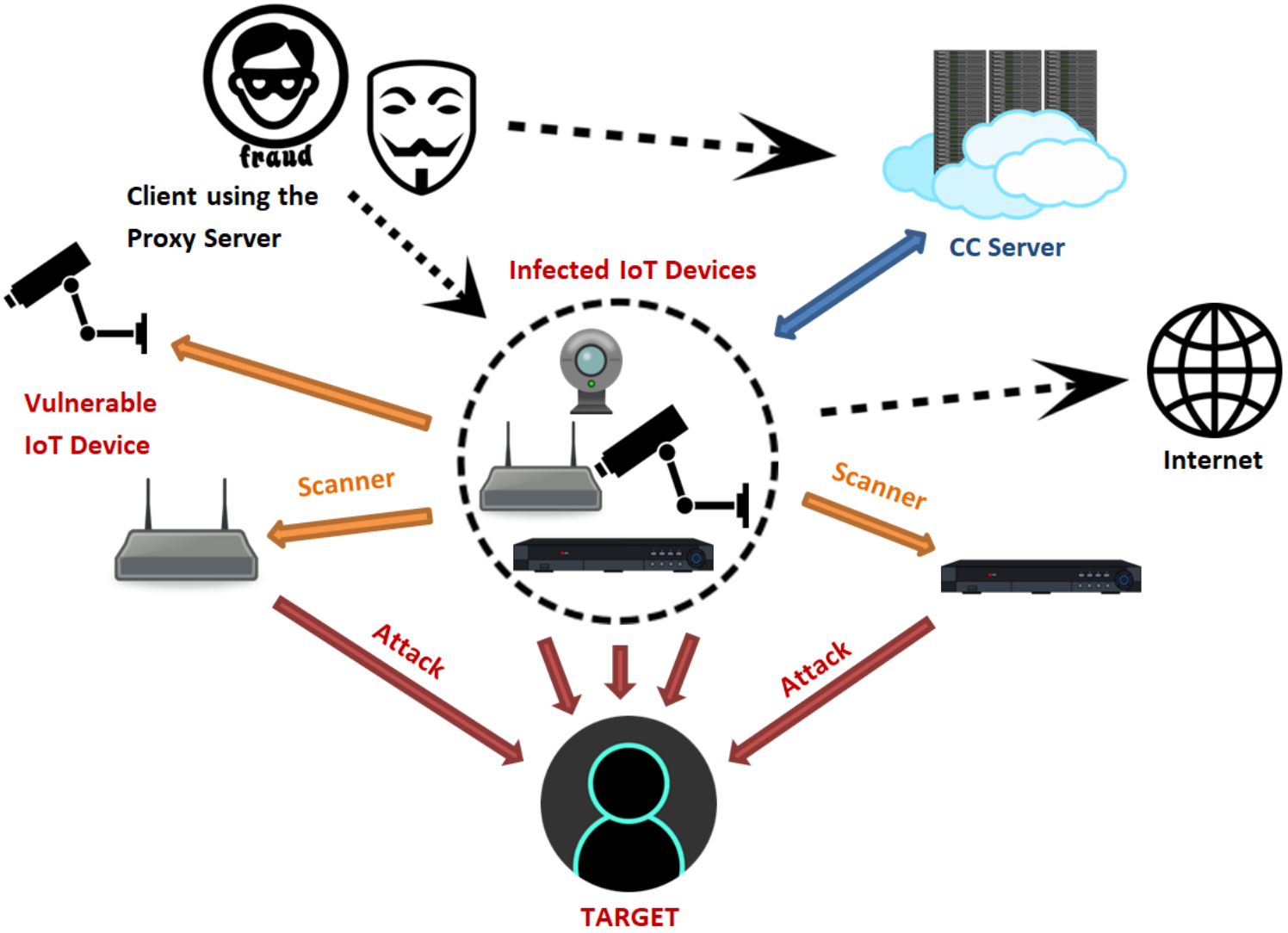
- Combinazione di MacroVirus e Virus EXE
- Usa diversi meccanismi di propagazione:
  - Web Upload
  - E-Mail
  - Condivisione dischi (se può le crea)
  - Infezione di file di Office
  - Creazione file infetti

# Un Malware IoT: MIRAI

- Botnet gigante basata su telecamere



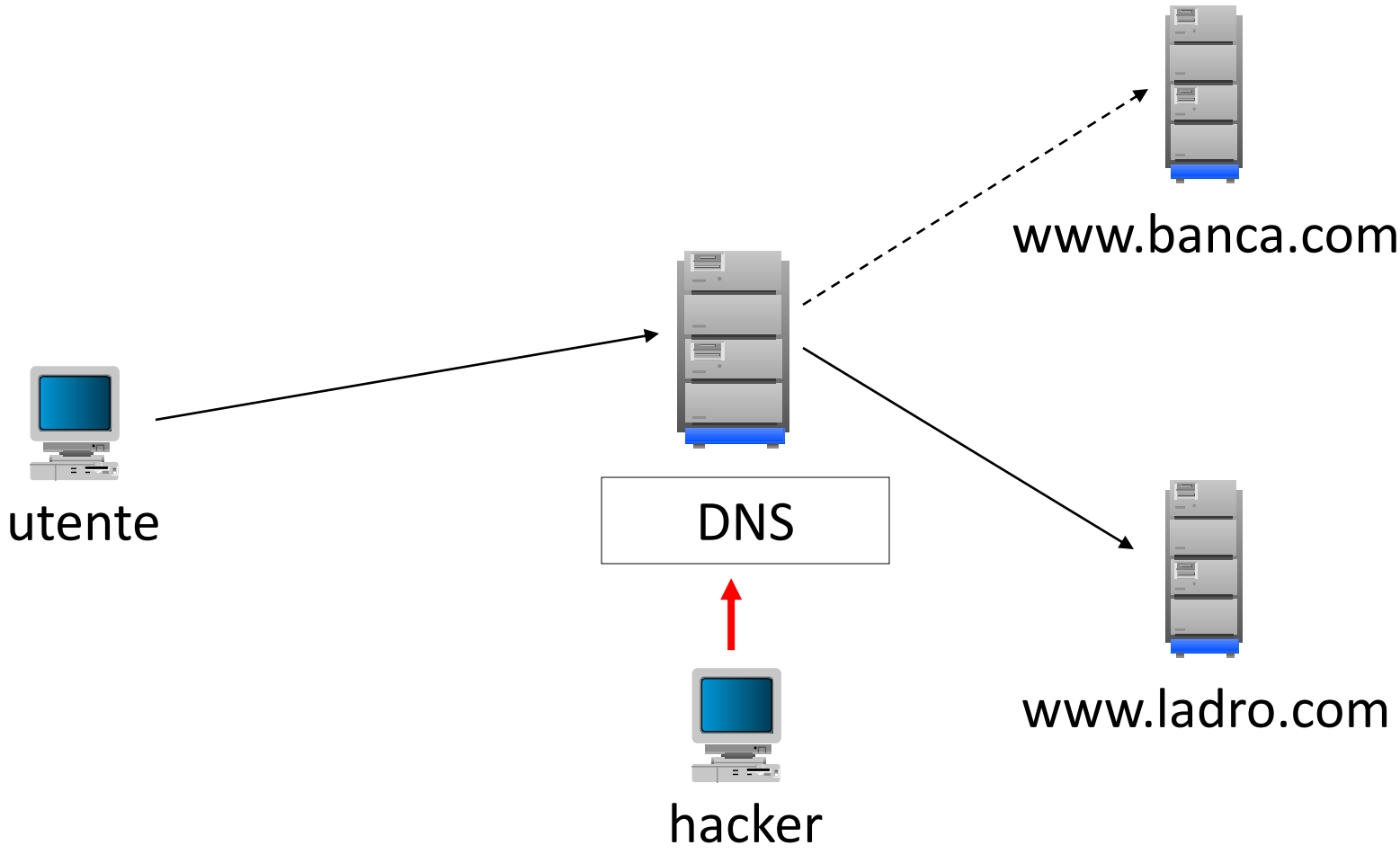
# Un Malware IoT: MIRAI



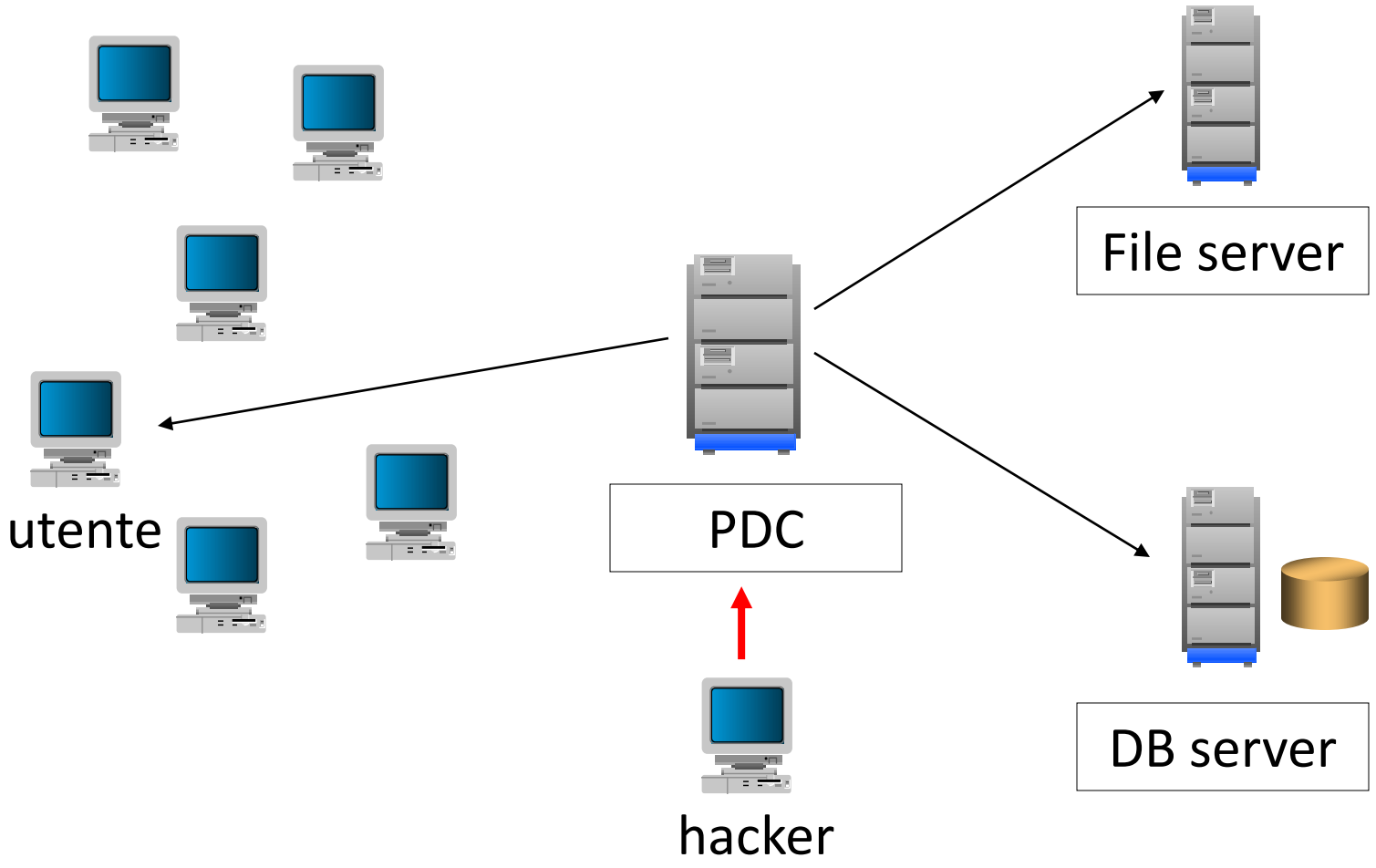
# Attacchi devastanti

- Hacking del Domain Name Server
- Hacking del Server di dominio
- Hacking di un Router

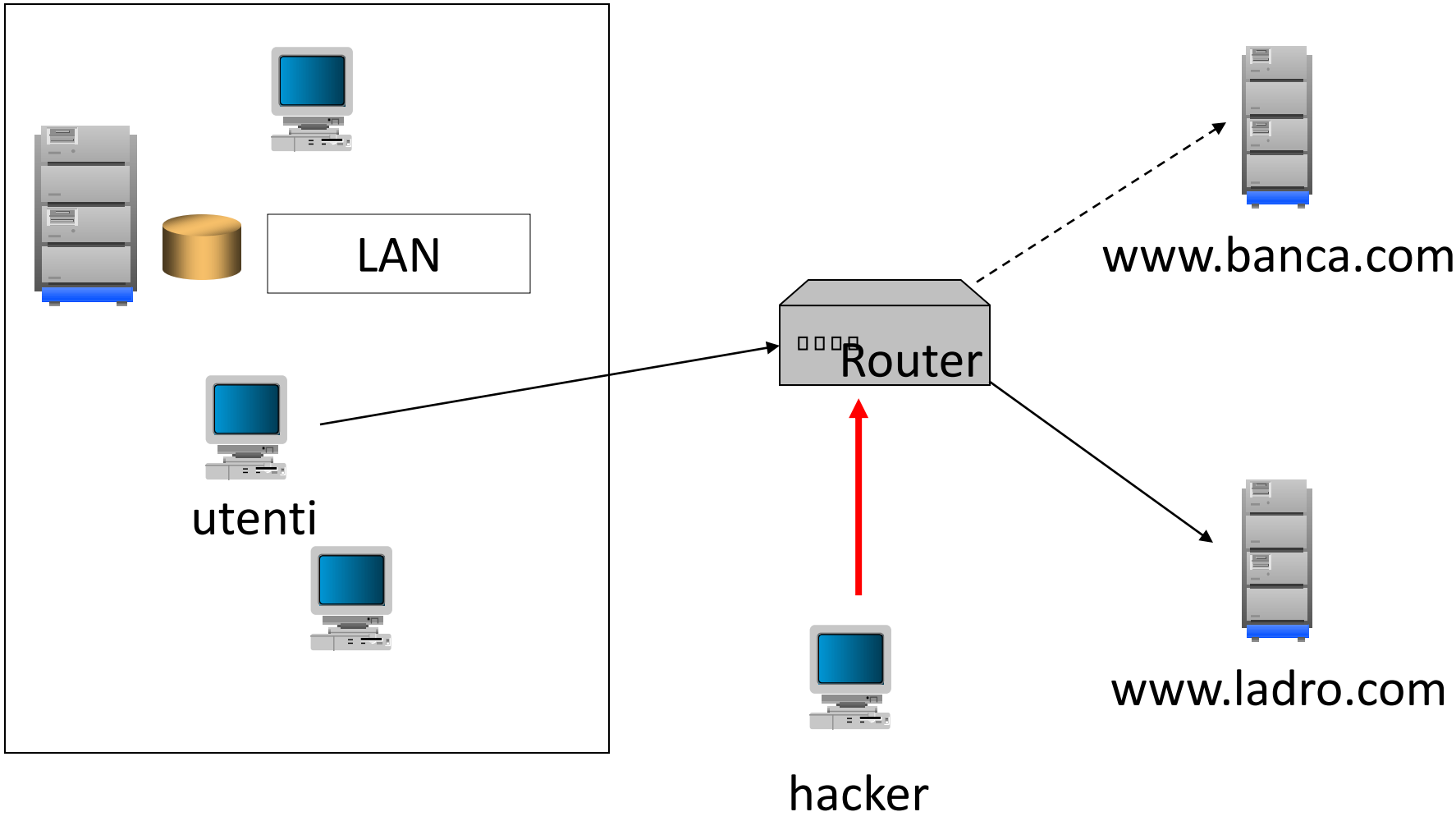
# Hacking del Domain Name Server



# Hacking del Server di Dominio



# Hacking del router



# I pericoli dal lato Client

- Virus via posta elettronica
- Inserimento di Trojan e BackDoor
- Pagine Web “virate”
- Intrusione nei dischi

# “Quis custodiet custodem?”

- Gli attacchi possono provenire anche dall’interno della rete aziendale
- Un amministratore locale può facilmente installare uno sniffer
- Nelle grandi reti è difficile verificare l’operato degli utenti

# Il fattore umano

- Spesso è il fattore umano il più debole
- Operazioni demandate a umani, ad esempio
  - Scansione manuale di file, e-mail…
  - Verifiche manuali di log

- Sono destinate a fallire, prima o poi!

# Social engineering

- L'ingegneria sociale (dall'inglese social engineering) è lo **studio del comportamento individuale di una persona al fine di carpire informazioni utili per un attacco informatico**.

# Il Social Engineer (1/2)

- Un ingegnere sociale (social engineer) per definirsi tale deve saper fingere, sapere ingannare gli altri, in una parola saper mentire.
- Un social engineer è molto bravo a nascondere la propria identità, fingendosi un'altra persona: in tal modo egli riesce a ricavare informazioni che non potrebbe mai ottenere con la sua identità reale.

# Il Social Engineer (2/2)

- Nel caso sia un cracker, può ricavare informazioni attinenti ad un sistema informatico.
- Il social engineering comporta (nell'ultima fase dell'attacco) il rapporto più diretto con la vittima, questa tecnica è una delle più importanti per carpire informazioni.
- In molti casi il cosiddetto ingegnere potrà riuscire a ricavare tutto ciò che gli serve dalla vittima ignara.

# Tecniche di Social Engineering

- Autorevolezza
- Colpa
- Panico
- Ignoranza
- Desiderio
- Avidità
- Buoni sentimenti (nei due sensi)

# La “battuta” del Social Engineering

- Come è bravo lei!
- Chissà quanto guadagna!
- E quanto riesce a stare con la sua famiglia?

# Prevenzione del Social Engineering (1/2)

- Creare un ambiente di fiducia per gli impiegati e il resto del personale (specificare dove, come, quando e da chi devono essere trattati i dati).
- Definire quali informazioni sono sensibili e valutare il loro livello di esposizione verso l'esterno.
- Stabilire protocolli di sicurezza, politiche e procedure per i dati sensibili.
- Addestrare il personale di interesse nelle procedure di sicurezza di interesse.

# Prevenzione del Social Engineering (2/2)

- Testare casualmente, senza riferirlo, tale infrastruttura.
- Revisionare periodicamente tutti i passaggi suddetti.
- Gestire correttamente i rifiuti informatici (possono essere utili per i possibili attaccanti).

# Sicurezza individuale (1/2)

- Diffidare di mail o telefonate non richieste da persone che chiedono informazioni su dipendenti o riguardo l'azienda (anche finanziarie).
- Documentarsi prima su chi richiede tali dati (autorità).
- Non diffondere informazioni sensibili nella rete senza verificare il livello di sicurezza e attendibilità di chi le chiede
- Evitare di aprire allegati o file eseguibili di dubbia provenienza.

# Sicurezza individuale (2/2)

- Controllare sempre le URL dei siti web, poiché potrebbe contenere alcune lievi differenze rispetto all'originale.
- In particolare fare attenzione agli errori di battitura
- Documentarsi meglio sul mittente di messaggi «insoliti»
- In caso il mittente sia noto, confrontare con possibili attacchi nelle liste di phishing rintracciabili tramite motore di ricerca.

# L’identità elettronica / digitale

- L'identità digitale è l'insieme delle **informazioni** e delle **risorse** concesse da un sistema informatico ad un particolare **utilizzatore** del suddetto attraverso un **processo di identificazione**.
- In un'accezione più ampia essa è costituita **dall'insieme di informazioni presenti on line e relative ad un soggetto/ente**

# Riassumendo: categorie di attacchi

- Intrusione
- Impersonificazione
- Intercettazione (es. Sniffing)
- Abuso (es. spamming)
- Denial-of-service (es. sovraccarico)
- Il ruolo dei Virus
- Social Engineering

# Classificazione della Sicurezza

- Sicurezza sui dati/programmi
- Sicurezza del canale trasmissivo
- Sicurezza dei server

# Protezioni

- Crittografia dati (PGP)
- Crittografia e autenticazione canale (SSL, SSH)

- Firewall, filtri IP e filtri per protocollo

- Verifiche sulle connessioni
- Controllo sul carico

# La crittografia per la protezione delle informazioni

# Protezioni: indice della sezione

- La protezione delle informazioni
- Steganografia
- Basi di crittografia
- Sistemi a chiave simmetrica
- Sistemi a chiave asimmetrica
- Applicazioni ai dati
- Applicazioni ai canali

# Protezione delle informazioni

- Quali sono i dati?
- Dove sono i dati?
- Come si accede ai dati?
- Come si interpretano i dati?

# Il formato dei dati

- Formato testo
- Formato documenti (es. MS-Office)
- Tabelle/dump DB
- Formati proprietari applicativi
- Immagini
- File audio
- Filmati

# Sicurezza dei formati

- Anche nel caso di formati proprietari la sicurezza non è garantita
- Un abile hacker, se accede ai file, è in grado di ricostruirne i tracciati
- L'unica garanzia è la **cifratura** o **crittografia** dei dati

# Le basi della crittografia

- L’operazione di cifratura o codifica di un messaggio consente di trasformarlo in modo illeggibile a tutti, tranne a chi possiede la chiave di decodifica opportuna

- Esistono vari tipi di cifratura

# I termini

- Testo in chiaro = testo originale
- Testo cifrato o codificato = testo crittografato
- Cifratura o codifica = operazione di "traduzione" del testo da "chiaro" a "cifrato"
- Decifratura o decodifica = operazione inversa
- Chiave = entità usata per la codifica

# Steganografia

- La steganografia è il “mimetizzare” un dato entro un altro
- Ad esempio dati possono essere nascosti entro un’immagine bitmap

# Crittoanalisi

- Scienza della ricostruzione del plaintext senza la conoscenza del metodo e/o della chiave

- Attacco ciphertext-only
- Attacco Known-plaintext
- Attacco Chosen-plaintext

- Attacco forza bruta (brute force)

# Crittoanalisi

- Può operare usando:
  - Analisi di frequenza
  - Indici di coincidenza
  - Ricerca forza bruta
- È una possibilità nell'attacco 'man in the middle'

# Crittografia di testo

- Algoritmo di Cesare
  - Tutti i caratteri son ruotati di un numero fisso di posizioni
- Algoritmo di Cesare con chiave
  - I caratteri sono ruotati di un numero di posizioni dipendenti da una chiave
- Sostituzione semplice (monoalfabetica)
  - Ogni carattere diventa sempre un altro
- Sostituzione polialfabetica
  - Sostituzione usando chiavi multple
- Tabella di Vigenère
  - Sostituzione usando una tavola/matrice

# L’algoritmo di Cesare

- Si basa sullo scorrimento (rotatorio) dell’alfabeto dei caratteri
- Si dice ordine dell’algoritmo il numero di posizioni di cui viene ruotato l’alfabeto durante l’operazione

# Esempio di algoritmo di Cesare

- Sia 4 l'ordine
- Si suppone che lo spazio sia il carattere avente indice zero
- La frase "Se magna" diventa "Widqekre"

# Limiti dell'algoritmo di Cesare

- Studiando la frequenza dei caratteri del testo cifrato si può intuire come funziona
- E' quindi facile indovinare che si tratta di uno scorrimento
- E' sensibile ad un attacco a "forza bruta" ossia per prove esaustive delle combinazioni possibili dello scorrimento

# Evoluzione: scorrimento con chiave

- In questa variante lo scorrimento dei singoli caratteri del messaggio avviene in base ai valori dei caratteri di una "parola chiave"
- Pertanto ogni carattere del messaggio risulta traslato in modo diverso rispetto agli altri
- E' evidente la maggiore robustezza

# Esempio di scorrimento con chiave

- Testo in chiaro: “fido”
- Parola chiave: “abcd”
- Testo cifrato: “gkgs”

- Più lunga è la chiave, più sicura è la protezione rispetto ad attacchi a “forza bruta”

# Applicazione della crittoanalisi all'algoritmo di Cesare con chiave

- Con l'uso dell'algoritmo di Cesare a chiave è più difficile applicare l'analisi basata sulla frequenza di occorrenza dei caratteri
- E la difficoltà è maggiore tanto maggiore è la lunghezza della chiave

# Sostituzione semplice completa

- Mappatura della chiave:
  ABCDEFGHIJKLMNOPQRSTUVWXYZ_
  QWERTYUIOPASD_FGHJKLZXCVBNM
- Testo in chiaro: “I AM”
- Testo cifrato: “HOQS”

# I passi per applicare la crittoanalisi agli algoritmi di cifratura del testo

- Individuazione della lingua usata.
- Individuazione del metodo di cifratura usato.
- Ricostruzione della chiave specifica usata.
- Ricostruzione del testo in chiaro.

# Applicazione della crittoanalisi al testo

- Si supponga che la lingua sia l'inglese
- Analizzando la frequenza di occorrenza delle lettere, possiamo determinare che la lettera "e" è la più frequente, con il 13% di occorrenze
- Nell'algoritmo di sostituzione semplice la lettera o simbolo con questa percentuale di occorrenza è un buon candidato per essere il corrispondente di "e"

# Sistemi polialfabetici

- In un sistema monoalfabetico un dato testo cifrato viene sempre trasfotmato nello stesso testo in chiaro.
- In un sistema polialfabetico invece un dato valore di testo cifrato può corrispondere a diversi testi in chiaro.

