Sicurezza Documentale a.a. 2017/2018

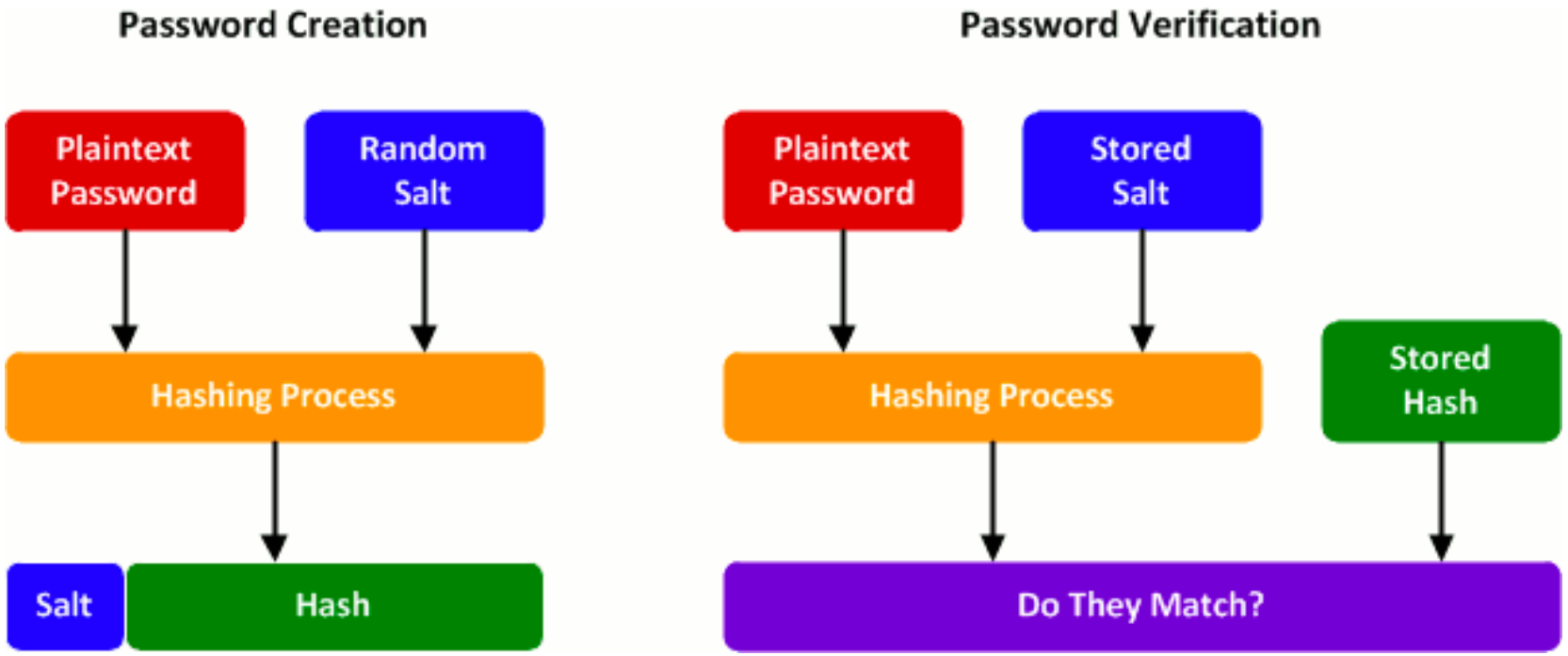
DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

