Rainbow tables

M0170 Kryptografie

Jak jsou uložená hesla v počítači?

- Plaintext – porovnává se přímo zadané heslo s heslem uloženým

  `uzivatel:tajneheslo`

- Hash – porovnává se hash zadaného hesla s hashem hesla uloženého

  `uzivatel:c2750a7d522eb4df4e842980ed3f3e78`

Odcizení databáze hesel

- Stává se maximálně jednou za deset let...
- V případě uložení hesel v plaintextu...
- V případě uložení hashů
  - Všichni používáme hesla délky alespoň 8 znaků
  - Kombinace velkých/malých písmen, čísel a speciálních znaků
  - Tzn. nic se neděje?

Crackování hashů hesel

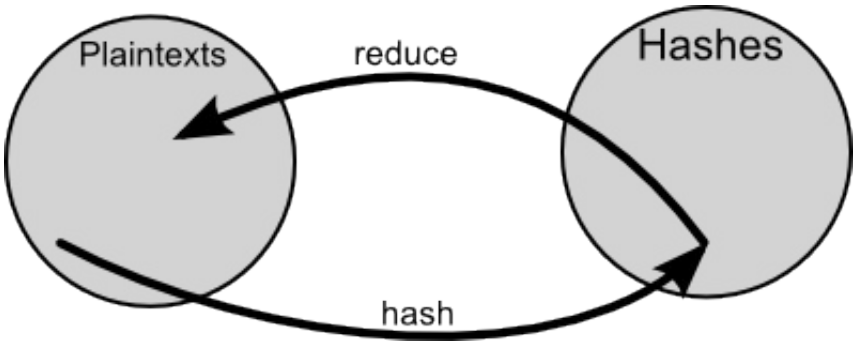
- Použití kryptoanalýzy
- Využití chyb v návrhu
  - LM hash – rozdělení po sedmi znacích a upper case
- Použití slovníkových útoků – proč složitě znovuobjevovat kolo..
- Použití brute force metody
  - Rozpor požadavku na rychlost hashovací funkce a zároveň na její pomalost (útočník vs. správce) „stretching“
  - Využití GPU, ale stále zdlouhavé a musíme vždy počítat znovu.. jde to lépe?

Předpočítání hashů

- Nejdříve si brute-force metodou, nebo i slovníkem předpočítáme hashe a setříděné si je uložíme
- Hledání hashů procházením v setříděných datech je snazší a rychlejší
- Dobré.. ale paměťově dost náročné.. existuje kompromis?

Rainbow tables

- Redukční funkce je zobrazení z množiny hashů do množiny plaintextu:
- Plaintext jsou šestimístná čísla:
- MD5 hash čísla 123456: e**10**adc**3949**ba59abbe56e057f20f883e
- Jednoduchá redukční funkce: prvních šest čísel: 103949



Rainbow tables

- Tento plaintext 103949 je opět hashovaný a opět redukovaný atd.. ale v tabulce jsou uloženy pouze startovací plaintexty a koncové hashe. Jeden řádek (chain) reprezentuje miliony hashů. Rainbow tabulka může vypadat následovně:

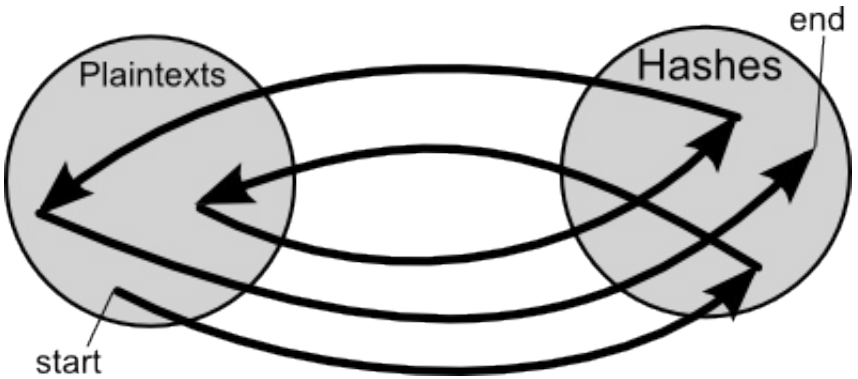
- iaisudhiu -> 4259cc34599c530b1e4a8f225d665802

  oxcvioix -> c744b1716cbf8d4dd0ff4ce31a177151

  9da8dasf -> 3cd696a8571a843cda453a229d741843

  ...

  sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f



Rainbow tables

- Jak se podle hashe hledá plaintext?