# Sistemi polialfabetici

- Un tipico sistema polialfabetico userà da 2 a 26 differenti alfabeti
- I sistemi polialfabetici che ripetono lo stesso insieme di alfabeti sempre nella stessa sequenza sono detti anche **sistemi periodici**
- I sistemi polialfabetici che non mantengono la ripetizione degli alfabeti sempre nello stesso orgine sono detti anche **sistemi aperiodici**

# Sistemi polialfabetici

- I sistemi periodici, a causa della loro ripetizione regolare di chiavi, sono in generale meno sicuri dei sistemi aperiodici
- I sistemi aperiodici, d'altra parte, sono in generale più difficili da usare
- Ma l'uso di opportuni algoritmi e di computer potenti risolve il problema

# Un esempio classico di Sistemi polialfabetici: Tavola di Vigenère

| Chiave \ Testo in chiaro | a | b | c | d | e | f | g | h | I | j | k | l | m | n | o | p | Q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **B** | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| **C** | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| **D** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| **E** | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| **F** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| **G** | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| **H** | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| **I** | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| **J** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| **K** | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| **L** | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| **M** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| **N** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **O** | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| **P** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **Q** | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| **R** | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| **S** | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| **T** | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| **U** | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| **V** | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| **W** | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| **X** | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| **Y** | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| **Z** | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

# Uso della tavola di Vigenère

- Tavola di Vigenère o quadrato di Vigenère
- Il quadrato di Vigenère include tutti I possibili allineamenti di un alfabeto diretto standard
- Nel quadrato di Vigenère possono anche essere usati alfabeti misti
- Se vengono usati tutti e 26 gli alfabeti, ogni lettera può corrispondere ad ogni altra lettera

# Uso della tavola di Vigenère

- Le lettere del testo in chiaro sono disposte in cima alla tabella
- Le lettere equivalenti del messaggio cifrato sono trovate nelle 26 sequenze sotto
- L'elemento finale è la chiave, disposta sul lato sinistro in verticale, che determina quale alfabeto viene usato a ogni dato momento

# Tavola di Vigenère: esempio periodico

- Messaggio originale (inglese)
  report at zero two two zero tomorrow
- Messaggio diviso
  repor tatze rotwo twoze rotom orrow
- CHIAVE
  RIFLE RIFLE RIFLE RIFLE RIFLE RIFLE
- TESTO CIFRATO
  IMUZV KIYKI IWYHS KETKI IWYZQ FZWZA

# Tavola di Vigenère: esempio aperiodico

- Messaggio originale (inglese)

  mountain passes blocked by heavy snow fall last night
- Messaggio diviso

  mount ainpa ssesb locke dbyhe avysn owfal llast night
- CHIAVI

  FOURS COREA NDSEV ENEYA RSAGO OURFO REFAT HERSB ROUGH
- TESTO CIFRATO

  RCOEL CWETA FVWWW PBAOE UTYNS OPPXB FAKAE SPRKU EWANA

# La crittografia moderna

- I moderni sistemi di crittografia impiegano sofisticate tecniche logico-matematiche per cifrare i dati
- Entro il computer tutte le informazioni sono rappresentate come numeri binari
- Non necessariamente la cifratura dei testi deve avvenire carattere per carattere

# La crittografia moderna - 2

- Nella maggior parte dei casi i computer eseguono le operazioni di crittografia moltiplicando e/o dividendo i valori numerici che rappresentano i dati per numeri molto estesi e decodificano i dati applicando gli stessi numeri

# Sicurezza di un metodo crittografico

- Segretezza del metodo
- Segretezza della chiave

# Attacchi possibili ad un metodo crittografico

- Confronto fra testo in chiaro e testo crittografato
- Individuazione del metodo
- Individuazione della chiave

# Decifratura fraudolenta

- Individuazione del metodo con studi statistici
- Tentativi di individuare la chiave
- Forza bruta

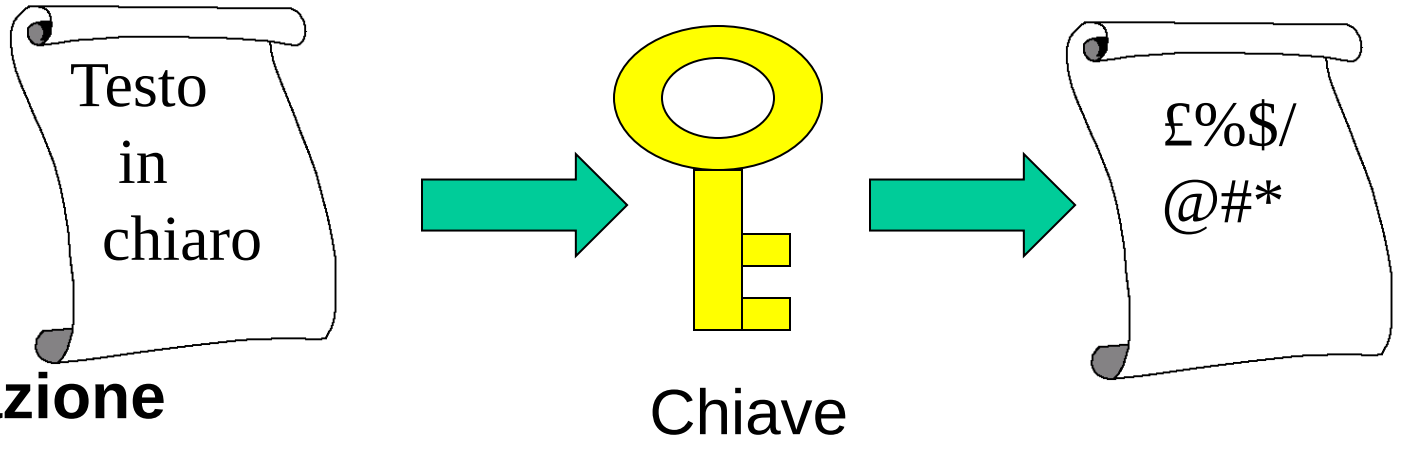
# Cifrari perfetti

I cifrari perfetti sono quelli "impossibili" da decifrare attraverso la crittoanalisi

- One-time pad
  - Viene usata una tavola di chiavi che non si ripetono
- Serie di numeri casuali
  - Vengono usati chiavi che non si ripetono generate dal computer
- Cifrario di Vernam
  - Simile a un one-time pad

Potrebbero essere perfetti, ma sono di solito troppo difficili da usare nel mondo reale

# Chiave simmetrica: lo scenario



# Chiave simmetrica

- La stessa chiave viene usata sia per la criptazione sia per la decriptazione
- Con lunghezza delle chiavi >= 128 bit il sistema è al sicuro da attacchi a forza bruta

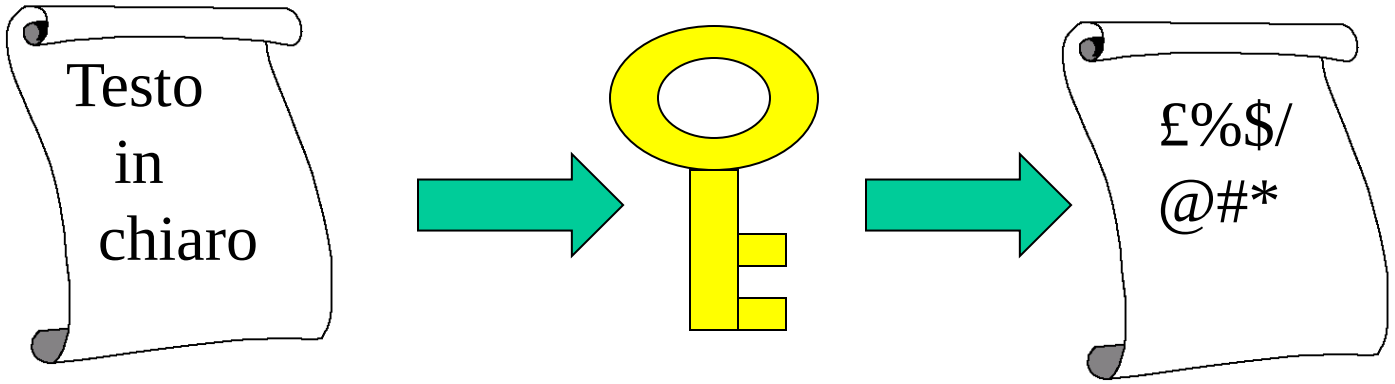
# Chiave simmetrica - 2

- Se la chiave viene intercettata i messaggi non sono più sicuri
- Non garantisce l'autenticazione del mittente

# Agoritmi di crittografia simmetrica

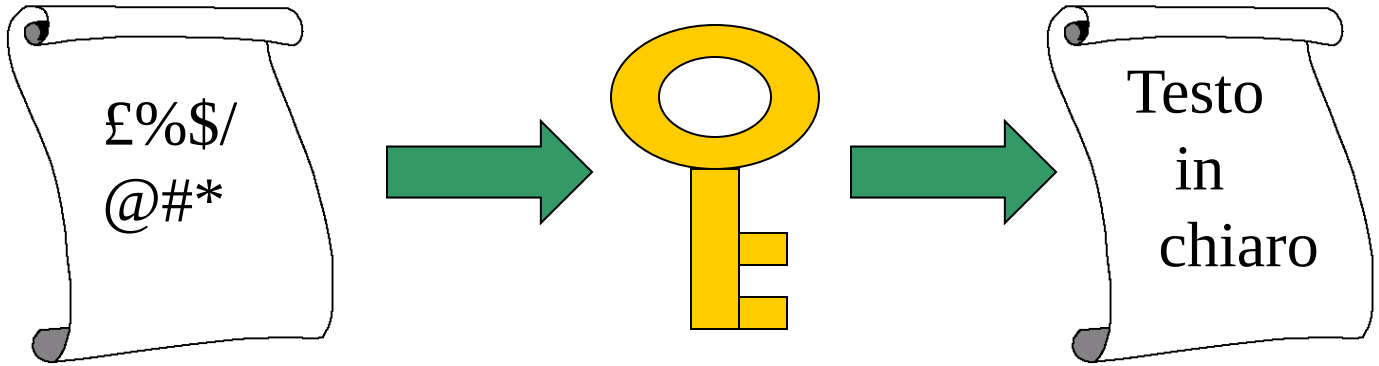
- DES (Data Encryption Standard)
- 3-DES
- Blowfish
- IDEA

# Chiavi asimmetriche: lo scenario




**Codifica**

Chiave privata




**Decodifica**

Chiave pubblica

# Chiave asimmetrica

- Il ruolo delle chiavi è duale: ciò che viene crittografato con una può essere decrittato solo con l'altra

- Si deve conoscere solo una chiave (pubblica)

# Chiave asimmetrica - 2

- Usando la mia chiave privata e quella pubblica del destinatario, garantisco contemporaneamente autenticazione e sicurezza

- Numero di bit elevato (>= 1024)

# La base di RSA

- E = azione di crittografia
- D = azione di decrittografia
- M = messaggio originale

- D(E(M)) = M
- E(D(M)) = M

# La base di RSA - 2

- E e D sono relativamente facili da calcolare
- Ma la disponibilità di E non offre alcun vantaggio nel trovare D e viceversa

# La base di RSA - 3

- Se valgono le proprietà suddette, l'unico modo per decifrare un messaggio è provare tutte le possibili chiavi sino a trovare quella che soddisfa il requisito E(M) = D

# Lunghezza minima delle chiavi

- Per le chiavi simmetriche: > 128 bit
- Per le chiavi asimmetriche: > 1024 bit

# Agoritmi di crittografia asimmetrica

- RSA (Rivest Shamir Adelman)
- Diffie-Hellman

# Protezioni sui dati: sommario

- Steganografia
- Basi di crittografia
- Sistemi a chiave simmetrica
- Sistemi a chiave asimmetrica

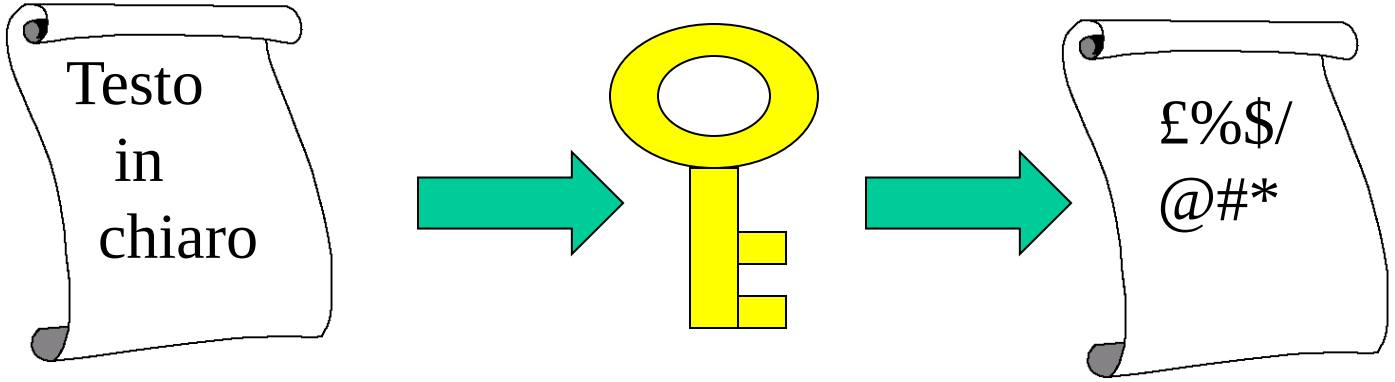
- Applicazioni ai dati
- Applicazioni ai canali

# L'Identità Elettronica

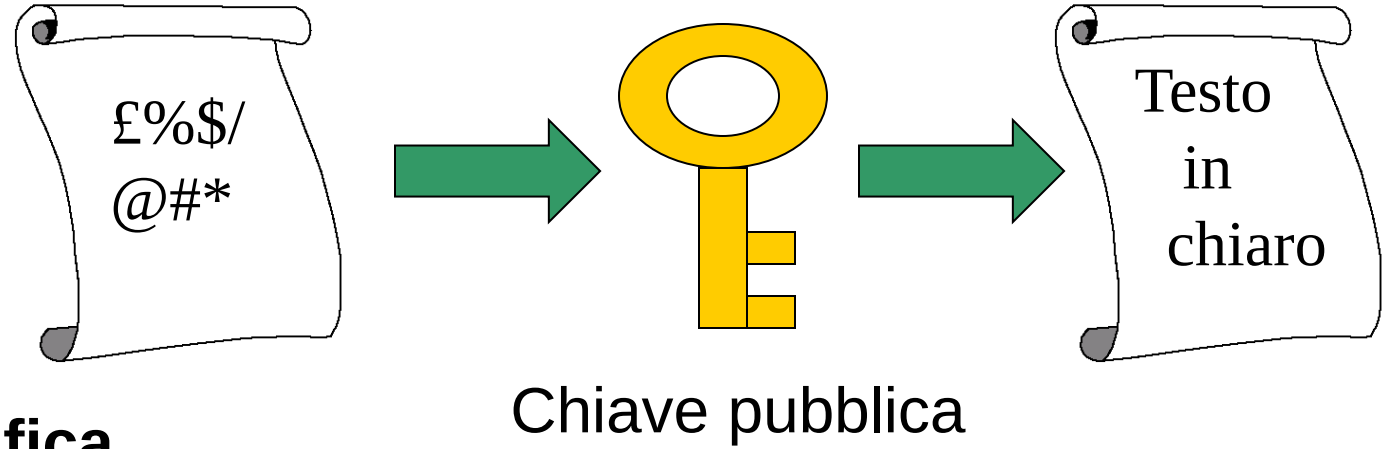
# Identità elettronica: argomenti

- Applicazione dei sistemi a chiave asimmetrica
- La firma digitale
- Il contratto informatico
- Questioni legali connesse
- Non ripudio di operazioni effettuate
- Applicazioni
- Smartcard ed altri supporti

# Lo scenario




**Codifica**




**Decodifica**

# Chiave asimmetrica

- Il ruolo delle chiavi è duale: ciò che viene crittografato con una può essere decrittato solo con l'altra

- Si deve conoscere solo una chiave (pubblica)

# Elenchi pubblici garantiti

- Le chiavi pubbliche possono essere raccolte in opportuni siti, gestiti da Autorità di Certificazione, a disposizione degli utenti

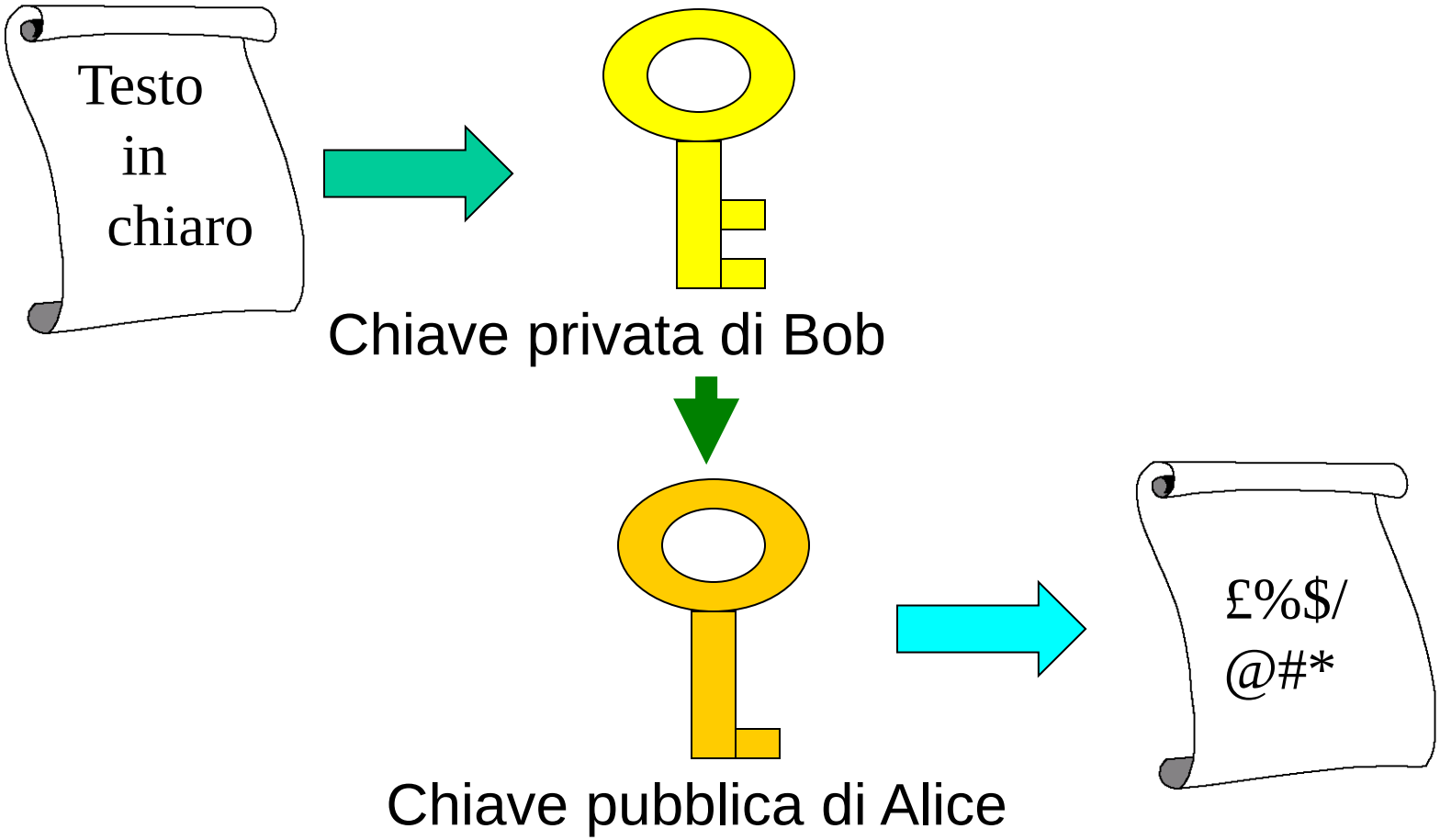
- Si deve conoscere solo una chiave (pubblica)

# Chiave asimmetrica - 2

- Usando la mia chiave privata e quella pubblica del destinatario, garantisco contemporaneamente autenticazione e sicurezza

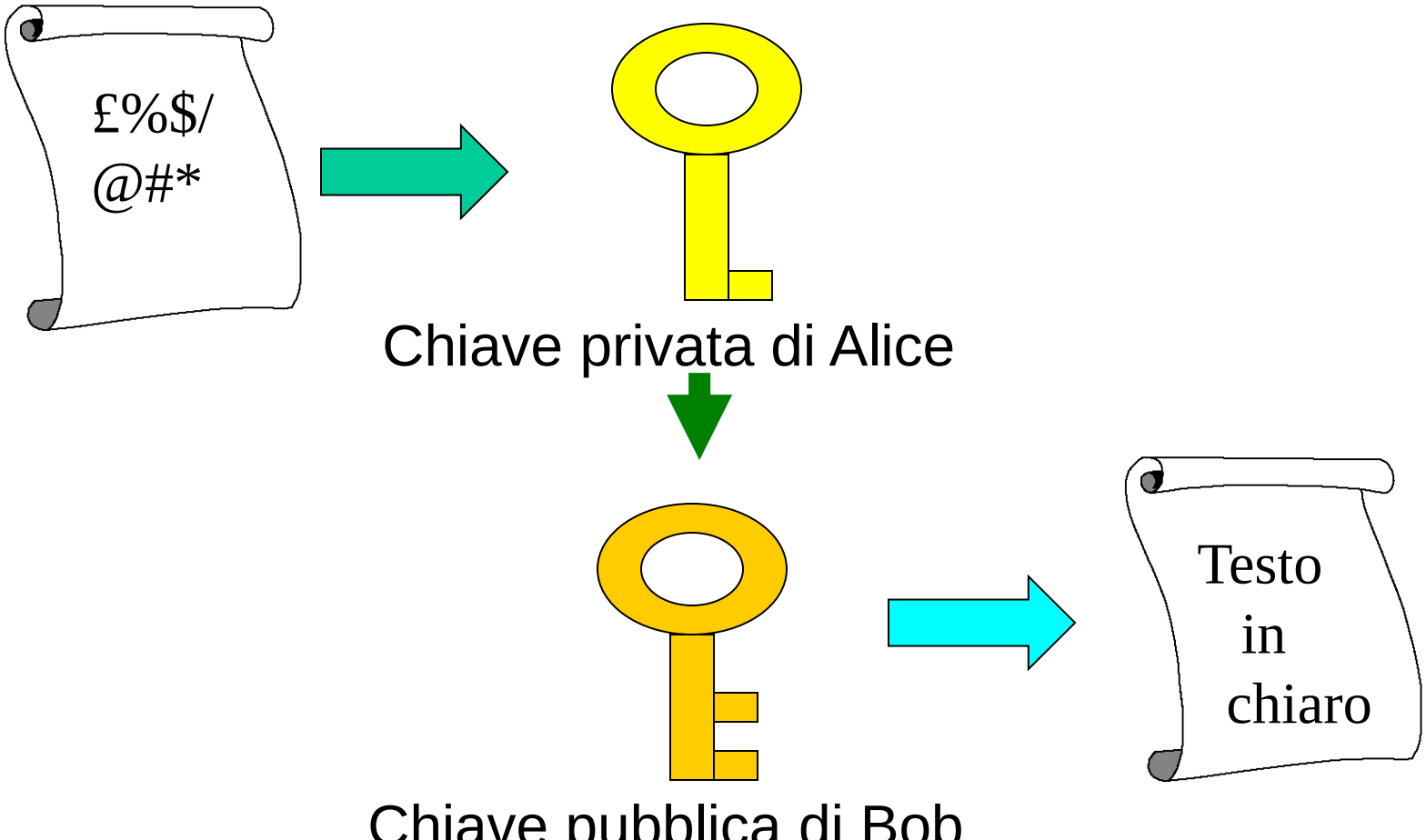
- Numero di bit elevato (>= 1024)

# Doppia chiave - codifica



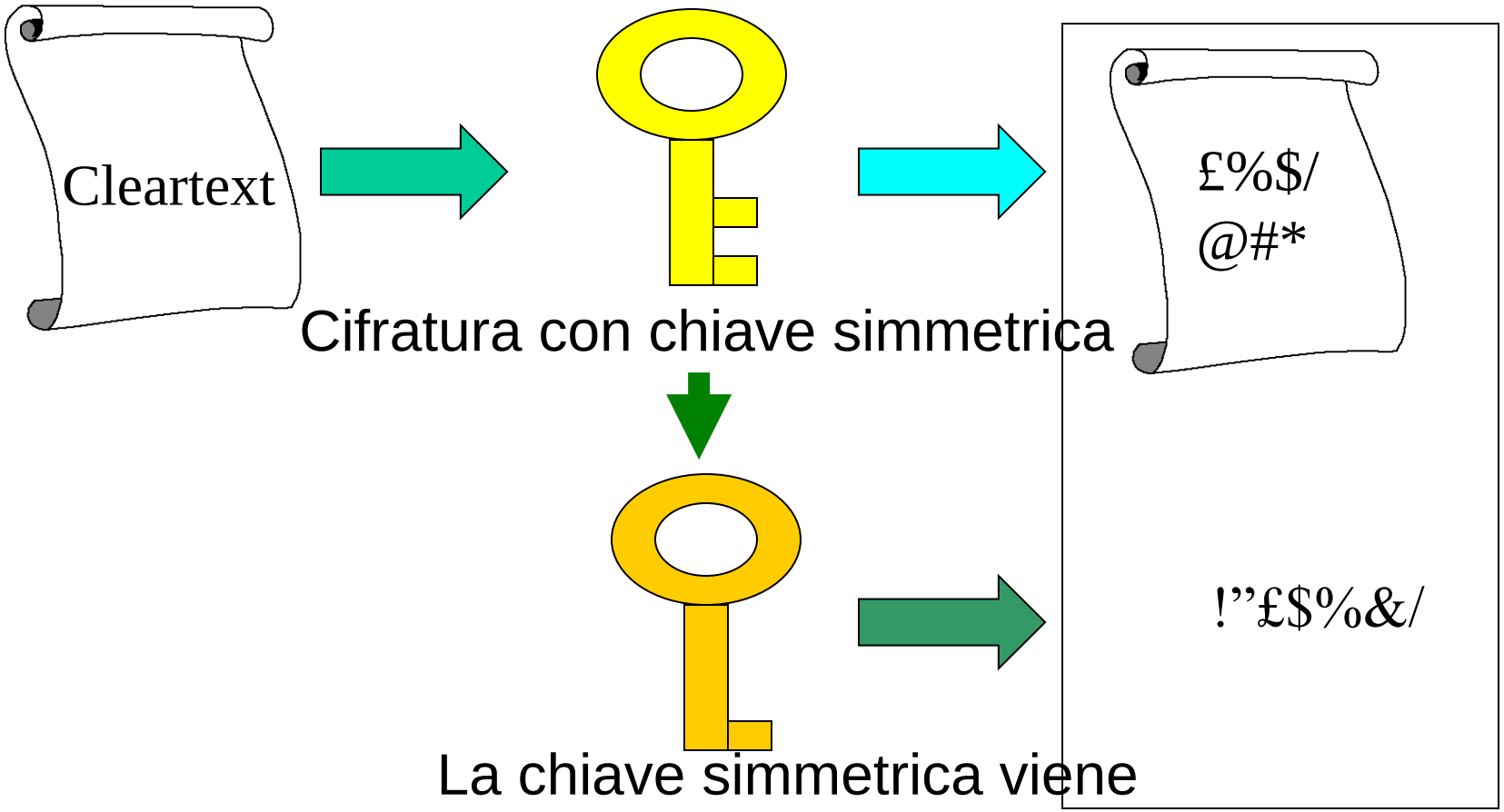

**Codifica da parte di Bob**

# Doppia chiave - decodifica




**Decodifica da parte di Alice**

# Message Enveloping



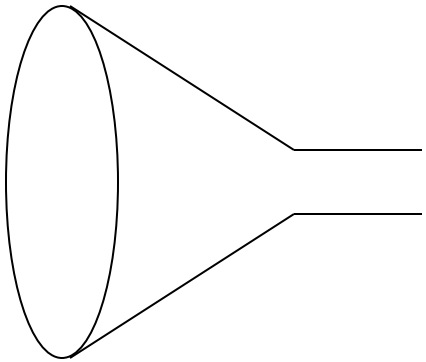

La chiave simmetrica viene poi cifrata con la chiave pubblica del destinatario (Alice)

