Università' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia
Lezione 01

Authors: Angelo Silvestri, Marcello Politi, Samir Salman

Ottobre 2019

1 Introduzione

Bob e Alice sono in una rete e si scambiano messaggi. La rete è in chiaro e chiunque può leggere i messaggi che passano attraverso essa, soprattutto Eve che ha un debole per Alice. Come fanno Bob e Alice a scambiarsi messaggi interpretabili solamente da loro due?

1.1 Crittografia e Cifratura

La **crittografa o cifratura** è una tecnica per tenere segrete le informazioni, limitandone l'accesso solo alle destinazioni autorizzate. La differenza tra crittografia e cifratura risiede nell'ambito di utilizzo; crittografa viene utilizzato in abito militare mentre cifratura in ambito civile.

Ogni sistema di cifratura ha due parti essenziali:

- un algoritmo
- una chiave

Il processo di *cifratura* non è altro che l'insieme delle operazioni che portano alla trasformazione di un messaggio in chiaro in un crittogramma, ovvero un insieme di simboli illeggibili, attraverso l'utilizzo di un algoritmo e di una chiave. Tale processo è reversibile e quindi permette di ricostruire il messaggio precedentemente cifrato avendo a disposizione l'algoritmo e la chiave.

1.2 Crittografia simmetrica o a chiave privata

Con **crittografia simmetrica, o a chiave privata**, si intende una tecnica di cifratura che consiste nell' utilizzo dello stesso valore di chiave per cifrare e decifrare il messaggio, ragion per cui mittente e destinatario devono esserne in possesso. Il mittente cifra il messaggio M con la chiave k usando un algoritmo S di cifratura simmetrica.

$$(P; k) = C$$

Il destinatario riceve il messaggio C cifrato e può decifrarlo applicando l'algoritmo D di decifratura con la chiave k in suo possesso che ha lo stesso valore della chiave che ha usato il mittente per cifrare.

$$D(C; k) = P$$

1.3 Numeri casuali e pseudo-casuali

Una variabile casuale (detta anche variabile aleatoria o variabile stocastica) è una variabile che può assumere valori diversi in dipendenza da qualche fenomeno aleatorio . Per **numero casuale** si intende un singolo risultato di una variabile aleatoria. Ogni sequenza di numeri casuali deve essere uniforme e indipendente ed il processo processo di generazione deve garantire che ogni elemento di un insieme abbia la stessa probabilità di essere generato. Una routine di generazione di numeri casuali deve poter produrre una sequenza con, approssimativamente, le stesse proprietà statistiche di una sequenza di numeri generata da un processo casuale ad una velocità relativemente alta attraverso un algoritmo deterministico; tale processo induce ad affermare che il numero generato è un numero **pseudo-casuale**.

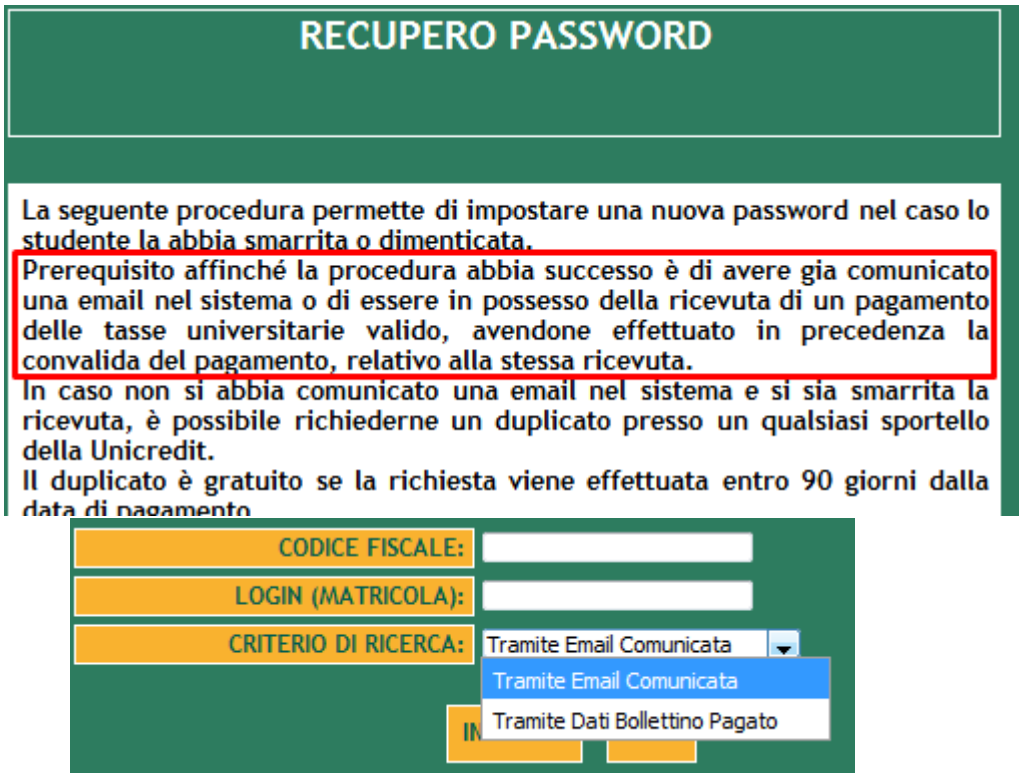
1.4 Conferma identità digitale

La **conferma dell'identità digitale** è un problema ancora non risolto; non esiste ancora un metodo semplice ed effciente che permetta di confermare l'identità di un utente, in più non si ha la certezza assoluta che la persona dietro un account sia effettivamente l'identità digitale da confermare. Ad esempio: immaginiamo che si voglia confermare l'identità di un utente che intende cambiare password su un sito di acquisti online. Il sito invia un codice per SMS con un pin che permette la modifica della password. Nessuno ci assicura che la persona con il telefono su cui è arrivato il messaggio sia effettivamente il proprietario dell'account. Descriviamo di seguito due casi di esempio.

1.4.1 Il caso Delphi

La procedura recupero password del delphi propone due modi recuperare la password

1. tramite email
2. tramite ricevuta di pagamento



Analizziamo il modo 1): La procedura chiede come input l'inserimento del codice fiscale e matricola e il metodo di recupero, nel nostro caso "tramite mail"; il sistema invia la nuova passaword, in chiaro, alla casella email registrata.

Possono verificarsi almeno 2 casi problematici

1. conoscendo matricola e codice fiscale di uno studente si può richiedere il reset password.

2. La password viene inviata in chiaro, quindi qualcuno che monitora la rete potrebbe intercettarla e farne un uso scorretto es: prenotare esami, vedere gli esami verbalizzati, prendere possesso dell'email universitaria impersonifcando quella persona.

1.4.2 Il caso Tripadwisor

Nel regolamento di TripAdvisor ci sono normative su azioni fraudolente. Supponiamo quindi di aver accesso all'account di un proprietario di un locale, con il quale si scrivono recensioni sul proprio locale, si può chiedere agli ospiti di rimuovere le recensioni negative proponendo uno sconto ed altre operazioni fraudolente che sono contro il regolamento del sito. In questo modo TripAdvisor potrà intraprendere provvedimenti per l'account del proprietario anche penali.