Department of Naval, Electrical,
Electronics and
Telecommunication Engineering
(DITEN)
University of Genoa

Cyber Security
(prima parte)

Prof. Raffaele Bolla

raffaele.bolla@unige.it

Visione generale

- Cosa significa sicurezza ?
  - Protezione e prevenzione
  - Identificazione e reazione
- Perché la Cyber Security è diventata così importante?
  - **Digitalizzazione**
    - Trasformazione (dematerializzazione) dei documenti cartacei in documenti digitali
    - Introduzione di capacità di calcolo (Intelligenza?) ovunque sia localmente che in centri specializzati (Datacentre)
    - Connessione della capacità di calcolo con elementi di raccolta dati e di attuazione
    - Interconnessione massiva del tutto -> Reti di Telecomunicazioni / Internet
  - Alcuni termini connessi: Cloud, IoT, Edge Computing, Fog, …
  - Quindi tutto sarà connesso e controllabile via remoto e tutti i servizi (per esempio commerciali) sono/sanno fatti digitalmente e via rete.

Visione generale

- Cosa rende diverso il caso digitale da quello fisico tradizionale?
  - la globalizzazione introdotta dalla rete, chiunque nel mondo senza spostarsi da dove si trova può diventare una minaccia.
  - Gli strumenti di protezione/identificazione sono totalmente diversi.
- Due condizioni di riferimento del mondo ICT:
  - Tradizionale
    - Isole di apparati con funzionalità importanti ma limitate, eventualmente interconnesse can Internet in un unico punto.
    - Va protetto principalmente il perimetro e controllato il collegamento ad Internet.
    - Un poco più simile al caso fisico.
  - Evoluto
    - Ogni funzionalità controllata e connessa in rete
    - Massivo uso di applicazioni/servizi virtuali che possono migrare ed essere dinamicamente localizzati ovunque nel mondo
    - Assenza di un perimetro reale da proteggere

Gli obiettivi

- Sicurezza del computer
  - protezione delle risorse del computer: documenti, risorse di calcolo interconnessioni.
- Sicurezza della rete
  - protezione dei dati scambiati tra due nodi terminali.
- Le problematiche cambiano, ad esempio, molti metodi possono essere utilizzati per garantire l'autenticità e l'integrità dei documenti cartacei ma l'uso di documenti digitali rende il problema più complesso:
  - un documento cartaceo originale si distingue "facilmente" da una copia;
  - l'alterazione dovrebbe lasciare tracce fisiche (macchie, abrasioni);
  - la validità di un documento cartaceo può essere riconosciuta dalle caratteristiche fisiche (firme, sigilli).

I concetti base

- Una definizione generale di "sicurezza informatica" è stata fornita dal NIST:

  la protezione offerta a un sistema di informazione automatizzato al fine di raggiungere gli obiettivi applicabili di preservare ***l'integrità, la disponibilità e la riservatezza*** *delle risorse del sistema di informazione (comprende hardware, software, informazioni / dati e telecomunicazioni).*

- I tre concetti espresso in tale definizione sono spesso identificati come triade **CIA**.

I concetti base

- **Confidentiality (Confidenzialità)**
  - **Data confidentiality**
    assicura che le informazioni riservate, private o segrete non siano rese disponibili o divulgate a persone non autorizzate
  - **Privacy**
    Garantisce che le persone sia in grado di controllare quali informazioni ad essi correlate possano essere raccolte e archiviate, da chi e a chi tali informazioni possono essere eventualmente divulgate.

I concetti base

- **Integrity** (Integrità)
  - **Data integrity** (Integrità dei dati)
    Assicura che le informazioni (memorizzate o trasmesse) e i programmi vengano modificati solo in modo specifico e autorizzato
  - **System Integrity** (Integrità del Sistema)
    Assicura che un sistema svolga le sue funzioni previste in modo inalterato, libero da manipolazioni non autorizzate intenzionali o involontarie..
- **Availability** (Disponibilità)
  Assicura che i sistemi funzionino tempestivamente e che i servizi non vengano negati agli utenti autorizzati.