# Funzione di Hash

Dato un documento in forma digitale, la funzione di hash produce in uscita un numero binario in corrispondenza pressochè biunivoca con esso (impronta del documento)

# Applicazione di Hash


Messaggio

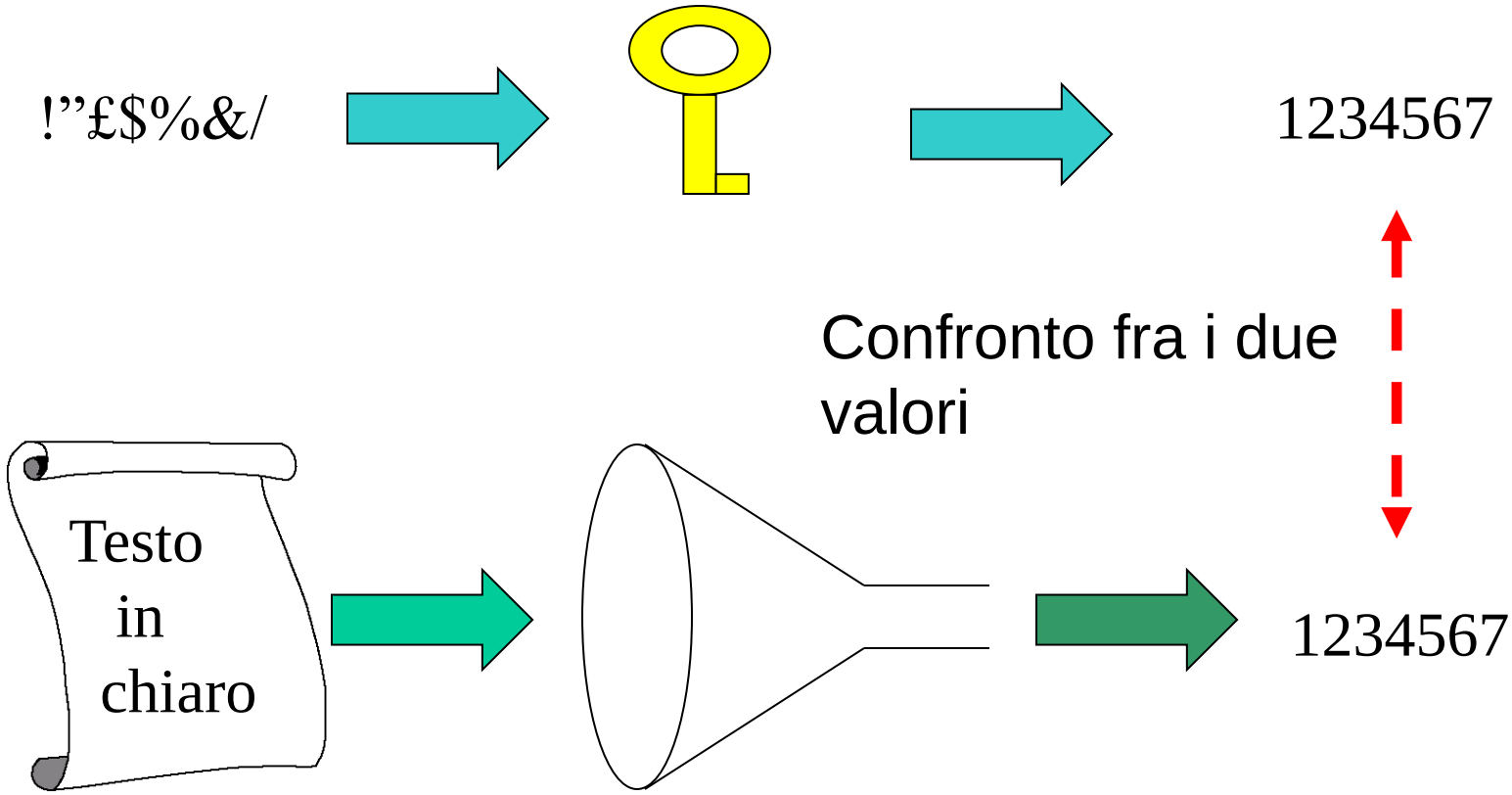


Funzione Hash
monodirezionale

1234567

Valore Hash
Univocamente
Associato al
Messaggio

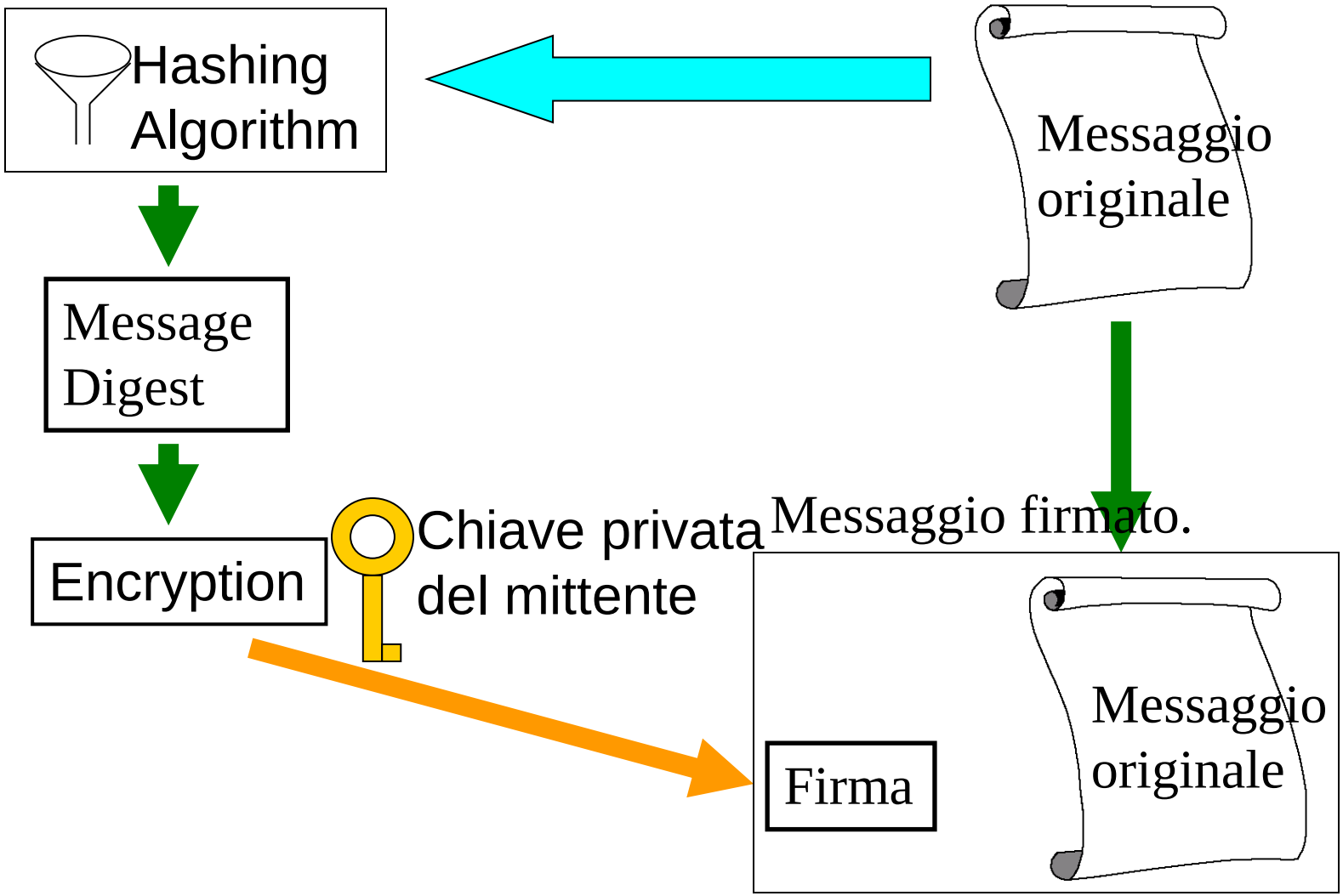
# Applicazione di Hash -verifica



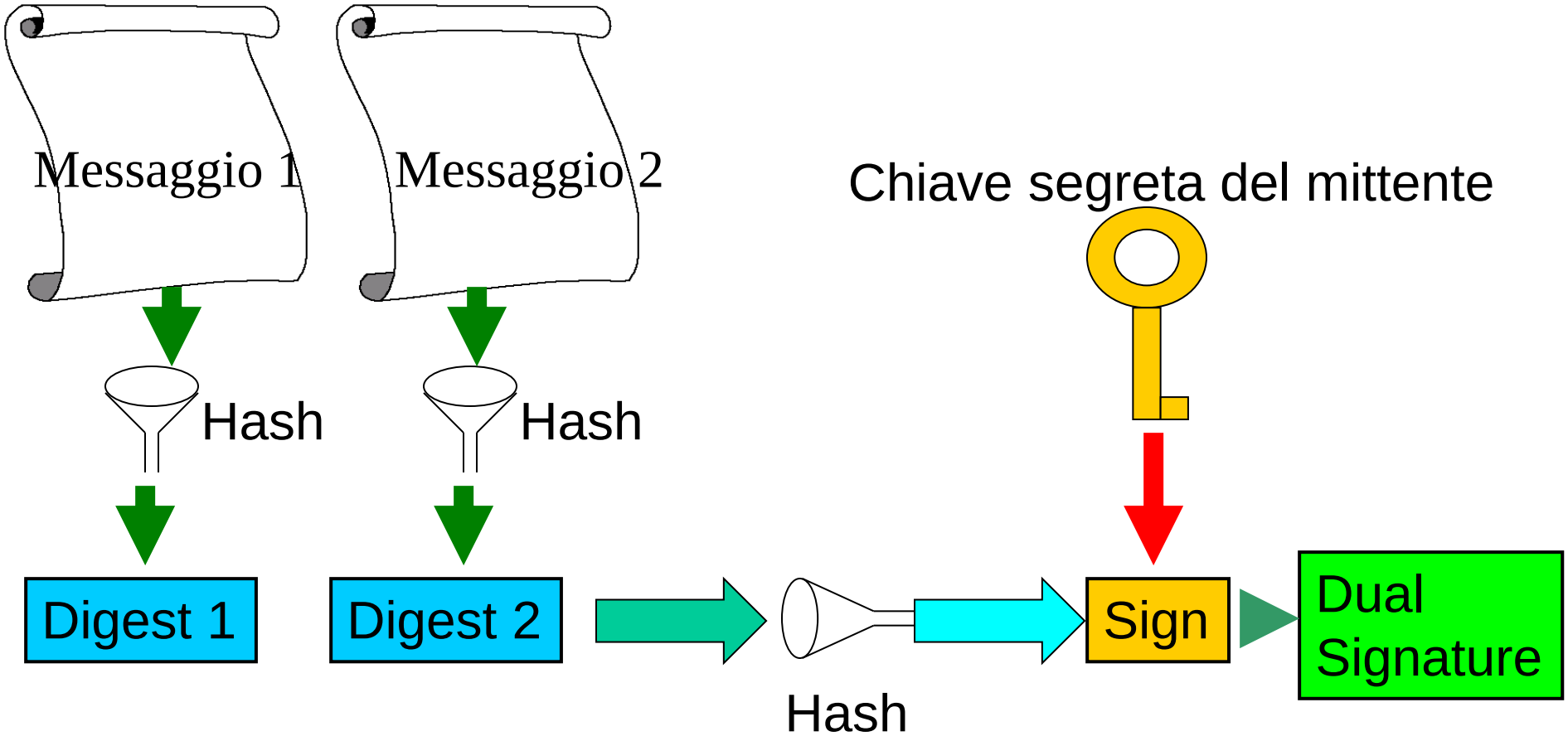
# Nonce

- Protezione contro gli attacchi a replica
- Basato su una informazione usata una sola volta
  - Interi sempre crescenti (non ciclici)
  - Timestamp
  - Timestamp+numero casuale

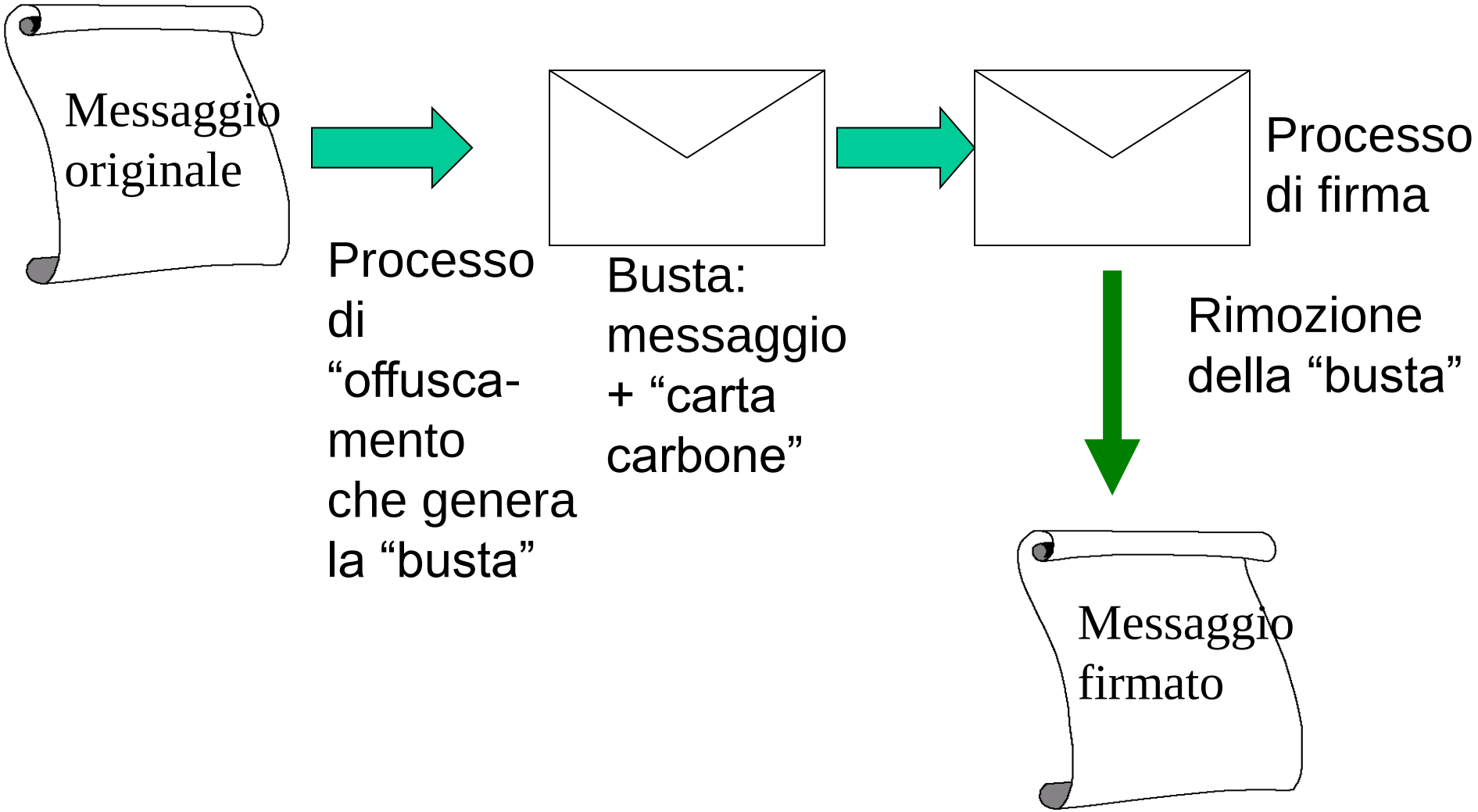
# Firma di un messaggio



# Doppia firma (dual signature)



# Firma cieca (blind signature)



# Proprietà della firma cieca

- La funzione di firma e quella di oscuramento devono essere commutative tra loro
- Dopo il processo di de-oscuramento la firma è una normale firma digitale
- Non dovrebbe potere essere provato che la firma è stata applicata ad un documento “oscurato”

# La firma digitale

"**Firma Elettronica Avanzata**"
insieme di dati in forma elettronica, allegati ad altri dati per garantire autenticazione, che soddisfa i seguenti requisiti:

1. essere connesso in maniera unica al firmatario
2. essere idoneo ad identificare il firmatario

# La firma digitale - 2

3. essere creato con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo
4. essere collegato ai dati cui si riferisce in modo da consentire la identificazione di ogni successiva modifica di detti dati

Dir. 1999\93\Ce (G.U.C.E. 13/12/1999)

# La firma digitale - 3

- Una firma digitale è un valore univoco che un particolare software crea applicando una funzione matematica e una chiave di codifica a un messaggio o un file
- Conferma sia l'identità dell'autore sia la non manipolazione del messaggio durante la trasmissione

# La firma digitale - 4

- Le firme digitali usate negli USA e le funzioni matematiche associate sono codificate nello standard DSS

- Un altro standard molto importante è l'MD-5 (RFC 1321)

# Certificati digitali

I **certificati digitali** sono una rappresentazione visuale di un valore univoco che verifica il contenuto di un file ed il suo produttore sulla base di un sistema di verifica e di firma controllato da terzi

# La firma digitale

Quando si trasmette una firma digitale nel Web il documento è verificato da un'**autorità di certificazione digitale** (es. Verisign)

# Public Key Infrastructure (PKI)

- Organizzazione tecnico-amministrativa che ha l'incarico di fornire, gestire, revocare I **certificati a chiave pubblica**
- Si compone di
  - Autorità di certificazione
  - Autorità di registrazione
  - Autorità di revoca

# Certificati a chiave pubblica

- Struttura dati elettronica che associa in modo biunivoco una chiave pubblica ad un dato (es. Un file)

- Sono praticamente un tipo di certificato digitale, a scadenza

# Struttura PKI

- Gerarchica
- Gestori primari (per UE EuroPKI)
- Gestori nazionali

# Il contratto informatico

- Contratto a distanza, in cui le informazioni sono trasmesse in formato digitale attraverso la rete in tempo reale
- Validità giuridica (D.P.R. 10 Nov. 1997 n.513)
- Presuppone sistemi di autenticazione, sicurezza e non ripudiabilità per potere essere valido

# Validità di una transazione

- la riservatezza dell'informazione digitale
- la paternità dell'informazione digitale
- l'integrità dell'informazione digitale
- la non ripudiabilità dell'informazione digitale
- la certezza del momento in cui è avvenuto l'accordo digitale
- la conferma della ricezione dell'informazione digitale

# Applicazioni

- E-Commerce reale!
- Voto Elettronico via Internet
- Ogni transazione finanziaria su rete pubblica

# Smartcard

- Piccola tessera di plastica
- Simile alle carte di credito
- Contiene un chip di memoria e/o un microprocessore
- Possibilità di conservare con maggiore sicurezza le informazioni memorizzate

# La carta d'identità elettronica

- Tessera simile a una smartcard
- Dotata sia di chip, sia di banda ottica
- Dati personali visibili
- Memorizza dati carta d'Identità
- Strumenti per autenticazione via rete

# Evoluzioni dell'identità elettronica

- Estensione dei meccanismi a chiave asimmetrica
- Identificazione del mittente
- Basi tecniche
- Basi organizzative

# Identità elettronica: sommario

- Applicazione dei sistemi a chiave asimmetrica
- La firma digitale
- Il contratto informatico
- Questioni legali connesse
- Non ripudio di operazioni effettuate
- Applicazioni
- Smartcard ed altri supporti

# La protezione dei dati

# Applicazione ai dati

- Protezione dei singoli file
- Protezione di tutto un file system

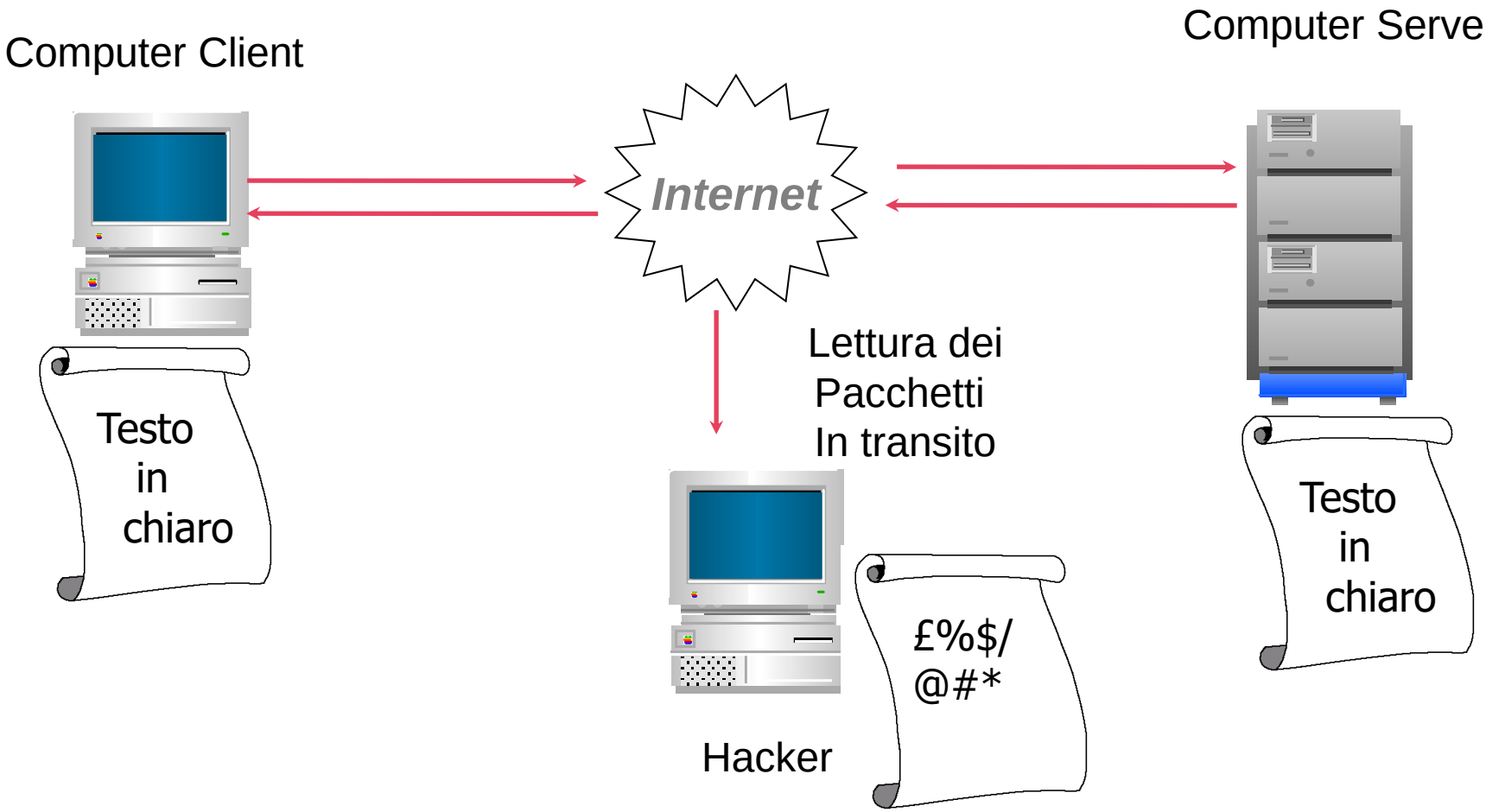
# Protezione di file: il PGP

- Pretty Good Privacy
- Disponibile su varie piattaforme
- Crittografia asimmetrica
- Consente di crittografare file e messaggi di posta elettronica
- Freeware per usi non commerciali
- Consente generazione di chiavi

# Protezione di filesystem: Win2000

- Esiste in Win2000 la funzione di encrypting del filesystem (EFS)
- Protegge completamente quanto cifrato
- E’ legata al profilo dell’utente e quindi i dati potrebbero non essere recuperabili se questo viene danneggiato

# Intercettazione dati criptati



# Applicazione alle comunicazioni

- Cifratura dei file prima della trasmissione (es. Mail)
- Protezione di tutto un canale

