



NETWORK SECURITY

“Concetti generali”

Corso di Laurea Magistrale in Ingegneria Informatica

Prof. Simon Pietro Romano

sromano@unina.it



CREDITS

- Alcune delle figure di questa presentazione sono tratte dal materiale didattico realizzato da William Stallings e messo a disposizione dei docenti sul sito della casa editrice Pearson
- Lo stesso dicasì per parti del contenuto delle slide
- Un'altra fonte di ispirazione per questa lezione è rappresentata dal materiale del corso di Network Security tenuto alla Columbia University dal Prof. Bellovin





“Non illuderti che il nemico possa non presentarsi, ma tieniti sempre pronto ad affrontarlo. Non illuderti che il nemico non ti attacchi, ma fai piuttosto in modo di renderti inattaccabile.

È una regola fondamentale dell'Arte della Guerra.”

- L'Arte della Guerra, Sun Tzu



OBIETTIVI

- Triade della sicurezza:
 - Confidentiality, Integrity, Availability
- Requisiti da garantire in due domini distinti:
 - sui collegamenti di rete (“on-the-wire”)
 - negli end-system
- Le strategie si differenziano moltissimo nei due domini menzionati



DICOTOMIA HOST/NETWORK

- Gli host tipicamente sono (o possono essere) ben controllati
 - Modelli di autenticazione e di autorizzazione ben consolidati
 - Concetto ben saldo di stato “privilegiato”
- Niente di tutto ciò risulta vero quando si passa ad esaminare la rete!



RETI ED “ANARCHIA”

- Tutti possono collegarsi alla rete
- La connettività può essere ‘controllata’ al più in contesti molto ristretti e sottoposti ad opportuna regolamentazione
- Sistemi Operativi differenti hanno concetti molto diversi di proprietà quali:
 - identificativi di utenti
 - privilegi degli utenti
- Non esiste dunque una definizione condivisa di cosa sia un “privilegio” in una rete di calcolatori eterogenei



PERCHÉ CON LE RETI TUTTO SI COMPLICA?

- Perché le reti, per loro natura, si interconnettono, sempre!
 - [cit.] “*Bellovin's Laws of Networking*”...
- Perché le reti, tipicamente, si interconnettono alla frontiera (“edge”), piuttosto che nelle parti centrali (“core”):
 - praticamente impossibile pensare a meccanismi centralizzati di controllo (e di enforcing) delle policy di sicurezza



FALLIMENTI “BENIGNI”

- La stragrande maggioranza dei fallimenti di una rete di calcolatori è di tipo benigno:
 - corruzione di dati in transito
 - timeout
 - end-system spenti
 - problemi di raggiungibilità (routing)
- Qualsiasi programma di rete deve tenere in considerazione questo tipo di fallimenti
- Regola generale:

“Tutto ciò che può accadere per errore, può senz’altro accadere per intenti malevoli!”



COMPUTER SECURITY vs NETWORK SECURITY

- Computer Security:
 - Termine generico utilizzato per indicare l'insieme di strumenti progettati per proteggere i dati e bloccare gli hacker
- Network Security:
 - Termine specifico utilizzato per indicare tutte le azioni che possono essere intraprese per dissuadere, prevenire e correggere violazioni alla sicurezza che coinvolgano la trasmissione di informazioni tra entità distribuite



ULTERIORI DEFINIZIONI*

- Vulnerabilità:
 - un errore o una imperfezione nel progetto, nella implementazione o nelle modalità operative di un sistema
- Attacco:
 - un modo di sfruttare una o più vulnerabilità di un sistema
- Minaccia (“threat”):
 - un ‘avversario’ che sia motivato a (e capace di) sfruttare una vulnerabilità di un sistema

*“Trust in Cyberspace”, Fred B. Schneider [Editor]



VULNERABILITÀ

- Il fallimento tecnico di un sistema
- L'argomento centrale di qualsiasi corso di sicurezza
- Domanda

