CERIAS

The Center for Education and Research in Information Assurance and Security

Not All Equal: Stronger Password Protection via Differentiated Hashing Costs

Jeremiah Blocki, Wenjie Bai

Department of Computer Science, Purdue University

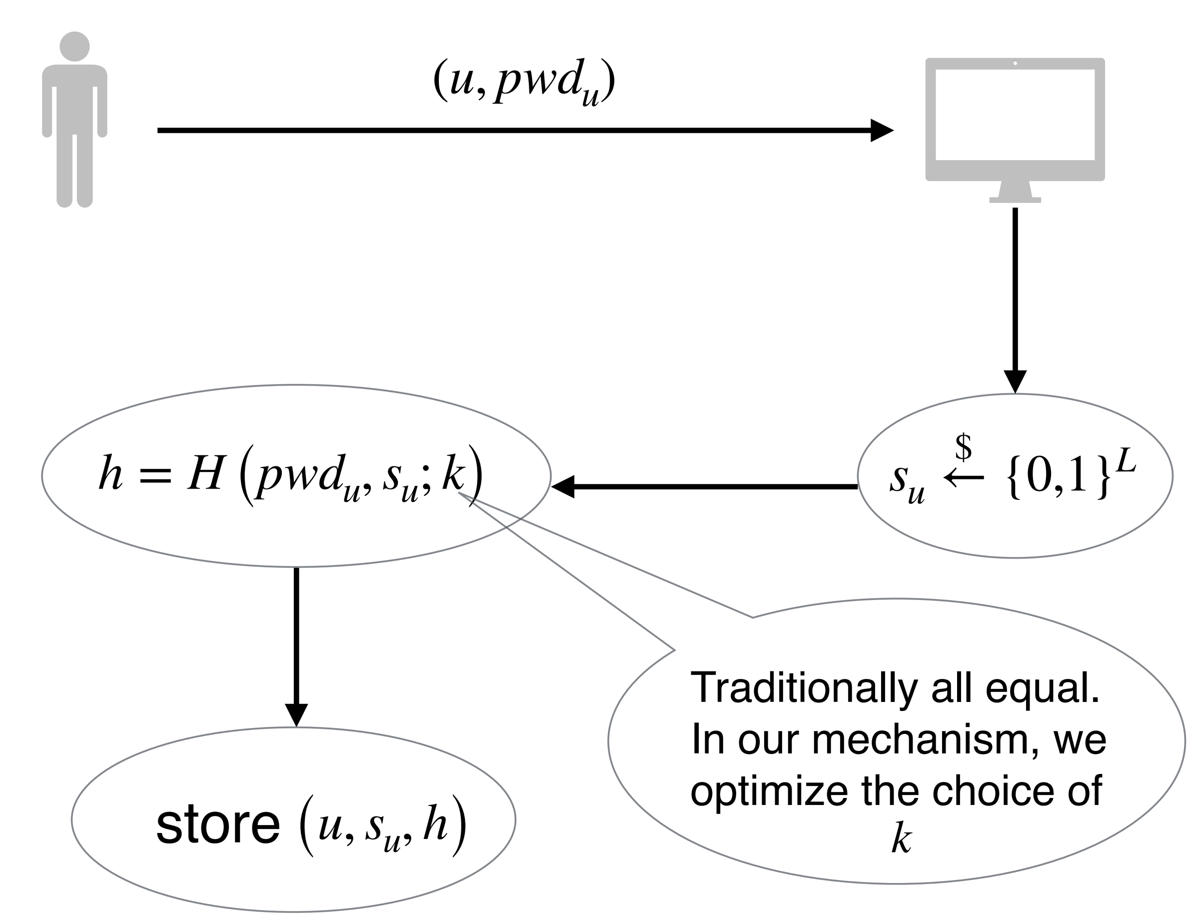
Introduction

- Severity of offline attack;
- Memory hard functions (MHFs) can be used to build ASIC resistant password hashing algorithms;
- A fundamental trade-off in the design of good password hashing algorithms:
  - **should be sufficiently expensive** to compute,
  - **cannot be too expensive** to compute.
- Rational Attacker keeps guessing until marginal guessing costs exceed marginal rewards.
- Some passwords are so weak that protecting them is infeasible. A rational attacker will always check these passwords.

Key Insight

- A resource-constrained authentication server **should not protect all passwords equally.**
- Our mechanism does *not overprotect weak passwords* that are destined to be cracked, *nor passwords that are strong enough* to disinterest a rational offline attacker.