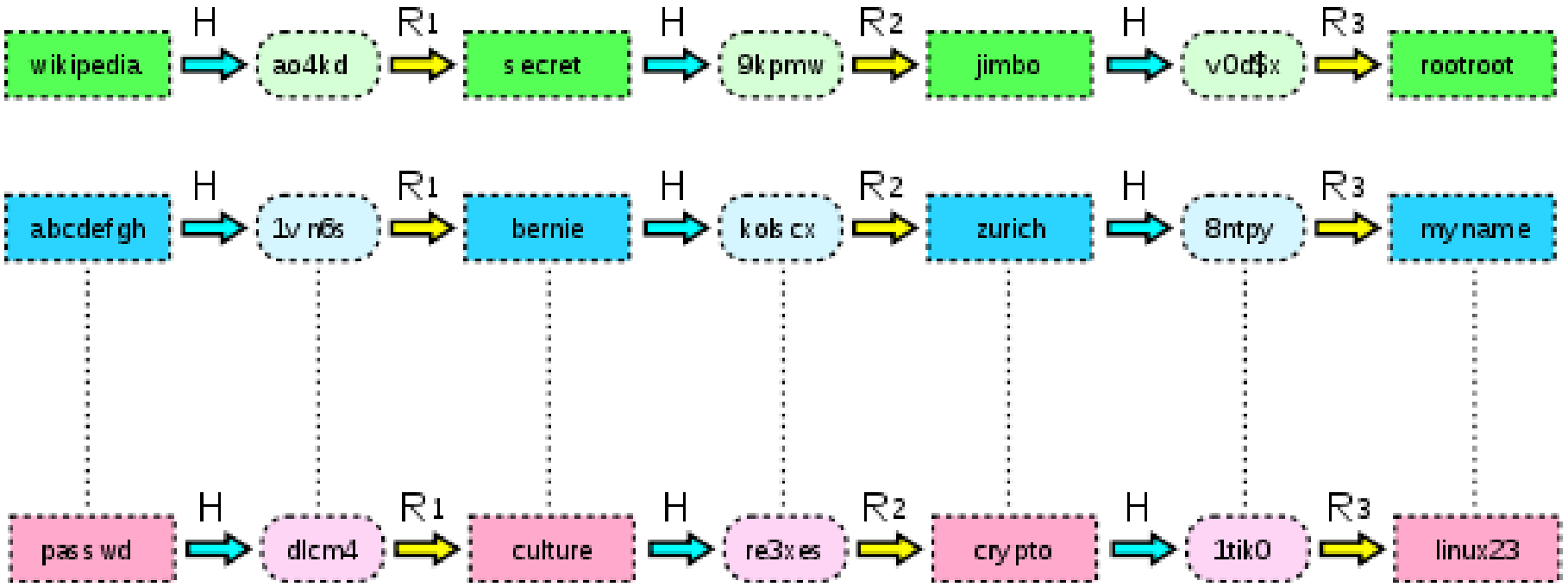
  1. najít hash v cílovém sloupci

  2. pokud tam není, redukovat ho na plaintext a spočítat hash

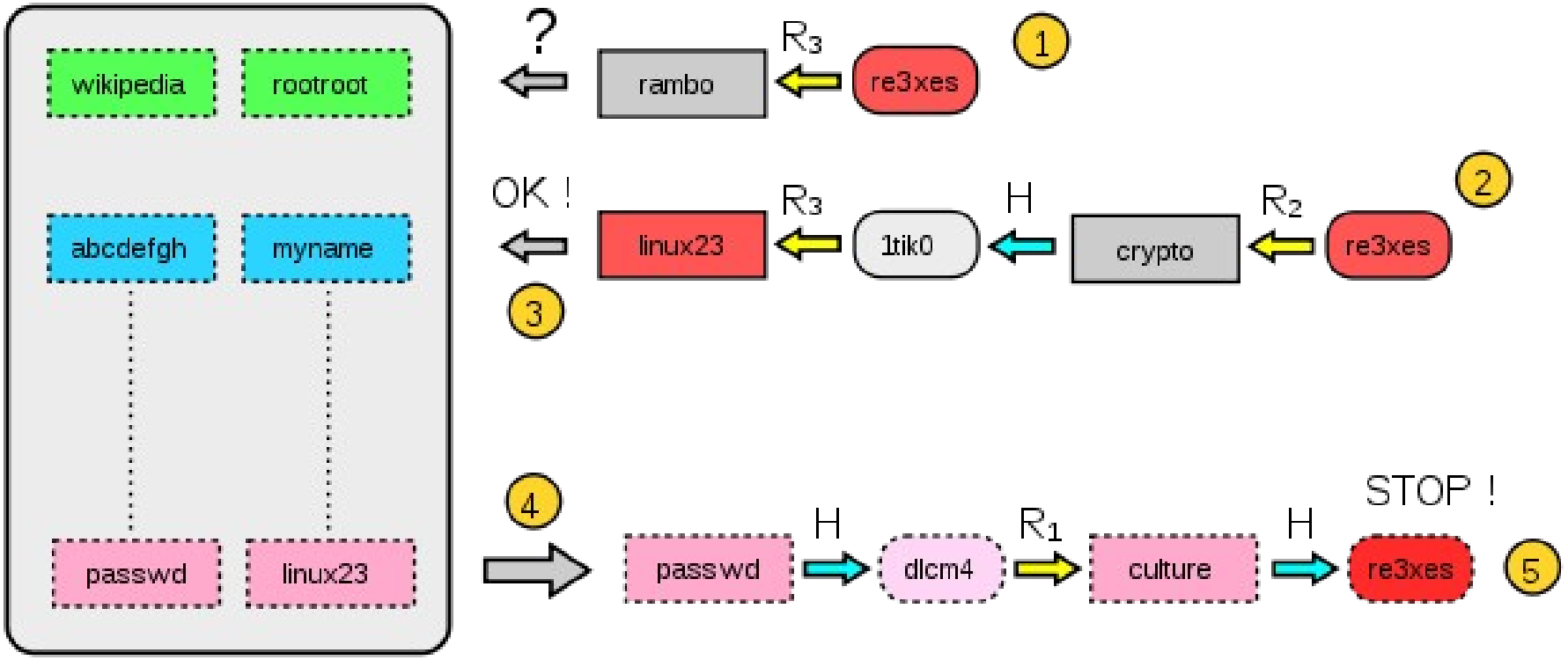
  3. začít od bodu 1.

- Pokud najdeme hash v cílovém sloupci, tento chain může obsahovat plaintextové heslo.

Rainbow tables



Rainbow tables



Rainbow tables

- Proč takové jméno?
  - Redukční funkce pro každý sloupec má jinou barvu, ve výsledku to vypadá jako duha
- Zajímavosti:

  Lze je využít pro rychlejší lámání šifrování WPA-PSK

Rainbow tables

- Obrana? Solit, solit, solit... Prohledávaný prostor se dostatečně zvětší.
- Dobrý byznys, na Internetu se rainbow tables hojně prodávají. Pokud máte nedostatek kapacity, lze si objednat DVD nebo i dodávku celých disků s nahranými tabulkami.

Zdroje

- http://en.wikipedia.org/wiki/Rainbow_table
- http://chargen.matasano.com/chargen/2007/9/7/enc
- http://kestas.kuliukas.com/RainbowTables/
- http://www.renderlab.net/projects/WPA-tables/