Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices

Maliheh Shirvanian	Stanislaw Jarecki	Nitesh Saxena	Naveen Nathan
University of Alabama at Birmingham	University of California, Irvine	University of Alabama at Birmingham	University of California, Irvine
maliheh@uab.edu	stasio@ics.uci.edu	saxena@cis.uab.edu	nnathan@uci.edu

Outline

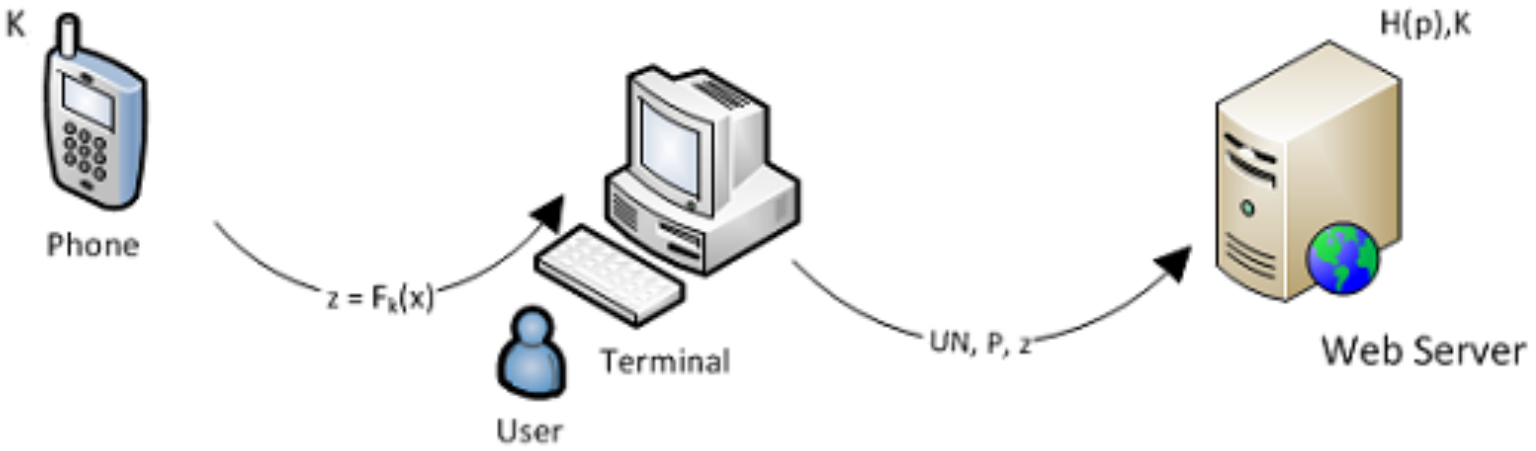
- Current State
- Desirable Properties
- Our Contributions
- Protocols and Security Analysis
- System Implementation
- Discussion

Introduction

- Password only systems
- Two Factor Authentication TFA
- Online guessing attack
- Offline dictionary attack
  - Many real-world instances
  - Password re-use

More than 200,000 of these passwords have reportedly been cracked so far.

Current State



|D| = 2^d = Size of a password dictionary

t = |z| = bandwidth of Device to Client channel

x = time

Desirable Goals

In case of:	Desired:
On-line guessing	Probability of (1/|D| x 1/2^t) instead of 1/|D|
Offline Dictionary attack	Complexity of O(|D| x 2^t) instead of O(|D|)
Lunch time attack/ C-D communication	Shouldn't affect above
Adversary breaks into the user's device	security degrades to password-only
Adversary learns the user's password	security degrades to the device-only

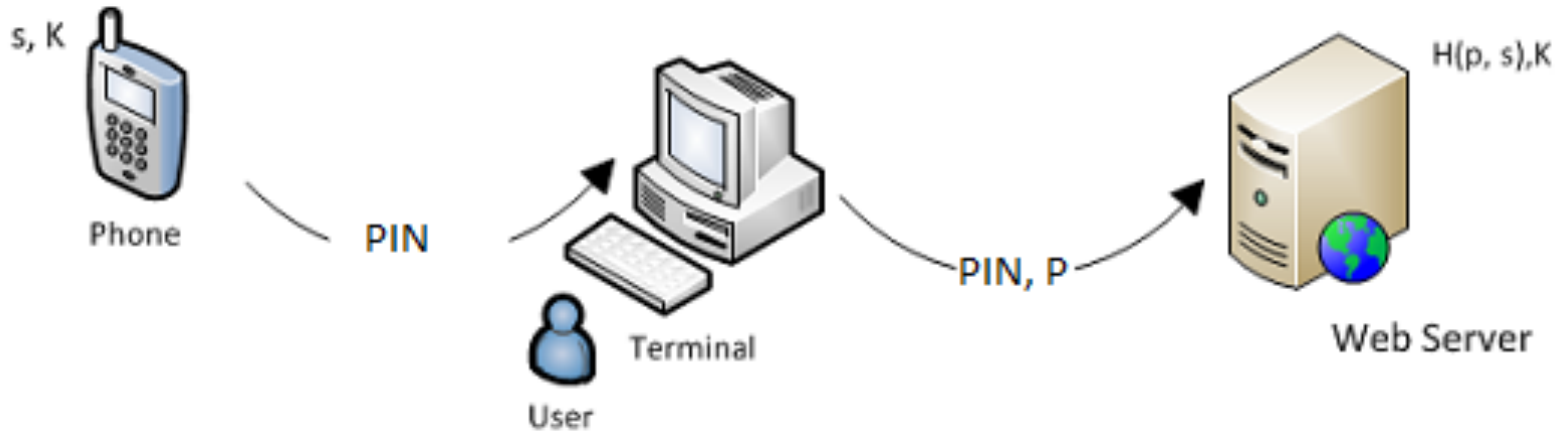
Our Contributions

- Novel TFA Protocols to achieve desired TFA properties and Improve security of TFA Schemes.