Sistemi di Autenticazione

Hashed password

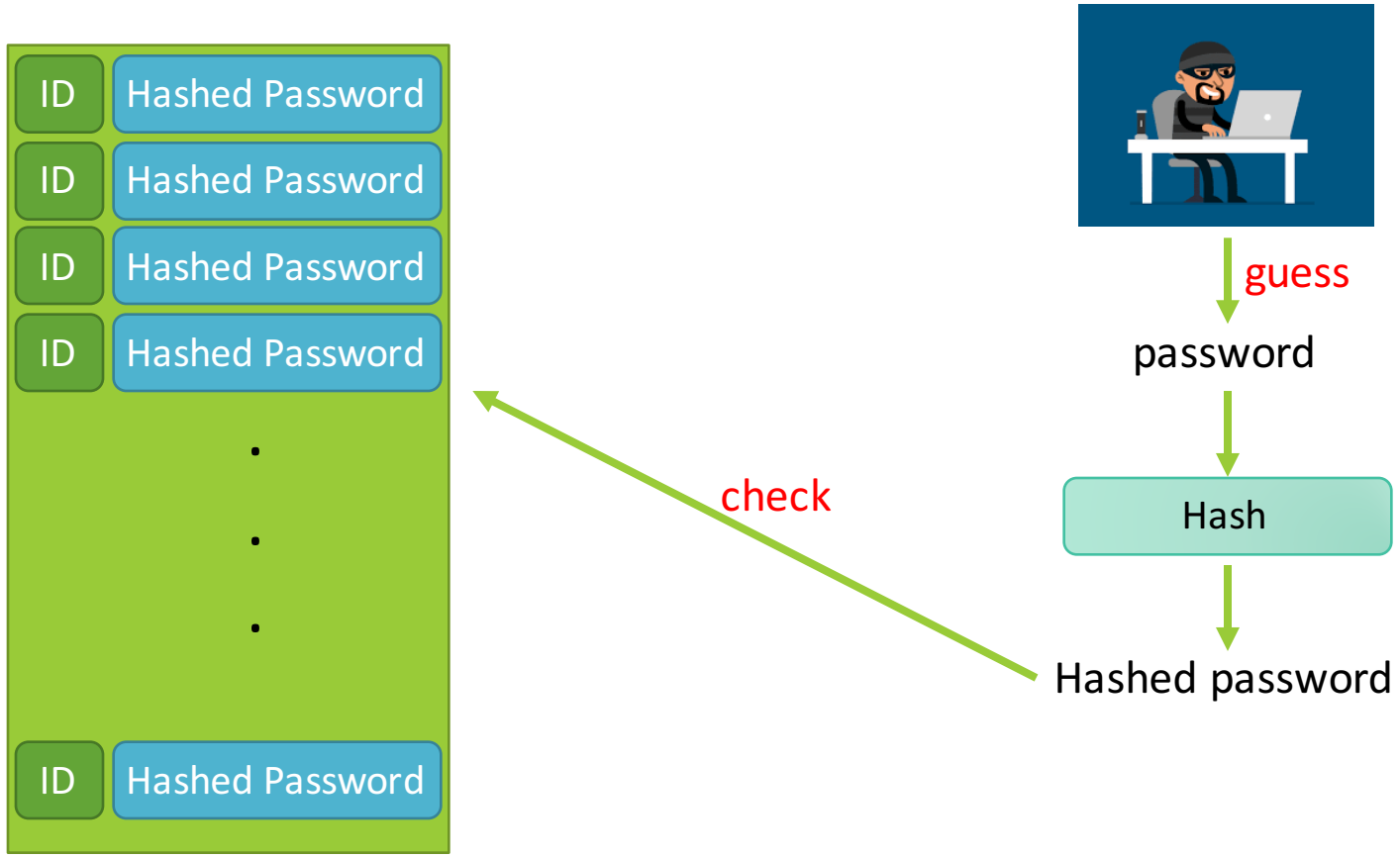
- Il salt è un numero random o pseudorandom che viene combinato con la password



