Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

X.800

- È una “raccomandazione” dell’ITU (International Communication Union)
  - Standard Internazionale
  - Definizione strutturata dei servizi e dei meccanismi
  - Panoramica utile ma astratta

X.800

X.800 definisce cinque categorie di servizi di sicurezza:

- Autenticazione: sicurezza dell'identita dei soggetti che comunicano
- Controllo degli accessi: prevenire uso non autorizzato di una risorsa
- Segretezza dei dati: protezione dei dati da osservatori non autorizzati
- Integrità dei dati: sicurezza che il dato ricevuto è uguale al dato inviato
- Non-ripudiabilità: sicurezza che il dato inviato sia stato ricevuto

X.800

X.800 definisce alcuni meccanismi di sicurezza:

- Cifratura
- Firme digitali
- Controllo degli accessi
- Codici di integrità dei dati
- Autenticazione
- Tecniche di riempimento del traffico

X.800

Cifratura o Crittografia

- Usa algoritmi matematici per trasformare i dati
- I dati trasformati sono illegibili se non si possiede la chiave
- Il ripristino dipende da 0 o più chiavi di crittografia

X.800

Firma Digitale

- Vengono aggiunti dati ed informazioni crittografiche ai dati originali
- Consente al destinatario di dimostrare
  - L'origine dei dati
  - L'integrità

X.800

Controllo degli Accessi

- Esistono una varietà di meccanismi diversi
- Permette il controllo dei limiti di accesso alle risorse
- Può essere statico e dinamico

X.800

Autenticazione

- Ha lo scopo di garantire l'identità di una entità tramite lo scambio di informazioni

X.800

Tecniche di riempimento del traffico

- Si inseriscono dei dati fasulli all'interno del flusso dati
- Tali dati non appartengono ai dati scambiati
- I peer devono essere a conoscenza dei dati da scartare
- Serve a complicare ulteriormente il tentativo di analisi del traffico da parte di utenti non autorizzati

X.800

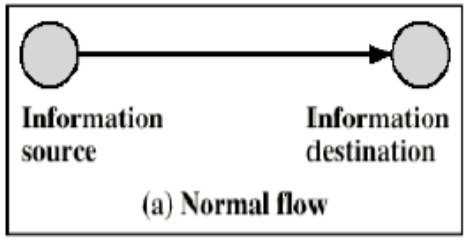
X.800 definisce due macro categorie di attacchi:

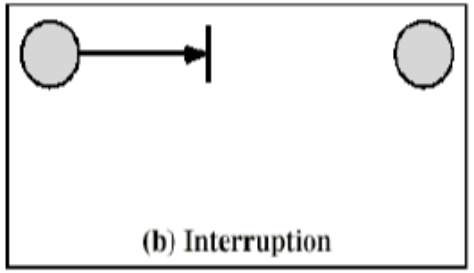
- Attacchi Passivi - intercettazione o monitoraggio delle trasmissioni per:
  - Ottenere i contenuti dei messaggi
  - Monitorare i flussi di traffico
- Attacchi Attivi – Prevede la “forzatura” di un sistema di sicurezza (ad esempio modifiche dei flussi di dati) per:
  - Mascheramento di un'entità come qualcun altro
  - Ripetere i messaggi precedenti
  - Modificare i messaggi in transito
  - Negazione del servizio

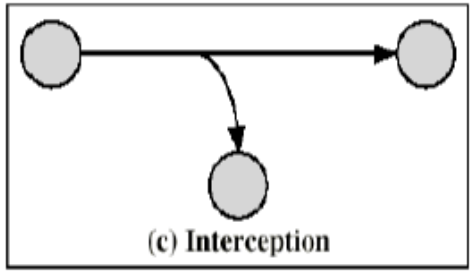
X.800

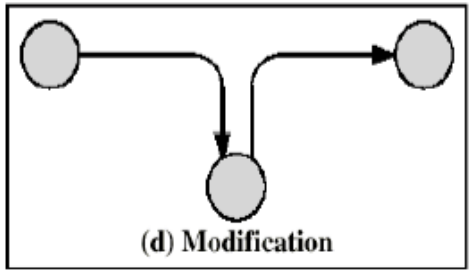
X.800 definisce quattro tipi di attacchi:

