Tecniche di furto d'identità basate su Deep Learning

Candidata: Federica Fino

Relatore: Prof. Marco Liverani

Dipartimento di Matematica e Fisica
Corso di Laurea Magistrale in Matematica

18 marzo 2021

Perché il Password Guessing?

Tutt'oggi le password costituiscono uno dei metodi di autenticazione maggiormente utilizzati

L'accesso di un utente ad un sistema informatico avviene introducendo uno ***username***, attraverso cui l'utente dichiara la propria identità, e una ***password*** segreta, attraverso cui l'utente fornisce una prova della propria identità

Il sistema ***autentica*** l'identità dell'utente, verificando che la password corrisponda con quella registrata sul sistema stesso sotto forma di ***hash***

Funzioni di hash

Un ***hash*** è una funzione **non invertibile** che mappa una stringa di lunghezza variabile in una stringa di lunghezza predefinita, chiamata ***digest***

Proprietà

- resistenza alla preimmagine
- resistenza alla seconda preimmagine
- resistenza alle collisioni

Password Guessing

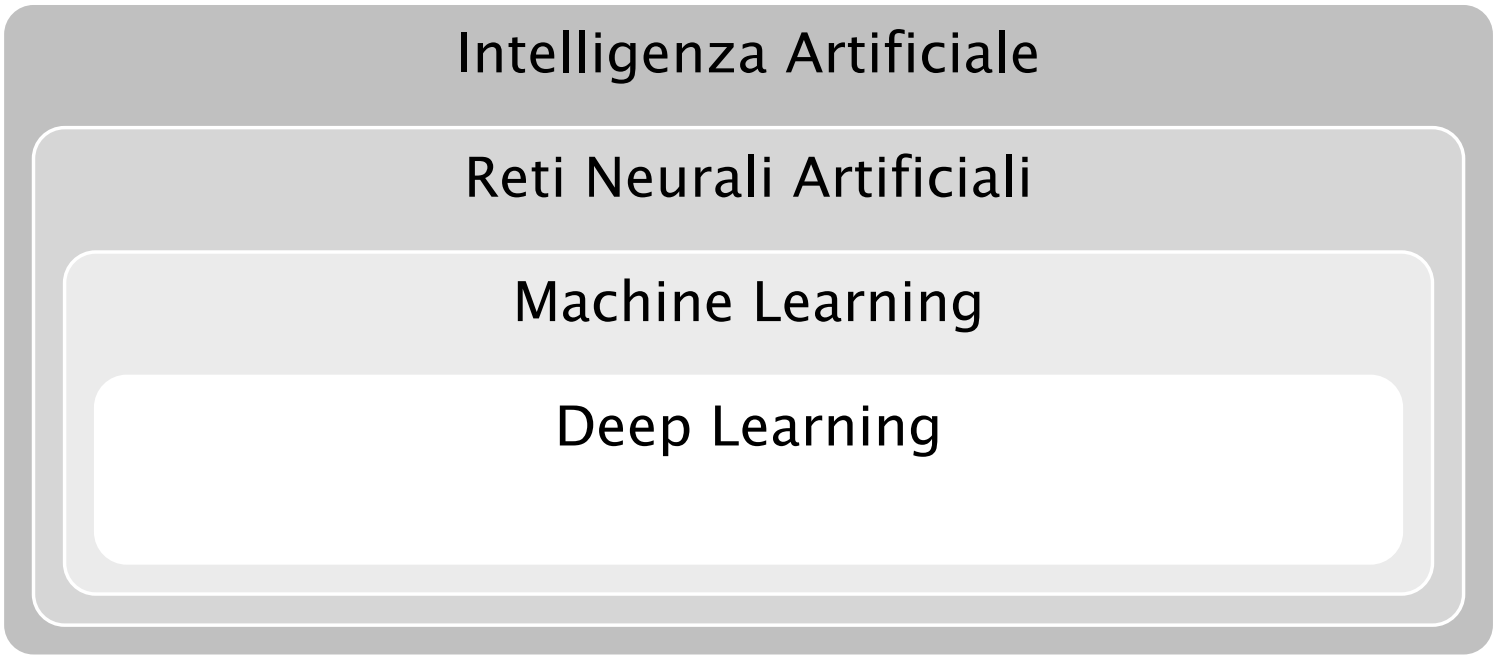
Il furto d'identità digitale è un attacco informatico in cui l'attaccante riesce ad entrare in possesso di informazioni riservate utilizzate per l'autenticazione degli utenti (password)

