Università degli Studi di Verona

Sicurezza delle reti

Riassunto dei principali argomenti

Davide Bianchi

October 24, 2018

Contents

1 Introduzione

Definizione 1.0.1 (Information Security) *Protezione delle informazioni e dei sistemi per impedirne l'accesso non autorizzato, uso, divulgazione, modifica o distruzione.*

Definizione 1.0.2 (Network Security) *Protezione dell'accesso a risorse situate all'interno di una rete.*

Nella sicurezza si distinguono una **policy**, un **meccanismo** e una **compliance**. Una security policy specifica il comportamento che il sistema può o non può assumere. I meccanismi di sicurezza sono l'implementazione di una data policy. Diciamo quindi che una security policy ϕ deve rimanere valida per un sistema P in ogni ambiente malevolo E, ovvero $P \parallel E \models \phi$.

Le politiche di sicurezza sono spesso formulate per arrivare ad alcune proprietà standard, le più comuni sono:

- Confidenzialità: non ci sono fughe di informazioni;
- Integrità: non ci sono modifiche alle informazioni;
- Disponibilità: non ci sono "danneggiamenti" ai servizi;
- Accountability[1]: le azioni sono sempre riconducibili ai diretti responsabili;
- Autenticazione: l'origine dei dati può essere identificata con sicurezza.

Contromisure per la protezione. Le principali tecniche di contromisura consistono in:

- Prevenzione di breach;
- Rilevamento di attacchi in corso;
- Reazione ad un possibile attacco.

2 Cenni di crittografia

2.1 Introduzione

Iniziamo dando alcune definizioni fondamentali. Si useranno i termini *ciphertext* e *plaintext* per indicare rispettivamente il testo cifrato e quello in chiaro.

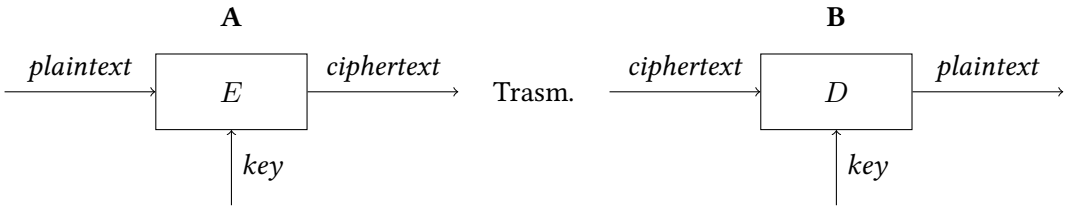
Definizione 2.1.1 (Crittografia) *Insieme dei metodi per rendere un messaggio non leggibile ad altri.*

Definizione 2.1.2 (Steganografia) *Insieme dei metodi per nascondere l'esistenza di un messaggio in un altro contenuto.*

Definizione 2.1.3 (Crittoanalisi) *Analisi del ciphertext per ottenere il plaintext corrispondente.*

[1] La traduzione più vicina è *responsabilità.*

Un generico sistema crittografico è strutturato come:



In crittografia si distinguono le due categorie *a chiave simmetrica* e *a chiave asimmetrica*. La differenza sta nel fatto che nella crittografia a chiave simmetrica le due entità che si scambiano il messaggio devono condividere una stessa chiave (che deve essere trasmessa su un canale sicuro), mentre nella crittografia a chiave asimmetrica le chiavi sono differenti e sono 2 per ogni entità, una pubblica e una privata. Nella crittografia a chiave asimmetrica si elimina il problema della condivisione della chiave; inoltre la chiave pubblica può essere compromessa da attaccanti senza che la chiave privata venga compromessa, e senza che venga compromessa la segretezza del messaggio.

Un altro aspetto fondamentale della crittografia è che la cifratura e la decodifica sono facili, *se le chiavi sono note*. Da ciò consegue che la sicurezza debba risiedere nella chiave, non nell'algoritmo in se.

2.2 Crittoanalisi

La scienza di recuperare il messaggio in chiaro senza conoscere il ciphertext si basa sostanzialmente su due differenti approcci:

- attacco brute-force;
- attacco crittoanalitico.

Attacco brute-force. Un attacco bruteforce è semplice: consiste nel provare tutte le chavi possibili fino ad indovinare quella corretta. Questa tipologia di attacco in generale è sempre possibile nella sua semplicità, tuttavia, se la dimensione dello spazio delle chiavi inizia ad essere elevata, il tempo che si deve impiegare diventa insostenibile, per cui in questi casi è necessario ricorrere ad altri stratagemmi.

Attacco crittoanalitico. In questo caso si assume che l'attaccante conosca l'algoritmo utilizzato nella cifratura dei messaggi; si trova quindi una qualche debolezza nell'algoritmo che permetta di farlo fallire.

In tal senso, si tende a rendere noto un algoritmo affinchè il maggior numero di persone tenti di attaccarlo, per aumentare al massimo le possibilità che venga trovata una falla. (In contrasto con la cosiddetta **security by obscurity**).

Tipologie di attacco. Consideriamo ora i possibili attacchi che un sistema crittografico deve affrontare per essere affidabile:

- *known cypertext attack:* questo attaccante è il meno aggressivo e conosce solamente il testo cifrato;
- *known plaintext attack:* conosce entrambi i tipi di testo;
- *choosen plaintext:* può scegliere il plaintext da codificare e analizzare il ciphertext ottenuto;

- *adaptive choosen plaintext:* può liberamente scegliere il plaintext da far codificare e comportarsi di conseguenza, sulla base del risultato appena ottenuto.
- *chosen ciphertext:*l'attaccante può scegliere differenti ciphertext e avere accesso al plaintext decriptato, per infine ricavare la chiave.