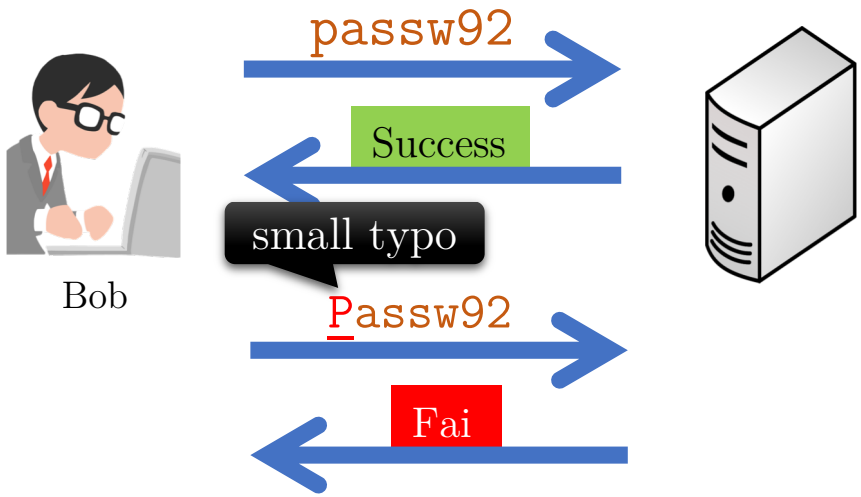
Improving Security by Tolerating Password Typos

Rahul Chatterjee

The talk covers joint work with Devdatta Akhawe (Dropbox), Anish Athalye (MIT), Anusha Chowdhury (Cornell), Ari Juels (Cornell Tech), Yuval Pnueli (Technion), Bijeeta Pal (Cornell Tech), Thomas Ristenpart (Cornell Tech), and Joanne Woodage (Royal Holloway).

Password checking systems and typos



Salted, slow cryptographic hash

How to know if it is a typo?

$H(\texttt{passw92}) \stackrel{?}{=} \texttt{a5idoiaU7p...}$ ✓

$H(\texttt{Passw92}) \stackrel{?}{=} \texttt{a5idoiaU7p...}$ ✗

Apply Caps lock Corrector

$H(\texttt{pASSW92}) \stackrel{?}{=} \texttt{a5idoiaU7p...}$ ✗

$H(\texttt{passw92}) \stackrel{?}{=} \texttt{a5idoiaU7p...}$ ✓

Apply shift Corrector

⋮

S&P '16

pASSWORD tYPOS and How to Correct Them Securely

Rahul Chatterjee*, Anish Athalye†‡, Devdatta Akhawe‡, Ari Juels*, Thomas Ristenpart*
* Cornell Tech, † MIT, ‡ Dropbox

***Abstract*—We provide the first treatment of typo-tolerant password authentication for arbitrary user-selected passwords. Such a system, rather than simply rejecting a login attempt with an incorrect password, tries to correct common typographical** typos made by users. We perform preliminary experiments with Amazon Mechanical Turk (MTurk) in which we task human workers with transcribing passwords drawn from the RockYou password leak.[1] This does not perfectly model pass-