*“Se eliminassimo tutte le vulnerabilità,
le minacce esisterebbero ancora?”*



VULNERABILITÀ: RETE E HOST

- In una rete ci sono:
 - gli host o end-system:
 - client e server
 - entità paritetiche in una rete peer-to-peer (p2p)
 - la “rete” in senso stretto, vale a dire i collegamenti
 - wired
 - wireless
- Dobbiamo proteggere sia gli uni (host) che l'altra (rete)
 - vulnerabilità diverse
 - tecniche differenti



VULNERABILITÀ NEGLI HOST

- In questo corso, l'host è di interesse in quanto nodo di rete
- Obiettivo:
 - evitare che un attaccante penetri in un nodo di rete (tipicamente sfruttando un'applicazione difettosa)
- Se l'applicazione difettosa è usata esclusivamente per minare la sicurezza dell'host:
 - problema di sicurezza legato al Sistema Operativo ed all'applicazione
- Se l'applicazione può essere modificata per compiere azioni indesiderate in rete:
 - problema di sicurezza di rete
- Il confine tra le due categorie citate sopra è MOLTO sfumato...



VULNERABILITÀ DI RETE

- Cosa può fare un potenziale attaccante?
- Dove è (fisicamente) localizzato l'attaccante?
- “Cosa” siamo intenzionati a proteggere?
 - la rete è, in realtà, un complesso insieme di ‘livelli protocollari’ interoperanti



VULNERABILITÀ IN UN MONDO “A LIVELLI”

- Ogni livello ha i suoi punti deboli:
 - Link Layer:
 - es: ARP spoofing
 - Network Layer:
 - es: IP ‘address forgery’
 - Transport Layer:
 - es: TCP sequence number guessing
 - Application Layer:
 - es: worm inviati via e-mail



ARP SPOOFING

- Traduzione di indirizzi IP in indirizzi di rete locale

```
sromano$ tcpdump -ennqt en1 |( arp |  
listening on en1, link-type EN10MB (Ethernet), capture size 65535 bytes  
ARP, length 42: Request who-has 192.168.178.20 tell 192.168.178.1, length 28  
ARP, length 42: Reply 192.168.178.20 is-at 00:23:12:0f:82:de, length 28
```

- E se rispondessimo al posto di un altro?
 - la prima risposta ‘di solito’ è quella che vince...

3-WAY HANDSHAKE IN TCP



$C \rightarrow S : \text{SYN}(\text{ISN}_C)$

$S \rightarrow C : \text{SYN}(\text{ISN}_S), \text{ACK}(\text{ISN}_C)$

$C \rightarrow S : \text{ACK}(\text{ISN}_S)$

$C \rightarrow S : \text{dati}$

- In alcune (obsolete) versioni di TCP, il numero di sequenza iniziale (Initial Sequence Number – ISN) viene incrementato di un valore costante ‘k’ dopo ogni connessione ed ogni 500 msec...



ATTACCO “SEQUENCE NUMBER GUESSING”

- X attiva una connessione legittima con S per apprendere il valore di ISN_S :

$$X \rightarrow S : SYN(ISN_X)$$
$$S \rightarrow X : SYN(ISN_S), ACK(ISN_X)$$

- X finge di essere T:

$$X \rightarrow S : SYN(ISN_X), SRC = T$$
$$S \rightarrow T : SYN(ISN_S + k), ACK(ISN_X)$$
$$X \rightarrow S : ACK(ISN_S + k), SRC = T,$$
$$X \rightarrow S : SRC = T, \text{ 'dati dell'attacco'}$$



SEQUENCE NUMBER GUESSING: PROBLEMI

- T vede il segmento “SYN+ACK” inviato da S:
 - secondo la specifica, risponderà con un segmento di tipo RST (RESET)
- X deve evitare che ciò avvenga
 - possibili soluzioni:
 - impersonare un host non attivo ('dead host')
 - sferrare, in parallelo, un attacco Denial of Service (DoS) verso T, per evitare che possa inviare il segmento RST
- Ma:
 - molto spesso, i firewall non inoltrano agli host pacchetti associati a connessioni che essi non hanno inizializzato:
 - in tal caso, l'host T non vedrà mai il segmento SYN+ACK e, di conseguenza, non invierà mai il segmento RST!
 - ...i cosiddetti “side-effect” dei meccanismi per la sicurezza.