Il ***password guessing*** consiste nella ricostruzione della password di un utente a partire da un file di hash

Sono due i possibili scenari:

- *online*
- *offline*

Deep Learning



Le reti neurali artificiali

La rete neurale artificiale è rappresentata come un *grafo bipartito*, con un insieme di vertici indipendenti che rappresenta lo strato di input ed un secondo insieme di vertici che rappresenta lo strato di output

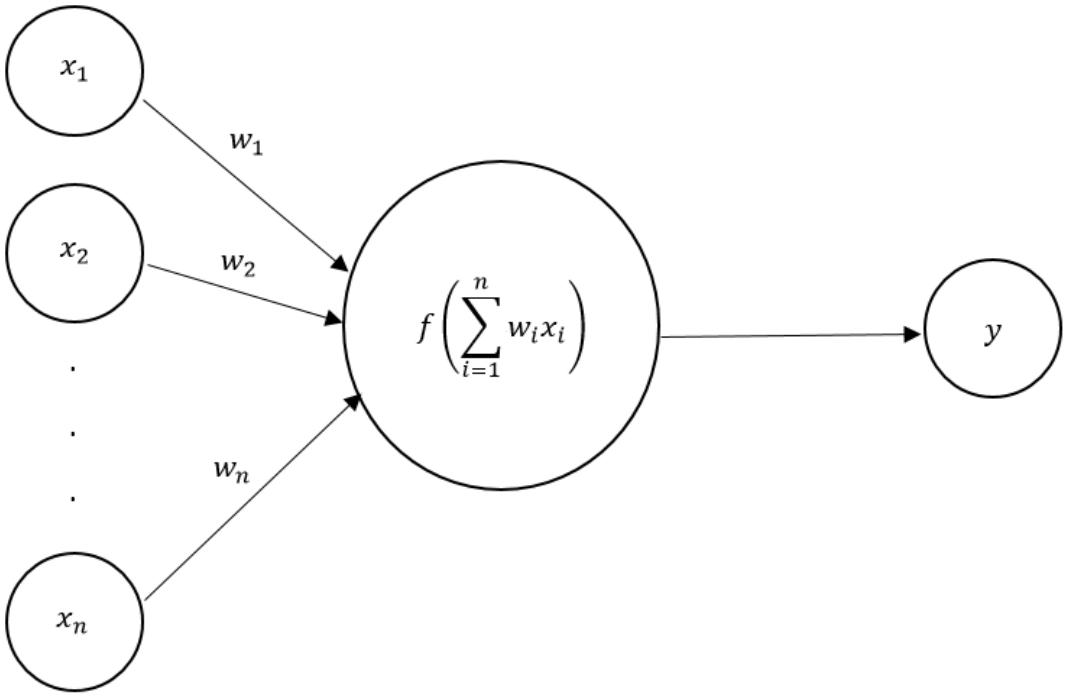
Quando tra questi due strati sono presenti uno o più strati intermedi (*hidden layers*), si parla di ***deep learning***

Strutture più diffuse nell'ambito del deep learning

- Multi-layer perceptron (MLP)
- Convolutional neural network (CNN)
- Recurrent neural network (RNN)