I concetti base

- Sebbene la triade della CIA copra la maggior parte degli obiettivi di sicurezza, per poter considerare tutti gli aspetti rilevanti, è necessario aggiungere due ulteriori concetti:
  - **Authenticity** (Autenticità)
    La proprietà di essere autentici e di poter essere verificati e attendibili: fiducia nella validità di una trasmissione, messaggi o nel creatore dei messaggi. Questo significa verificare che gli utenti siano chi dicono di essere e che ogni input che arriva provienga da fonti attendibili.
  - **Accountability** (Responsabilità)
    L'obiettivo di sicurezza che impone tracciare in modo univoco le azioni di un'entità. Questo obiettivo aiuta o consente il non ripudio, la deterrenza, l'isolamento dei problemi, il rilevamento e la prevenzione delle intrusioni, il recupero a posteriori dei guasti e le azioni legali.

Terminologia relativa ai problemi di sicurezza

- **Security breach** (Violazione della sicurezza)
  Una violazione della sicurezza è un qualsiasi incidente che provoca l'accesso non autorizzato a dati, applicazioni, servizi, reti e / o dispositivi evitando i meccanismi di sicurezza presenti. Una violazione della sicurezza si verifica quando un individuo o un'applicazione entra illegalmente in un perimetro informatico logico privato, confidenziale o non autorizzato.
- **Vulnerability** (Vulnerabilità)
  È un difetto in un sistema che può renderlo vulnerabile a degli attacchi. Una vulnerabilità può riferirsi a qualsiasi tipo di debolezza nel sistema stesso, o in delle procedure o in qualsiasi cosa che lasci la sicurezza delle informazioni esposta a una minaccia.

Terminologia relativa ai problemi di sicurezza

- **Security Threat** (Minaccia alla sicurezza)
  Un potenziale rischio di violazione della sicurezza, che esiste in presenza di circostanze, abilità, azioni o eventi che potrebbero permettere a qualcuno o qualcosa di violare la sicurezza e causare danni. Cioè, una minaccia è un possibile pericolo che potrebbe concretizzarsi attraverso lo sfruttamento di una vulnerabilità.
- **Attack** (Attacco)
  Un assalto alla sicurezza del sistema che deriva da una minaccia esplicita messa in atto coscientemente; cioè un tentativo deliberato (specialmente nel senso di un metodo o una tecnica) di eludere i servizi di sicurezza e violare la politica di sicurezza di un sistema.

Chi realizza l'attacco

- Esistono diversi termini utilizzati per identificare le persone che realizzano gli attacchi informatici
  - **Hacker**
  - **Opponent** (Avversario)
  - **Intruder** (Intruso)
  - Trudy
- Il termine hacker è spesso usato in modo inappropriato. Infatti gli viene spesso associata una accezione positiva che indica un programmatore esperto, non motivato dal denaro e attento a non danneggiare nessuno. Ma non è questo il vero significato del termine. Anche una figura con queste caratteristiche, se realizza attacchi (non pre-concordati) rimane nella sostanza un criminale.
- Trudy suona come "intruder", per questo motivo viene spesso utilizzato negli esempi o nelle spiegazioni.

