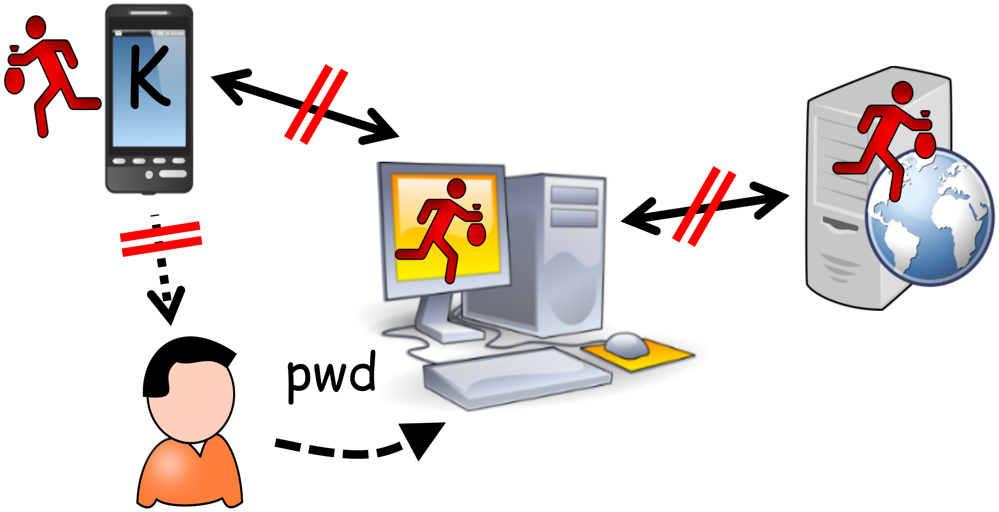
Improving Security of Password and 2nd Factor Authentication



MOTIVATION:

- Password authentication is a *major security bottleneck*
- Web services are routinely compromised and their DB's of hashed passwords leak → Hackers recover majority of passwords via Offline Dictionary Attack
- Current PwdAuth/TFA insecure against this (and other attacks)

OBJECTIVES:

- Eliminate hashed passwords on servers → security even if servers are compromised
- Improve TFA *usability* (PIN-copying is not necessary)
- Achieve maximal security in all attack scenarios

POTENTIAL ADOPTERS:

- *Any internet user*: New PA/TFA transparent to Web Server
- *Any internet service*: New PA/TFA transparent to end-user

FIST ADOPTERS (PILOTS):

- Education and research entities: e.g. University IT
- Internet end-users using academic-run 3rd party service
- Industry PwdAuth/TFA providers as partners?

TECHNOLOGY TRANSFER:

- Software libraries will be made available

Contact:

- Stanislaw Jarecki, UC Irvine, sjarecki@uci.edu
- Nitesh Saxena, UA Birmingham, saxena@uab.edu

BROADER IMPACTS (for cyberinfrastructure):

- Improve protection of digital identity on the internet
- Improve security of internet communication and commerce

BROADER IMPACTS (for cryptography):

- Make authentication security easier to understand and study
- Introduce new Pwd+TFA objectives to cryptographers

BROADER IMPACTS (academic and educational):

- Student-friendly project: practically-relevant, simple to state, with big impact potential
- Modular protocols: Easy place of entry into cryptography
- Many engagement levels: design, prototyping, user-study