# Trasmissione di file cifrati

- PGP applicato alla posta (es. Outlook plug-in)
- Cifratura e trasmissione di file (es. FTP)
- Protocolli semi-cifrati

# Un protocollo semi-cifrato: SCMP

- Canale dati su HTTP standard
- Ogni transazione corrisponde a un pacchetto dati
- Indicazioni di sessione
- Dati sensibili crittografati tramite lo standard SCMP (Simple Commerce Messaging Protocol)

# Protezione dei canali

- Protocolli a livello applicativo (S-HTTP, SSL, SSH, SSH-VPN)
- Protocolli a livello trasporto (IPSec, IPSec-VPN)

# Protocollo Secure Socket Layer (SSL)

- Protocollo di sicurezza general-purpose
- Opera al di sopra del livello trasporto nello stack TCP/IP
- Le parti si identificano (autenticano) producendo certificati che associano il loro nome a una chiave pubblica

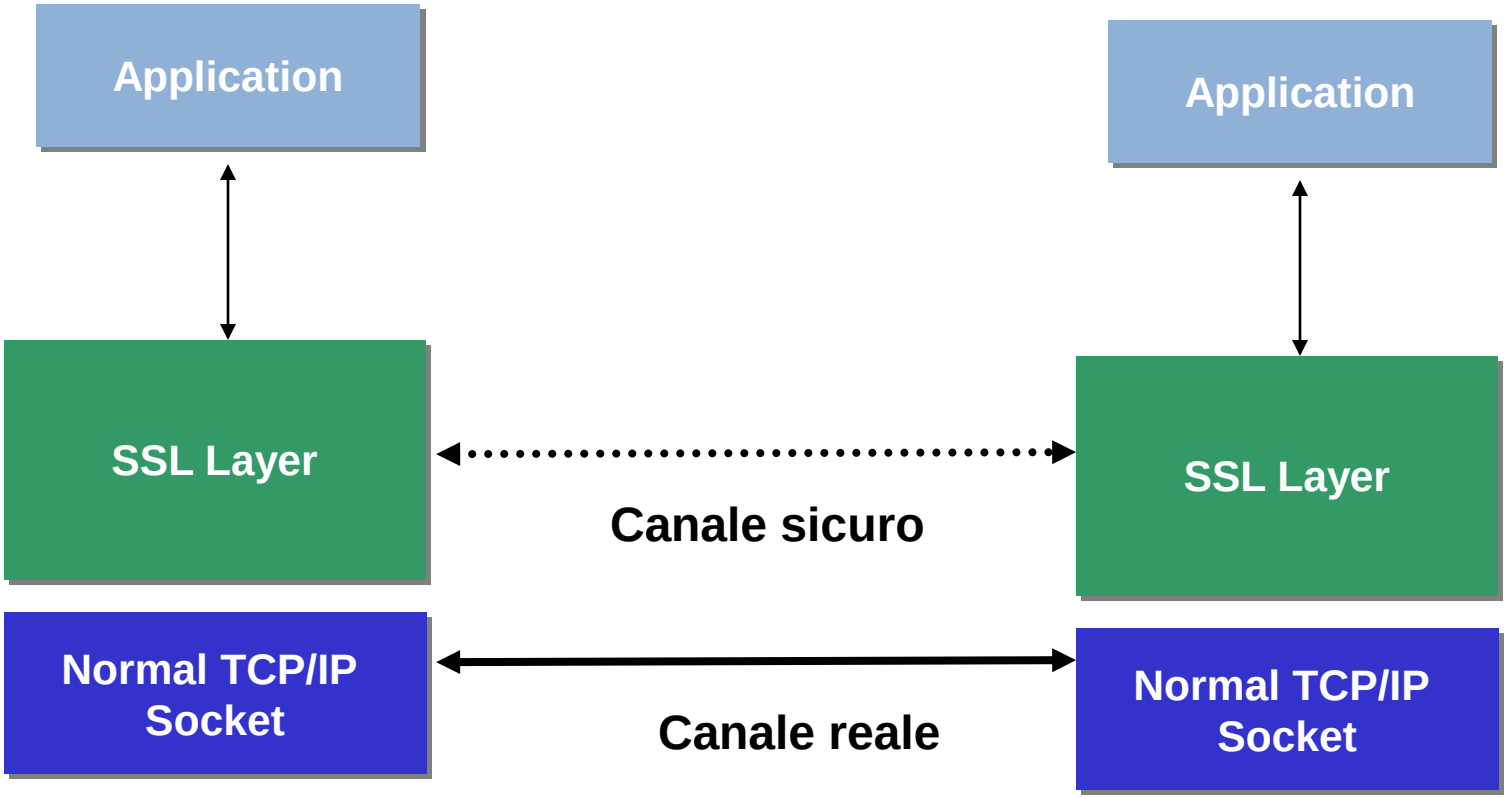
# Protocollo SSL

- Autenticazione di server e client sono basate sui certificati a chiave pubblica
- Handshaking e authenticazione usano le chiavi asimmetriche
- Una chiave simmetrica (di sessione) viene generata durante la fase di handshaking

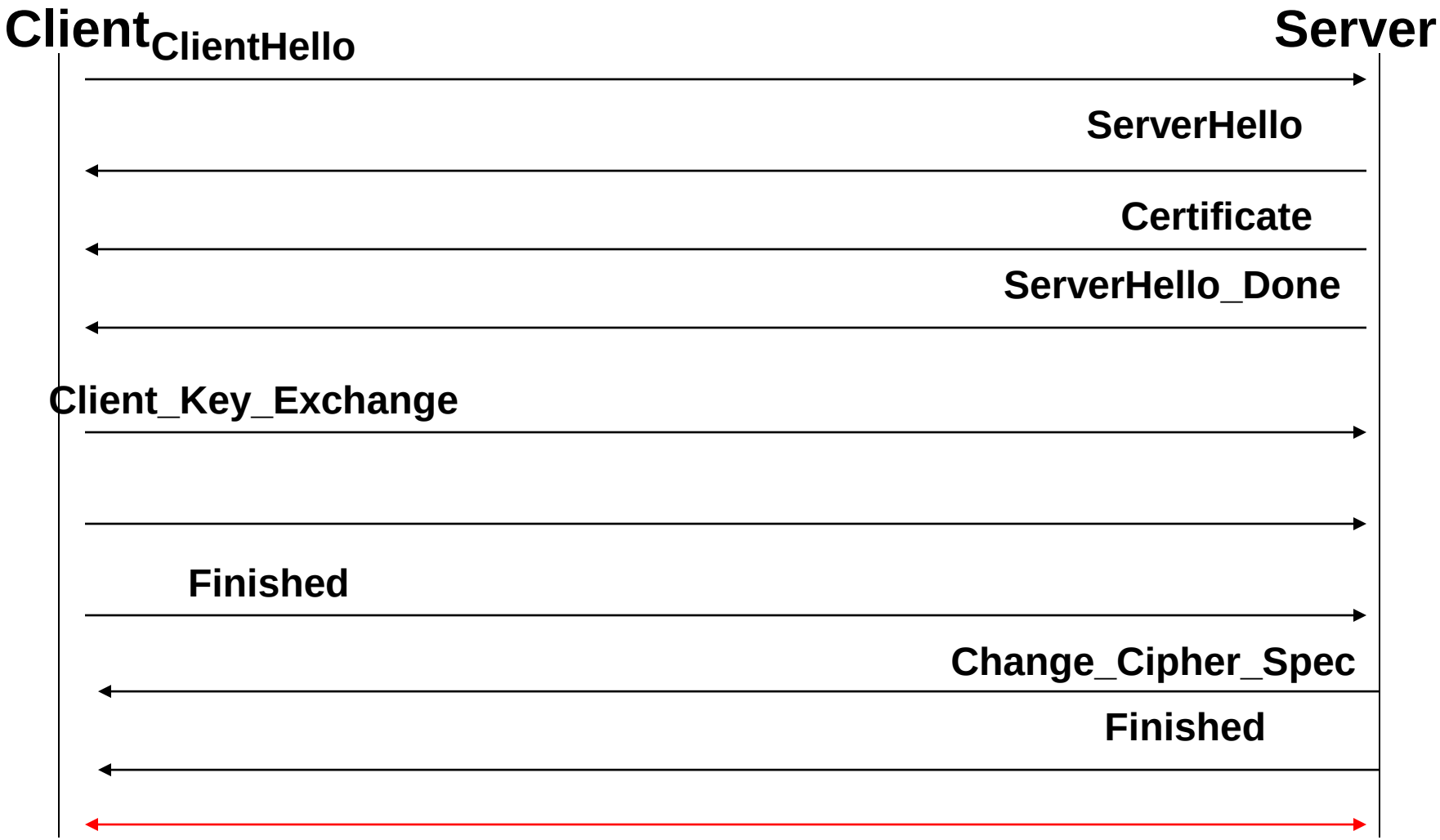
# Protocollo SSL

- La protezione dei dai sul canale sfrutta questa chiave simmetrica
- Diversi standard crittografici sono supportati (DES, RC4, IDEA per la trasmissione, RSA, DSS per l'autenticazione)
- I Pacchetti sono inoltre protetti con codici hash

# Protocollo SSL: l'architettura



# Protocollo SSL: handshaking



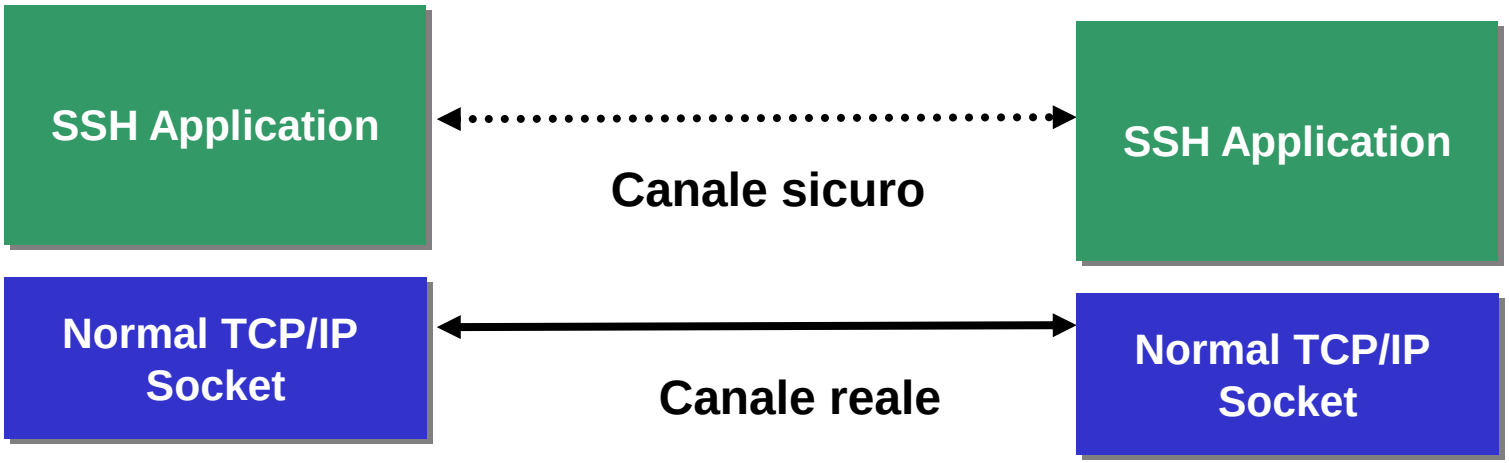
# Protocollo SSL: applicazioni

- Ogni servizio basato su TCP/IP può essere protetto usando SSL
- L'uso più frequente è HTTPS (HTTP su SSL)
- Anche SSL-telnet viene usato

# Protocollo Secure Shell (SSH)

- Protocollo general-purpose per l'autenticazione e la crittografia di canali
- E' iniziato come rimpiazzo del protocollo **rsh** di UNIX
- L'implementazione avviene al livello applicativo
- Esistono versioni commerciali e public domain (OpenSSH)

# SSH: l'architettura



# SSH: caratteristiche

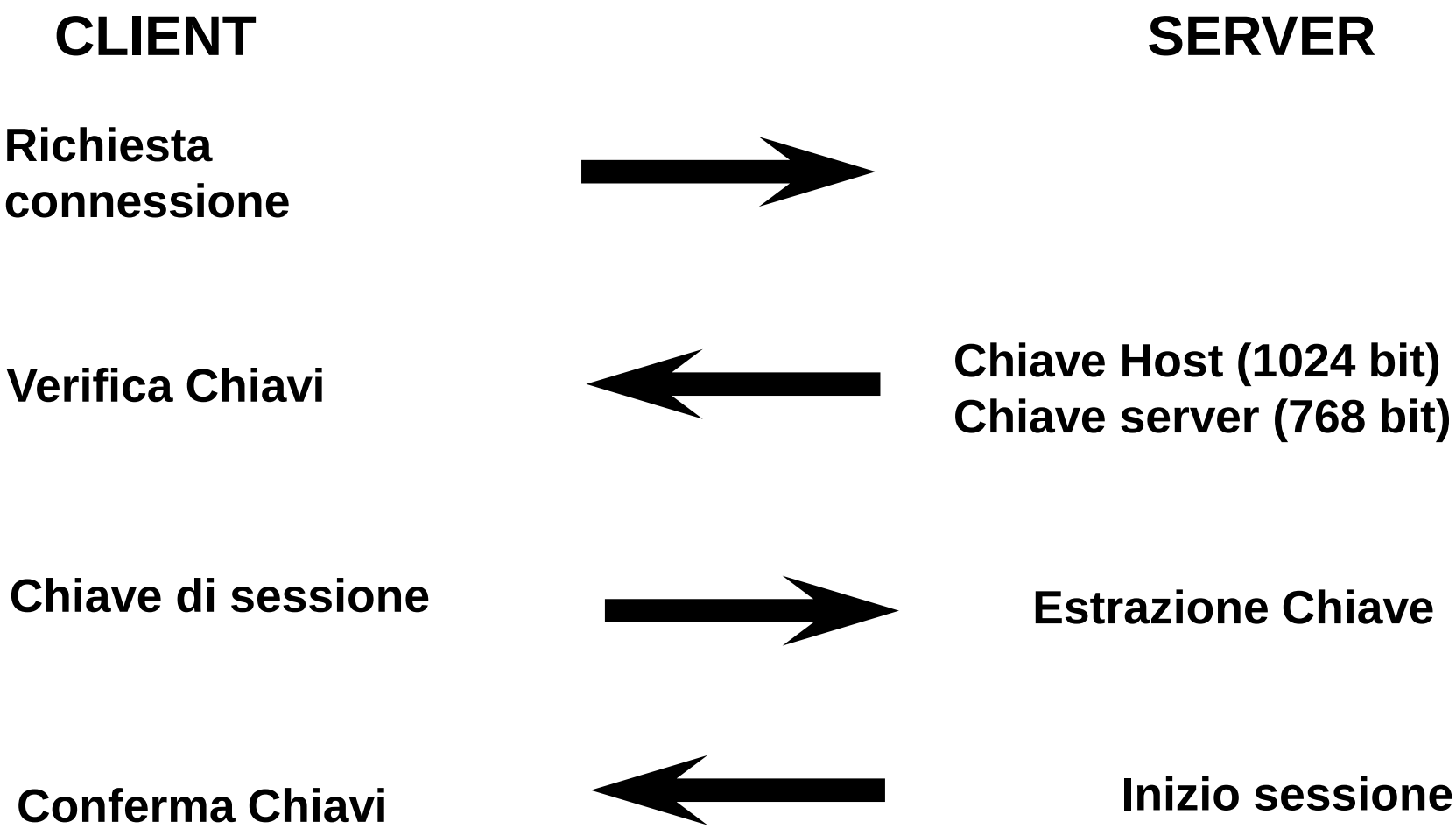
- Trasporto sicuro dei Dati
- Si appoggia sul protocollo TCP/IP
- Autenticazione con chiavi asimmetriche
- Autenticazione Host
- Autenticazione Utenti
- Crittografia dati fino a 256 bit (vari metodi supportati)

# SSH: usi

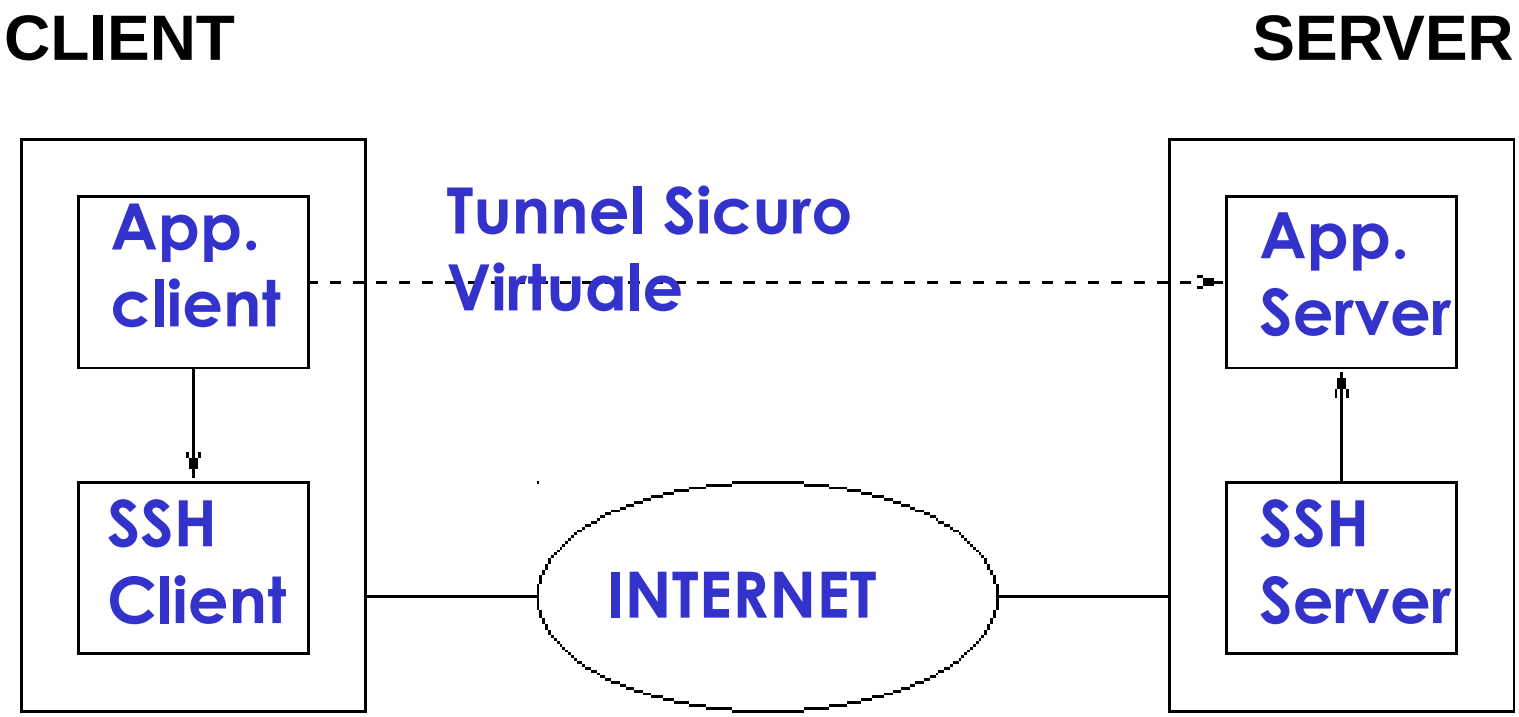
- Le applicazioni SSH garantiscono accesso sicuro a server (es. telnet, esecuzione remota di programmi) e trasferimenti sicuri dei dati (SFTP e secure copy)

- SSH offre anche un utilissimo meccanismo di tunneling basato sul port forwarding

# SSH: handshaking



# SSH: tunneling




PORT FORWARDING

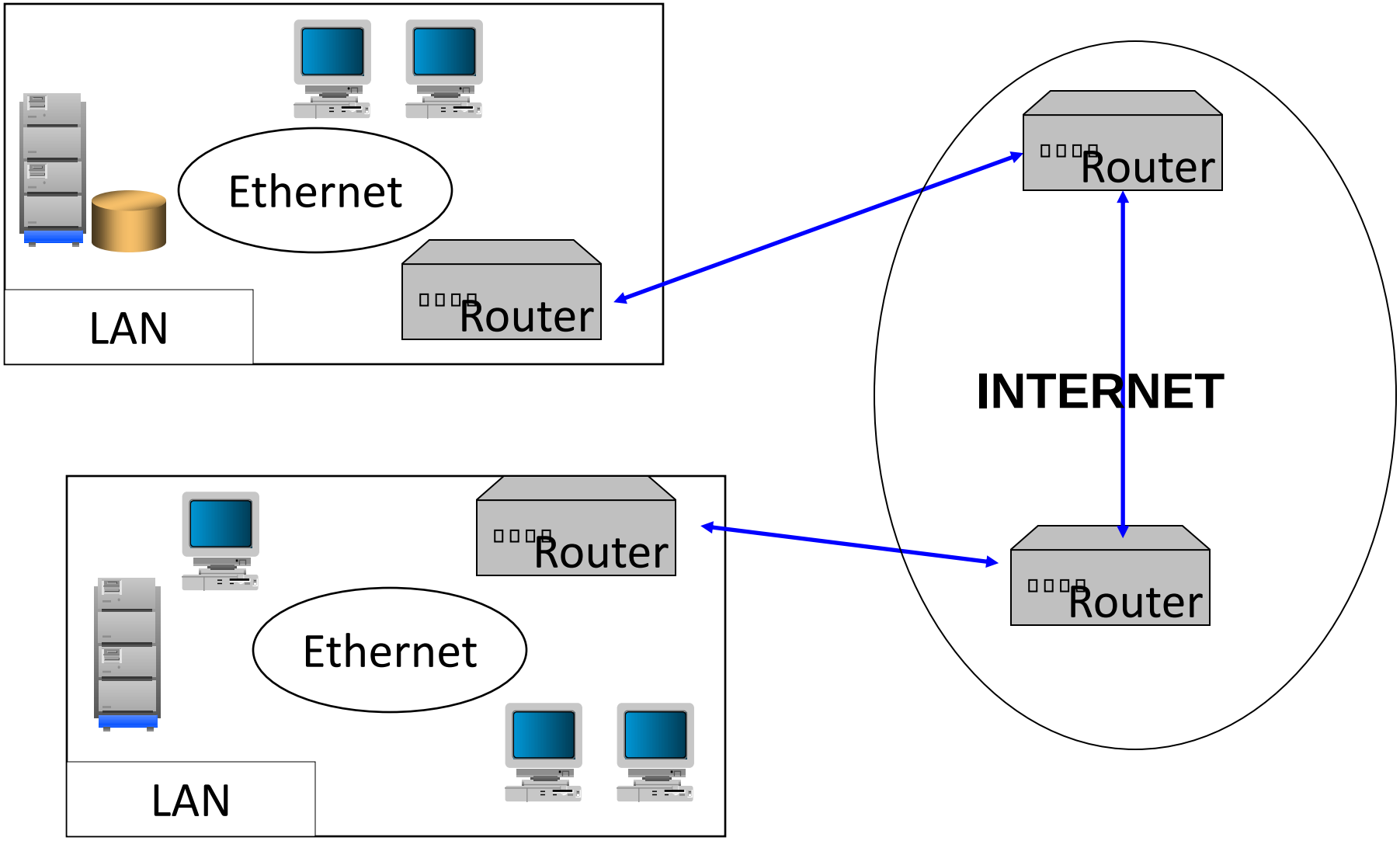
# IPSec-VPN

- IPSec è un'estensione standard di TCP/IP che consente crittografia e autenticazione del canale già al livello trasporto
- Una VPN o rete privata virtuale è un insieme di computer collegati fra loro in modo "riservato" attraverso una rete pubblica di comunicazione come Internet.