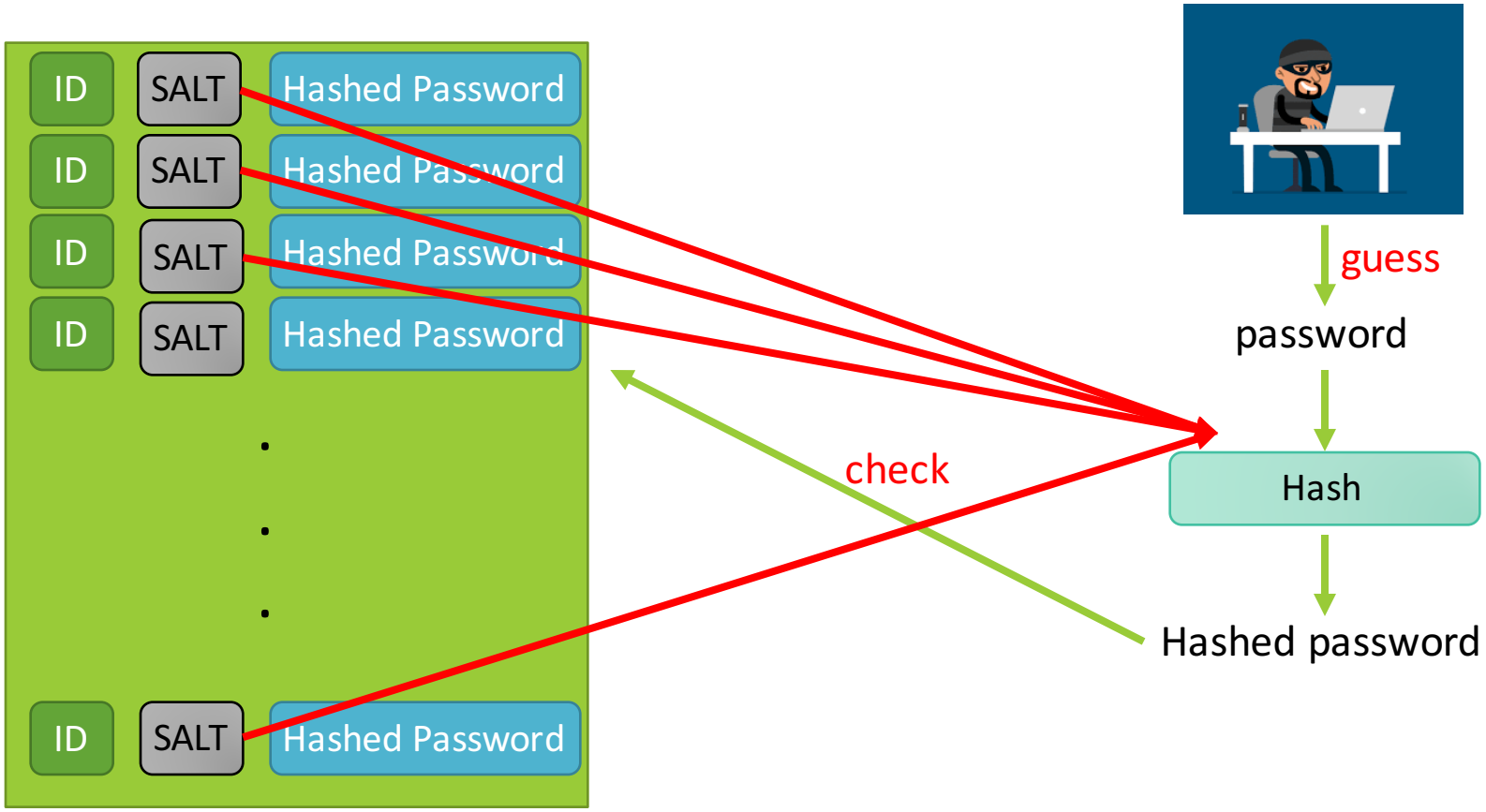
Hashed password

- Il salt è utile in tre modi:
  - Fa in modo che password duplicate non siano riconoscibili nel dizionario delle password
  - Incrementa la difficolta di attaccare il dizionario offline: le password vengono allungate
    - Se si usa un salt di *b* bit il numero di possibili passwords è incrementato di un fattore 2^b
  - Diventa quasi impossibile capire se un utente che ha password su due o più sistemi ha utilizzato la stessa password