amazon mechanical turk

Top-3 correctors correct 20% of all typos

Typo-tolerant password checking
Allow registered password or typos of it

Study with Dropbox

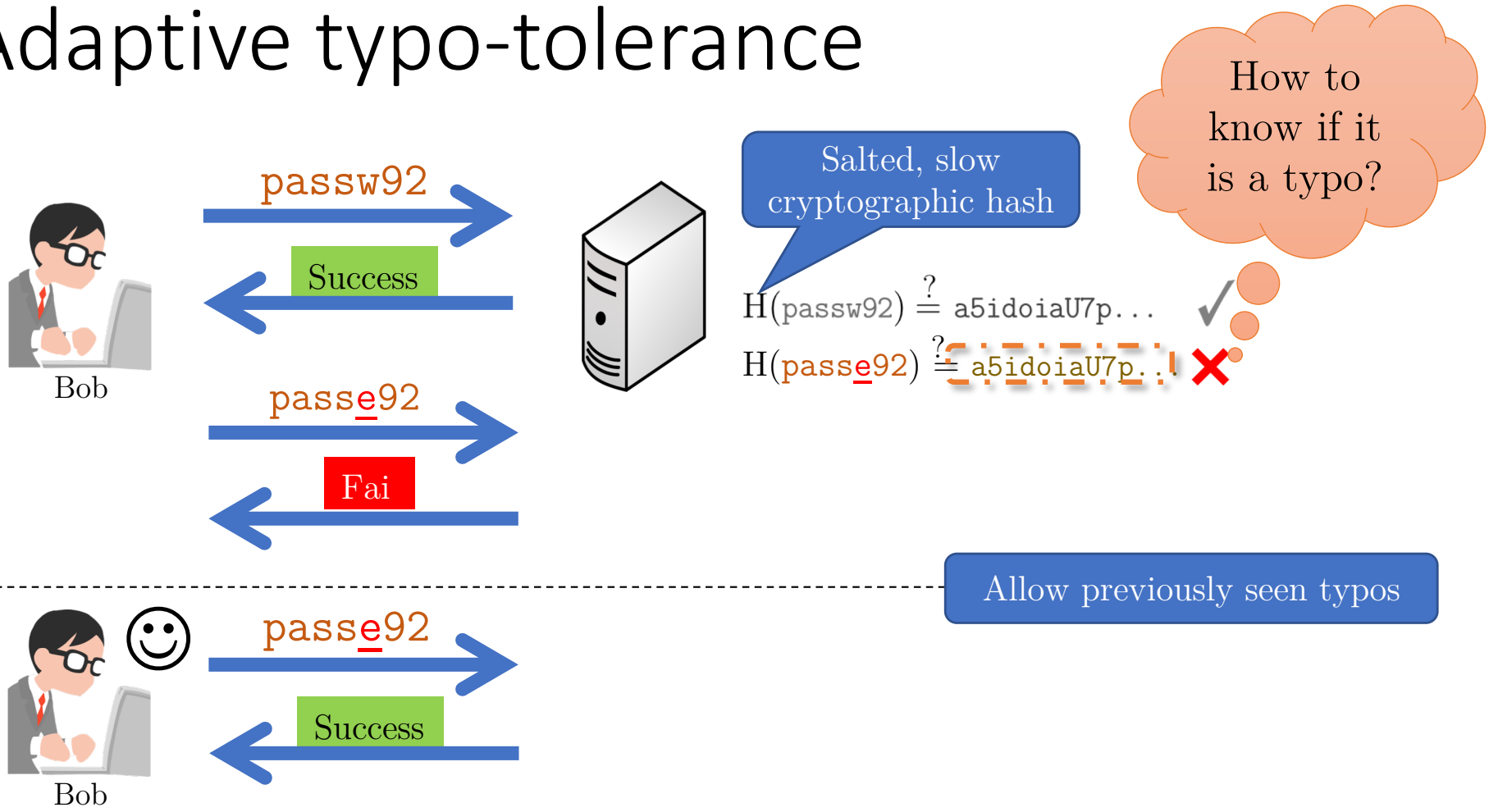
We found, correcting only **three types** of typos will

1. Increase login by 3%
2. Save several person-months of login time

Leaving 80% of typos uncorrected

Top-3 correctors correct 20% of all typos

Adaptive typo-tolerance



CCS '17

The TypTop System: Personalized Typo-Tolerant Password Checking*

Rahul Chatterjee[1,2], Joanne Woodage[3], Yuval Pnueli[4], Anusha Chowdhury[1], Thomas Ristenpart[2]

[1] Cornell University [2] Cornell Tech [3] Royal Holloway, University of London [4] Technion – Israel Institute of Technology