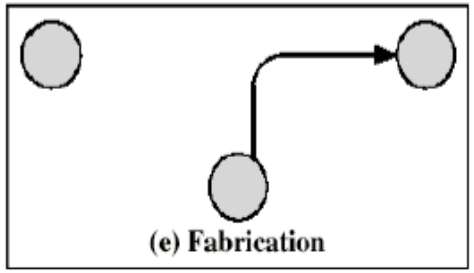
- Interruzione – attacco della fruibilità del servizio
- Intercettazione – attacco della confidenzialità
- Modifica – attacco dell'integrità
- Fabbricazione – attacco dell'autenticità



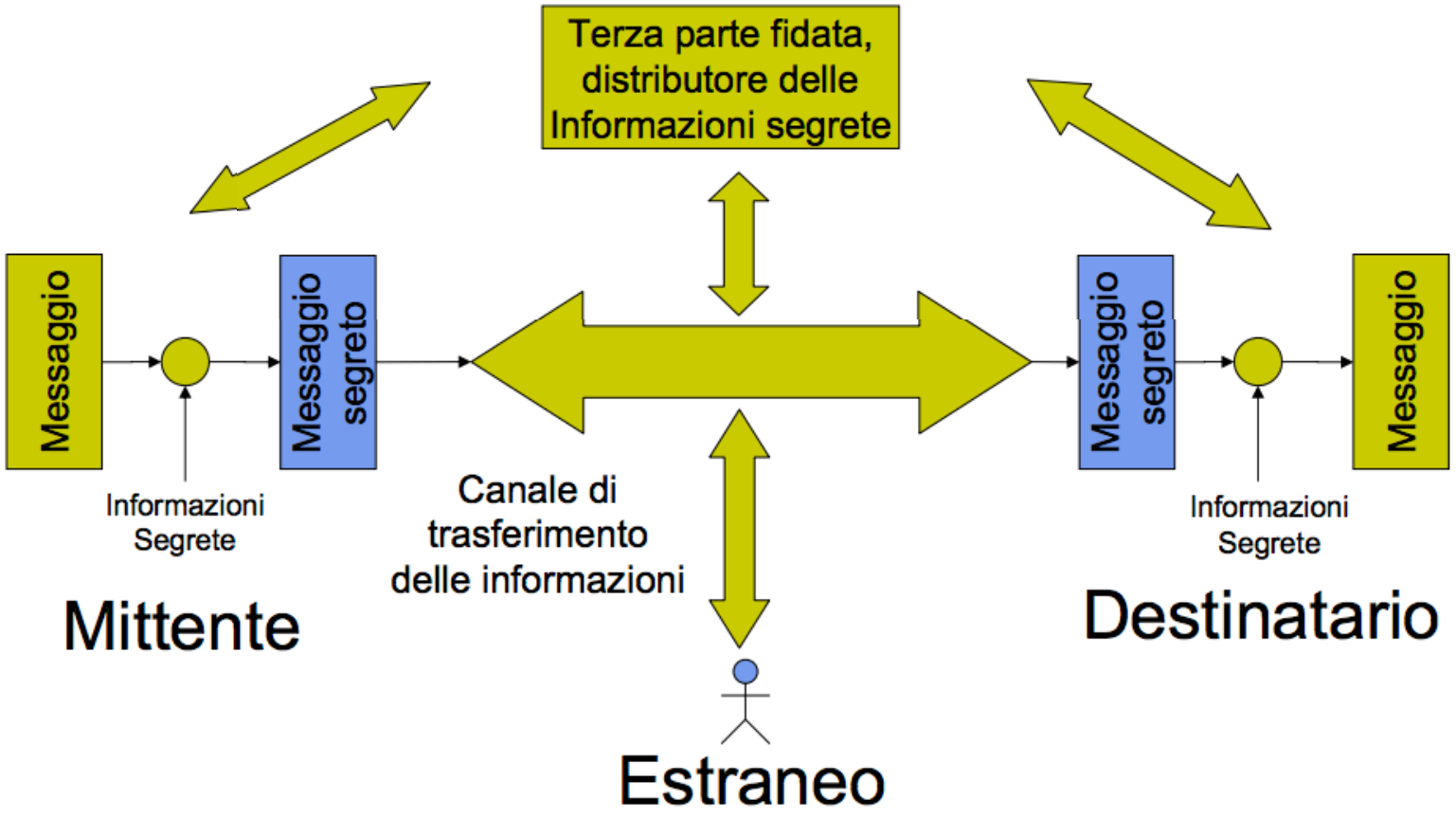








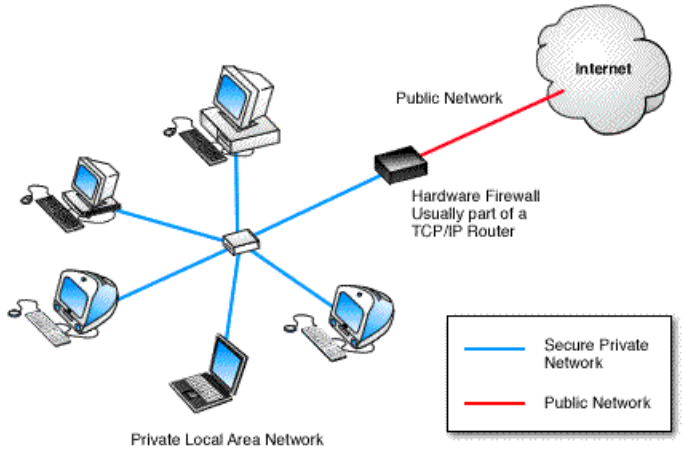
Un modello per la sicurezza di una rete



Vulnerabilità informatiche

Terminologia

- Intranet
  - Rete locale
  - rete aziendale privata che utilizza il protocollo TCP/IP
- Internet
  - Rete di collegamenti informatici a livello planetario



Terminologia

- Hacker
  - esperto di vulnerabilità e attacchi
  - non necessariamente malevolo
  - in italiano l'accezione è spesso negativa
- vedi wikipedia "Hacker (computer security)"
  - Hacker: esperto buono
  - Cracker: esperto malevolo

Terminologia

- Vulnerabilità o vulnerabity exposure
  - un problema hw, sw, di configurazione o di procedura che rende possibile un uso improprio di dati o risorse hw e sw
- Minaccia (threat)
  - un insieme di circostanze potenzialmente pericolose
- es. un bug di explorer assieme alla possibilità di navigare liberamente su Internet costituiscono una minaccia per la sicurezza del sistema degli utenti

Terminologia

- Exploit, Exploitation
  - la procedura per sfruttare una vulnerabilità
- Attacco
  - tentativo di violazione di riservatezza, integrità o disponibilità tramite lo sfruttamento (exploitation) di una vulnerabilità
- Intrusione
  - un attacco riuscito

Terminologia

- Privilege Excalation
  - l'azione di guadagnare accesso a risorse che normalmente sono precluse.
  - è un attacco andato a buon fine
- Root Compromise