# IPSec-VPN - 2

- Attraverso il TCP tunnelling, meccanismo simile al port forwarding, tutte le comunicazioni fra due reti possono essere fatte transitare in un tunnel IPSec sicuro
- Occorre però il controllo di tutti i router attraverso cui si transita (fornito dall'ISP)
- Oppure essere sicuri che non vi siano filtri (FreeS/WAN)

# IPSec-VPN - 3



# La protezione dei Sistemi

# Controllo anti-intrusione: argomenti

- Firewall e loro caratteristiche
- Il controllo fine dei protocolli
- Filtri IP e ACL dei router
- Controllo degli ingressi via chiave
- Controllo globale delle reti: tipi di Monitoraggio
- Auditing globale delle operazioni e Accounting

# I componenti per la protezione dei sistemi

- Firewall
- Screening Router
- SmartHub
- Network monitor

# L’intrusione

- Ingresso non autorizzato in un sistema (login)
- Accesso non autorizzato a servizi e/o dati di un sistema
- DoS di un sistema

# Livelli operativi delle infrastrutture

- Applicazione
- Trasporto (TCP)
- Rete (IP)
- Data Link
- Fisico

Firewall/proxy
Router
IP Filter
Smart Hub
Interruttori

# Il Firewall

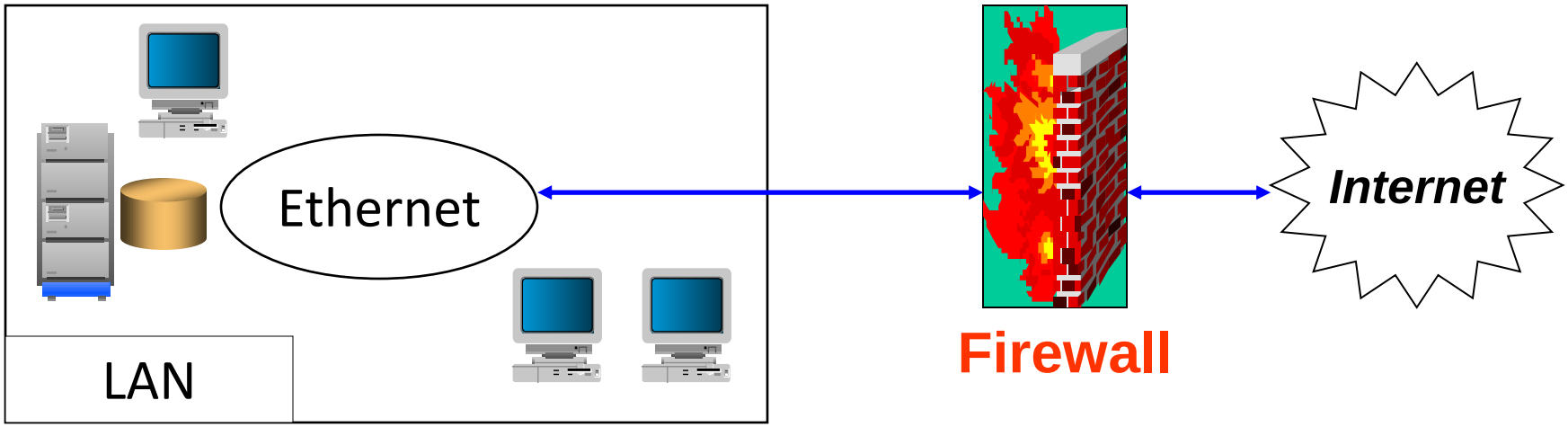
- "Sistema o gruppo di sistemi che impongono una politica di controllo degli accessi fra due reti".(NCSA)

- I firewall possono essere usati entro una rete per garantire la sicurezza fra i vari dipartimenti di un'organizzazione

# Categorie principali di Firewall

- Firewall personale
- Firewall interno
- Firewall di confine

# Una rete tipo




**Tipicamente una rete è isolata da Internet**
**e tutto il traffico transita attraverso il firewall**

# Il Firewall - 2

- Un firewall da solo non può bloccare l'accesso dei virus alla rete che protegge
- Prima di mettere in opera un firewall, si deve sviluppare un piano di sicurezza che definisca il tipo di accesso consentito agli utenti esterni e a quelli interni

# Tipi principali di Firewall

- Firewall a livello rete
- Firewall a livello applicazione
- Firewall a livello circuiti

# Architetture principali di Firewall

- Firewall dual-home host
- Firewall screened-host
- Firewall screened-subnet

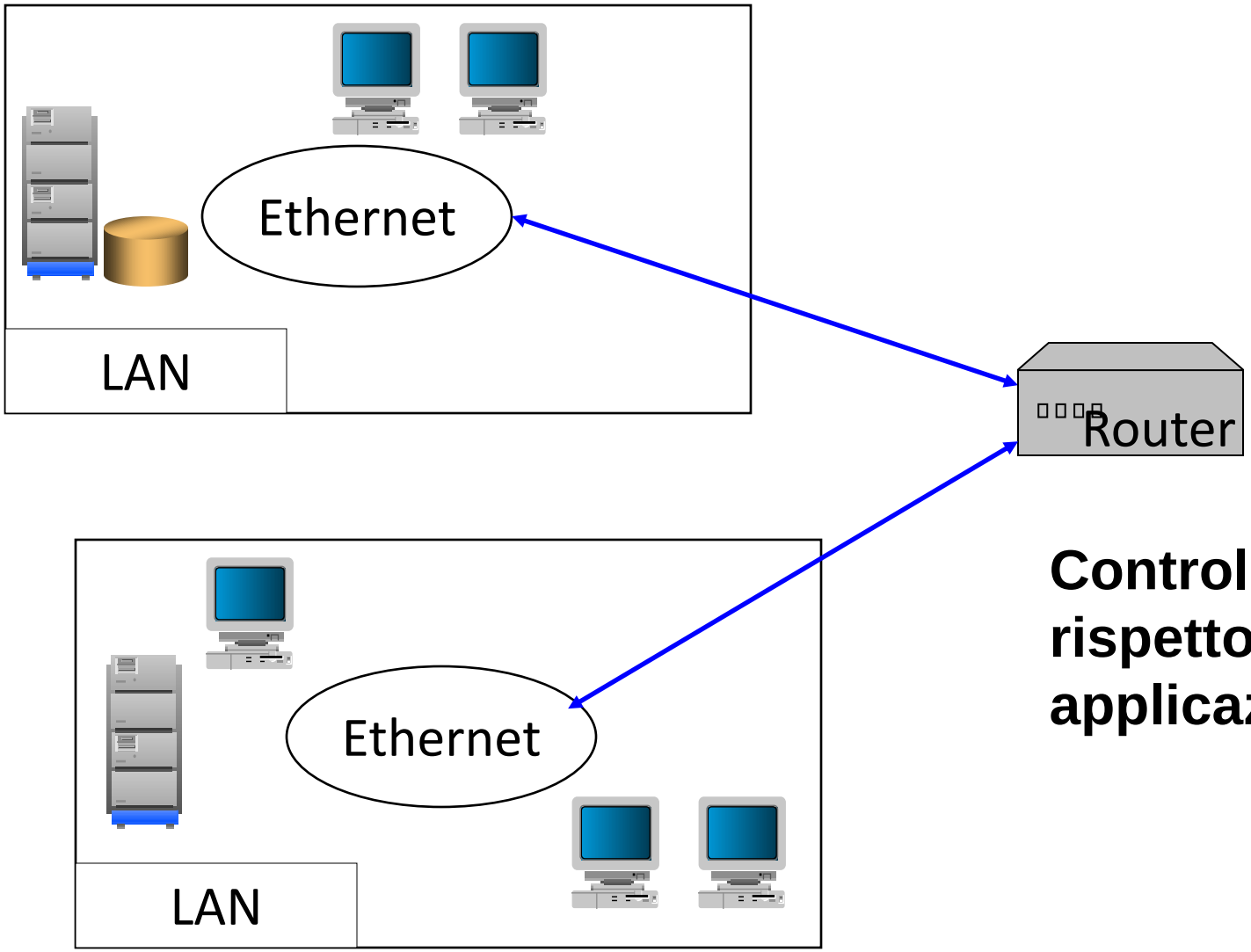
# Bastion Host

- Computer della rete “particolarmente preparato a respingere attacchi contro la rete stessa” (bastione)
- Punto nevralgico per l’ingresso/uscita dalla rete stessa
- Può “contenere” il firewall

# Screening Router

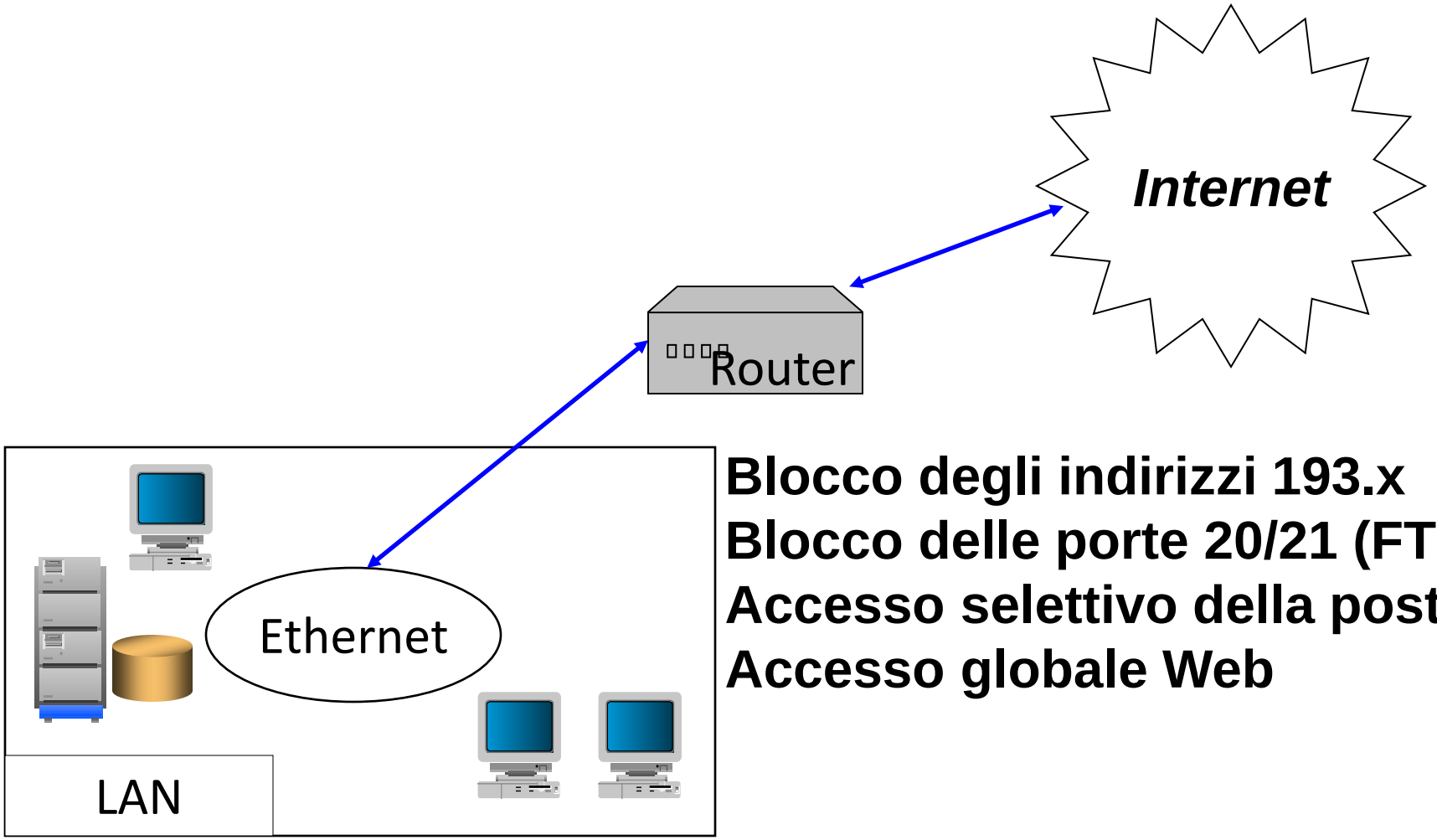
- Dispositivo che filtra i pacchetti che lo attraversano in base a determinati criteri
- Filtro per indirizzi IP
- Filtro per porta (servizio)

# Uno screening router in azione



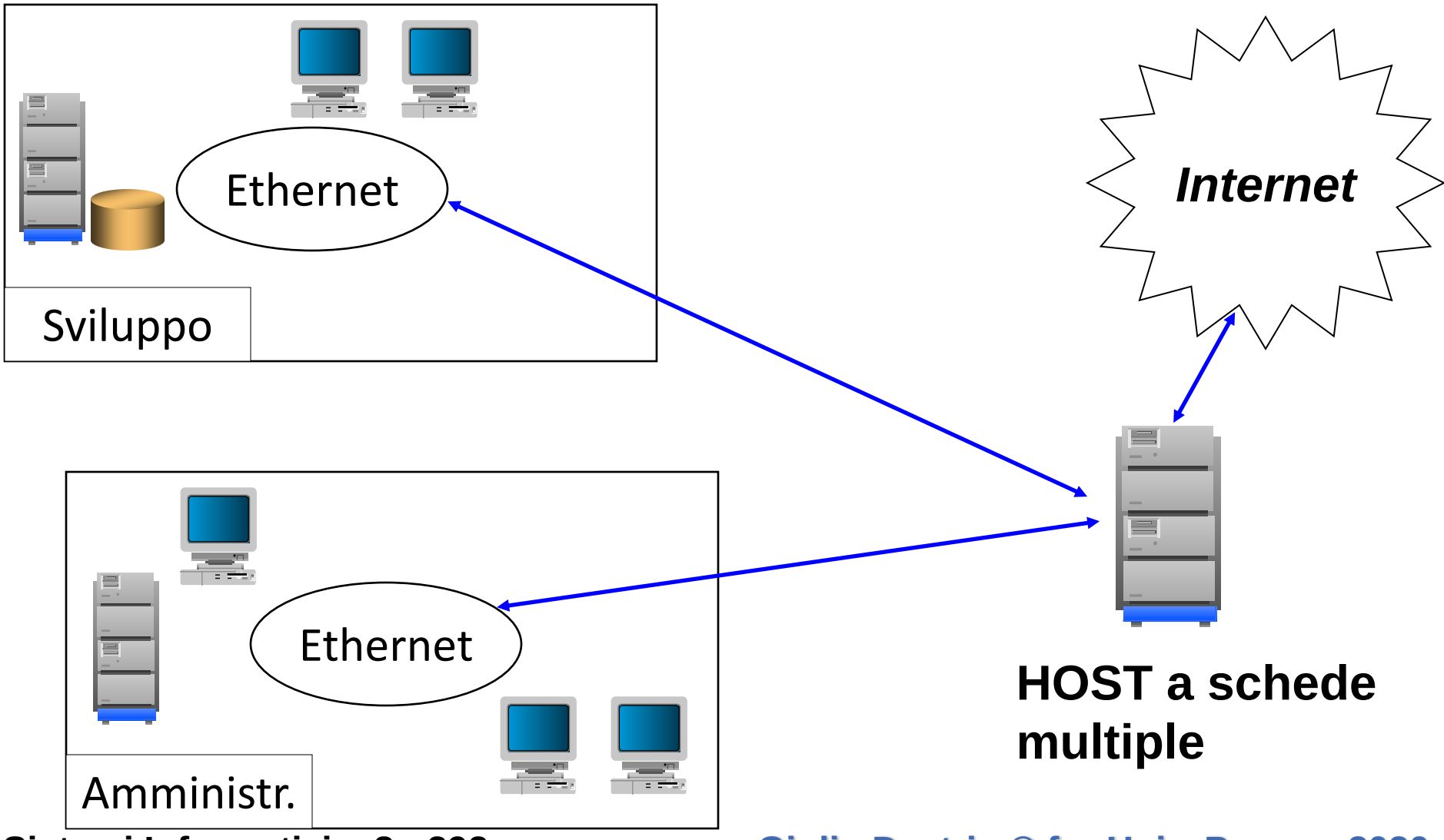

**Controllo trasparente rispetto alle applicazioni**

# Il ruolo dello screening router




**Blocco degli indirizzi 193.x**
**Blocco delle porte 20/21 (FTP)**
**Accesso selettivo della posta**
**Accesso globale Web**

# Protezione di più reti



# Cosa un Firewall non fa

- Garantire l'integrità dei dati
- Proteggere dai virus

- Proteggere da disastri

- Autenticare le fonti dei dati
- Garantire la riservatezza dei dati

# Definire un Firewall

- Gli utenti Internet devono poter prelevare file dal server della rete?
- Gli utenti Internet devono poter inviare file al server della rete?
- Devono esistere sbarramenti selettivi per determinati utenti o per determinati host?

# Definire un Firewall - 2

- Esiste un sito Web interno alla rete accessibile da Internet?
- Devono essere fatte sessioni Telnet attraverso il firewall (in un senso o nell'altro)?
- Che protocolli devono passare attraverso il firewall?

# Definire un Firewall - 3

- Che livello di accesso a Internet e al Web devono avere i dipendenti?
- Che risorse umane si possono/devono impiegare per la gestione/verifica del firewall?
- Cosa può succedere alla rete se un hacker riesce comunque ad entrare?

# ACL e regole

- Le ACL (ACcess List) sono le regole che governano il funzionamento dei filtri
- Ogni pacchetto viene valutato in base alle ACL e respinto o fatto passare

# ACL e regole - 2

Sono possibili due politiche:

- Tutto ciò che non è esplicitamente negato è permesso (default allow)
- Tutto ciò che non è esplicitamente permesso è negato (default deny)

# ACL e regole - 3

Vengono considerate varie informazioni:

- Indirizzo di origine dei dati
- Indirizzo di destinazione
- Tipo di protocollo: TCP, UDP, ICMP
- Porta di origine e di destinazione (servizio)
- Se il pacchetto indica una richiesta di connessione

# Firewall a livello della rete

- E’ praticamente uno screening router in funzione su un computer
- Per ogni pacchetto, in funzione delle ACL impostate, stabilisce se deve passare o no
- E’ trasparente rispetto alle applicazioni

# Firewall a livello applicazione

- E’ praticamente un **server proxy**
- Un server proxy comunica con i server della rete esterna per conto dei client della rete interna (es. tunneling)
- Le applicazioni client devono supportarlo
- Proxy Web e FTP
- Proxy SOCKS

# Firewall a livello circuito

- E’ simile al caso precedente
- E’ trasparente per le applicazioni
- Realizza tunneling
- Circuiti bloccati (da IP e porta  a IP e porta)
- Circuiti trasparenti (es. DNS)
- Specifico per singole applicazioni (protocol check)

# Firewall a livello circuito - 2

- Esempio: proxy per servizio POP o IMAP
- Esempio: Apache come proxy per servizio HTTP IIS
- Esempio: Oracle SQL*Net 8 attraverso i firewall

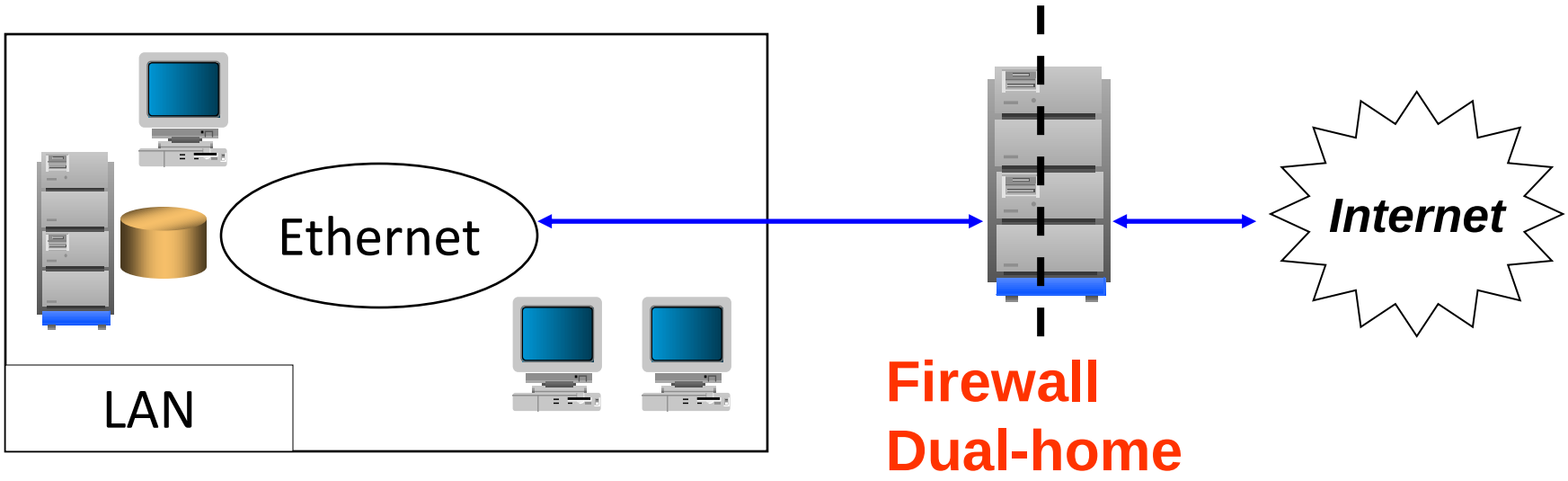
# Un Firewall completo

- Comprende tutti e 3 i servizi precedentemente definiti
- Può essere software (operare cioè su un host dedicato, es. Linux)
- Può essere hardware (es. Cisco PIX o Nokia)

# Firewall dual-home host

- Esistono due interfacce di rete (interna ed esterna)
- Il routing diretto fra le schede è disabilitato
- A livello applicazione avviene il Checkpoint sui pacchetti
- Un gruppo di proxy a livello applicazione e/o circuito realizza solo le connessioni abilitate dalle ACL

# Firewall dual-home host - 2

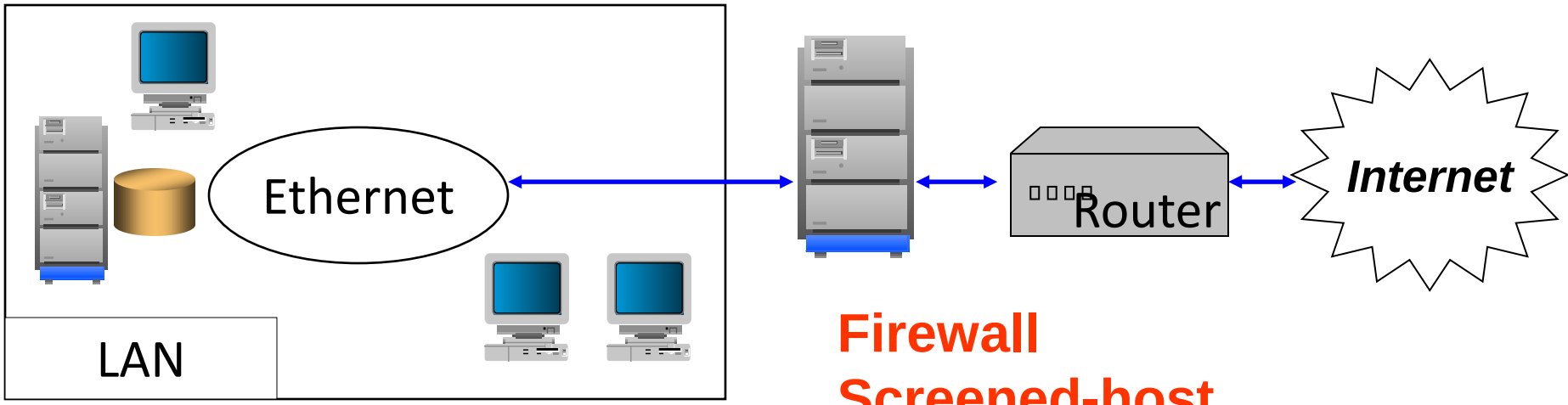



**La LAN vede l'interfaccia di rete "interna" del Firewall, mentre Internet vede l'interfaccia "esterna"**
**Anche gli indirizzi IP delle due schede sono diversi**

# Firewall screened-host

- Si compone di uno screening router e di un host
- Il router filtra il traffico secondo le ACL
- L'host non è connesso alla rete ma la vede attraverso il router
- La rete interna passa attraverso l'host

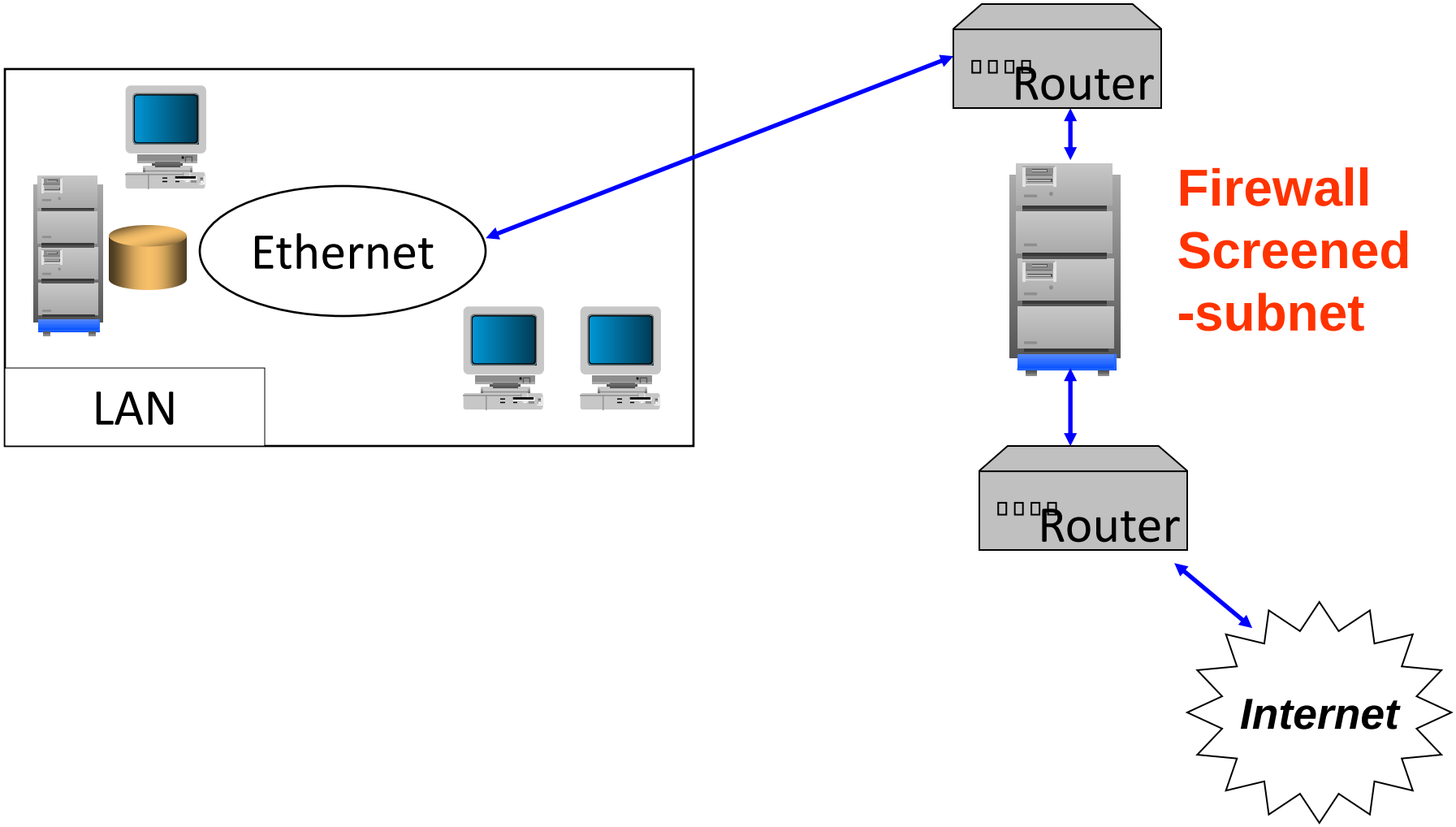
# Firewall screened-host - 2



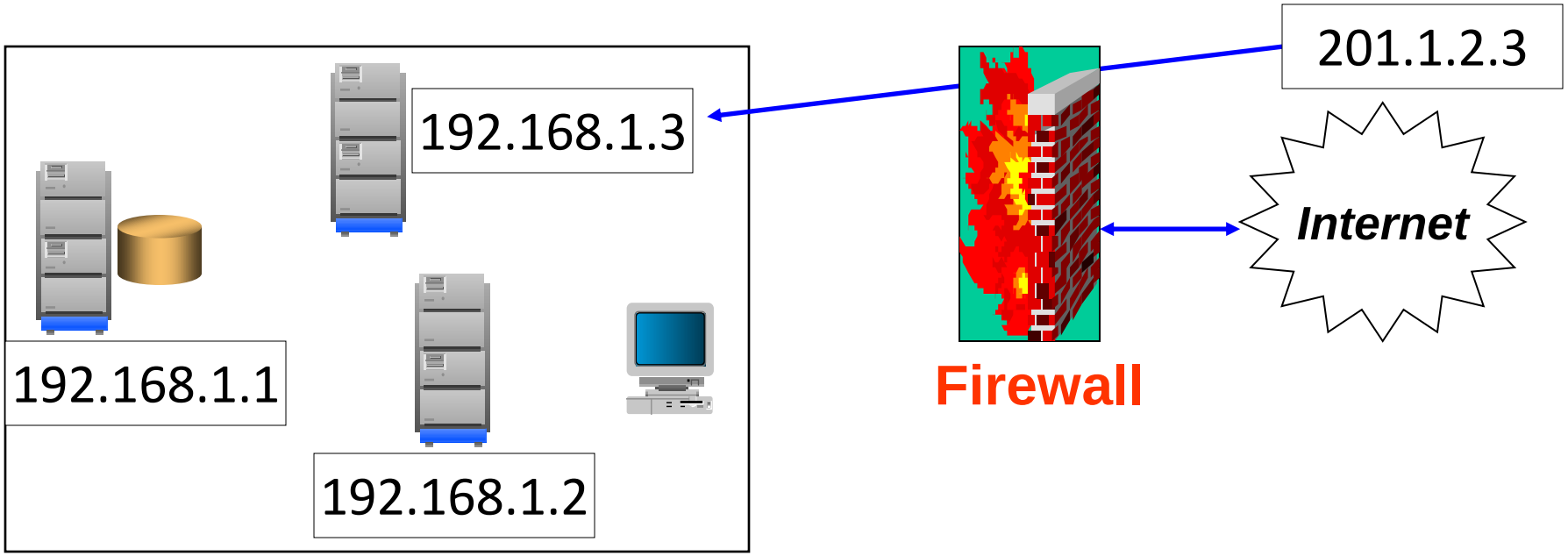
# Firewall screened-subnet

- Si compone di due screening router e di un host
- I router filtrano il traffico secondo le ACL, il primo controlla la LAN ed il secondo il traffico in ingresso
- Offre la protezione migliore in assoluto

