Towards Secure and Usable User Authentication

Robert H. Deng
School of Information Systems
Singapore Management University
Typical SSL-based user authentication architecture over the Internet today

• How it works?
  1. SSL authenticates web server and sets up a secure tunnel with user
  2. User inputs password, or password +OTP
Vulnerabilities

MITM (SSLSniff)

User

Internet

Web Server

Corp. Net

App Server

Database

Authentication Server

Phishing

Security Gap
Countermeasure

- It is critical that the end-to-end encryption is secure!
- Solution
  - **PAKE**: Password Authenticated Key Exchange
  - IETF, IEEE, ISO and 3GPPS standards
Biometric Authentication

- No need to remember anything; identify the physical presence of user
Thank You!