CS 465
Computer Security

An Administrator’s Guide to Password Research
Dinei Florencio, Cormac Herley, Paul C. van Oorschot
Usenix LISA | November 2014

Daniel Zappala
Fall 2018

Motivation

- examines the research literature on passwords and identifies what works, what does not work, and what remains unknown
- offers practical advice for system administrators

Categorizing Impact of Password Breaches on Various Accounts

- *don't care*: no impact
  - one-time email, nuisance accounts for free articles
  - don't bother users about security of these passwords
- *low consequence*: minimal impact or easily repaired
  - social networks (infrequent users), discussion groups (infrequent users), online newspapers, accounts not storing credit cards
  - users may just rely on password reset

Categorizing Impact of Password Breaches on Various Accounts

- *medium consequence*: limited loss (e.g. $50 cap on credit card loss)
  - secondary email account, online shopping sites, social network accounts (casual users), human resource sites
- user effort resisting online attacks is well spent

Categorizing Impact of Password Breaches on Various Accounts

- *high consequence*: critical accounts related to employment, finance, or important documents
  - primary or professional email accounts, social networks (heavy users and celebrities), online banking, SSH and VPN access, corporate databases
  - spend user effort securing passwords, provide two-factor authentication
- *ultra-sensitive*: major, life-altering, irreversible damage
  - multi-million dollar banking transactions, authorization to launch military weapons, encryption of national secrets
  - use something better than a password

Password Strength

- examined leaked datasets from Rockyou, Gawker, Tianya, eHarmony, LinkedIn, Evernote, Adobe, Cupid Media

- only Gawker and Evernote were hashed and salted

- ideally, users choose passwords randomly

  - in practice, users choose common words (password, monkey, princess), proper nouns (julie, snoopy), and predictable sequences (abcdefg, asdfgh, 123456)

