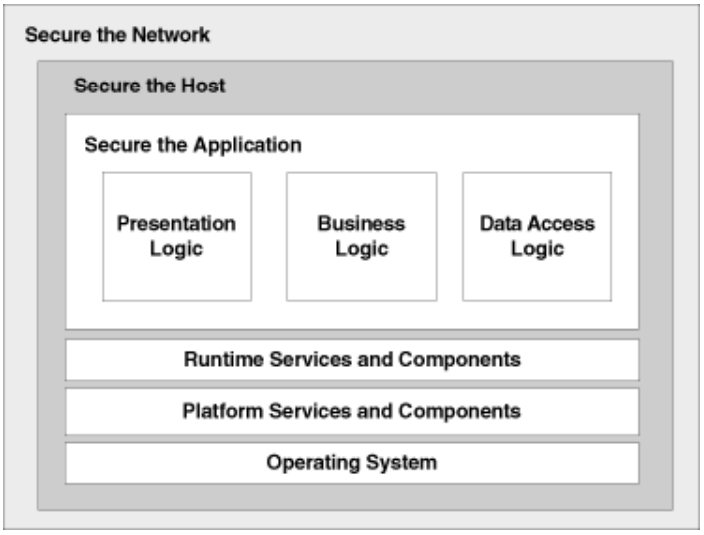
Introduzione alla sicurezza di rete

Proprietà
Attacchi
Contromisure

Prof. Filippo Lanubile

Sicurezza: difesa dai malintenzionati



Scenario tipico della sicurezza di rete: man in the middle

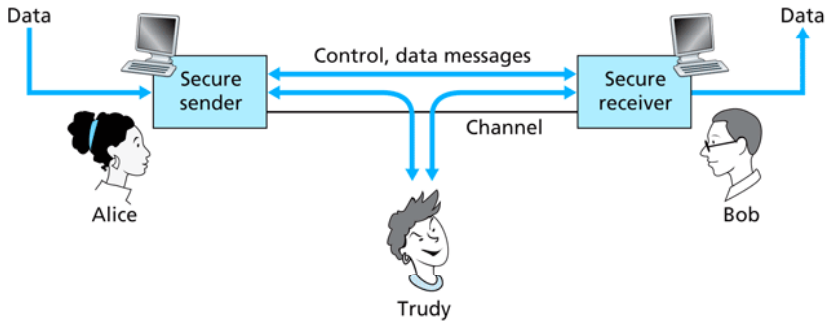


Figure 8.1 ♦ Sender, receiver, and intruder (Alice, Bob, and Trudy)

Proprietà fondamentali della sicurezza di rete (CIA triad)

- Riservatezza
  - Solo mittente e destinatario devono comprendere il contenuto del messaggio
  - Ha lo scopo di impedire l'utilizzo illegittimo di informazioni riservate
- Integrità
  - Mittente e destinatario devono essere sicuri che il contenuto di un messaggio non subisca alterazioni durante la trasmissione
  - Ha lo scopo di assicurare che un messaggio ricevuto sia esattamente quello spedito
- Disponibilità
  - Un servizio deve essere accessibile a chi è legittimamente autorizzato
  - Ha lo scopo di garantire la fruizione dei servizi di rete

Altre proprietà della sicurezza di rete

- Autenticità
  - Chi sei? Possibilità di identificare in modo certo e univoco mittente e destinatario
    - Può essere semplice (solo mittente) o mutua (sia mittente che destinatario)
- Non ripudio
  - prova formale per dimostrare che una certa persona ha sottoscritto (firmato) un documento
    - Integrità e autenticità sono condizioni necessarie per garantire il non ripudio

