CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Towards Quantum Large-Scale Password Guessing on Real-World Distributions

CANS, 2021

M. Dürmuth[1], M. Golla[2], P. Markert[1], A. May[1], and **L. Schlieper**[1]
Ruhr University Bochum[1], Max Planck Institute for Security and Privacy[2]

RUHR UNIVERSITÄT BOCHUM RUB

hgi Horst Görtz Institut für IT-Sicherheit

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Introduction

Scenario:

- Passwords are highly biased.
- Increasingly powerful quantum computers emerge.

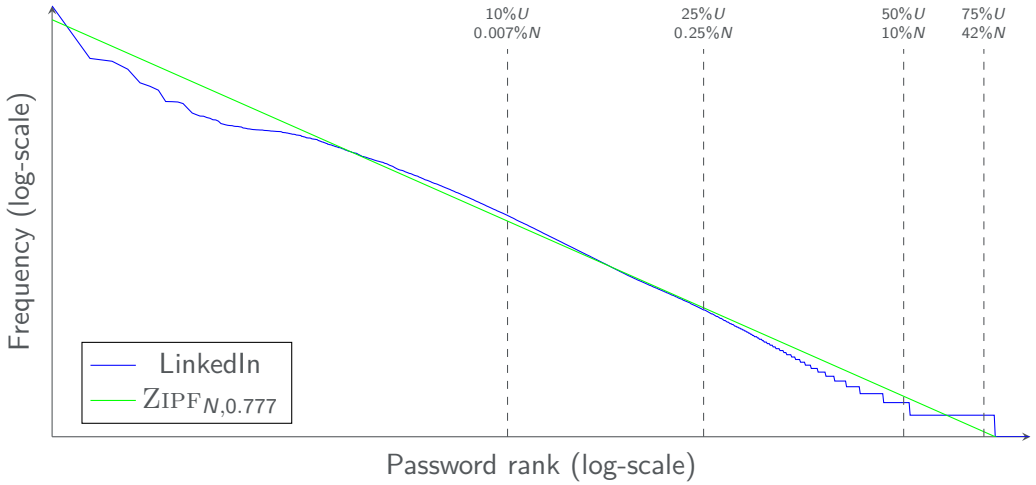
Setting:

- Access to a password leak L with $\ell_u := (\text{user } u, \text{salt } s_u, \text{password-hash } h(s_u, pw_u)) \in L$.
- Knowledge about passwords and distribution $\mathbb{P}_u[u \sim pw_i] = p_i$.
- Access to a powerful quantum computer.

Questions:

- Can we combine the advantage of knowing the distribution of the passwords and the usage of quantum computers?
- How fast can we determine a fraction of all user-password pairs?

Approximation



Results

CASA
Cyber Security in the Age of Large-Scale Adversaries

Setting	Distribution	Average required Hash Evaluations per User				
		10 %	25 %	50 %	75 %	100 %
Classical	Ideal	∼ 2 years	52 600 000	45 100 000	37 500 000	30 000 000
	$\text{ZIPF}_{0.777}$	∼ 10 hours	473 000	3 430 000	8 800 000	11 100 000
	LinkedIn $\mathcal{D}_{\text{Pw}}$	∼ 10 hours	482 000	6 820 000	14 300 000	14 600 000
Quantum	Ideal	∼ 2 hours	7 750	7 750	7 750	7 750
	$\text{ZIPF}_{0.777}$	∼ 3 min	613	1 880	3 710	6 030
	LinkedIn $\mathcal{D}_{\text{Pw}}$	∼ 3 min	622	2 520	4 640	6 380

- Greatest advantage for small numbers.
- Later good passwords turn the tide.

Assuming h required 1 sec classically as well as quantumly.

Conclusion

CASA
Cyber Security in the Age of Large-Scale Adversaries

We have shown that:

- We can combine the advantage of quantum computers and advantage from distribution.
  - We can carry over a square-root of the speed-up.
- Quantum computers can be an even greater potential threat.

Countermeasures:

- Use password managers.
- Increase computation-costs of h.

Thank you for your attention.