ABSTRACT

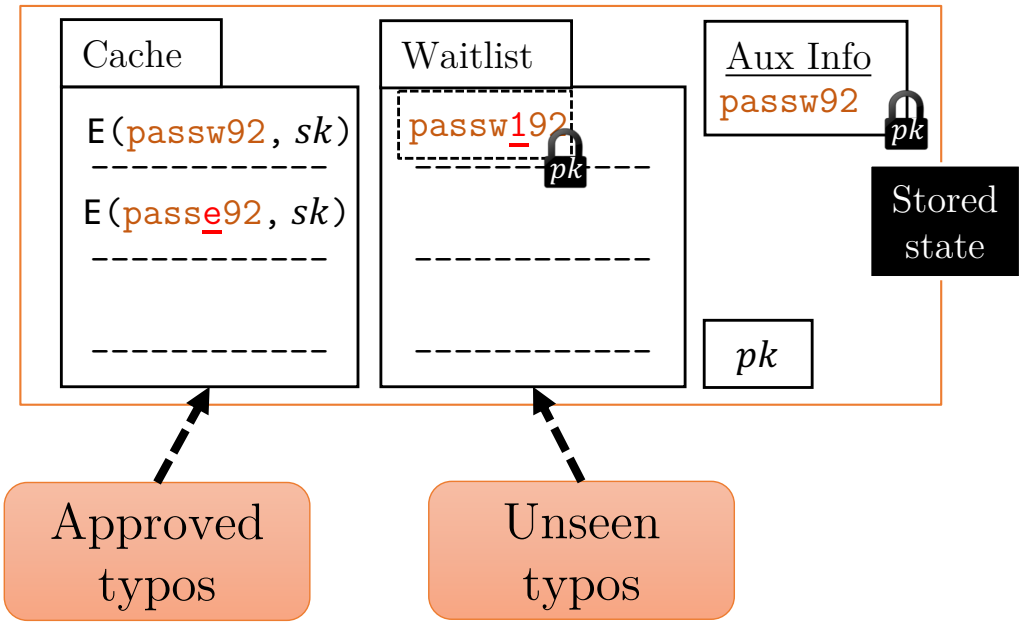
Password checking systems traditionally allow login only if the correct password is submitted. Recent work on typo-tolerant password checking suggests that usability can be improved, with negligible

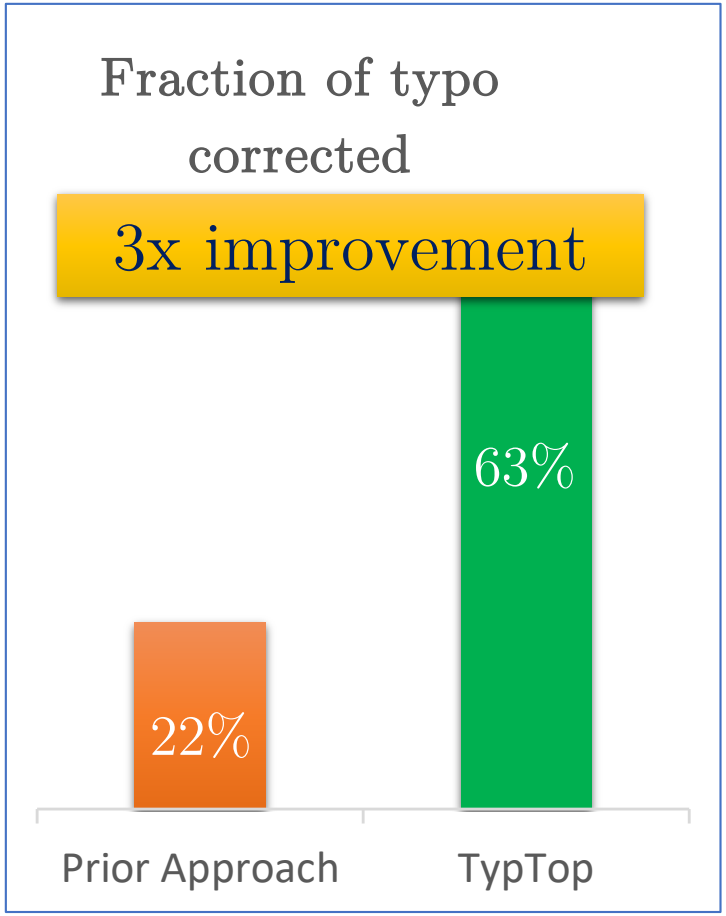
particular typos on behalf of the user at the time of authentication (e.g., flipping the case of all letters to correct a caps lock error). The authors show empirically that for a carefully selected set of correctors, the resulting security degradation is minimal.