Password Creation



Differentiated Hashing Cost Mechanism

1. First partitions all passwords into mutually exclusive τ groups $|G_i|$ with $i \in \{1, \cdots, \tau\}$
2. For each of the passwords $|G_i|$ we assign the same hash cost parameter k_i

An Economic Model

- Attacker Strategy (π, B): Check B top password in π list and then quit.
- Rational Attacker: Plays utility maximizing strategy (GAIN-COST).

$$U_{ADV}\left(v, \vec{k}, (\pi, B)\right) = v \cdot \lambda(\pi, B) - \sum_{i=1}^{B} k(pwd_{\pi(i)}) \cdot \left(1 - \lambda(\pi, i-1)\right).$$

- Defender Action: Select cost parameters $\vec{k}$
  - subject to workload constraints
  - goal: Minimize attacker success rate $\lambda(\pi, B)$

Formal Stackelberg Game Model

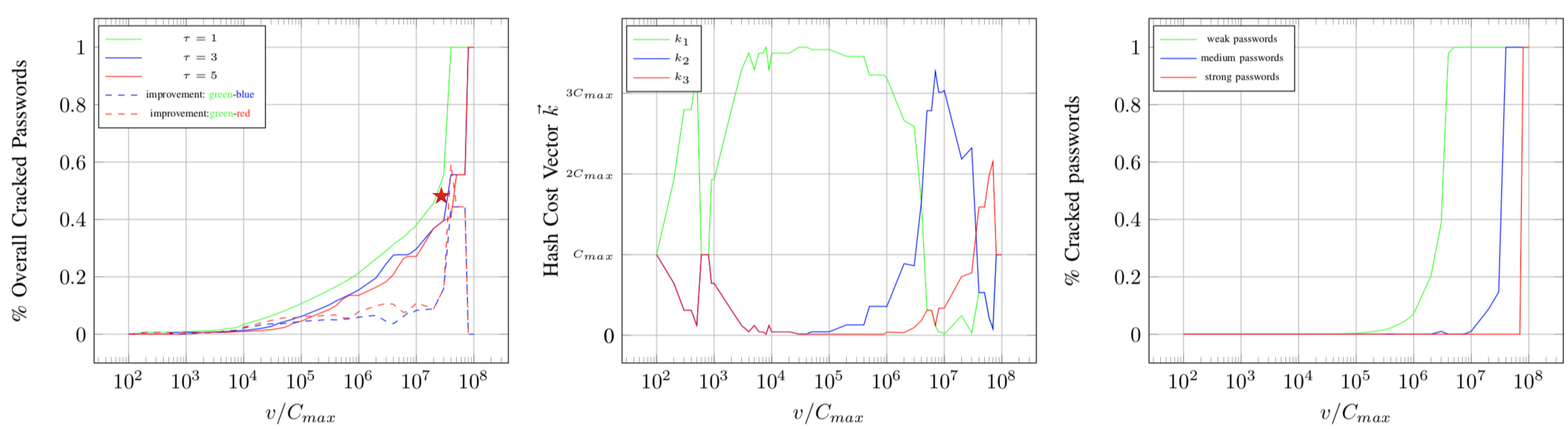
In stage I, the authentication server commits hash cost vector $\vec{k}$ for all groups of passwords;
In stage II, the adversary yields the optimal strategy (π, B) for cracking a random user's password.

$$\begin{cases} U_{SRV}(\vec{k}^*, v) \geq U_{SRV}(\vec{k}, v), & \forall \vec{k} \in \mathcal{F}_{C_{max}}, \\ U_{ADV}\left(v, \vec{k}^*, (\pi^*, B^*)\right) \geq U_{ADV}\left(v, \vec{k}^*, (\pi, B)\right), & \forall (\pi, B) \end{cases}$$

Conclusions

- We present a Stackleberg game model to capture the essentials of the interaction between leader and follower.
- We design highly efficient algorithms to provably compute equilibrium strategy profile.
- We analyze the performance of our differentiated cost password hashing algorithm using empirical password data.
- The percentage of passwords that would be cracked by a rational attacker is reduced by up to 44%.

Emperical Analysis



(a) P_{ADV} for different τ (b) k_i^* against v/C_{max} when $\tau = 3$ (c) Cracked passwords of different strength ($\tau = 3$)

LinkedIn dataset