  - situazione in cui l'hacker ha ottenuto il pieno controllo della macchina

Terminologia

- Contromisura
  - procedura, installazione hw o sw, configurazione o altro atto a diminuire la probabilità che una minaccia possa dar luogo ad un attacco o a limitarne le conseguenze
- es. installare un antivirus è una contromisura che protegge una intranet da semplici tipi di attacchi
- scollegare la intranet da Internet è una contromisura più efficace ma potrebbe essere non “gradita” dall’utenza

Terminologia

- Soggetto
  - chi (o cosa) accede ad una risorsa, in modo lecito o illecito, anche inconsapevolmente
- Oggetto
  - una risorsa da “proteggere”
- Diritti (di un soggetto su un oggetto)
  - operazioni che il soggetto può compiere sull’oggetto in maniera lecita
  - dal punto di vista dell’oggetto sono detti “permessi”

Terminologia

Esempio

- in unix è vero l'utente root può cancellare qualsiasi file
  - soggetto: utente root
  - oggetto: un qualsiasi file
  - diritto: cancellazione

Terminologia

Policy

- un insieme di regole che stabiliscono quali soggetti hanno quali diritti su quali oggetti
- definisce il concetto di sicurezza in un certo contesto (un sistema, una organizzazione, ecc.)
- una policy può essere espressa:
  - in linguaggio naturale
  - tramite modello matematico
  - tramite linguaggio ad hoc, ecc
- in certi contesti (pianificazione) si assume un significato più ampio

Terminologia

Meccanismo

- ciò che per progetto ha lo scopo di far rispettare la policy
- es. autenticazione + controllo di accesso sui file permettono di realizzare politiche di “visibilità” dei file tra i vari utenti in windows o unix