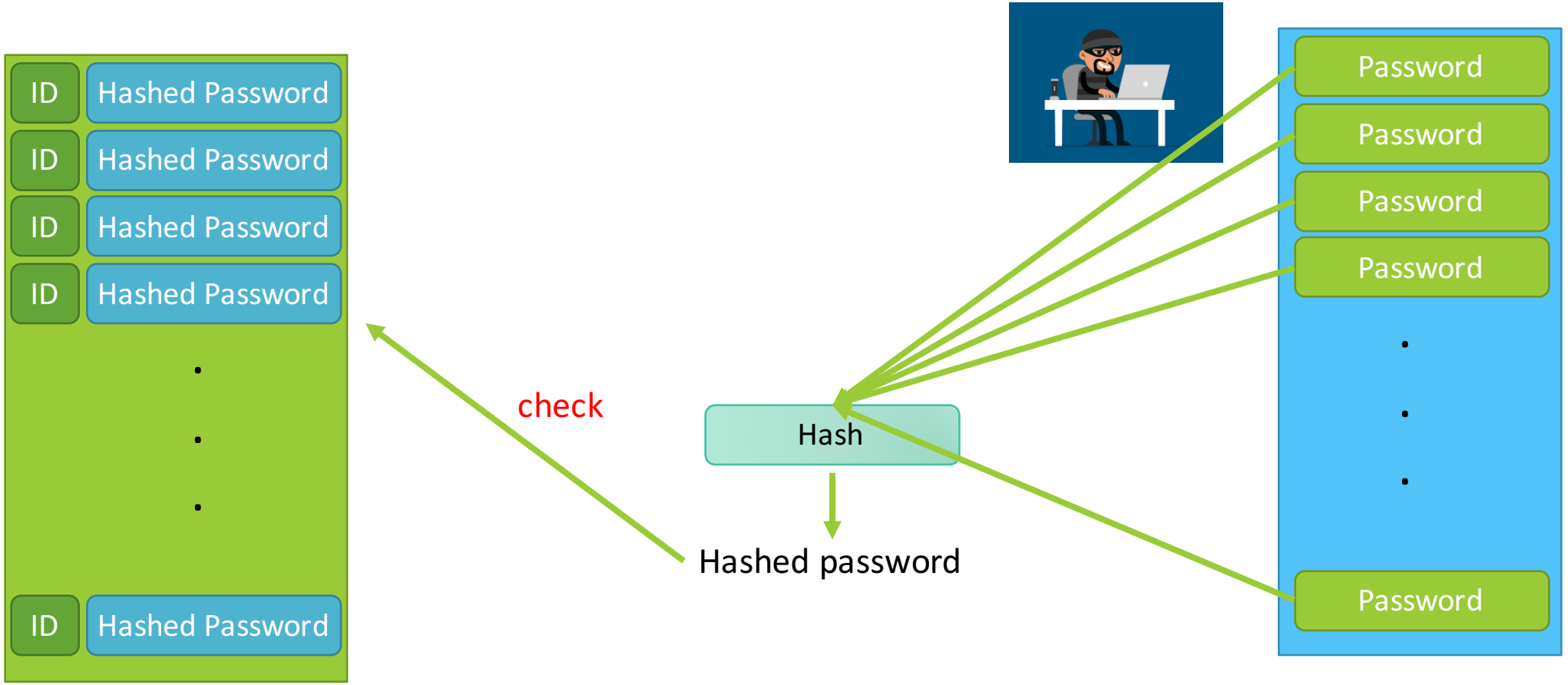
Hashed password



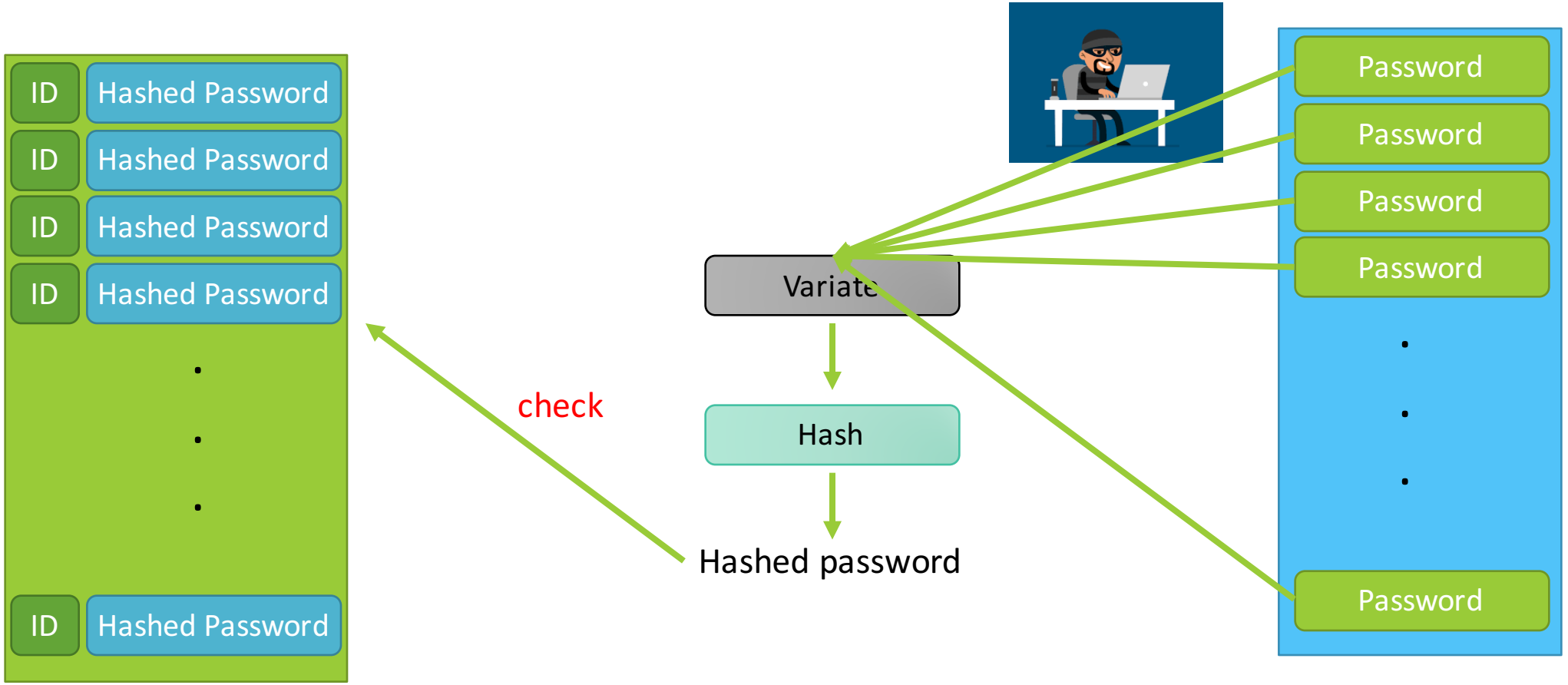
Hashed password



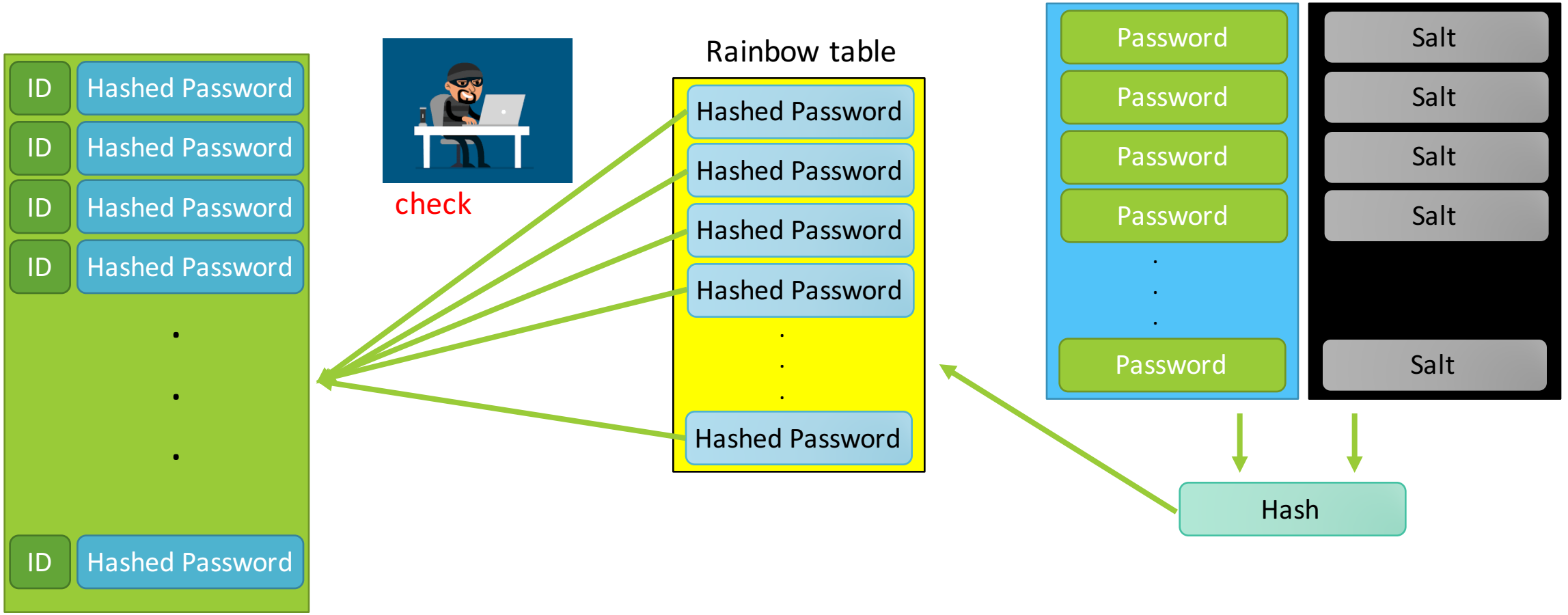
Password cracking approaches



Password cracking approaches



Password cracking approaches



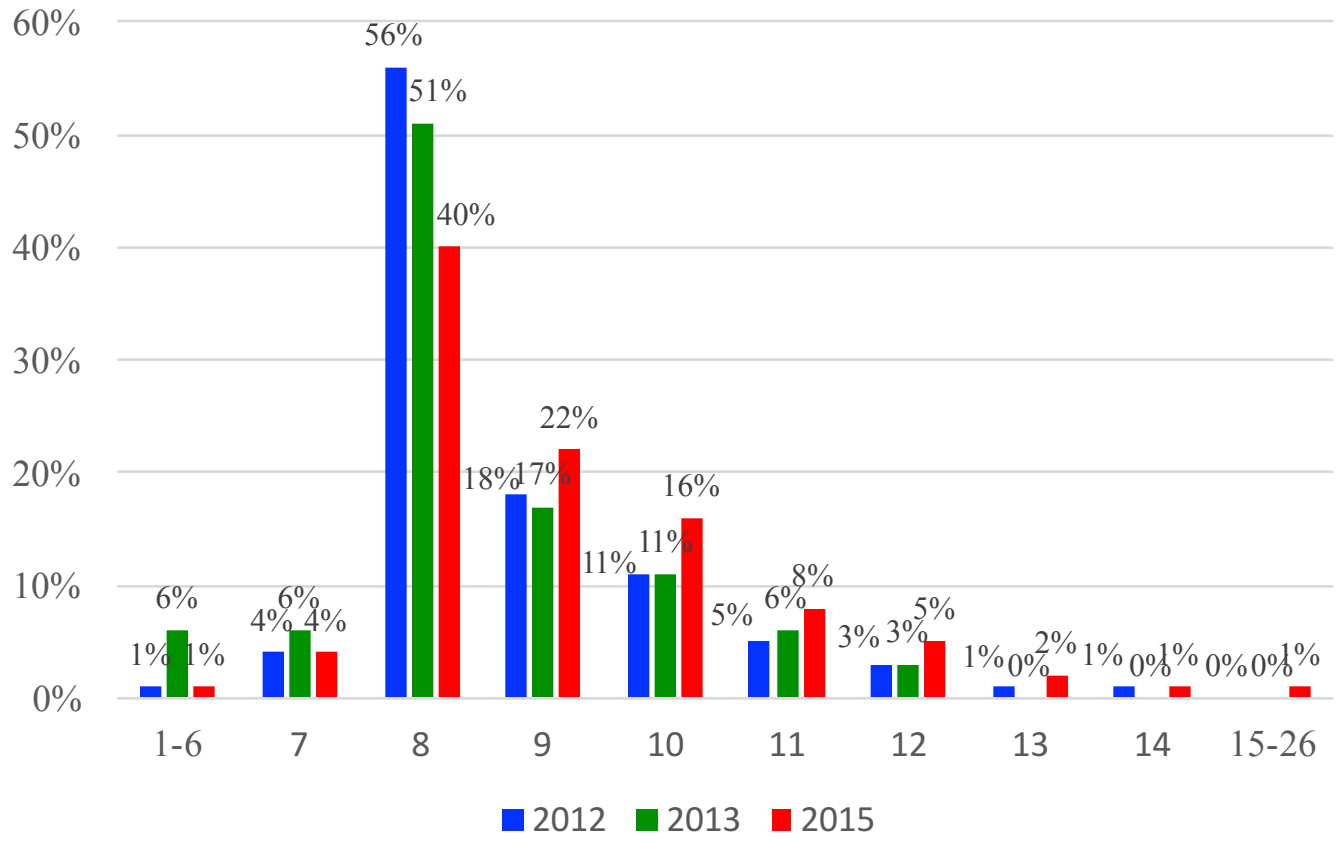
Password cracking approaches

- Nel 2003 è stato dimostrato che utilizzando una rainbow table di 1.4 GB era possibile crackare il 99,9% delle password di Windows in 13.8 secondi
  - Le rainbow table diventano inefficaci scegliendo valori di salt sufficientemente lunghi e password sufficientemente lunghe

User Password Choices

- I password crackers confidano nel fatto che alcune persone scelgono password che sono facilmente indovinabili.