A limitation of this approach is that checking each correction

https://typtop.info

An encrypted mutable state

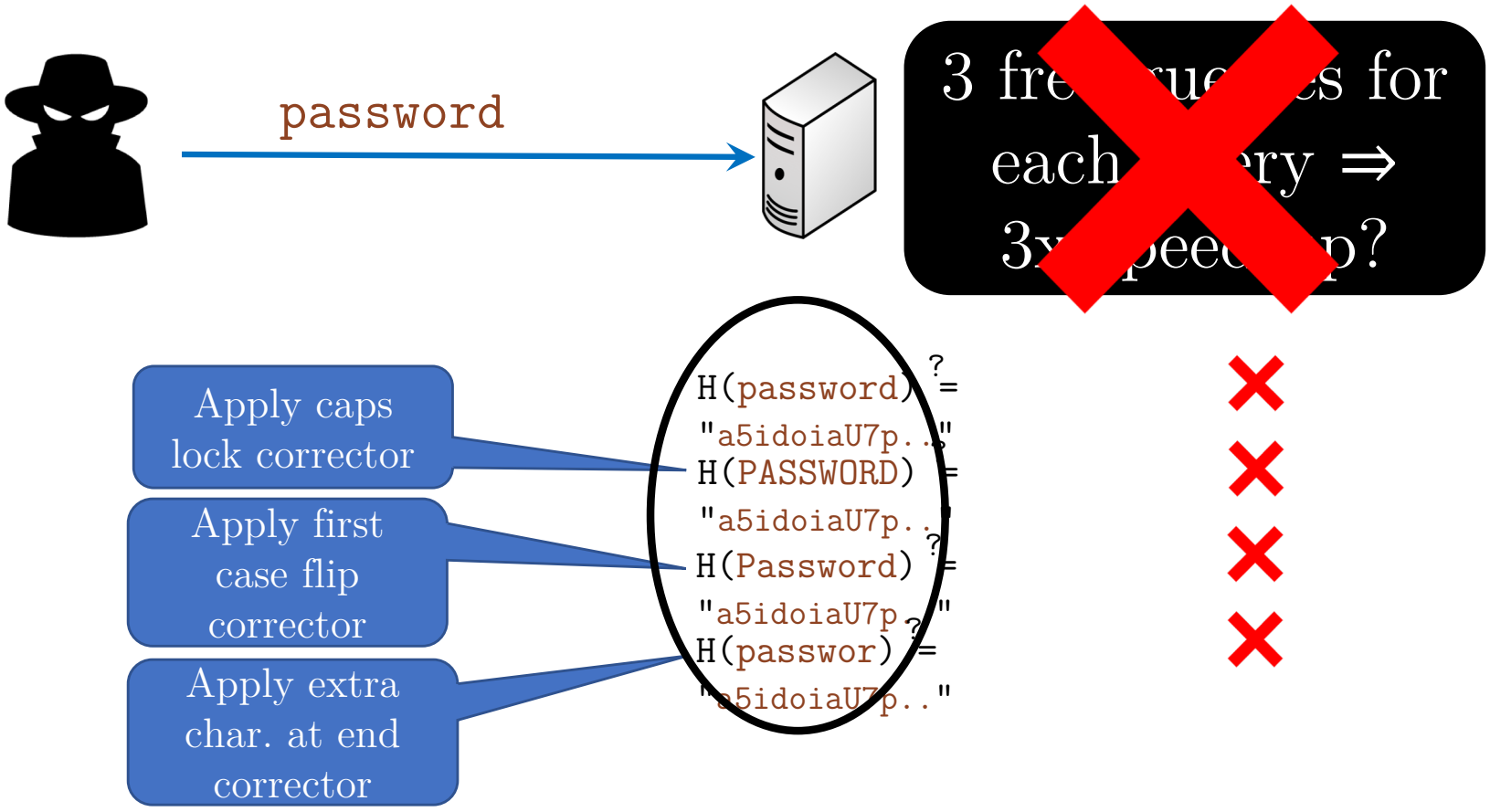




https://typtop.info

What about security?