IL FATTORE UMANO!

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations.

They are also large, expensive to maintain, difficult to manage, and they pollute the environment.

It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations.”

Kaufman et al.



MINACCE

- Avversari differenti hanno caratteristiche e competenze differenti
- Un hacker alle prime armi non riuscirà mai a violare un moderno algoritmo di crittografia
- Un hacker esperto è invece in grado di sfruttare le cosiddette “3 B”:
 - *“Burglary”*
 - violazione (di domicilio, ma anche di una risorsa di rete...)
 - *“Bribery”*
 - corruzione
 - *“Blackmail”*
 - estorsione
 - <https://hbr.org/2009/10/when-hackers-turn-to-blackmail-2>
- Qualsiasi progetto di un sistema sicuro dipende fortemente dalla conoscenza del nemico!



MINACCE E TIPI DI HACKER

- Hacker per divertimento (joy hackers)
 - alcuni sono semplici “skiddies”..
 - ...altri sono molto competenti
- Da tenere presente:
 - gli script sono spesso molto sofisticati (e possono fare molti danni)
 - gli hacker condividono i propri strumenti molto più volentieri di quanto non lo facciano i cosiddetti bravi ragazzi



I JOY HACKER SONO UN PROBLEMA?

- Loro si divertono...
- ...ma:
 - noi dobbiamo rimettere in piedi i nodi attaccati con successo
 - noi ci facciamo brutta figura quando la notizia trapela!
 - noi rischiamo di perdere il posto se il nostro ruolo nell'azienda è quello dell'amministratore di sistema ☹



HACKING ED IL VIL DENARO

- Gli hacker sono spesso anche “spammer” e “phisher”
- La principale motivazione per un hacker, oggi, sono i soldi
- La possibilità di trarre profitto dalle attività di hacking ha:
 - attirato persone talentuose in questa nuova arena
 - stimolato lo sviluppo di tecniche di attacco molto sofisticate
 - la maggior parte dei virus e dei ‘worm’ prodotti ultimamente ha lo scopo di trasformare i computer delle vittime in membri di cosiddette “botnets”
 - ridotto notevolmente i casi di vandalismo puro, a favore di situazioni di vero e proprio ‘crimine informatico organizzato’



SPIONAGGIO INDUSTRIALE

- Una percentuale minima degli attacchi viene effettivamente rilevata
- Molto spesso, lo scopo di attaccanti professionisti è quello di:
 - penetrare in un sistema di un'organizzazione
 - assumere un profilo quanto più ‘normale’ possibile una volta entrati
 - raccogliere, trasmettere ed elaborare informazioni relative all'organizzazione
- Si parla, in questo caso, di “Advanced Persistent Threats” (APT)



HACKER PROFESSIONISTI

- Più spesso di quanto si possa immaginare, utilizzano strumenti di natura non tecnica:
 - social engineering, bribery, wiretapping (intercettazione)
- I professionisti:
 - sanno quello che fanno
 - sanno quello che vogliono



E SE IL PROBLEMA RISIEDEsse ALL'INTERNO?

- Il problema degli “insider” (persone interne all’organizzazione):
 - conoscono i tuoi asset
 - conoscono i tuoi punti deboli
 - si trovano ‘dietro’ al firewall aziendale
 - a volte ti si ritorcono contro
 - che succede se l’amministratore di sistema passa dalla parte del nemico?!



E LE SPIE?