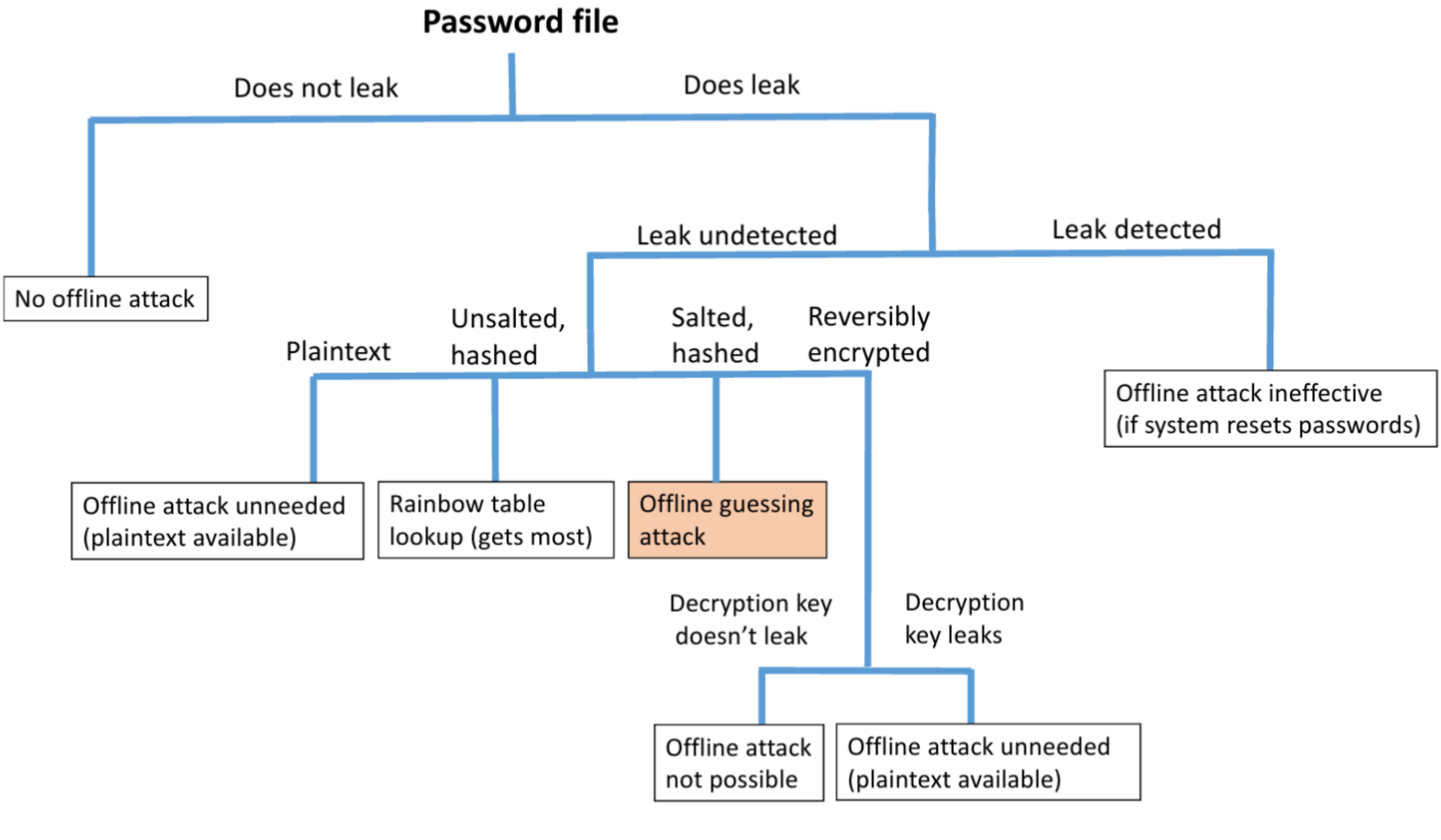
Password Strength

- metrics such as entropy are misleading
  - entropy = L*log_2(C), L = length, C = size of alphabet
    - P@sswOrd is far more common than gunpyo, but has higher entropy
- *guessing resistance*: estimate of how many guesses needed to crack password

Online vs Offline Guessing

- attacks on client don't involve guessing: malware, phishing, sniffing
- attacks on server's public facing web site: online guessing
- attacks on server's back end web site: offline guessing
  - gain access to system
  - be undetected (sysadmin can otherwise force system-wide password resets)
  - test passwords against hashes and salts

Offline Attacks



How Many Guesses?

- determines how difficult a password must be to guess

- attackers can't make as many online guesses: need to be indistinguishable from ordinary traffic

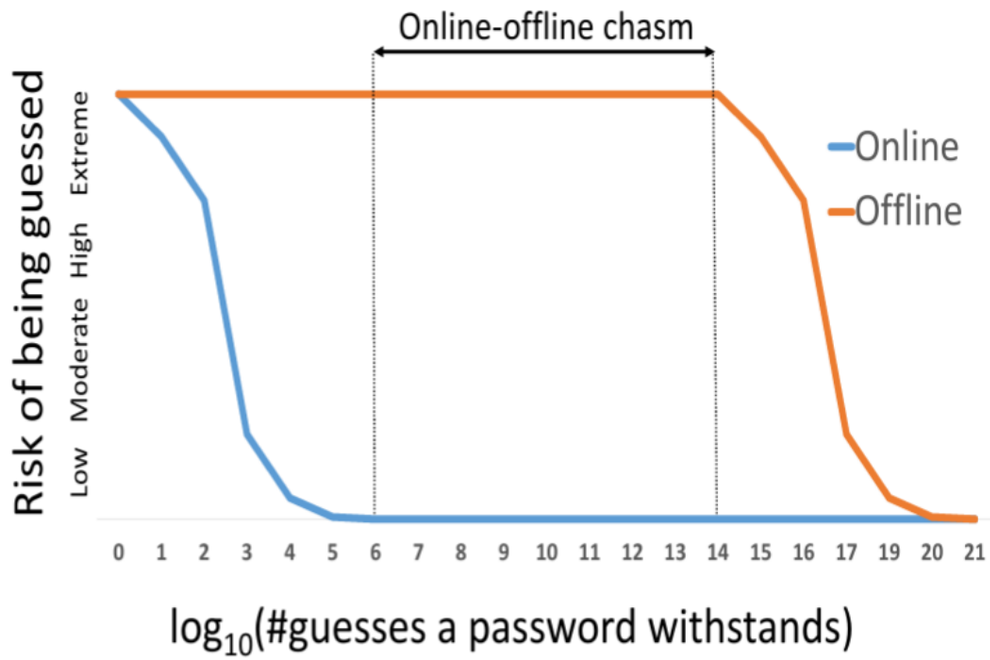


Figure 2: Conceptualized risk from online and offline guessing as a function of the number of guesses a password will withstand over a 4-month campaign. In the region from 10^6 to about 10^{14}, improved guessing-resistance has little effect on outcome (online or offline).

Policies

- composition and length
  - e.g. at least 8 characters, some uppercase and numbers
  - users respond with minimally compliant choices
  - overall, policies help to protect against online attacks, but not offline ones
  - users dislike them strongly
  - authors feel there are better alternatives

Policies

- blacklists: common or leaked passwords
  - protects users most at risk
  - can ban most popular passwords used at your site
- expiration
  - only helpful for offline attacks
  - users choose highly predictable variants

Policies

- rate-limiting and lockout
  - lockout can be abused for denial of service attack
  - rate-limiting effective against online attacks
  - can require CAPTCHA for new IPs