Threat #1: Remote guessing attack

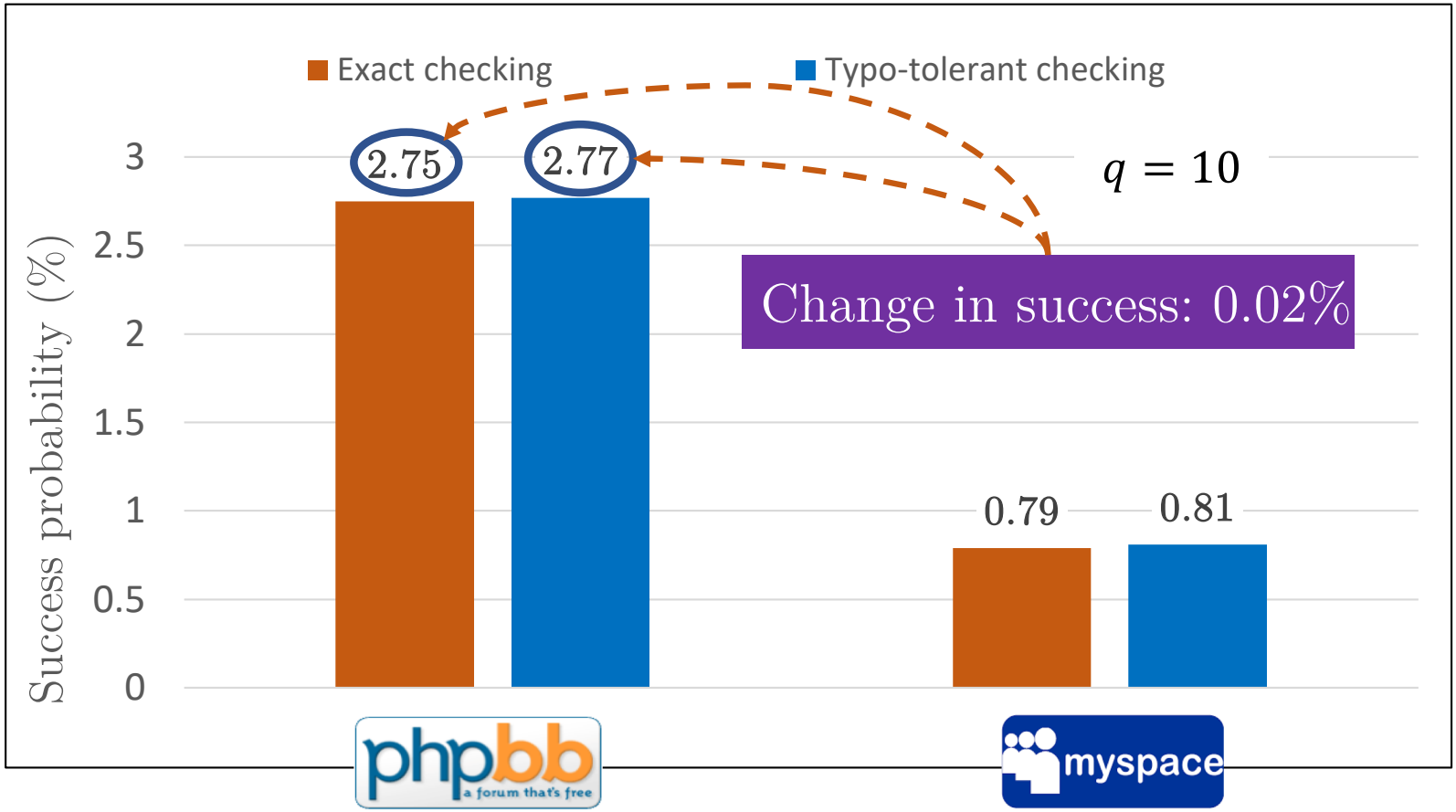


Passwords are not chosen uniformly

3x, only if all checked passwords are equally probable

BUT, humans do not chose random passwords.