Attacchi alla sicurezza di rete

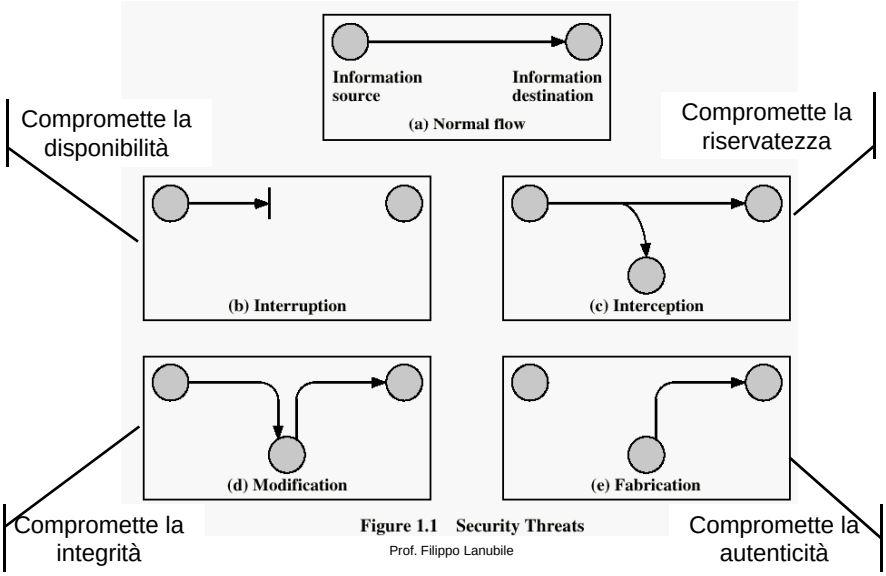


Figure 1.1 Security Threats

Alcuni attacchi

Attacchi passivi

- Network mapping
- Port scanning
- Sniffing

Attacchi attivi

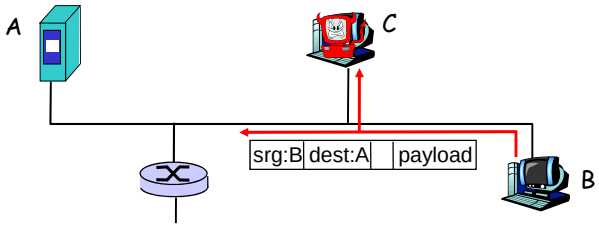
- Spoofing
- Replay
- Connection hijacking
- Exploit
- Malware
- DoS e DDoS

Network mapping e port scanning

- Obiettivo: determinare quali sono gli host attivi in una rete e quali sono i servizi offerti
- Network mapping: ricostruzione di quali sono gli indirizzi IP attivi di una stessa rete
  - Es. Uso di utility basate su ICMP per l'esplorazione di una rete
- Port scanning
  - Contatto sequenziale dei numeri di porta di uno stesso host per vedere cosa succede
    - Sia con segmenti TCP che con datagrammi UDP

Sniffing

- Anche detto packet sniffing, eavesdropping o wire tapping
- Lettura dei pacchetti destinati ad un altro nodo della rete
  - Quando i dati viaggiano su una rete a mezzo condiviso è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri host



- L'intercettazione dei dati è fatta attraverso appositi programmi, detti sniffer (es. Wireshark)

Spoofing

- L'attaccante fa finta di essere qualcosa o qualcuno che non è
- Si possono così carpire informazioni riservate
- Vari tipi
  - User account spoofing
  - DNS spoofing
  - IP spoofing
  - MAC spoofing

User account spoofing

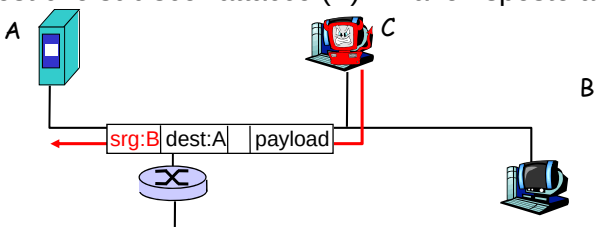
- L'identità elettronica dell'utente è abusata utilizzando le sue credenziali di autenticazione
  - Ottenute attraverso confidenze incaute, promemoria esposti, dictionary attack, exploit, malware, sniffing
- I problemi più gravi si hanno quando:
  - l'abuso produce gravi violazioni alle norme vigenti
  - l'abuso avviene in un contesto commerciale e dà origine a obblighi per la persona che subisce l'abuso
  - è abusata l'identità dell'amministratore del sistema