- Molti utenti se sono lasciati liberi di scegliere la propria password ne scelgono una molto corta.

Password length statistics



Password cracking approaches

- La lunghezza delle password scelte è solo una parte del problema
- Se i sistemi permettono agli utenti di scegliere liberamente le proprie password generalemnte essi scelgono password semplici da ricordare
  - Il loro nome, indrizzo, date, parole comuni

Password cracking approaches

- Negli anni 90 è stato fatto uno studio in cui sono stati raccolte circa 14000 password criptate da alcuni sistemi unix.
- L'approccio usato è stato di provare:
  1. Informazioni personali rilevanti per gli utenti, ad esempio il nome o le iniziali. Di queste informazioni sono state considerate inoltre 130 permutazioni
  2. 60000 parole prese da dizionari
  3. Varie permutazioni delle parole del passo 2 – ad esempio mettendo la prima lettera in maiuscolo o scambiando le o con 0 – altre 1M di parole
  4. Altre permutazioni che si basano sulla sostituzione di lettere maiuscole alle lettere minuscole nelle parole non considerate al passo 3 – altre 2M di parole
- Il 25% delle password sono state indovinate in meno di 1 ora

Controllo degli accesi al file delle password

- Un primo meccanismo di protezione contro gli attacchi alle password degli utenti è prevedere un meccanismo di controllo degli accessi al file delle password
  - Garantire l'accesso al file delle password solo ad utenti privilegiati
  - Il cracker non può leggere il file delle password senza conoscere giá la password di un utente privilegiato
- Un secondo meccanismo è di mantenere l'elenco degli ID degli utenti e il dizionario delle password separati
  - Shadow password file
- I sistemi rimangono comunque attaccabili se il cracker sfrutta qualche vulnerabilitá

Strategie di selezione delle password

- Meccanismi che guidano gli utenti nella scelta di una password sicura
  - Il fine è di eliminare le password facilmente indivinabili
  - Consentire la scelta di password che l'utente può facilmente memorizzare
- Quattro strategie:
  - Educazione dell'utente
  - Password generate dal computer
  - Controllo reattivo delle password
  - Controllo proattivo delle password

