Cybersecurity Transition to Practice Workshop

April 17, 2018 | New York, NY

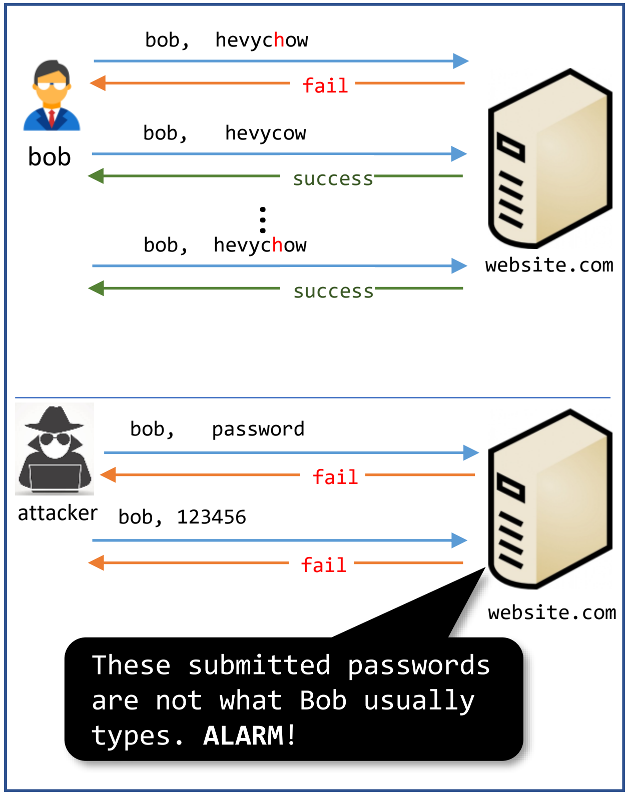
Quad Chart for: Improving Password Security by Tolerating Typos

Approach:

- Allow users to login with small variants (typos) of their passwords
- Adaptively and securely learn what typos a user frequently makes, and let them log in with a safe subset of those
- Build model for memory error: typing password of different website
- Main challenge is detecting typos when registered password is in hashed form

Solution:

- Distinguish user's behaviors from attacker's --- detect if an incorrect password submission is a typo or memory error from the user or a guess from an attacker
- Can detect (in theory) both targeted and untargeted attacks



These submitted passwords are not what Bob usually types. **ALARM!**

Broader Impact:

Passwords are the primary mode of authentication in the web

- Improve usability of passwords by reducing login failure due to typos in password submissions
- Users might be encouraged to choose stronger passwords
- More fine-grained attack detection strategy; improves password security

Metadata tag:

- *https://typtop.info/*
- *Work in progress*
- *Need real world authentication data to measure efficacy*
- *Working with Cornell IT Security Office. More industry collaboration are welcome*