# Firewall screened-subnet - 2

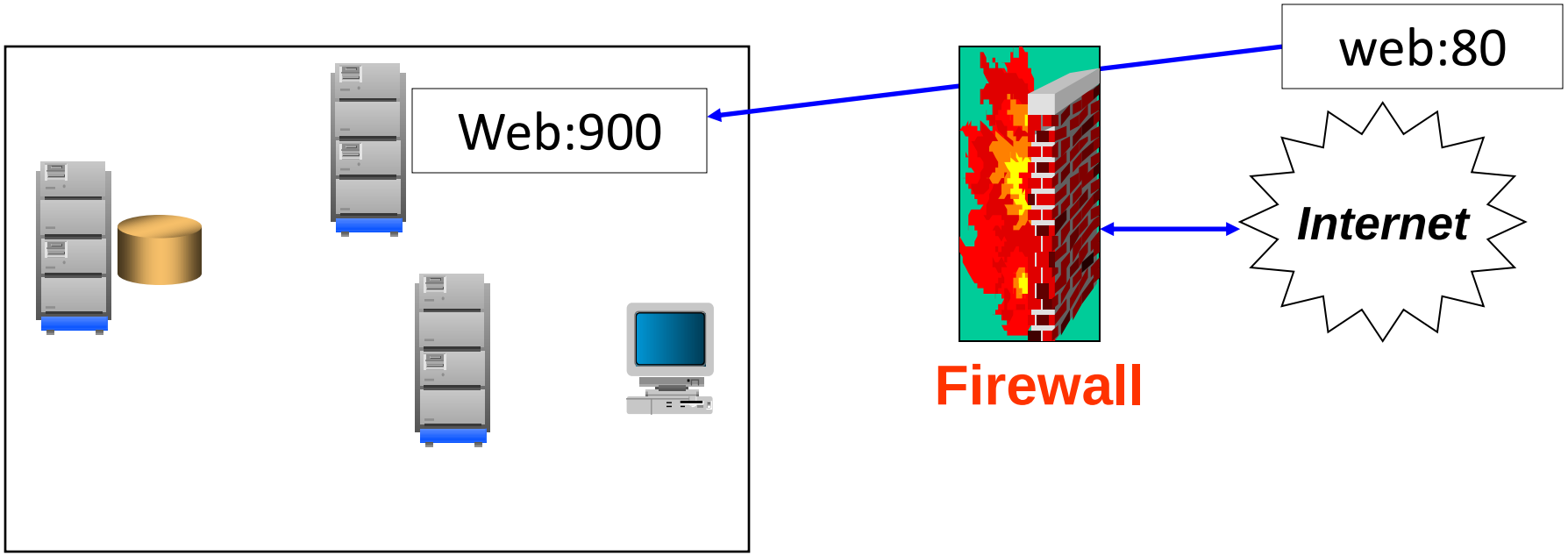


# NAT (Network Address Translator)




**Gli host sono visti dall'esterno con un IP diverso dal loro**

# PAT (Port Address Translator)




**La porta vista “esternamente” al firewall è diversa da quella “reale” interna alla rete**

# Smart Hub e Switch V-LAN

- Si comporta in modo analogo ad un filtro IP, ma agisce a livello MAC (Data Link ovvero Ethernet)
- I pacchetti vengono filtrati in base al codice identificativo della scheda Ethernet che li ha emessi
- Consente la segmentazione di LAN (V-LAN)
- E' vincolato alle schede hardware

# Controllo degli accessi con chiave

- Permette di validare l'ingresso in un sistema (o l'accesso ad un particolare servizio) tramite una coppia chiave pubblica-chiave privata
- Solo chi possiede la chiave (ed eventualmente proviene da un dato IP) può entrare
- Es. SSH

# Network monitor

Strumento di osservazione e registrazione del traffico di rete

- Suddivisione traffico tra locale e remoto
- Suddivisione per protocolli (IP, Netbios…)
- Suddivisione per servizi (HTTP, SMTP…)

# Network monitor - 2

- Elenco connessioni attive sull'intera rete (identificate da IP src, IP dest, port src, port dest)
- Visualizzazione del contenuto di ogni connessione (Sniffer) e salvataggio
- Scansione di ciascun host
- Valutazione statistica

# Controllo globale delle reti

- Monitoraggio del traffico e dei suoi flussi (network monitor)
- Monitoraggio del carico dei sistemi
- Monitoraggio dei processi

# Il controllo dei processi

- Il processo è il programma in esecuzione
- Esistono nei sistemi operativi strumenti per il controllo (es. ps, task manager ecc…)
- Una sessione non autorizzata o un trojan in esecuzione producono un processo

# Il carico dei sistemi

- Numero utenti collegati via servizi (Telnet, FTP, connessioni disco, Oracle ecc…)
- Numero di connessioni socket TCP/IP aperte
- Carico della macchina (CPU, RAM)
- Spazio disco disponibile su varie partizioni

# Auditing globale delle operazioni

- In generale dovrebbero essere controllate tutte le operazioni più importanti che avvengono sia a livello di rete sia a livello dei singoli server
- Ciò presuppone un'accurata analisi dei log
- Con analisi statistiche dei risultati dovrebbero risultare evidenti attività "anomale"

# Accounting

- Per avere un controllo ancora migliore, bisogna andare oltre, cercando di risalire a "chi ha fatto un'attività insolita e perché" (potrebbe essere perfettamente lecita)
- L'accounting riprenderà spazio man mano che si diffonderà l'outsourcing dei sistemi informatici

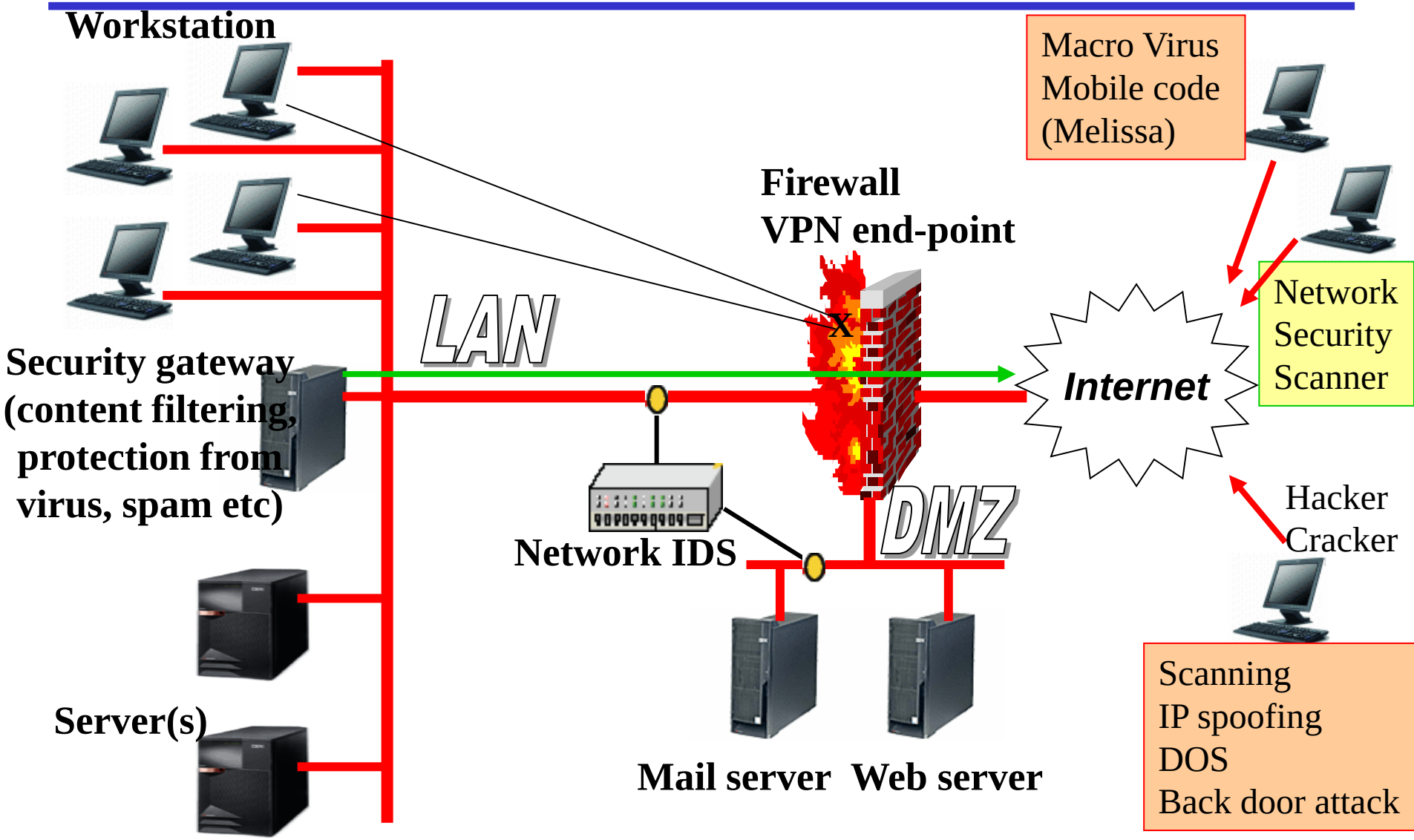
# Controllo anti-intrusione: sommario

- Firewall, filtri e loro caratteristiche
- Controllo globale delle reti: tipi di Monitoraggio

# Sistemi di controllo

- Sistemi di gestione globale possono essere implementati attraverso suite di controllo
- Commerciali: IBM Tivoli, CA Unicenter…
- Freeware: Nagios…

# Scenario di protezione totale



# La gestione della Sicurezza

# I punti chiave per la gestione

- Scopo della rete e dei sistemi
- Tipologie di applicativi in uso
- Esperienza tecnica e pratica (in inglese ***skill***) degli amministratori e degli utenti
- Politica del rischio stabilita in azienda
- Rapporto costi/benefici, tra le misure di sicurezza adottate e il loro costo

# La gestione dei sistemi informatici

- Le politiche globali di gestione
- Il compromesso fra sicurezza ed uso
- Sistemi ed utenti
- Il problema delle password
- Necessità del coinvolgimento operativo degli utenti

# Il problema dell'aggiornamento

- Aggiornamento periodico dei sistemi
- Verifiche periodiche dei bollettini di sicurezza
- Installazione delle patch di sicurezza
- Aggiornamento continuo dei gestori

# Non esiste una politica buona per tutti

La politica di gestione va decisa caso per caso, in funzione di tanti fattori:

- Scopo della rete/sistemi
- Applicativi in uso
- Skill degli amministratori e degli utenti
- Politica del rischio
- Rapporto costi/benefici

# I problemi organizzativi sono complessi

"I problemi tecnici sono molto spesso risolubili, quelli umani quasi mai"

Antico Proverbio

# L’approccio “Militare”…

- Obiettivo: Sicurezza “Assoluta”
- Scoprire in anticipo i tipi di attacco e prevenirli
- La tecnologia può risolvere i problemi
- I prodotti nuovi per la sicurezza sono sempre migliori

# … e le sue conseguenze

- Il responsabile della sicurezza dice sempre "no"
- La sicurezza assorbe troppe risorse
- La sicurezza diviene un ostacolo per il Business

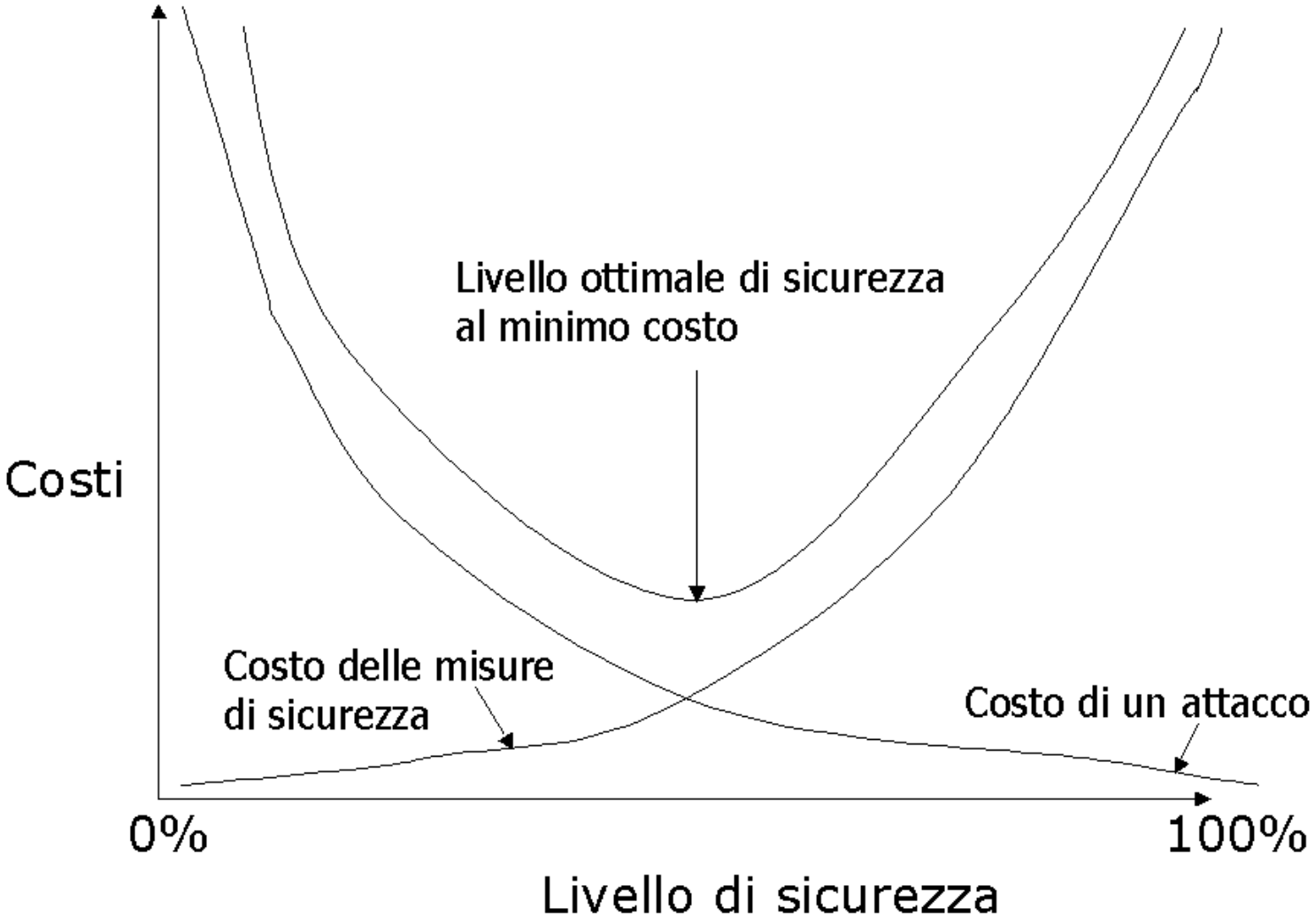
# L’approccio “Risk management”…

- La Sicurezza è "relativa"!
- Ci sono molti rischi e bisogna tenerli in considerazione
- Ci sono molte soluzioni, dipendono dal contesto
- Sono sempre esistiti gli incidenti: le aziende previdenti si riprendono e vanno avanti

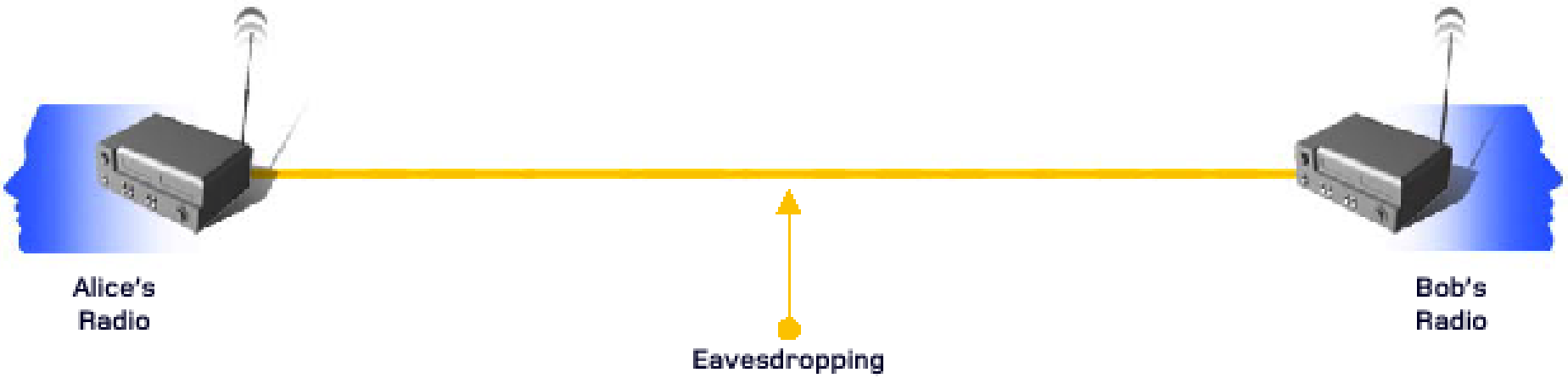
# ...ed i suoi metodi

- Accettare il rischio ("il rischio è insito negli affari")
- Ridurre il rischio con la tecnologia
- Ridurre il rischio con procedure opportune
- Ridurre il rischio traferendolo (assicurazioni e/o outsourcing)

# Rapporto costi/benefici

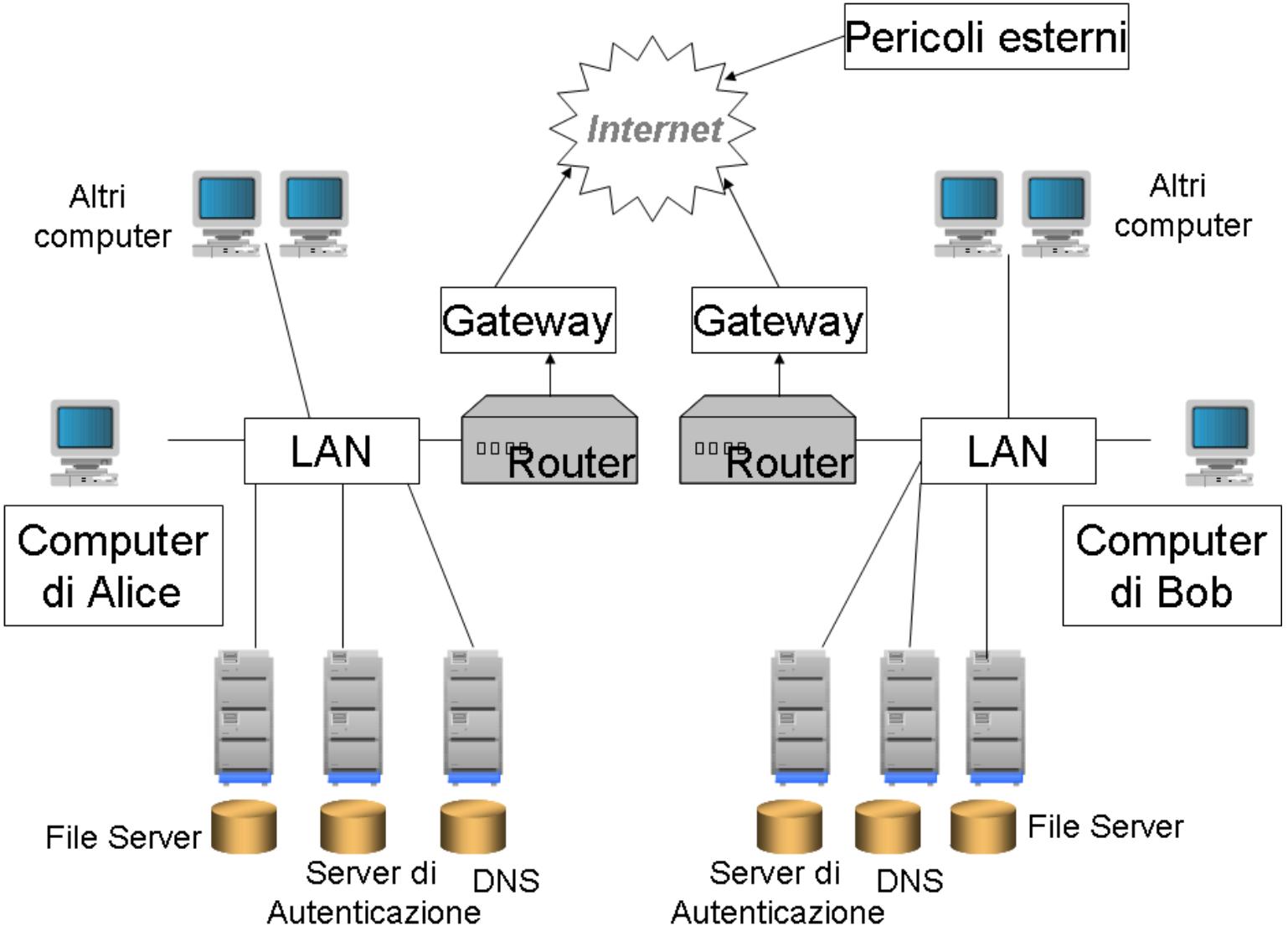


# Determinazione della sicurezza




Nel modello presentato la sicurezza è assoluta: basta crittografare la trasmissione, in quanto l'unico pericolo è l'ascolto fraudolento dei dati in transito

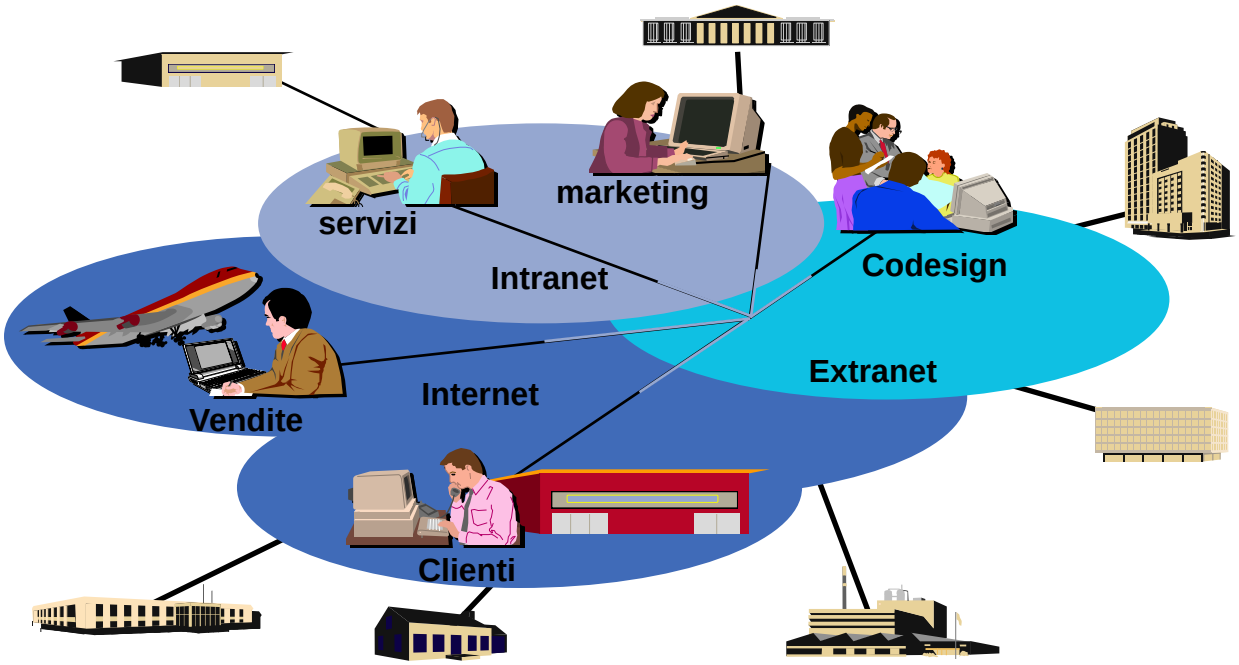
# … e su Internet?