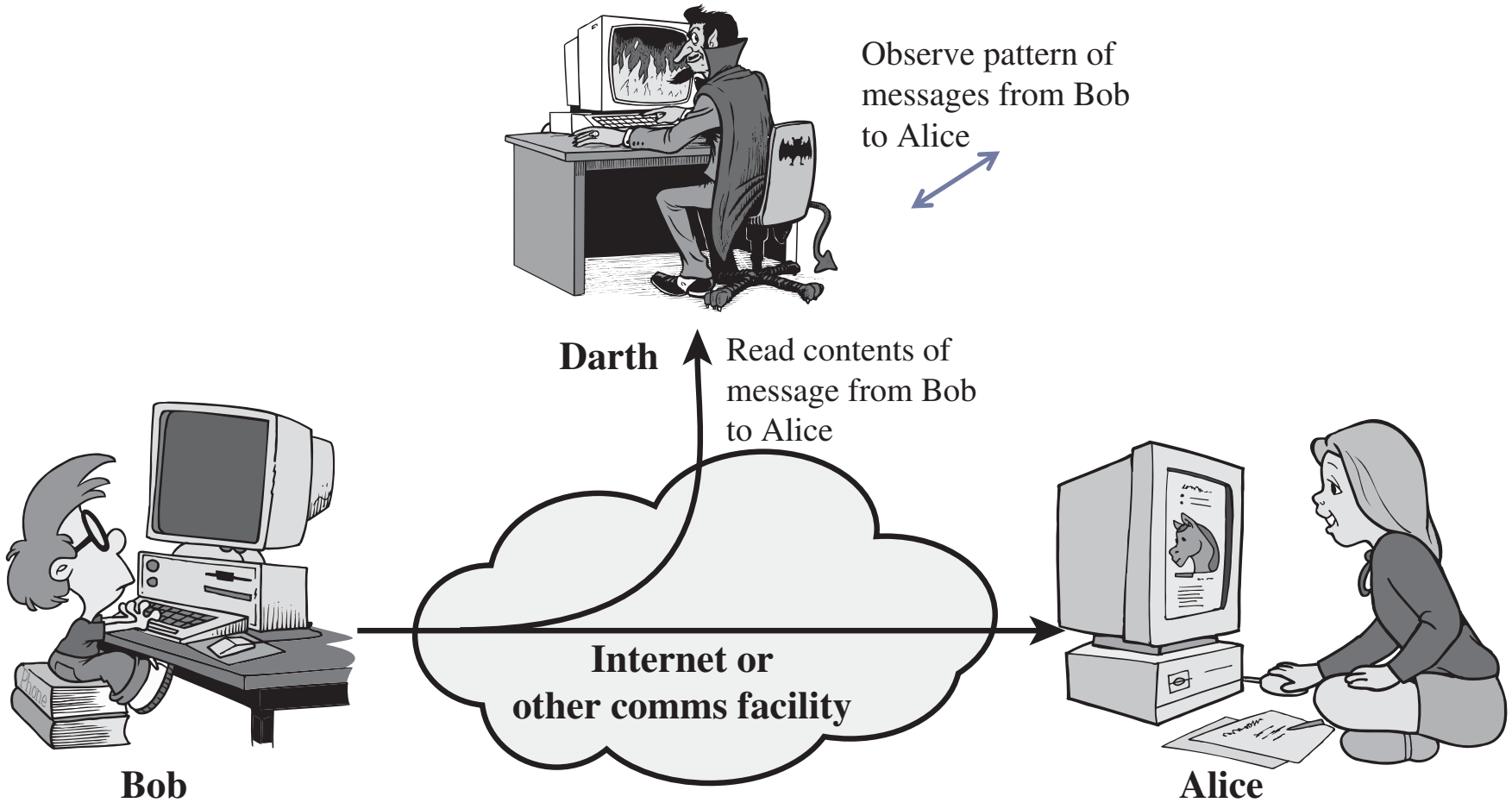
Le componenti base

- **Security attack** (attacco alla sicurezza)
  Qualunque azione che comprometta la sicurezza dell'informazioni o dei servizi informatici di una organizzazione.
- **Security mechanism** (meccanismo di sicurezza)
  Un processo (o un apparato che inglobi il processo) che è progettato per identificare, prevenire o recuperare le condizioni originarie a fronte di un attacco.
- **Security service** (servizio di sicurezza)
  Un servizio di elaborazione o di comunicazione che aumenta il livello di sicurezza dei sistemi di elaborazione o di trasferimento dell'informazione stessi. Tali servizi sono realizzati facendo uso di uno o più meccanismi di sicurezza.

Attacchi passivi

- Gli attacchi passivi consistono nel intercettare o monitorare trasmissioni. L'obiettivo de
- Gli attacchi passivi sono molto difficili da rilevare ll'avversario è ottenere le informazioni che vengono trasmesse. Due esempi
  - **Rilascio di contenuti:** acquisire informazioni riservate (ad es. Sniffing di pacchetti su supporti condivisi (WLAN)).
  - **Analisi del traffico:** senza leggere il contenuto specifico, riconoscere le entità comunicanti e il tipo e la frequenza dei messaggi. (perché non comportano alcuna alterazione dei dati): la principale azione di protezione qui è la **prevenzione**.