- Alcuni governi potrebbero essere interessati a scoprire i segreti di una specifica tecnologia...
 - ...pagando profumatamente per ottenerli
- Le spie informatiche sono tipicamente altamente professionalizzate e molto ben pagate
- ...e spesso si fanno la guerra tra di loro per ottenere nuove fette di mercato!
 - Mai sentito parlare degli italiani di “Hacking Team”?

http://www.repubblica.it/tecnologia/sicurezza/2015/07/06/news/hackerato_hacking_team-118452298/?refresh_ce

UN OCCHIO AGLI STANDARD



OSI SECURITY ARCHITECTURE

- “Security attack”
 - una qualsiasi azione che comprometta la sicurezza delle informazioni possedute da un’organizzazione
- “Security mechanism”
 - un processo (o un dispositivo che incorpori tale processo) progettato per rilevare, prevenire o ‘riprendersi’ da un attacco
- “Security service”
 - un servizio di elaborazione o di comunicazione che migliori la sicurezza dei sistemi di elaborazione ed il trasferimento delle informazioni di un’organizzazione
 - concepito per rispondere ad attacchi alla sicurezza
 - basato su uno o più ‘meccanismi di sicurezza’



ANCORA SU THREATS ED ATTACCHI [RFC4949]

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

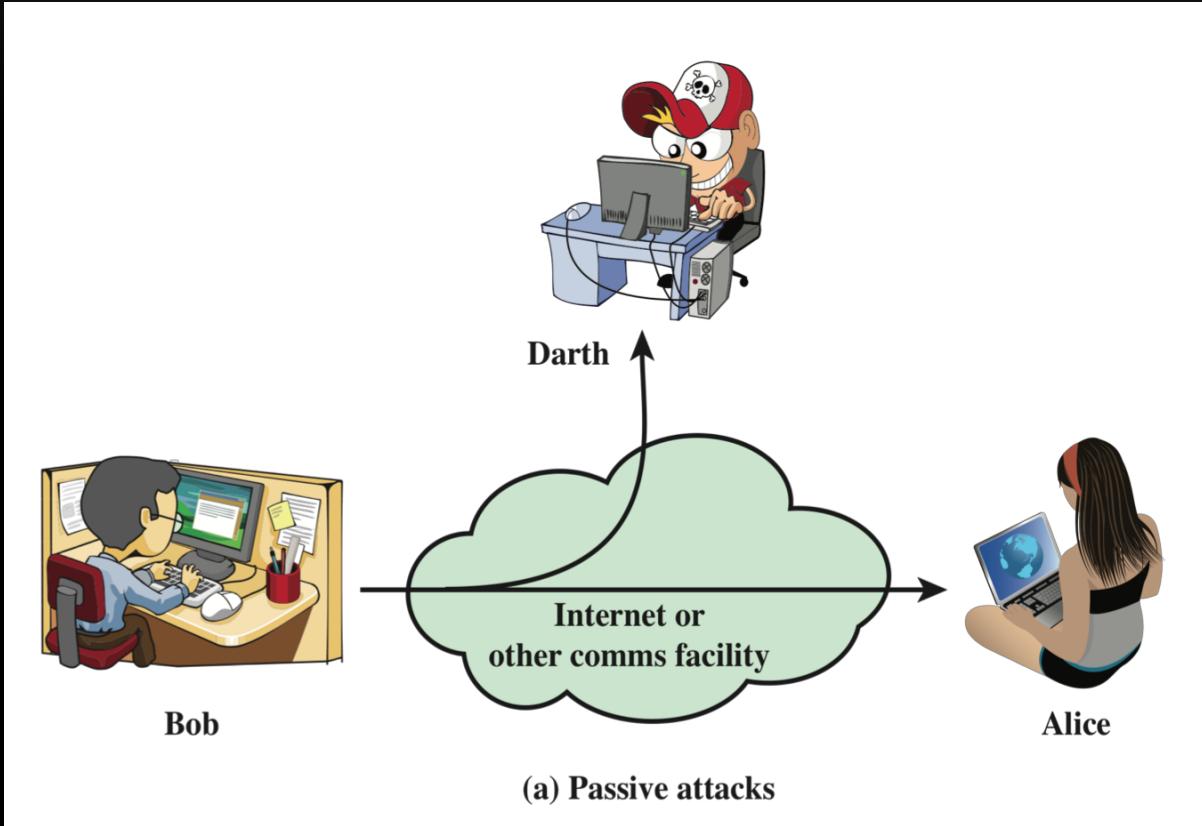
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.