Educazione dell'utente

- Istruire gli utenti sull'importanza di scegliere password sicure
- Di difficile successo
  - Troppi utenti
  - Utenti che cambiano molto spesso
  - Gli utenti possono semplicemente ignorare le linee guida
  - Potrebbero non saper giudicare se una password è sicura o meno

Educazione dell'utente

- Gli utenti potrebbero pensare che utilizzare una parola scritta al contrario o con la prima lettera maiuscola sia sufficiente ma non è cosi.
- Una buona prassi ad esempio è di consigliare agli utenti di scegliere le prime lettere delle parole di una frase di senso compiuto (non banale)
  - Il nome del mio cane è Polly → IndmceP
  - Mia sorella Simona ha 38 anni → MsSh38a

Password generate automaticamente

- Quasi impossibili da indovinare
- ….
- Quasi impossibili da ricordare!
  - Gli utenti possono essere tentati di scriverle da qualche parte per ricordarle
- Ci sono alcune inizative di generatori di password che riescono a generare password che creano una sequenza di sillabe pronunciabili
  - http://www.generate-password.com/?language=it

Controllo reattivo delle password

- Il sistema periodicamente fa girare la sua routine per cercare password non sicure, le cancella e notifica l'utente

- Costoso dal punto di vista delle risorse e del tempo
- Ogni password che non viene rilevata come non sicura rimane vulnerabile

Controllo proattivo delle password

- L’utente può selezionare la propria password, ma al momento della selezione il sistema controlla che sia abbastanza sicura.
- Esistono diversi approcci per il controllo proattivo delle password:
  - Rule enforcement
  - Password Cracker
  - Markov Model

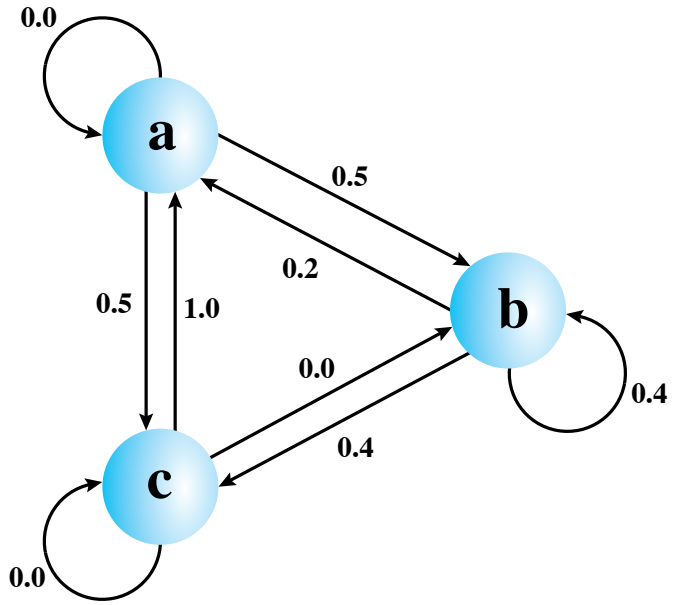
Controllo proattivo delle password – Rule Enforcement

- Il sistema da delle regole per la scelta delle password:
  - Ad esempio:
    - Almeno 8 caratteri
    - Almeno una lettera maiuscola, una moniscola, un numero e un simbolo di punteggiatura
- Questo sistema fornisce ai cracker una schema per selezionare le password da evitare quando tentano di violare il sistema

Controllo proattivo delle password – Password Cracker

- Costruire un dizionario delle possibili password non sicure
- Quando un utente sceglie una password confontarla con il dizionario ed eventualemnte rigettarla
- Problemi:
  - Spazio per memorizzare il dizionario
  - Tempo per cercare le password nel dizionario

Controllo proattivo delle password – Markov Model



- Password ottenibile con elevata probabilitá da questo sistema: abbcacaba
- Password non ottenibile con elevata probabilitá da questo sistema: aacccbaaa
- Se un utente seleziona una password generabile con elevata probabilitá essa viene rifiutata