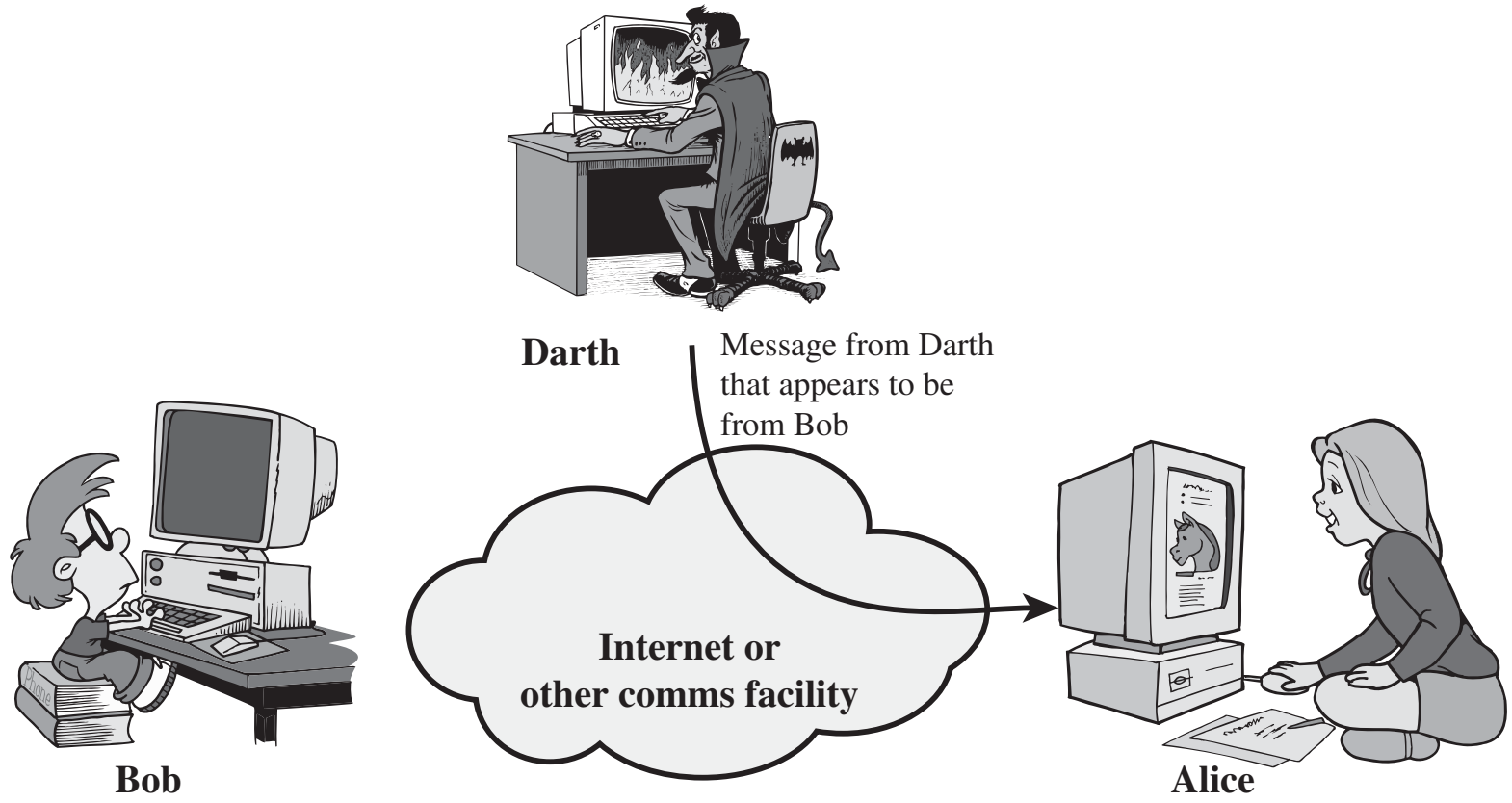
Attacchi passivi



Attacchi attivi

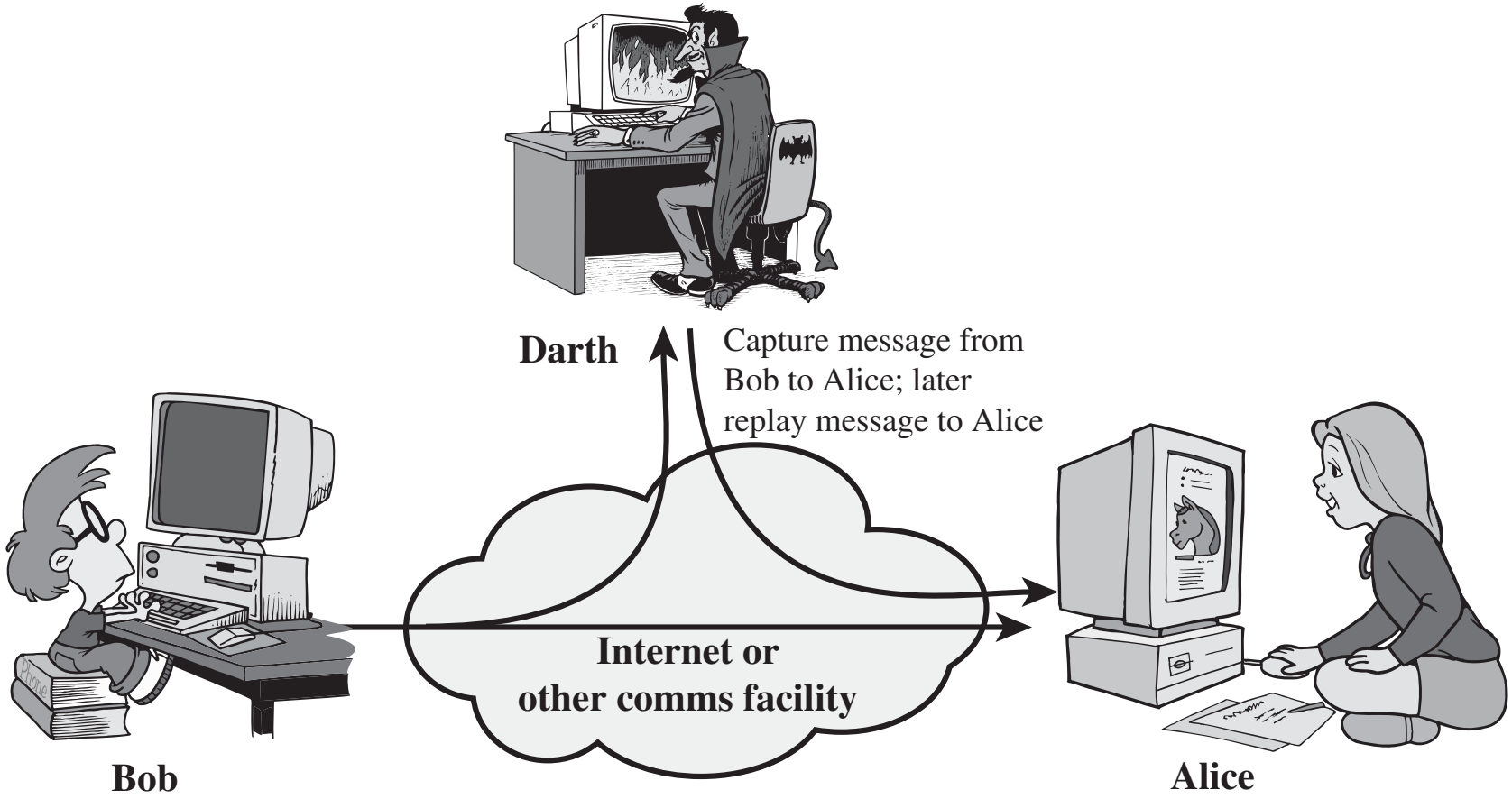
- Gli attacchi attivi comportano una modifica del flusso di dati o la creazione di un flusso falso e possono essere suddivisi in quattro categorie:
  - **Masquerade**: un'entità finge di essere un'entità diversa.
  - **Replay**: comporta l'acquisizione passiva di un'unità dati e la sua successiva ritrasmissione per produrre un effetto non autorizzato (ad esempio un doppio trasferimento di denaro).
  - **Modifica dei messaggi**: una parte di un messaggio legittimo viene modificata o l'intero messaggio viene ritardato o riordinato.
  - **Denial of service:** impedisce o inibisce il normale utilizzo o la gestione delle comunicazioni; ad esempio, la cancellazione di tutti i messaggi verso una destinazione o il sovraccarico di un sistema (singola macchina o intera rete).
- Entrambe le azioni possono essere **rilevate** (e quindi interrotte) e **prevenute**.