DNS spoofing

- Falsificazione del nome DNS
  - Basato sulla modifica della cache del DNS server a cui la vittima si rivolge, direttamente o indirettamente
- La richiesta di una pagina web o di un altro servizio è fatta a un fornitore sbagliato

IP spoofing

- Agisce a livello rete (layer 3)
- Falsificazione dell'indirizzo IP dell'attaccante-mittente
  - L'host che effettua l'attacco (C) si spaccia per un altro (B)
  - L'host che subisce l'attacco (A) invia le risposte a B



- Spesso usato per mascherare l'host da cui partono attacchi di tipo DoS

MAC spoofing

- Agisce a livello data link (layer 2)
- Falsificazione dell'indirizzo fisico (*MAC address*) assegnato dal costruttore alla scheda di rete
- L'attaccante riceve le risposte all'interno del dominio di broadcast locale
- Spesso usato per raggirare i controlli di accesso a una rete

Replay

Attacco di replica
- o di playback
- Intercettazione passiva di dati e successiva ritrasmissione per generare un effetto non autorizzato

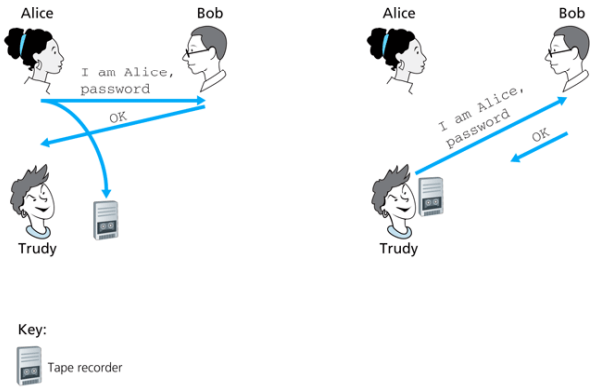


Figure 8.17 ♦ Protocol *ap3.0* and a failure scenario

Connection hijacking

- Il traffico generato tra mittente e destinatario è dirottato verso l'attaccante che finge di essere il punto finale legittimo della comunicazione
- L'attaccante modifica i dati trasmessi senza che le parti coinvolte nella comunicazione se ne accorgano

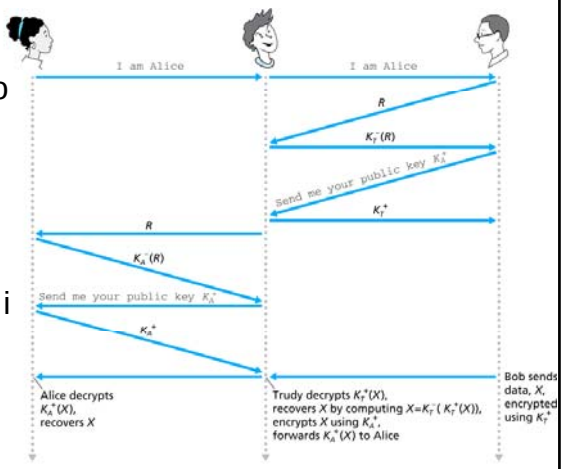


Figure 8.21 ♦ A man-in-the-middle attack

Exploit

- Esecuzione delle azioni necessarie ad approfittare di una vulnerabilità del software per sferrare un attacco (tipicamente DoS)
  - Vulnerabilità tipicamente generate da un difetto noto del software
  - Possono anche dipendere da errori di configurazione o installazione
- La vulnerabilità può essere sfruttata solo mettendo in opera un procedimento apposito volto a sfruttarla per danneggiare la sicurezza del sistema
  - Esempio: WinNT server ver. 3.51 e 4.0
    - telnet alla porta 135
    - 10 caratteri a caso, poi CR
    - server non disponibile! (CPU al 100% senza che venga svolto alcun lavoro)

Malware (malicious software)