# Esame di case study

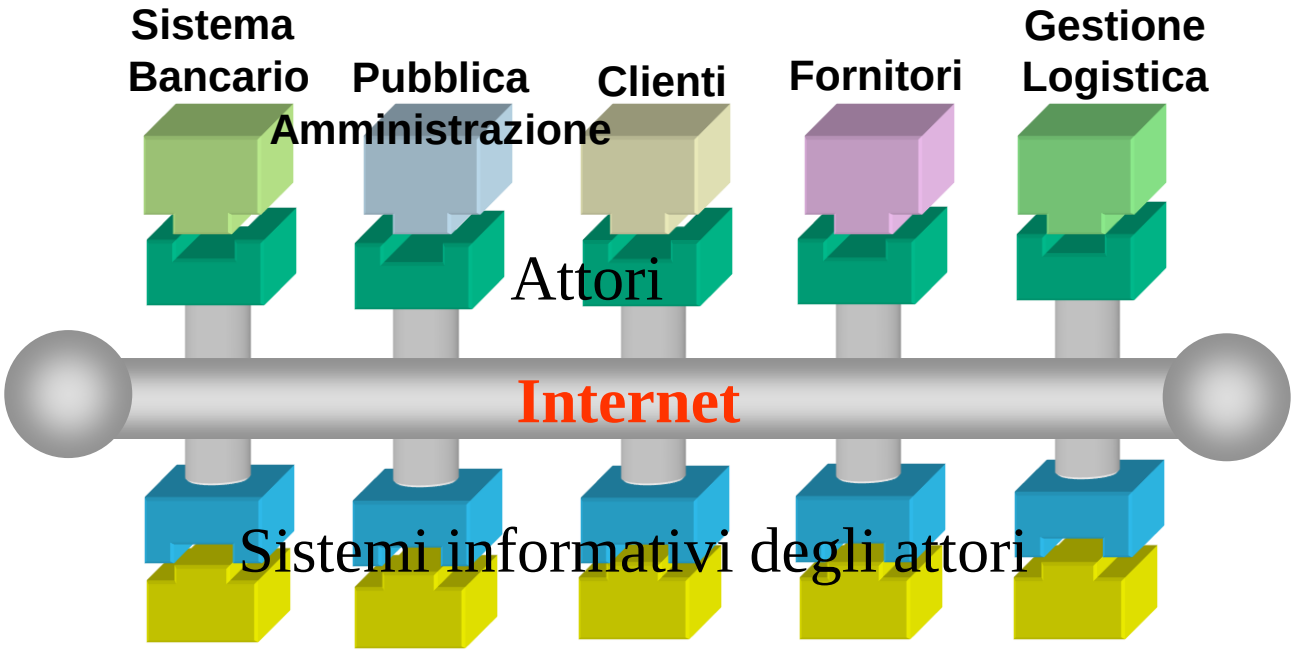
- Integrazione di sistemi informativi
- Servizi Web
- La rete-tipo della PMI
- Le politiche di gestione interna

# L’azienda On-Line

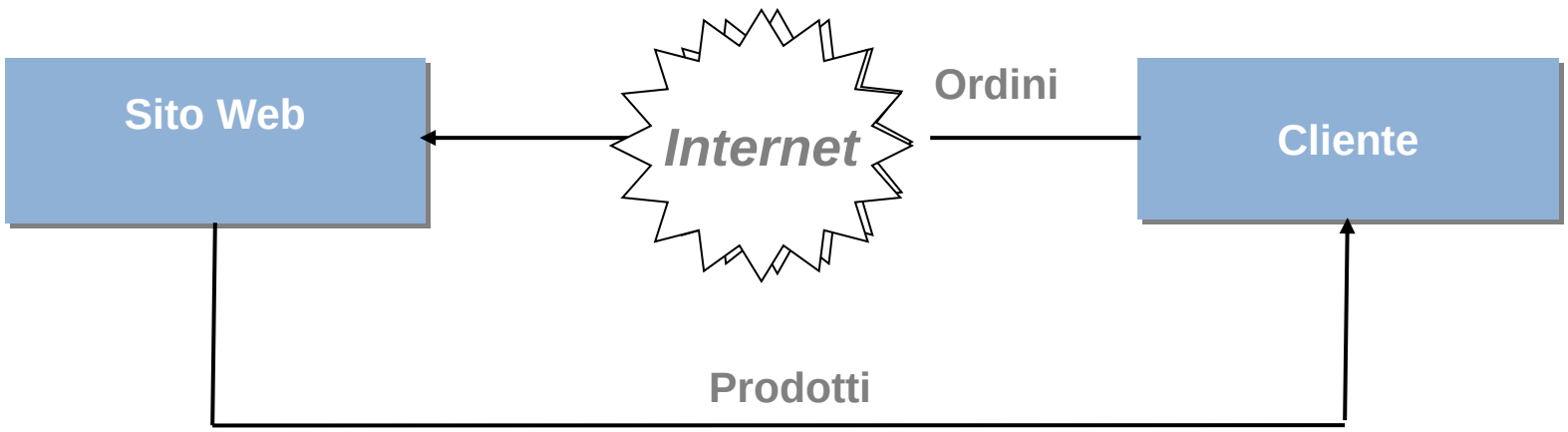



- **Intranet aziendale** affidabile ed efficiente, quale prerequisito per la realizzazione di un **sistema informatico integrato** e la creazione di un modello di integrazione applicativa.
- **Extranet,** rete privata virtuale sicura**,** basata su tecnologia IP, per abilitare interazioni applicative dirette (e non semplicemente browser based) con fornitori, partner, terze parti, clienti business.
- **Internet** quale canale preferenziale di interazione con gli utenti consumer, che richiede ai sistemi aziendali la fornitura di informazioni in maniera immediata e accurata.

