Improving Security and Usability of Two-Factor Authentication

Stanislaw Jarecki (University of California Irvine)

Nitesh Saxena (University of Alabama Birmingham)

PhD students focused on the project:

Maliheh Shirvanian (UA Birmingham)

Jiayu Xu (UC Irvine)

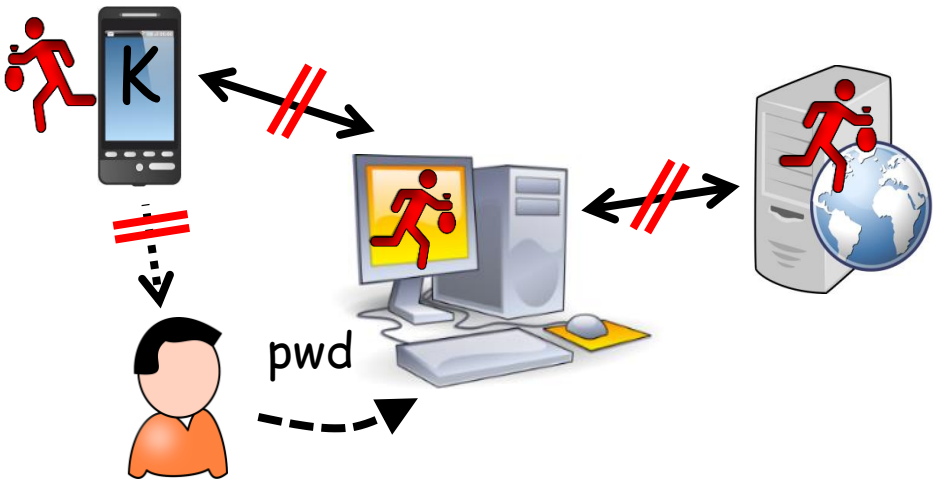
Other main collaborators (so far):

Aggelos Kiayas (U Edinburgh)

Hugo Krawczyk (IBM Research)

.

Improving Security and Usability of Two-Factor Authentication (TFA)



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 Offlline Dictionary Attack
- Current 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 TFA can be transparent to Web Server
- *Any internet service*: New TFA can be 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 TFA and Authentication 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 study and understand
- Introduce practical TFA objectives to cryptographers and highlight power of cryptography in solving practical problems

BROADER IMPACTS (outreach to undergraduates):

- 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

Outreach

- Female students (still minority in CS): Maliheh Shirvanian, PhD student at UA, is building her academic career on related topics, from crypto to systems, many publications, will be on the job market this year.
- High School students: worked over summer(s) with PI Saxena, reviewing papers and evaluating proposed schemes, learning about security, excited by high-impact topic
- Undergraduates: PI Jarecki hired undergraduate CS students, working on prototypes, but engaging in security design, entry-point for learning cryptography
- Technology Transfer: we are working to make our prototypes publicly available
- Transition to Practice: PI Saxena has recently won a TTP grant on the SPHINX password manager, working towards creating a start-up based on this technology