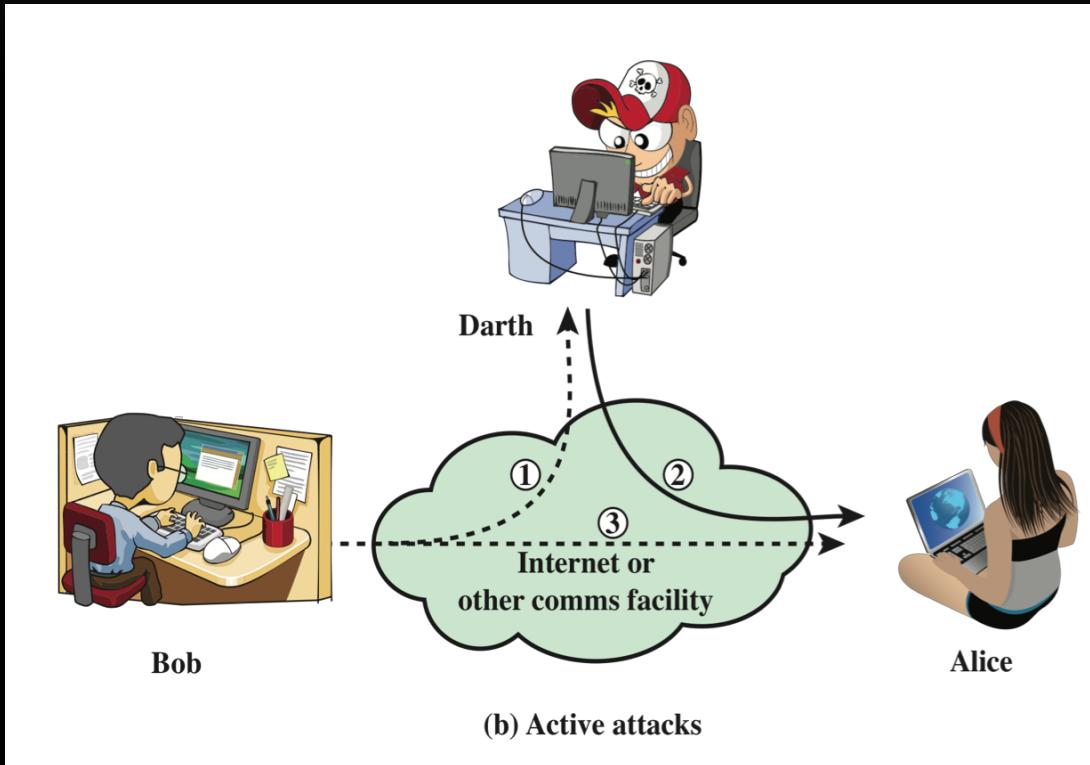
ATTACCHI [RFC4949]

- Attacco passivo:
 - un tentativo di apprendere o utilizzare informazioni provenienti dal/dai sistema/i target
 - non ha nessun impatto evidente sulle risorse del sistema stesso
- Attacco attivo:
 - un tentativo di alterare le risorse del sistema o modificarne le modalità operative

ATTACCHI PASSIVI [Stallings]



ATTACCHI ATTIVI [Stallings]



CARATTERISTICHE DEGLI ATTACCHI PASSIVI

- Tipicamente utilizzati per:
 - intercettazione (“eavesdropping”)
 - monitoraggio
- Obiettivo principale:
 - ottenere informazioni utili contenute nei dati trasmessi in rete
- Classici tipi di attacco:
 - accesso al contenuto dei messaggi
 - analisi del traffico





