Intrusion-Tolerant Outsourced Storage for Cyber-Infrastructure (TTP: Medium)

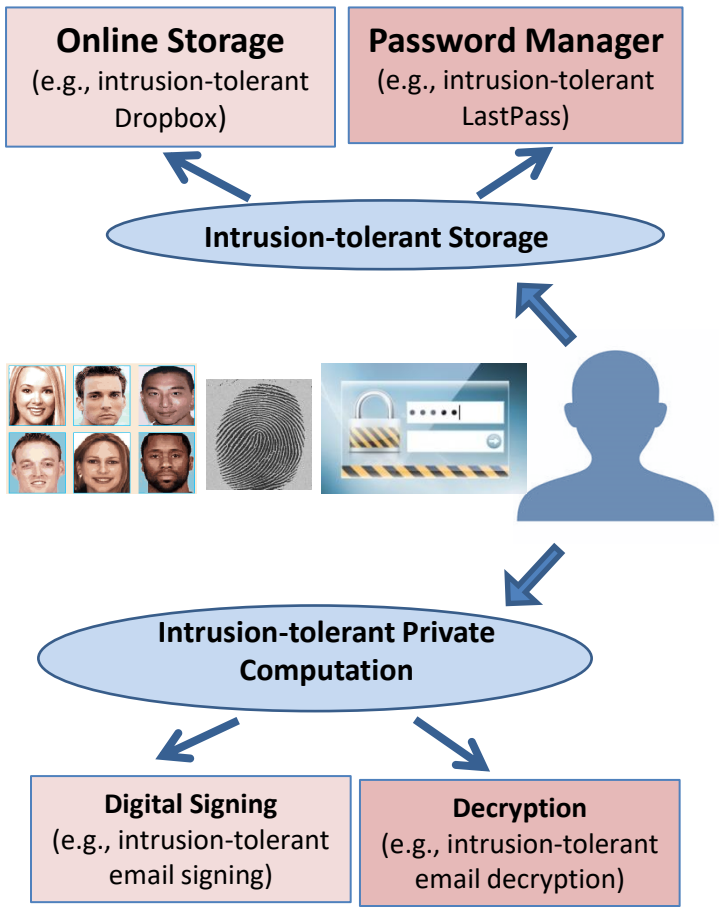
PI's: Stanislaw Jarecki (UC Irvine) and Nitesh Saxena (Texas A&M)

Challenge:

- Achieve Intrusion-tolerant **Storage** by encrypting remote data under user's authentication information
- Enable efficient **computation** on remote data encrypted under user's authentication
- Support:
  - password authentication
  - two-factor authentication
  - biometric authentication

Solution:

- Use remote Oblivious Pseudorandom Function (OPRF) to map user's authentication information to cryptographic keys
- Secret-Share OPRF computation to achieve fault-tolerance



Scientific Impact:

- Efficient *Multi-Party Computation* on **obfuscated authentication,** i.e. a secret-shared obfuscation of an authentication procedure
- Extending *OPAQUE* [JKX'18], a strong authenticated Password-Authenticated Key Exchange (PAKE), winner of IETF PAKE competition, to secret-shared operation and other forms of authentication

Broader Impact and Broader Participation:

- Increased security for remotely stored data
- Protecting users' cryptographic credentials
- Protecting user's authentication information even from remote services to which the user authenticates
- Making data-encryption keys recoverable only by the end-user

NSF Award # 2030575
UC Irvine PI: sjarecki@uci.edu
Texas A&M University PI: nsaxena@tamu.edu