Attacchi attivi



(a) Masquerade

Attacchi attivi



(b) Replay

Servizi di sicurezza

- **Autenticazione**
  - Nel caso di un singolo messaggio, assicura che il messaggio provenga dalla fonte da cui afferma di provenire.
  - Nel caso di interazione in corso, le due entità sono autentiche e non sono interferite in modo da essere di terze parti.
- **Controllo d'accesso**
  - La capacità di limitare e controllare l'accesso ai sistemi e alle applicazioni tramite I collegamenti di rete
  - Per raggiungere questo obiettivo, ogni entità che cerca di ottenere l'accesso deve prima essere identificata o autenticata, in modo che i diritti di accesso possano essere personalizzati
- **Confidenzialità dei dati**
  - Il servizio più completo protegge tutti i dati trasmessi tra due utenti.
  - Le forme di servizio più limitate includono la protezione di un singolo messaggio o solo di campi specifici all'interno di un messaggio.
  - La protezione del flusso di traffico dall'analisi
    - Ciò richiede che un utente malintenzionato non sia in grado di osservare l'origine e la destinazione, la frequenza, la lunghezza o altre caratteristiche del traffico su una struttura di comunicazione.

Servizi di sicurezza

- **Integrità dei dati**
- **Non disconoscimento**
  - Impedisce al mittente o al destinatario di negare un messaggio trasmesso.
  - Quando viene inviato un messaggio, il destinatario può provare che il mittente ha effettivamente inviato il messaggio.
  - Quando viene ricevuto un messaggio, il mittente può provare che il destinatario ha effettivamente ricevuto il messaggio
- **Disponibilità del servizio**
  - Protegge un sistema per garantirne la disponibilità
  - Questo servizio risolve i problemi di sicurezza sollevati dagli attacchi denial-of-service

Meccanismi di sicurezza

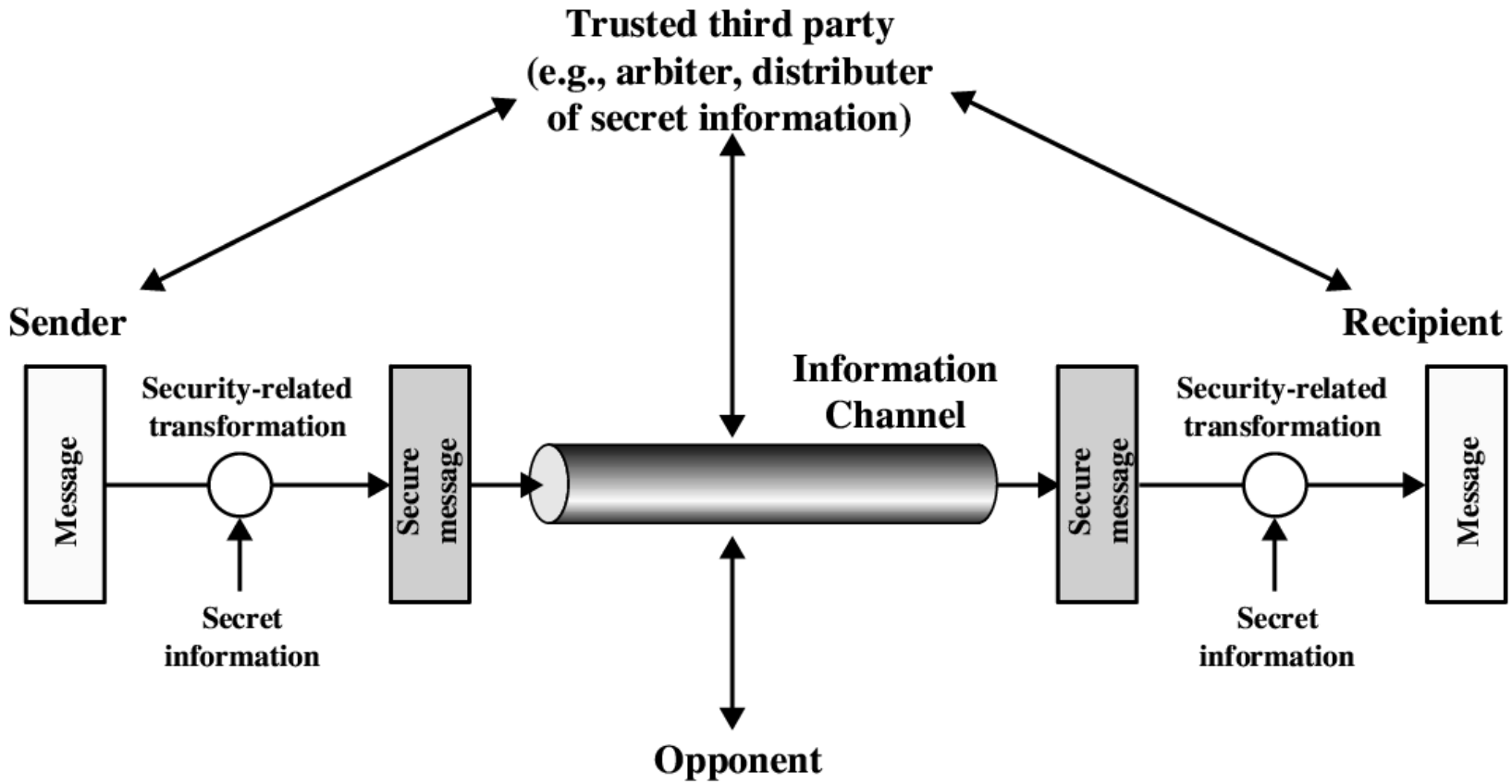
- **Cifratura**
  - L'uso di algoritmi matematici per trasformare i dati in una forma non facilmente comprensibile
- **Firma digitale**
  - Dati aggiunti a, o una trasformazione crittografica di un'unità dati che consente a un destinatario dei dati di provare l'origine e l'integrità di tali dati e di proteggersi dalla falsificazione
- **Controllo di accesso**
  - Una varietà di meccanismi che impongono diritti di accesso alle risorse.
- **Integrità dei dati**
  - Una varietà di meccanismi utilizzati per assicurare l'integrità di un'unità di dati o flusso di unità di dati.
- **Scambio di autenticazione**
  - Un meccanismo inteso a garantire l'identità di un'entità mediante lo scambio di informazioni.