CARATTERISTICHE DEGLI ATTACCHI ATTIVI

- Prevedono la modifica (almeno parziale) del flusso dei dati, o la creazione di flussi di dati ‘falsi’
- Difficili da prevenire a causa dell’enorme varietà di potenziali vulnerabilità al livello fisico, del software o della rete
- Le strategie di difesa, in questi casi, mirano a:
 - rilevare l’attacco
 - ripristinare il sistema da eventuali danni o rallentamenti dovuti ad esso



ATTACCHI ATTIVI: TIPOLOGIE

Masquerade

- Si verifica quando un'entità finge di essere un'entità diversa
- Richiede l'impiego di una delle forme menzionate di attacco attivo (modifica o creazione di flussi di dati)

Replay

- Prevede la cattura 'passiva' di un'unità di dati e la sua successiva ritrasmissione al fine di produrre un effetto 'autorizzato'

Modification of messages

- Alcune porzioni di un messaggio 'legittimo' vengono modificate, oppure alcuni messaggi vengono ritardati o riordinati per produrre un effetto autorizzato

Denial of service

- Impedisce il normale uso (o la gestione) degli strumenti di comunicazione in rete (cfr. Availability)



SECURITY SERVICES

- Secondo lo standard X.800*:
"A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers"
- Secondo la solita RFC 4949:
"A processing or communication service provided by a system to give a specific kind of protection to system resources"

*X.800 : Security architecture for Open Systems Interconnection for CCITT applications