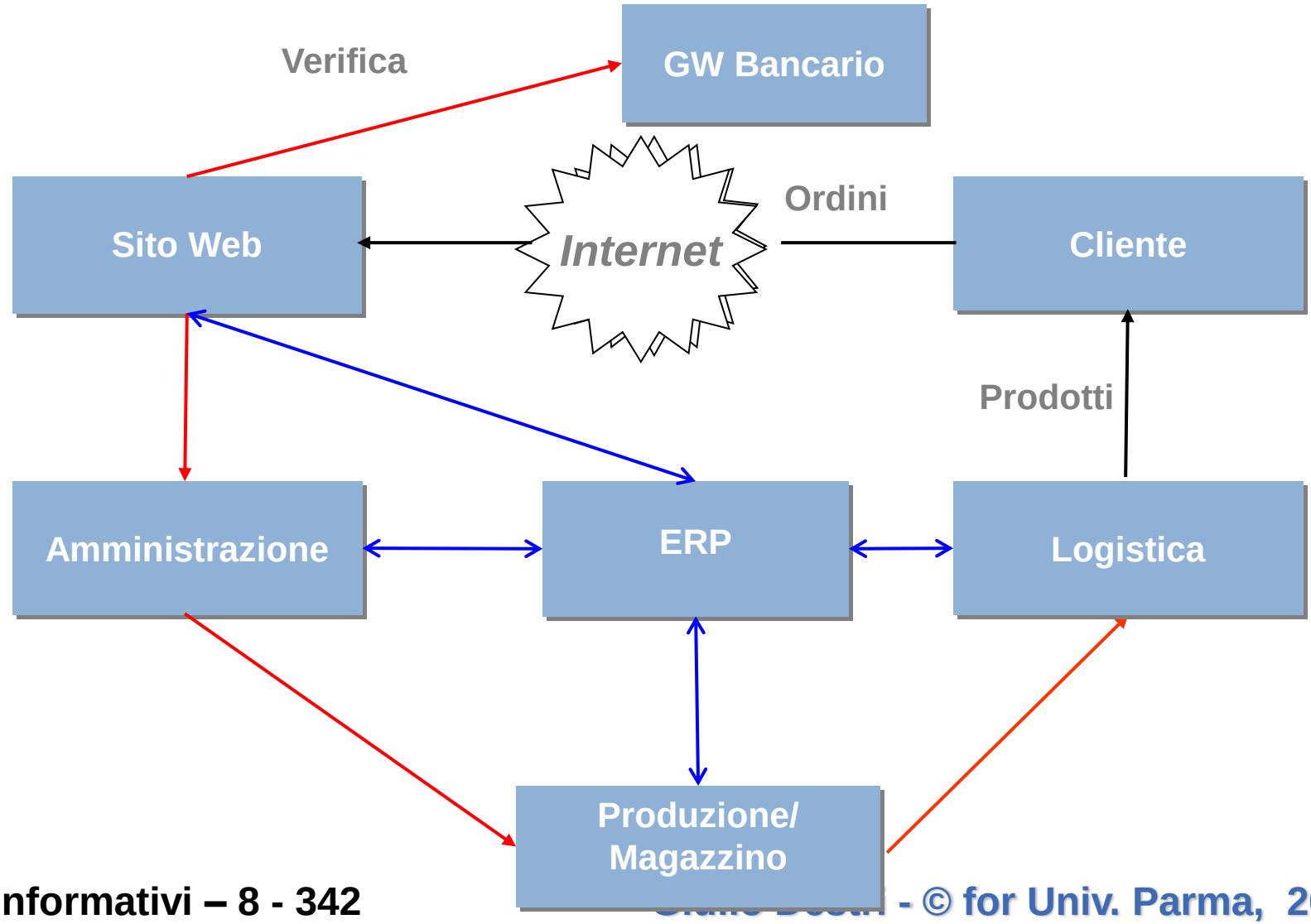
# L'azienda e gli altri attori



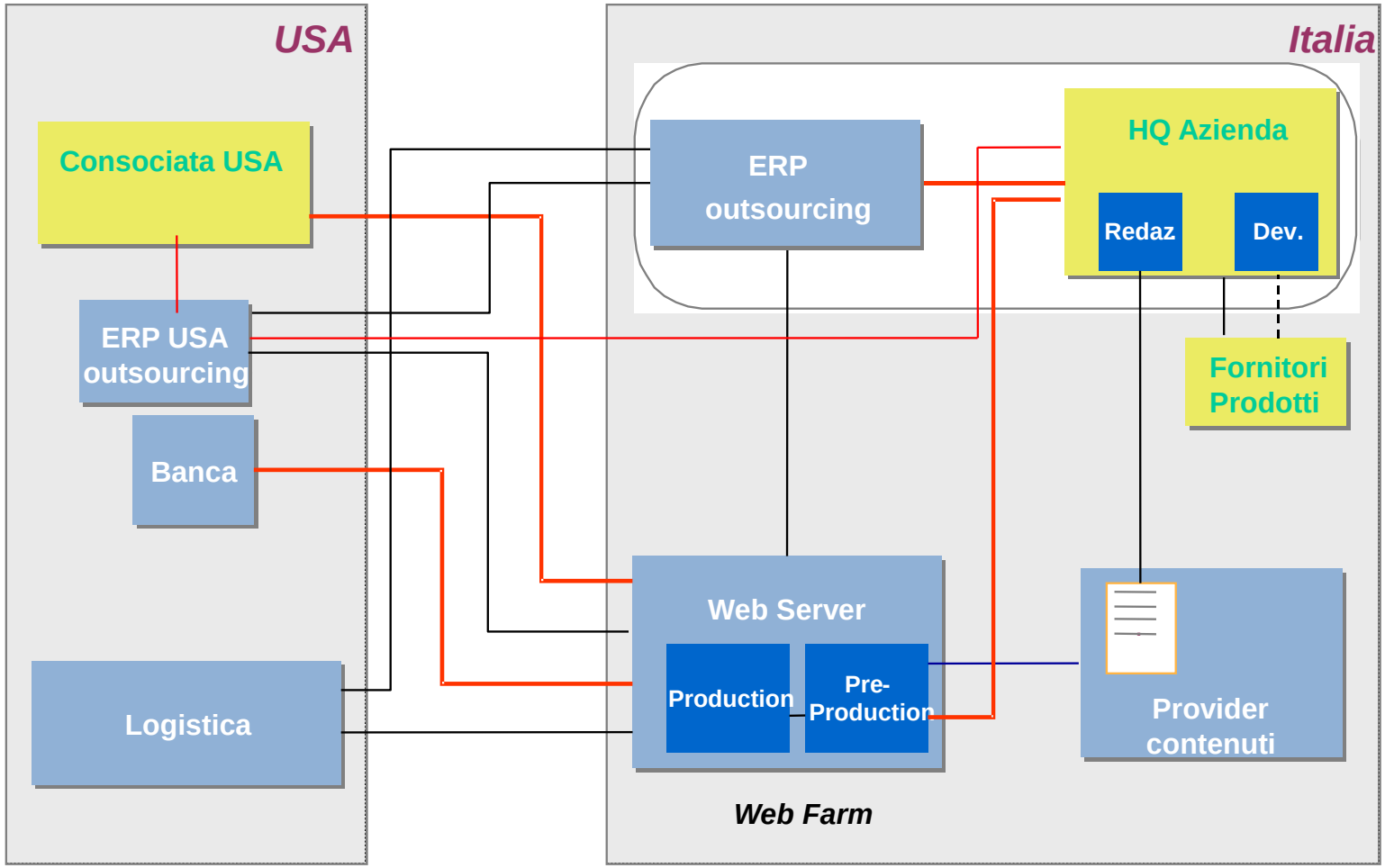
# Integrazione con sistemi esterni



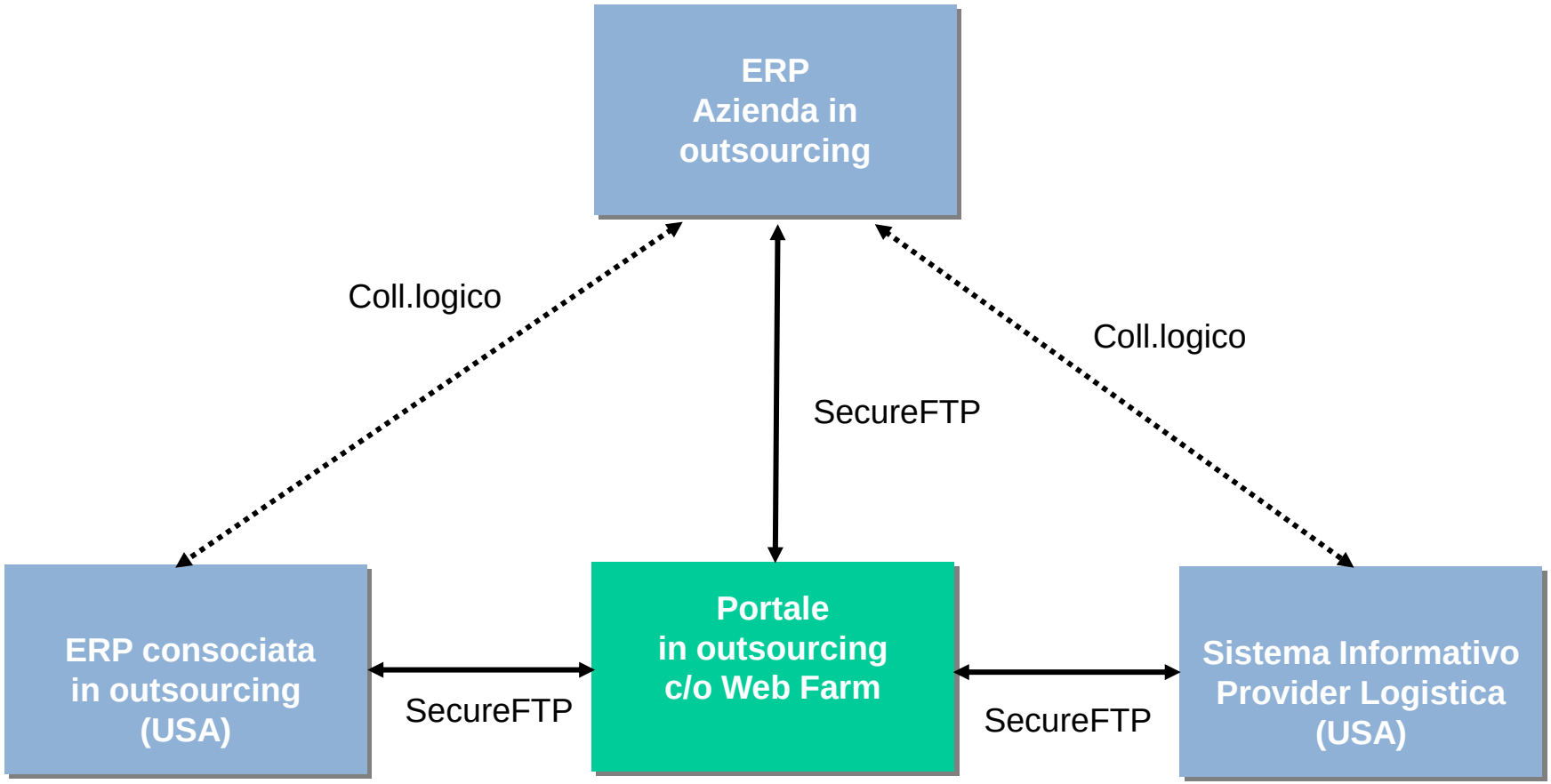
# Integrazione con sistemi esterni - 2



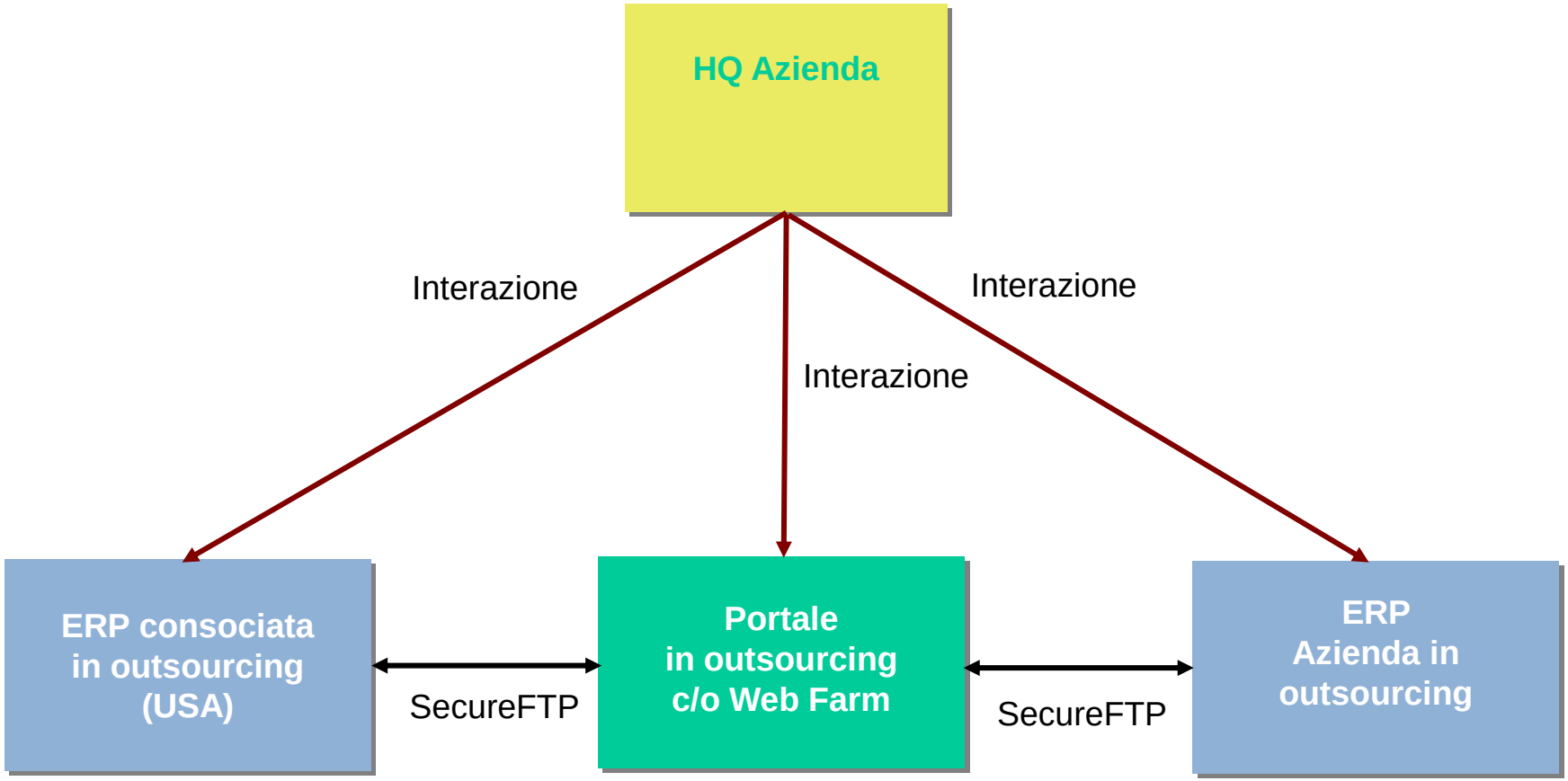
# Un esempio di azienda distribuita



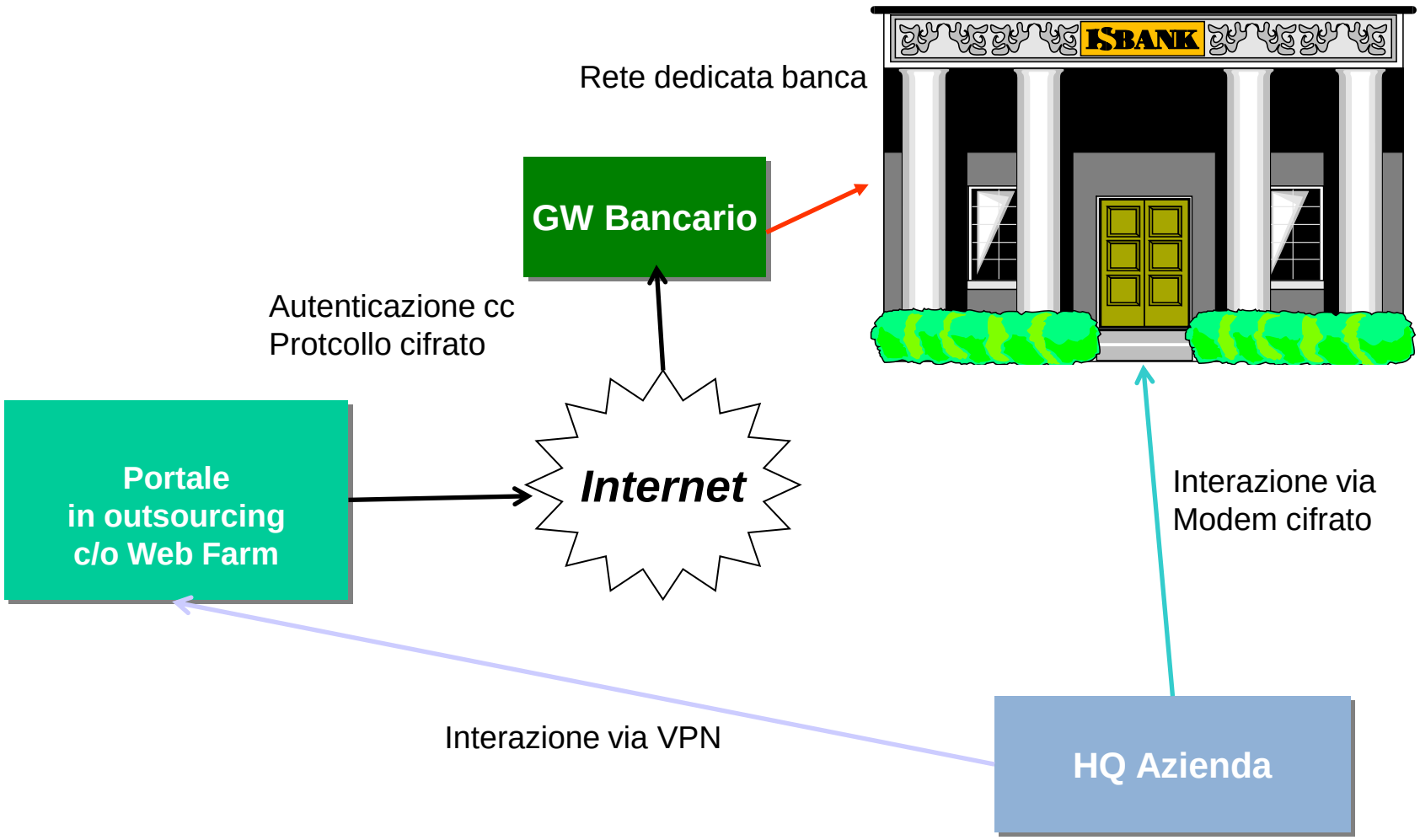
# La struttura della rete: integrazione



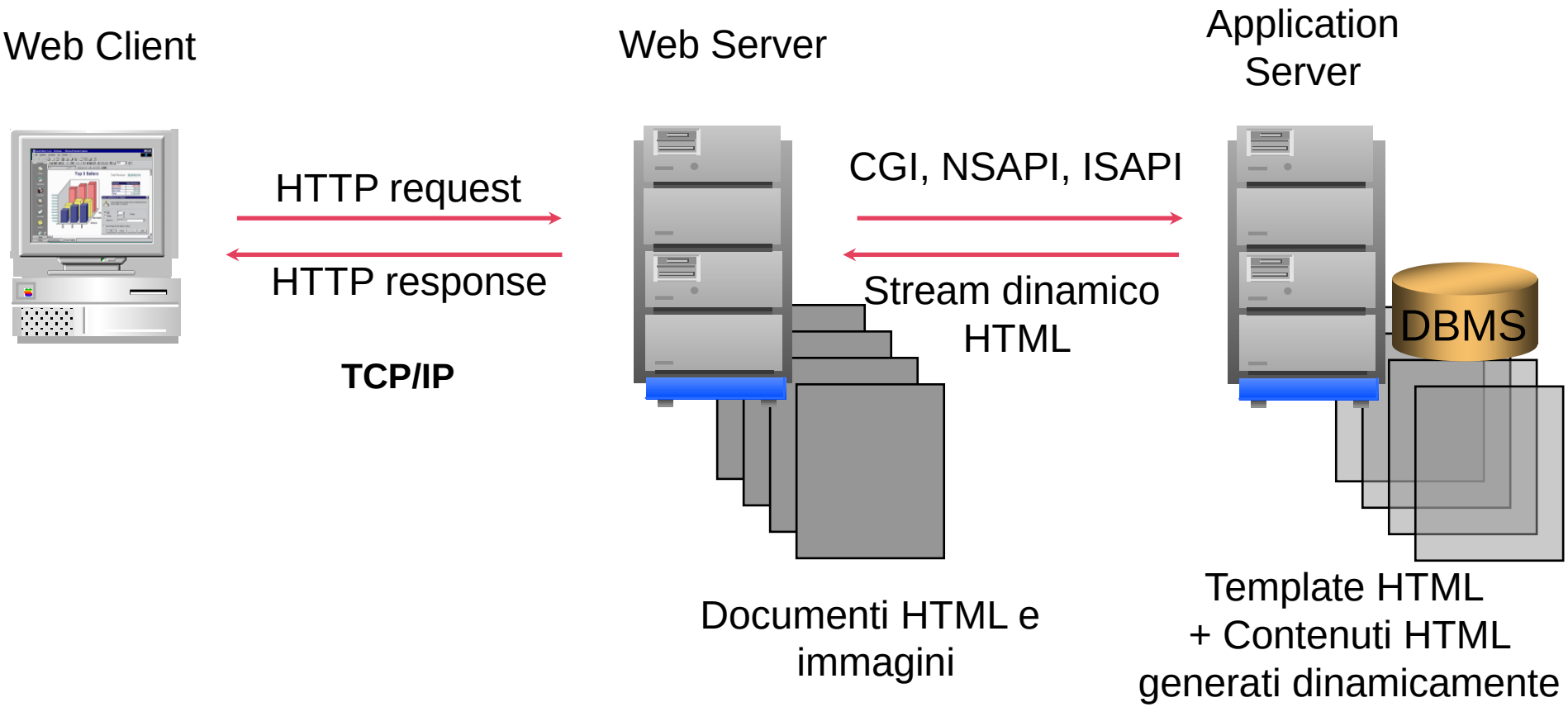
# La struttura della rete: controllo



# I gateway bancari



# Stratificazione fisica di un sistema Web



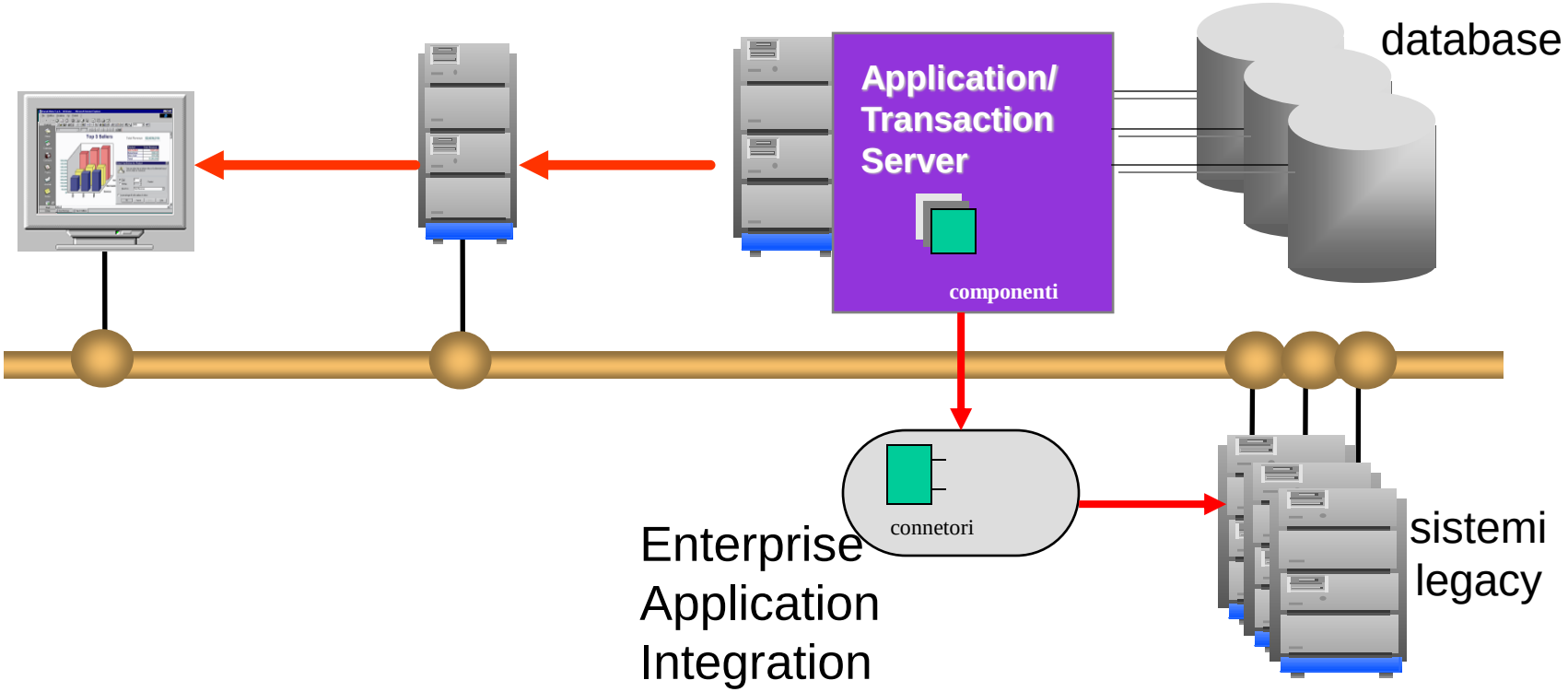
# Stratificazione fisica di un sistema Web - estensioni

Primo livello
Web Browser

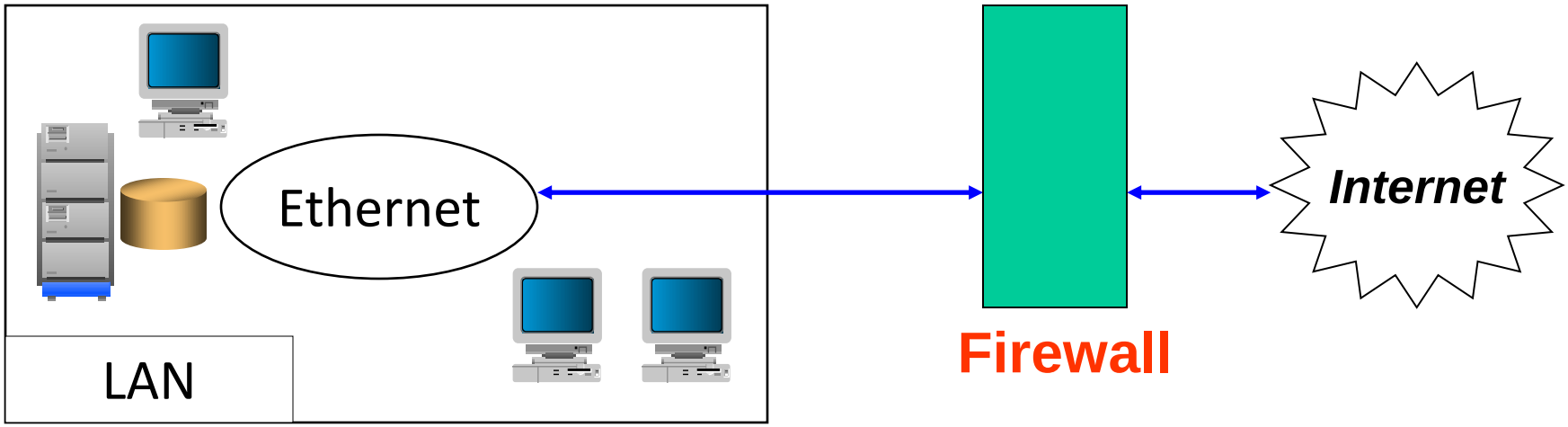
Secondo livello
Web Server

Terzo livello
Regole business

Quarto livello
Sorgenti di dati

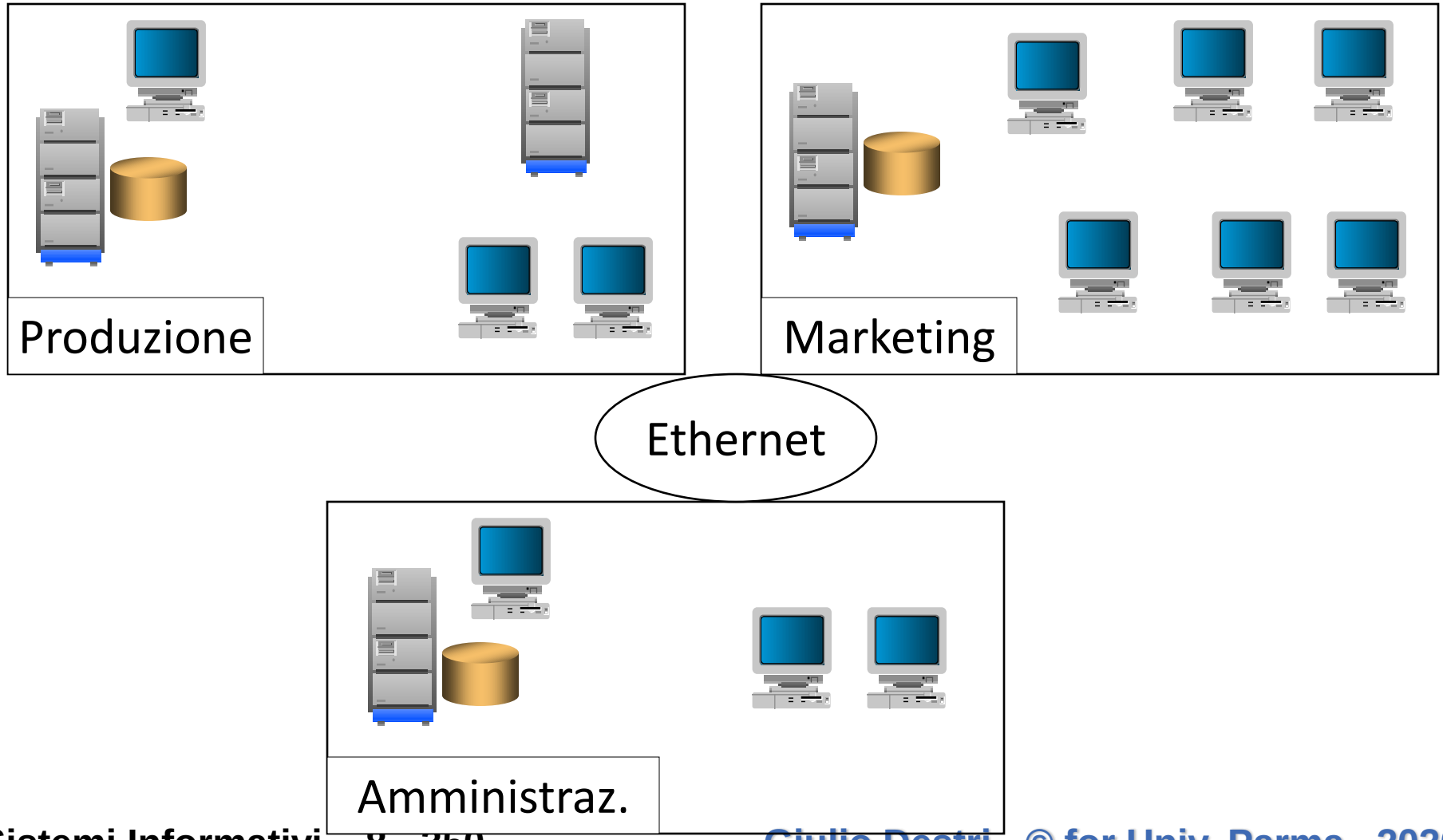


# Una rete tipo

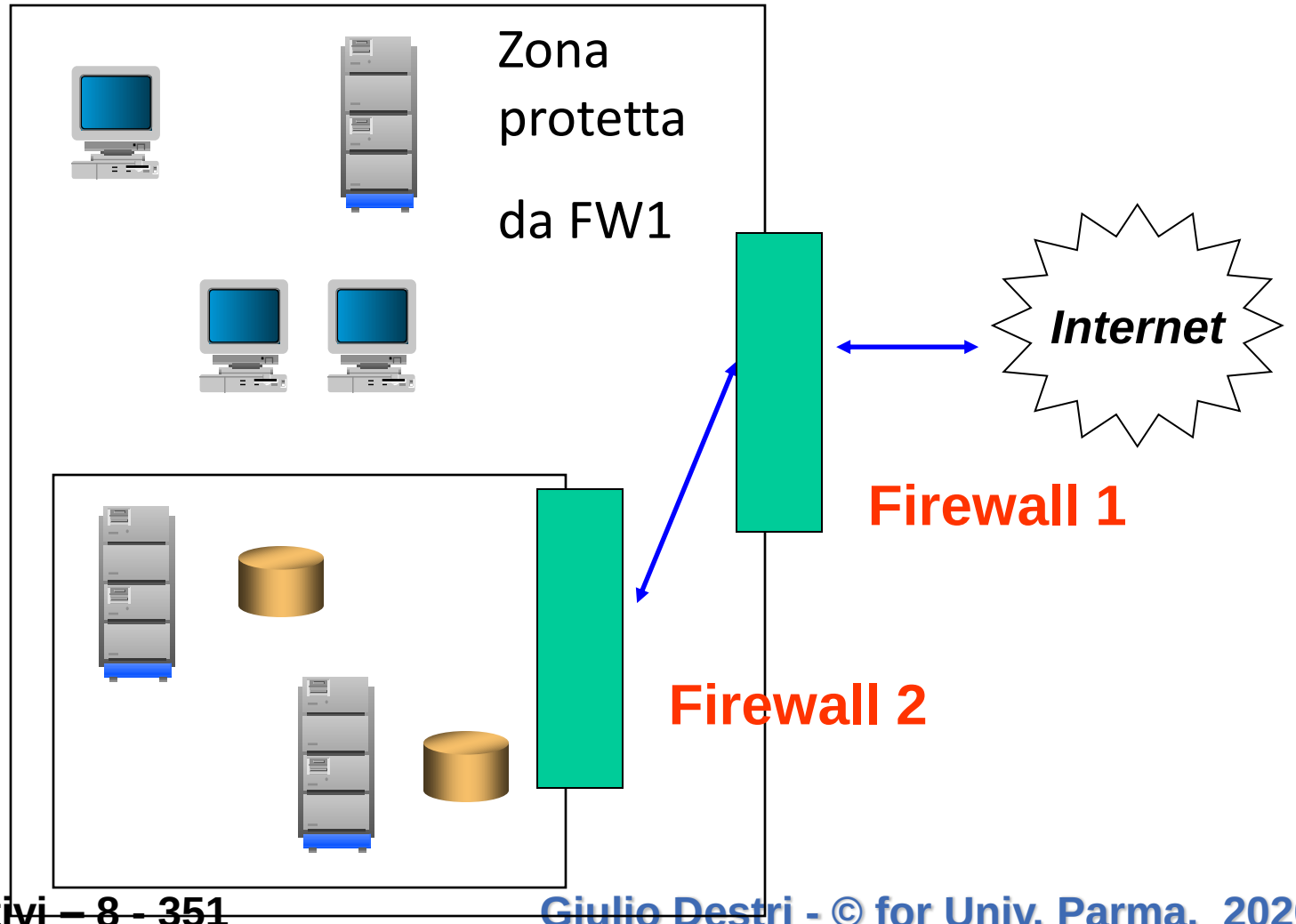



**Tipicamente una rete è isolata da Internet e tutto il traffico transita dal firewall**

# … e dentro l'azienda?



# Il modello di sicurezza a cipolla



# Il modello di sicurezza a cipolla: controlli a strati secondo IBM


**Difesa Perimetrale**
Tenere fuori gli intrusi con
- Firewalls
- Anti-Virus
- Intrusion Detection, etc.

**Livello di Controllo**
- Che utenti possono entrare?
- Cosa possono vedere e fare?
- Sono supportate personalizzazioni?
- Puo' essere protetta la user privacy?

**Assurance Layer**
- Sono conforme con i regolamenti?
- Posso rilasciare audit reports?
- Quanto sto rischiando?
- Posso rispondere a security events?

# Politiche di gestione

- Il tipo di uso del sistema che si vuole proteggere condiziona la politica di gestione
- Analisi dei rischi
- Conivolgimento del management

# Il compromesso fra sicurezza ed uso

"Il computer più sicuro è quello spento e chiuso in una cassaforte"

Frase attribuita ad un esperto di security del Pentagono

# Il compromesso fra sicurezza ed uso - 2

- Lo scopo primario dei sistemi informatici è fare business, più o meno direttamente
- Non sempre i produttori di software tengono presenti le necessità di sicurezza ed integrazione
- Una conoscenza d'insieme del sistema è indispensabile per pianificare qualsiasi politica di sicurezza

# Il compromesso fra sicurezza ed uso - 3

- Le misure di sicurezza non devono **mai** essere di ostacolo reale al funzionamento dei programmi
- Allo stesso tempo però le richieste degli utenti devono avere un limite nelle esigenze di sicurezza

# Sistemi ed utenti

- Il punto debole della sicurezza sono molto spesso gli utenti
- Connessioni “non ufficiali” ad Internet (es. via modem) consentono di bypassare qualsiasi firewall

# Sistemi ed utenti - 2

- Qualsiasi operazione di sicurezza che richieda un intervento esplicito dell'utente o che richieda uno sforzo di attenzione è statisticamente destinata prima o poi a fallire

- Es. sottoporre manualmente al controllo antivirus tutti i dischetti

# La gestione

- Gestione Operativa
- Gestione delle Risorse
- Gestione dei Problemi
- Gestione della Configurazione
- Procedure di Salvataggio
- Piani di Disaster Recovery

# Il problema delle password

**Password**: nome della fidanzata o dell'amante o combinazione della loro data di nascita

Definizione dal "dizionario dell'hacker"

# Il problema delle password - 2

- La gestione delle password dei sistemi è una delle attività più complesse e allo stesso tempo critiche
- In una rete WindowsNT/2000 è molto spesso necessario che l'utente di una workstation sia in possesso della sua password di Administrator

# Il problema delle password - 3

- Occorre forzare gli utenti all'aggiornamento periodico delle password
- Sarebbe buona cosa anche costringerli ad una scelta minimamente sicura
  - Alternanza maiuscola-minuscola
  - Numeri e altri caratteri
  - Lunghezza minima

# Coinvolgimento operativo degli utenti

- E’ necessario che gli utenti siano responsabilizzati rispetto ai rischi di sicurezza
- Se un utente sente regolamenti/procedure come un peso, tenderà a non rispettarli
- Coinvolgimento del management

# Coinvolgimento del Management

- Gli addetti ai sistemi informatici devono rendere il management consapevole dei rischi
- Dovranno poi fornire al management l'elenco delle possibili soluzioni, con pro e contro ovvero rapporto costi-benefici

# Aggiornamento dei sistemi

- Il trend degli ultimi anni rende necessario un aggiornamento (almeno nelle postazioni client) dei sistemi ogni 4 anni
- Sistemi nuovi possono significare problemi nuovi, anche di sicurezza

# Verifiche dei bollettini di sicurezza

- Esistono molti canali che garantiscono una segnalazione rapida di problemi di sicurezza
- E’ necessario che i responsabili dei sistemi siano aggiornati
- Caso per caso si valuterà se mettere in atto le contromisure suggerite

# Le patch di sicurezza

- Non sempre una patch di sicurezza è la panacea
- Spesso corregge problemi ma ne crea degli altri
- Tuttavia se il problema è critico è necessario comunque applicare la patch il prima possibile

# Anti-Virus

- Il problema dei Virus è il più grave di tutti
- Non è realisticamente possibile "chiudere le porte di accesso ai Virus"
- E' necessario l'uso degli anti-Virus

# Anti-Virus - 2

- Un anti-Virus deve funzionare in automatico sui nuovi file
- Tali anti-Virus provocano rallentamenti dei sistemi
- Deve esistere una combinazione fra server e client (es. posta elettronica)
- La combinazione firewall con anti-virus funziona solo entro certi limiti di traffico

# Quando aggiornare gli Anti-Virus

- L’evoluzione dei Virus è divenuta estremamente rapida
- Occorre (almeno sui server) aggiornare le impronte ogni 2-3 giorni al massimo
- In automatico le impronte devono poi essere trasferite sui client
- Comunque essere pronti con piani di emergenza in caso di Virus non segnalati

# Problemi con gli Anti-Virus

- Gli anti-Virus più moderni offrono servizi di integrazione con i sistemi, per esempio i domini Win2000
- Un anti-Virus è comunque un elemento "estraneo" ai sistemi e potenzialmente un fagocitatore di risorse
- L'anti-Virus può provocare problemi ai sistemi (es. Active Directory)

# Aggiornamento dei Gestori

- I responsabili dei sistemi informatici devono essere consapevoli dei principi base del loro funzionamento
- L'inserimento di nuove tecnologie deve essere accompagnato dalla formazione relativa

# Un po di buon senso

- Firewall ben configurato
- Anti-Virus
- Organizzazione degli accessi interni
- Filtri sui router
- Auditing

# Gestione della sicurezza: elementi principali

- Il compromesso fra sicurezza ed uso
- Sistemi ed utenti
- Case Study
- Le politiche globali di gestione

# ISO 27001 e la legislazione

# Cos'è l'ISO 27001

- Lo Standard UNI CEI ISO/IEC 27001:2017 è la  norma internazionale di riferimento che definisce i requisiti per impostare e gestire un **Sistema di Gestione della Sicurezza delle Informazioni**
- ISO/IEC 27000 definisce il glossario
- Include aspetti relativi alla sicurezza logica, fisica ed organizzativa
- Sicurezza delle informazioni, non solo IT!

# La famiglia di ISO 27000: 27001

- ***ISO 27001***: fornire un modello per stabilire, attuare, rendere operativo, il monitoraggio, la revisione, il mantenimento e il miglioramento di un Security Management Information System

- Vi corrisponde il profilo ISO27001 Lead Auditor

# La famiglia ISO 27000: 27002

- ***ISO 27002***: è la evoluzione diretta della norma ISO 17799

- è un codice di condotta per la sicurezza informatica

- delinea essenzialmente 114 gruppi di potenziali controlli e meccanismi di controllo, usati nell'appendice A della 27001

# Le sezioni di ISO 27000: 27021

- ***ISO 27021:2017***: definisce la figura del professionista di ISMS

- Vi corrisponde il profilo ISO27021
- Prevede ampia conoscenza di processi, tecnologie, organizzazione, leggi e soft skill come comunicazione e leadership

# Le sezioni di ISO 27000: 27701

- ***ISO 27701***: estende alla privacy (conforme GDPR) la ISO27001

# Definizioni legali fondamentali - 1

- ***Sistemi Informatici***: "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnessi o collegati, uno o più dei quali, in base ad un programma, eseguono l'elaborazione automatica di dati"

# Definizioni legali fondamentali - 1

- ***Dati informatici***: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione".

# Suddivisione dei crimini informatici

- **Attacco ad un dato**, per copiarlo o modificarlo senza autorizzazione, che non impedisce l'ulteriore funzionamento del sistema informatico che lo ospita

- **Attacco ad un sistema** per impedire il suo uso e l'accesso a tutti i dati in esso memorizzati

# Leggi importanti

- **Europa:** Convenzione di Budapest del 23/11/2001

- **Italia**:
  - Ratificazione della suddetta
  - Articolo 24 bis del decreto legislativo 231 dell'8/06/2001
  - Articoli 615 e seguenti codice penale

# Leggi importanti: GDPR

- **General Data Protection Regulation**
- Regolamento europeo per la protezione dei dati personali
- In vigore dal 25 maggio 2018
- Definisce i diritti delle persone in relazione ai propri dati personali
- Prescrive metodologie tecniche ed organizzative da attuare per proteggere i dati (basate in parte sull'ISO27001)

# Sommario

- Introduzione alla Sicurezza Informatica
- Problemi da guasti ed eventi naturali
- Le minacce umane alla sicurezza
- La crittografia per la protezione delle informazioni
- L'Identità Elettronica
- La protezione dei dati
- La protezione dei Sistemi
- Gestire la Sicurezza
- ISO 27001 e la legislazione