Il neurone neurale artificiale

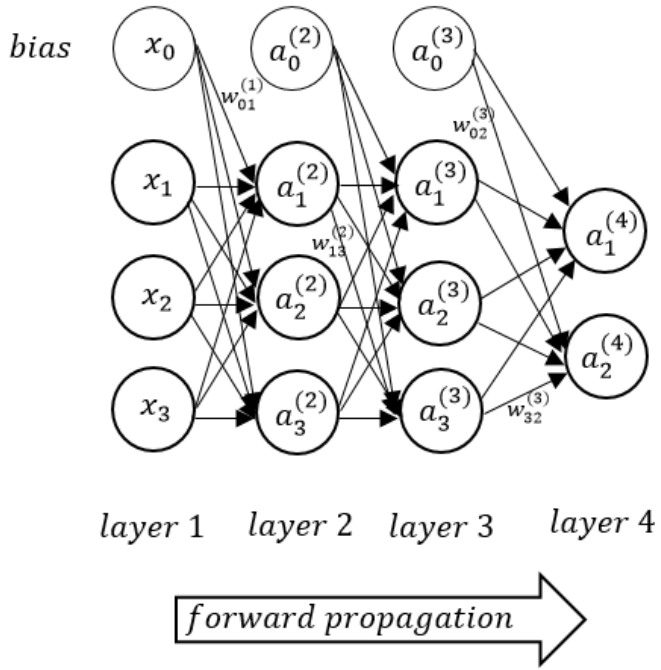
L'elemento di elaborazione di base di una rete neurale è il **neurone artificiale**: una funzione della somma dei valori in ingresso moltiplicati per i relativi pesi, nota anche con il nome di **funzione di attivazione**



L'addestramento di una rete neurale

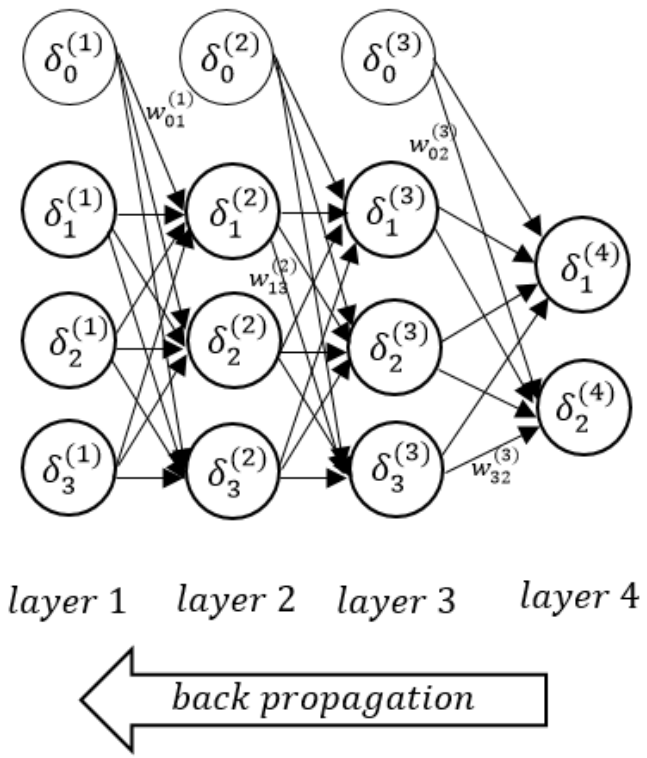
Possiamo distinguere tre fasi principali nel processo di addestramento di una rete neurale:

- ***forward propagation***: la propagazione dei dati di input lungo la rete



L'addestramento di una rete neurale

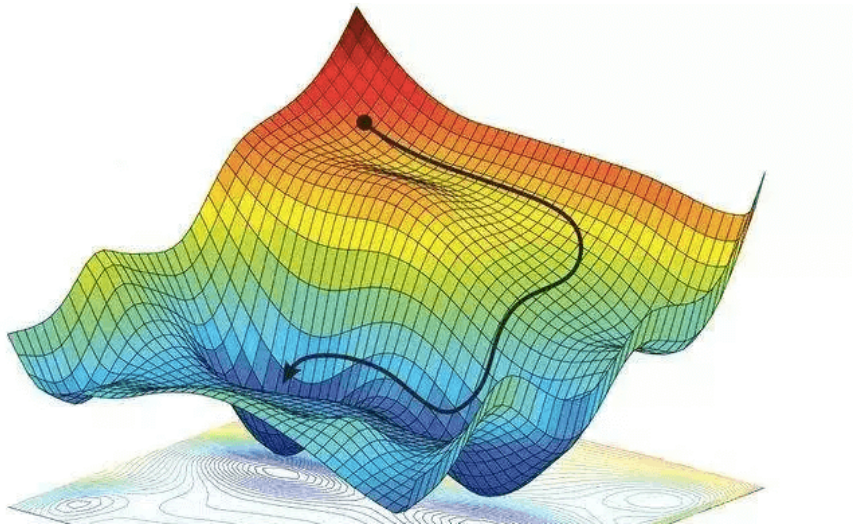
- ***error back propagation***: la ripropagazione all'indietro dell'errore commesso dalla rete