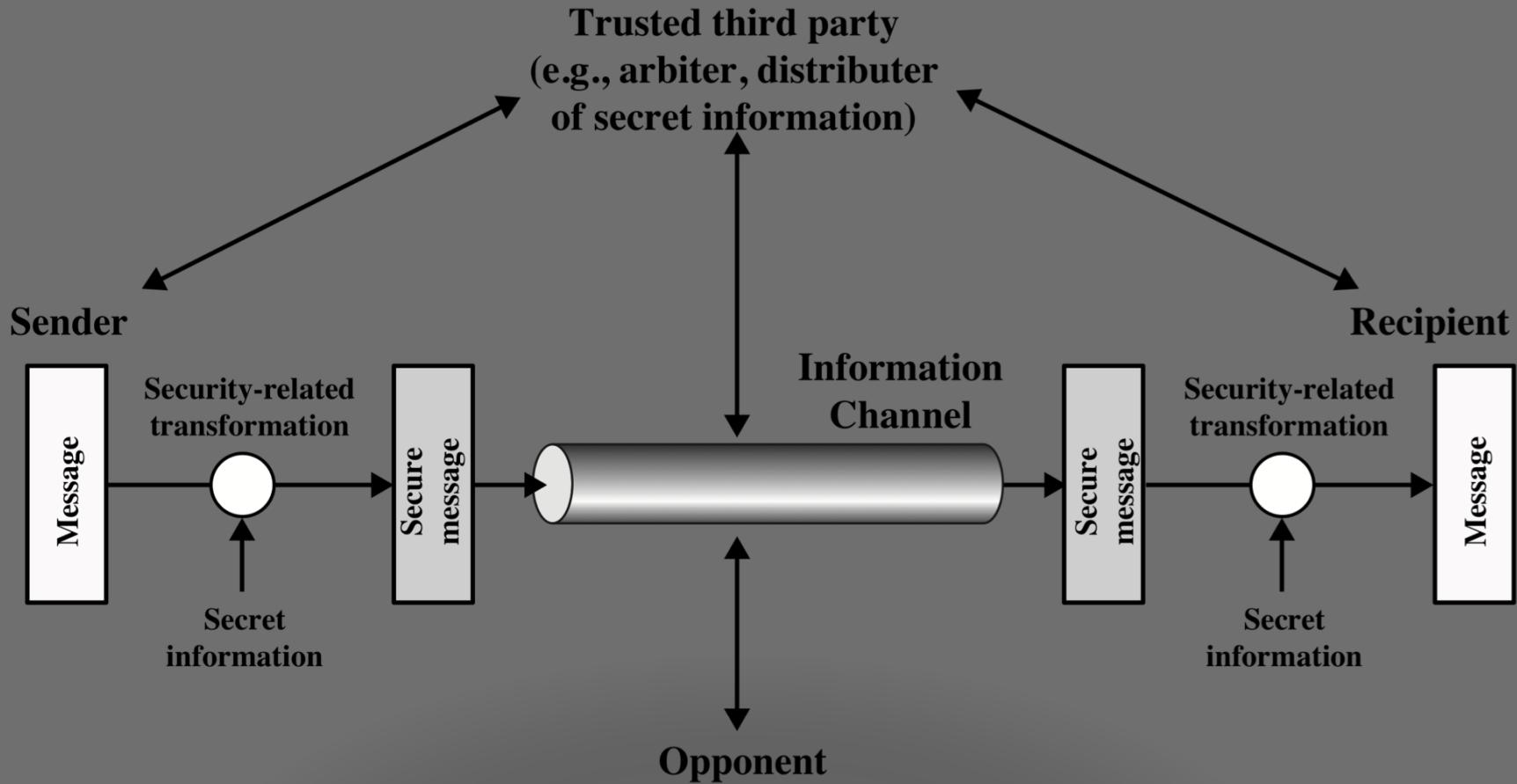


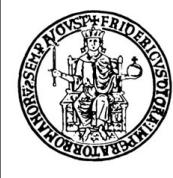
X.800 SERVICE CATEGORIES

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation

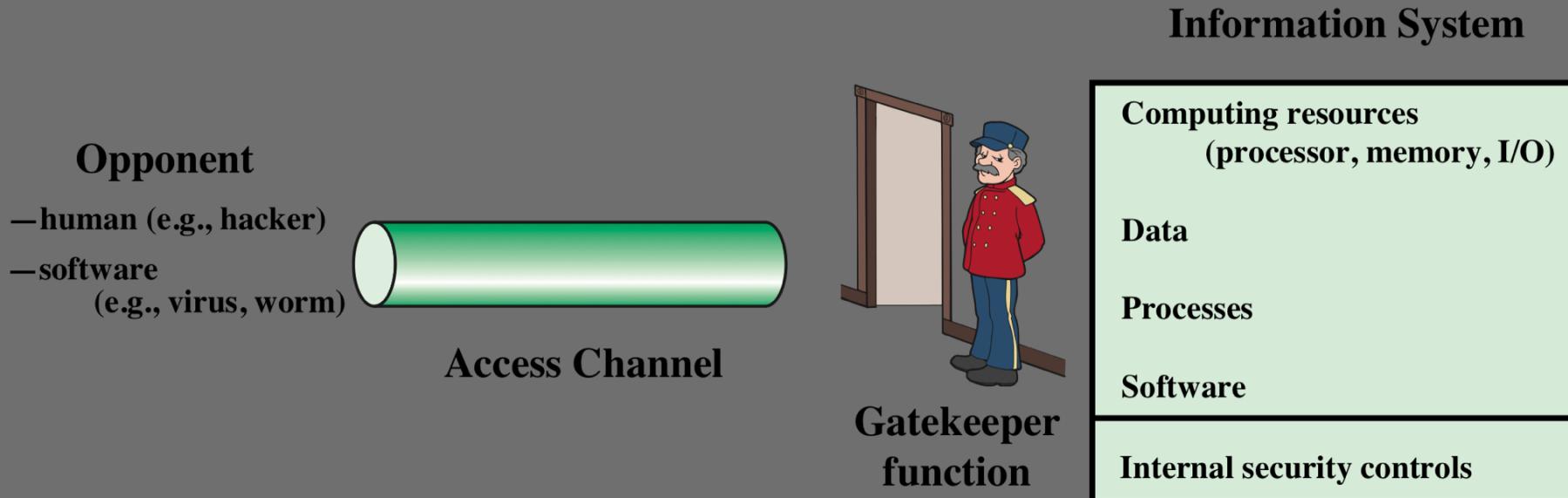


UN MODELLO PER LA NETWORK SECURITY



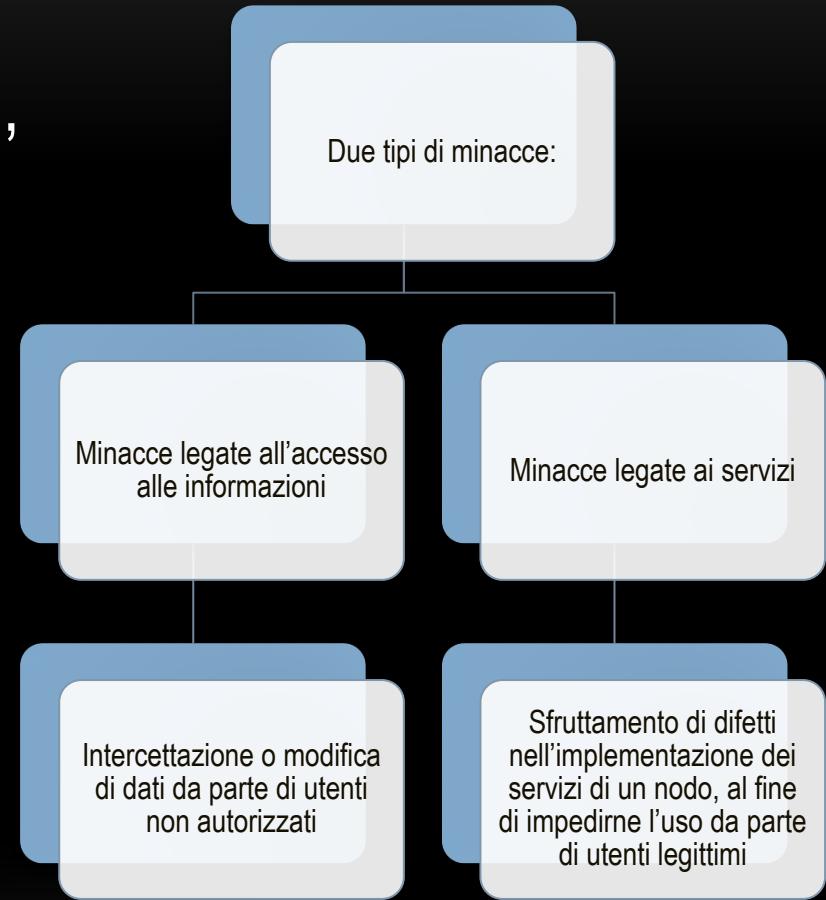


UN MODELLO DI SICUREZZA PER L'ACCESSO IN RETE



ACCESSO INDESIDERATO

- Introduzione, in un nodo, di meccanismi capaci di sfruttare le vulnerabilità del sistema e che possono influenzare sia i programmi applicativi, che quelli di utilità





STANDARD E ORGANIZZAZIONI

NIST

- National Institute of Standards and Technology
- Agenzia federale americana che si occupa di scienze della misura, di standard e di tecnologie legate all'impiego da parte del governo degli Stati Uniti, nonché alla promozione dell'innovazione nel settore privato
- I documenti emanati dal NIST hanno un impatto globale:
 - NIST Federal Information Processing Standards (FIPS)
 - Special Publications (SP)

ISOC

- Internet Society
- Una società mondiale di professionisti che partecipano, a titolo individuale, alla definizione, gestione ed evoluzione della rete Internet
- La casa madre di gruppi che si occupano degli standard per l'infrastruttura di Internet, ivi compresi l'IETF (Internet Engineering Task Force) e l'IAB (Internet Architecture Board)
- Gli standard (de facto) di Internet sono pubblicati sotto forma di “Requests for Comments” (RFC)

DOMANDE?