I perimetri di un attacco

- Network attack surface (Perimetro di attacco della rete)
  - Fa riferimento a vulnerabilità su una rete aziendale, su una vasta area o su Internet
- Software attack surface (Perimetro di attacco del Software)
  - Fa riferimento a vulnerabilità nell'applicazione, utilità o codice del sistema operativo
- Human attack surface (Perimetro di attacco umano)
  - Si riferisce alle vulnerabilità create da personale o estranei

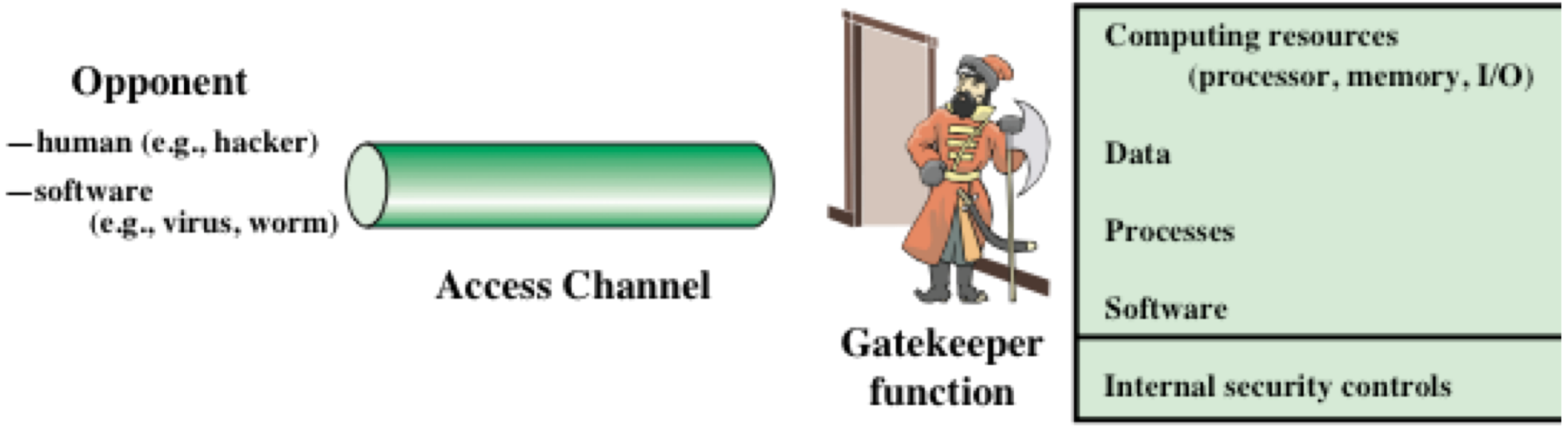
Modelli per la sicurezza

Telecomunicazioni

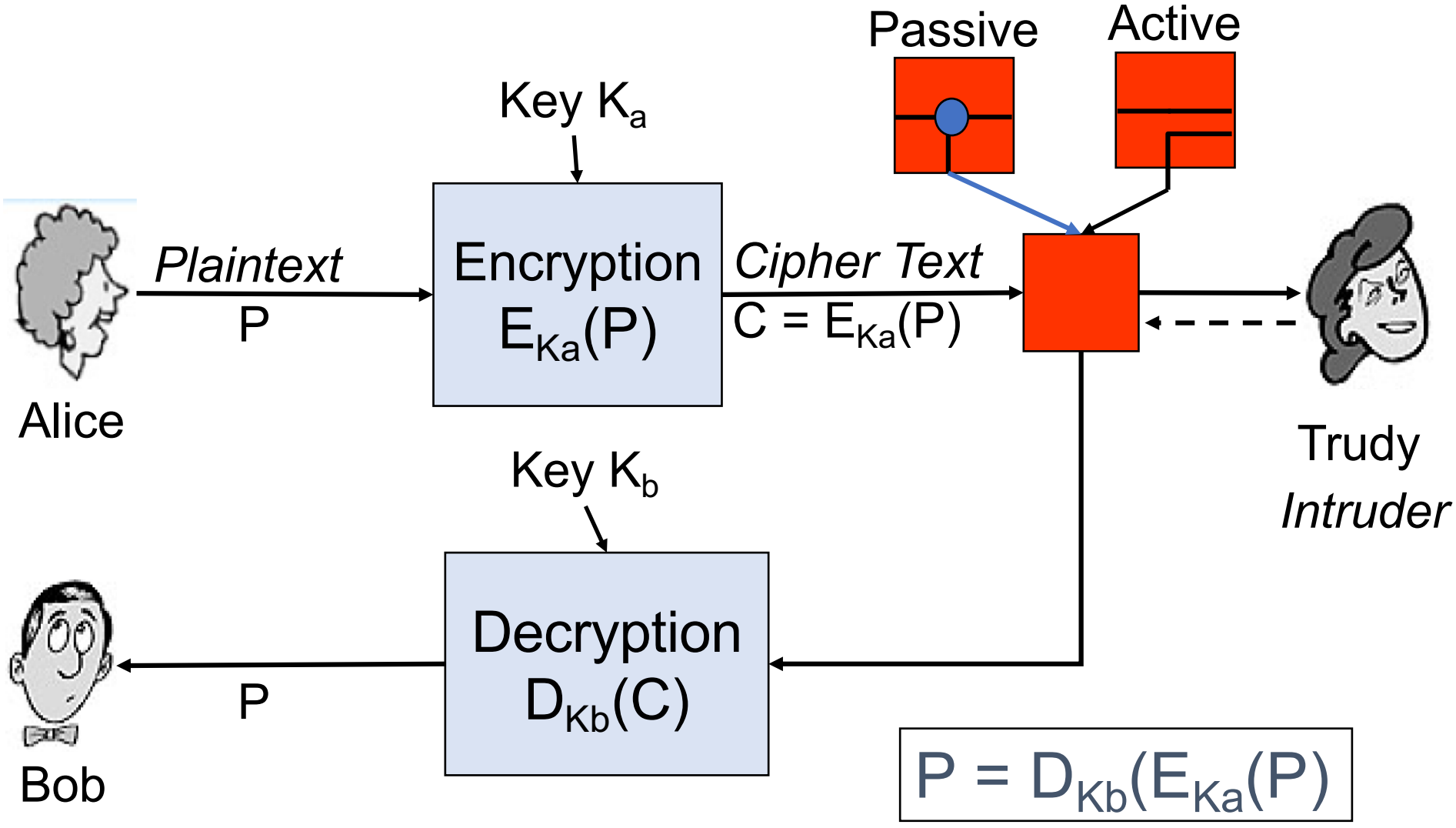


Modelli per la sicurezza

Information System



Confidenzialità: Criptografia



Definizioni

Plaintext

- Il messaggio originale

Ciphertext

- Il messaggio criptato

Enciphering/ encryption

- Il processo di conversion da plain a ciphertext

Deciphering/ decryption

- Il processo di conversion inversa cipher -plain

Cryptography

- La disciplina che studia gli algoritmi di cifratura

Cryptographic system/cipher

- Uno schema di cifratura

Cryptanalysis

- Tecniche per la decifratura di un messaggio cifrato senza conoscere I parametri di decifratura

Cryptology

- La disciplina complessiva che investe sia la cryptography che la cryptanalysis