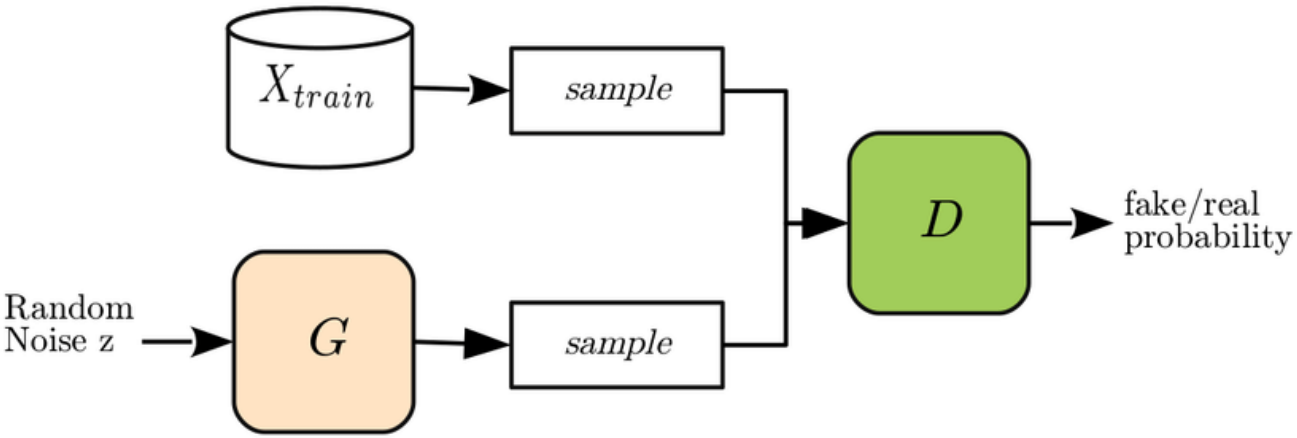
L'addestramento di una rete neurale

- ***aggiornamento dei pesi***: l'aggiornamento dei parametri della rete con l'obiettivo di minimizzare la funzione costo

$$\min_{w} J(w)$$



Le reti GAN



Il problema di ottimizzazione per un sistema GAN è il seguente:

$$\min_G \max_D V(G,D) = \mathbb{E}_{x\sim p_t(x)}[\log(D(x))] + \mathbb{E}_{z\sim p_z(z)}[\log(1-D(G(z)))]$$

PassGAN

Nel 2019 è stata proposta una nuova tecnica di password guessing, basata proprio sulle reti neurali GAN. Questa tecnica, battezzata dagli ideatori Briland Hitaj, Paolo Gasti, Giuseppe Ateniese e Fernando Perez-Cruz con il nome di ***PassGAN***, sfrutta due reti neurali, una per la generazione di stringhe e l'altra per verificare il grado di bontà della stringa generata

Un sistema di Password Guessing basato su Deep Learning

Prendendo ispirazione da tale articolo, utilizzando il linguaggio di programmazione Python abbiamo realizzato una rete GAN originale e l'abbiamo inserita all'interno di un sistema di password guessing

In particolare abbiamo implementato un sistema composto dai seguenti elementi:

- una ***rete discriminativa*** *D* in grado di riconoscere se una password ricevuta in input è reale o generata

Un sistema di Password Guessing basato su Deep Learning

- una ***rete generativa*** *G* in grado di generare stringhe di caratteri assimilabili a delle password
- un sistema GAN, composto dalle reti *D* e *G*, con l'obiettivo di addestrare la rete *G* a generare stringhe di caratteri che possano essere riconducibili a «password verosimili»
- un sistema di password guessing che utilizza la rete *G* per indovinare le password inserite dagli utenti in un determinato sistema con l'obiettivo di riuscire a violarlo

Grazie per la vostra attenzione!