

SPHINX: A Password Store that Perfectly Hides Passwords from Itself

Nitesh Saxena, UAB

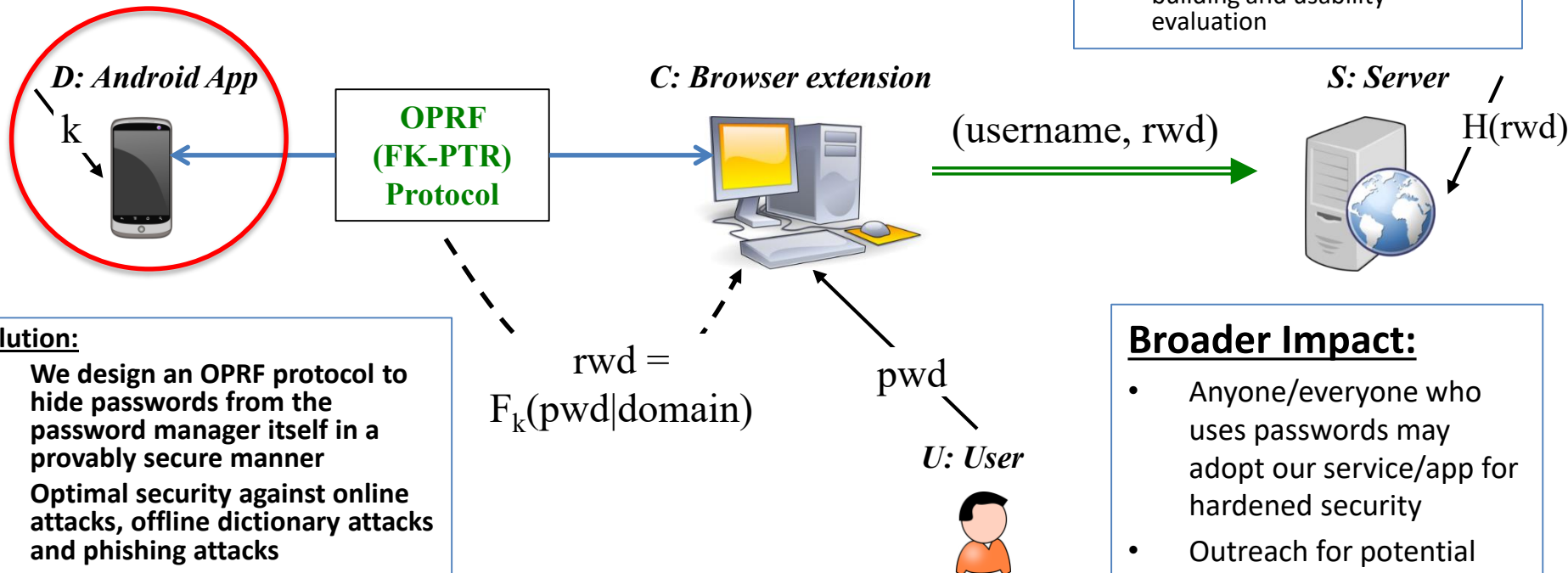
<http://spies.cs.uab.edu/sphinx-a-password-store-that-perfectly-hides-passwords-from-itself>

Challenge:

- Current password managers expose passwords to the password manager.
- If manager is compromised or malicious, all passwords are exposed.

Scientific Impact:

- Contribute a password manager system that would be secure even when the manager itself is compromised
- Can be a mobile app or an online service
- Protocol design, system building and usability evaluation



Solution:

- We design an OPRF protocol to hide passwords from the password manager itself in a provably secure manner
- Optimal security against online attacks, offline dictionary attacks and phishing attacks
- Key Pubs: ICDCS'17; PKC'18; TDSC'19

Broader Impact:

- Anyone/everyone who uses passwords may adopt our service/app for hardened security
- Outreach for potential deployment

Award # 1714807

Contact: PI: Nitesh Saxena (saxena@uab.edu)