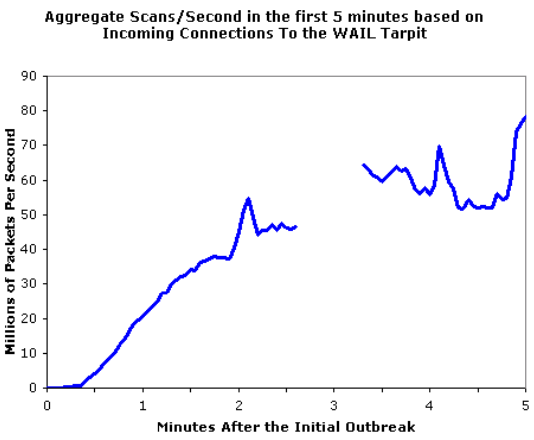
- Software che produce effetti dannosi o non desiderati e quindi potenzialmente lesivo della sicurezza di un sistema
  - Esempio: può registrare quanto viene digitato, i siti visitati e informazioni di upload
- Gli host infettati possono essere “arruolati” in botnet, e usati per lo spamming e per gli attacchi di DDoS
- Spesso auto-replicante: da un host infettato può passare ad altri host
- Può raggiungere gli host attraverso virus, worm, o cavalli di Troia

Malware: Virus

- L'infezione proviene da un oggetto ricevuto e mandato in esecuzione
- Auto-replicante: si propaga da solo ad altri host e utenti
- Realizza tipicamente due attività:
  - Diffusione
  - Attivazione

Malware: Worm

- L'infezione proviene da un oggetto passivamente ricevuto, attraverso i servizi di rete, che si auto-esegue
- Auto-replicante: si propaga da solo ad altri host e utenti
- Autosufficienti: in grado di funzionare senza bisogno di un programma ospite



Malware: Cavalli di Troia

- Parte nascosta di un software installato perché considerato utile
  - Si possono trovare anche su pagine web che contengono componenti eseguibili sul client
- Una volta eseguiti, effettuano operazioni diverse da quelle per le quali l'utente li aveva utilizzati e tipicamente dannose
- Hanno spesso lo scopo di mascherare altri attacchi (tipo DDoS), procurarsi informazioni aggiuntive o creare un accesso (backdoor) da sfruttare successivamente

Denial of Service (DoS)

- Interruzione di un servizio che risulta indisponibile agli utenti legittimi
- Può essere ottenuto
  - mandando in crash il sistema che quindi necessita dell'intervento dell'amministratore per riprendere il corretto funzionamento e l'erogazione dei servizi
  - rendendo le risorse troppo impegnate, in modo da provocare risposte negative a richieste di servizio legittime
- Esempi:
  - mail bombing
  - SYN flooding
  - ICMP flooding

Distributed Denial of Service (DDoS)

- L'attaccante ottiene l'accesso su numerosi host in rete
- L'attaccante installa un programma slave su ognuno degli host compromessi
- Un programma master contatta i programmi slave dando il via a un attacco DoS che si concentra su uno stesso host target

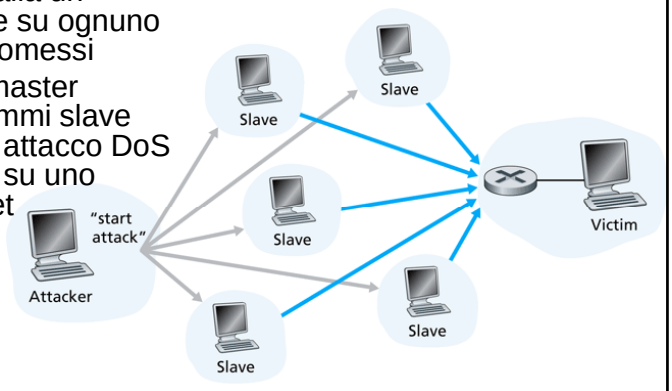


Figure 1.21 ♦ A distributed denial-of-service attack

Contromisure

- Linee guida per la prevenzione dei problemi
  - Aggiornamenti frequenti del software, monitoraggio tramite log, chiusura dei processi in ascolto che non servono, politica di accessi autorizzati alle risorse, politica di gestione delle password, non operare quando non serve con diritti di root, ecc.
- Antivirus
- **Firewall**
- **IDS**
- **Strumenti crittografici**