Security of tolerating typos

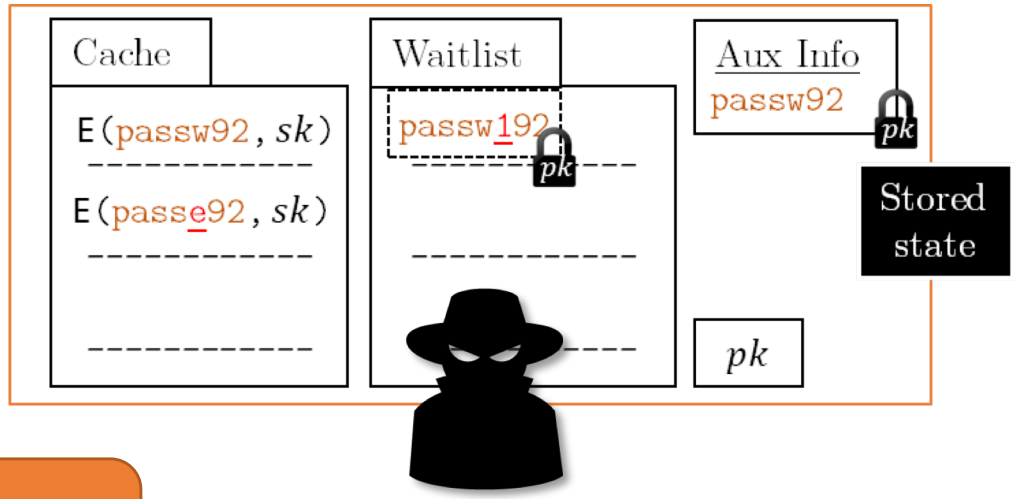


Threat #2: Password store compromise

We proved

The attacker learns nothing unless he guesses the registered password.