Azioni di sicurezza

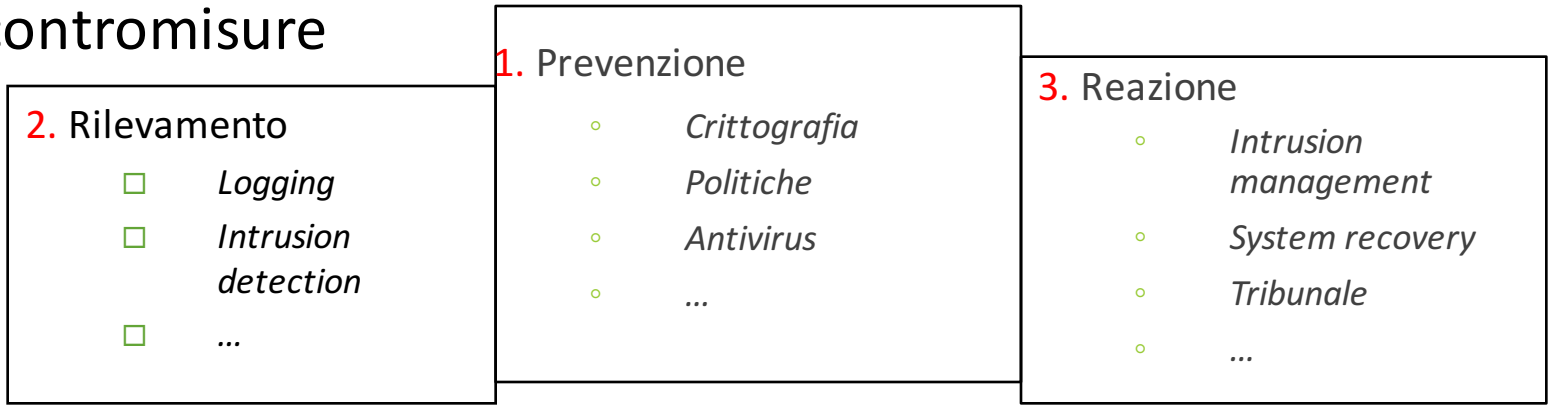
- Prevenzione
  - ciò che si fa prima che un certo attacco si manifesti in modo da impedirlo
  - es. installazione di un antivirus
- Rilevazione (Detection)
  - l'azione di accertare se una violazione della policy è in atto in un certo momento
- Contrasto
  - l'azione di fronteggiare un attacco mentre avviene
  - es. cambio la configurazione del firewall per bloccare un certo traffico malevolo
- Recovery
  - il ripristino della normale operatività del sistema
  - aspetti importanti: tempo, costo
  - certe azioni preventive riducono (o annullano) il tempo e il costo di recovery

Azioni di sicurezza

- Resilienza
  - la capacità di un sistema di continuare a funzionare in presenza di problemi
  - è un modo per assicurare disponibilità dei servizi
- Fail-over
  - un azione automatica per recuperare ad un problema (es. un guasto)
  - per estensione anche i meccanismi che permettono il fail-over

Azioni di sicurezza

- spesso la prevenzione è meglio degli altri approcci ma...
  - ...può non essere percorribile
  - ...può essere troppo costosa
  - ...può essere non sostenibile dal punto di vista della utilizzabilità del sistema
- Pianificazione
  - prevede una valutazione dei rischi e dei costi per la scelta delle eventuali contromisure



Minacce

- Social media scammers
  - Obiettivi: credenziali degli utenti sui social media
- Phishers
  - Obiettivi: credenziali su siti bancari, numeri di conto e di carta di credito
- Fakeav creators
  - Obiettivi: vendere finti antivirus
- App trojanizer
  - Obiettivi:
    - impossessarsi delle rubriche, dei messaggi e altri dati memorizzati sui dispositivi mobili
    - indurre a pagare per servizi addizionali non desiderati

Minacce

- Spammers
  - Obiettivi:
    - far pagare per ciò che non si vuole
    - alimentare lo spamming confermando gli indirizzi
- Malvertisers
  - Obiettivi: Ottenere nomi indirizzi di email numeri di telefono
- (Crypto)Kidnapper
  - Obiettivi: Prendere in ostaggio il PC o i dati dell'utente e chiedere un riscatto