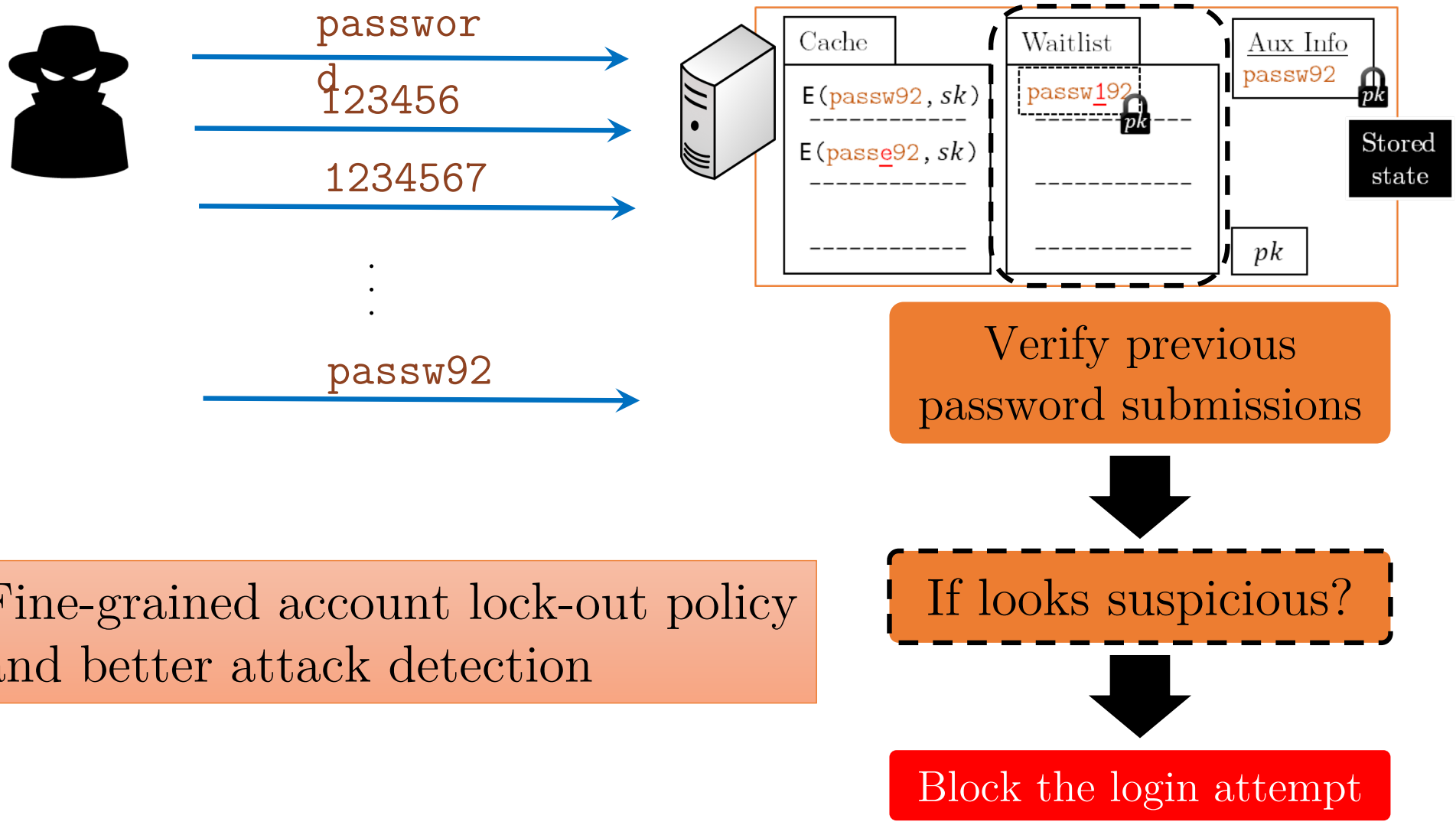
Exactly the case of exact checking



Typo-tolerance does not degrade security

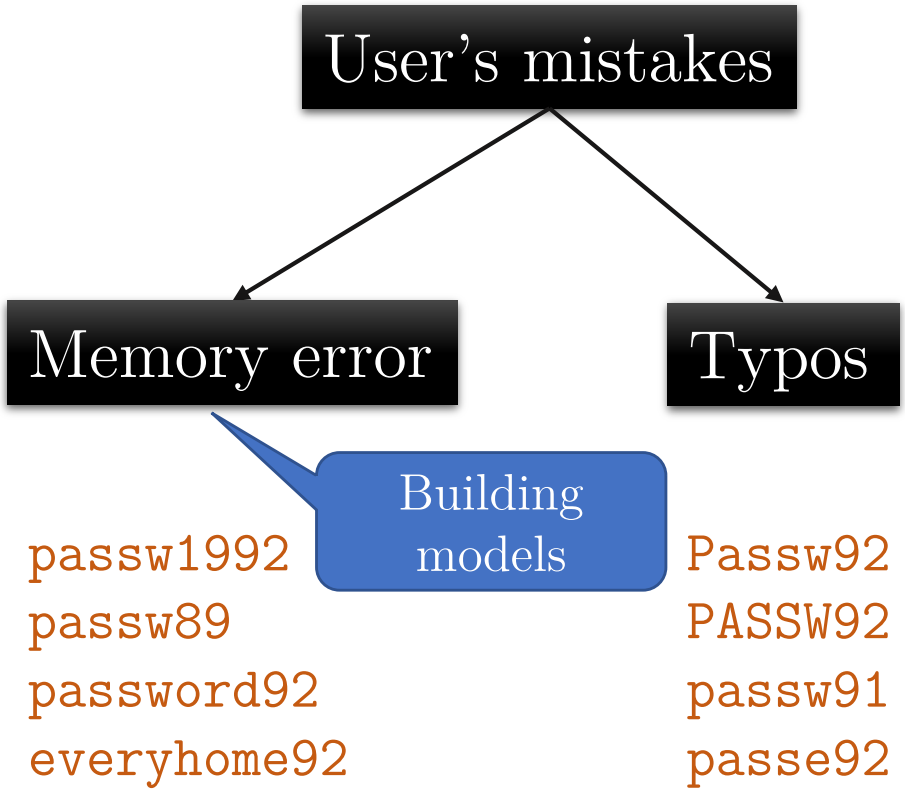
rather it can improve security…

Model user's mistakes to detect Attack



Fine-grained account lock-out policy and better attack detection

If looks suspicious?



Collaborating with Cornell IT Security to test efficacy of such system

Increase security by tolerating typos

- Securely tolerate typos; improve ease of use
- More effective account lockout policy
  - Tolerate only legitimate mistakes
  - Better attack detection
- Might improve user's security practices
  - Choose stronger passwords
  - Lock computers more often

Thanks!

https://typtop.info
https://www.cs.cornell.edu/~rahul/