- Mix-Bandwidth Device TFA Mechanisms to improve ODA resistance by increasing bandwidth t.

The Main Idea

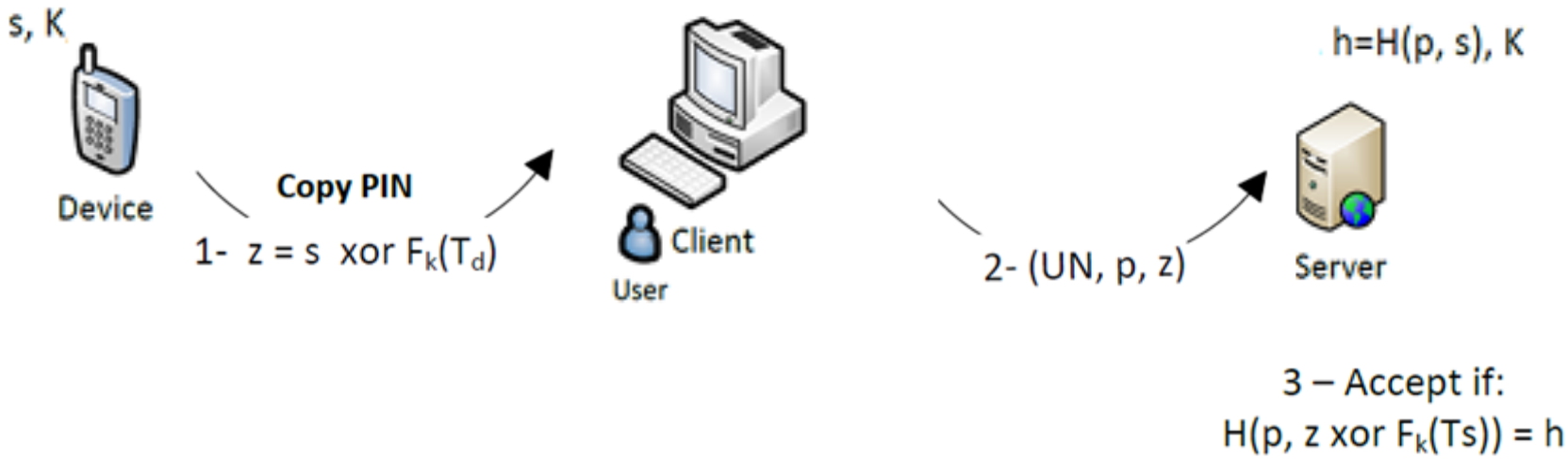
- Server stores a hash of the password and a secret s, h=H(p,s)
- Device stores the secret s
- Authentication decision based on whether user provides the correct password and owns the device which stores s



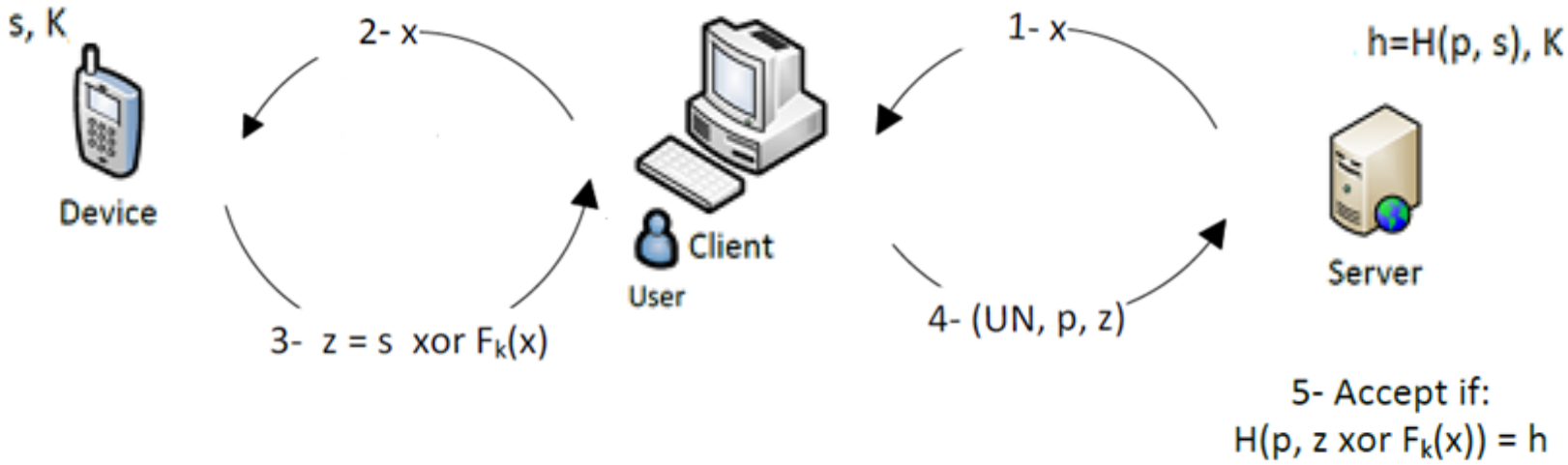
Protocols

- Time-based TFA protocol
  - Applicable to all device types (Low, Mid, High Bandwidth)
  - Rely on a clock synchronized with the server
- Challenge-Response TFA Protocols
  - Symmetric-key and public-key TFA protocols
  - Applicable for devices that receive a challenge and show PIN

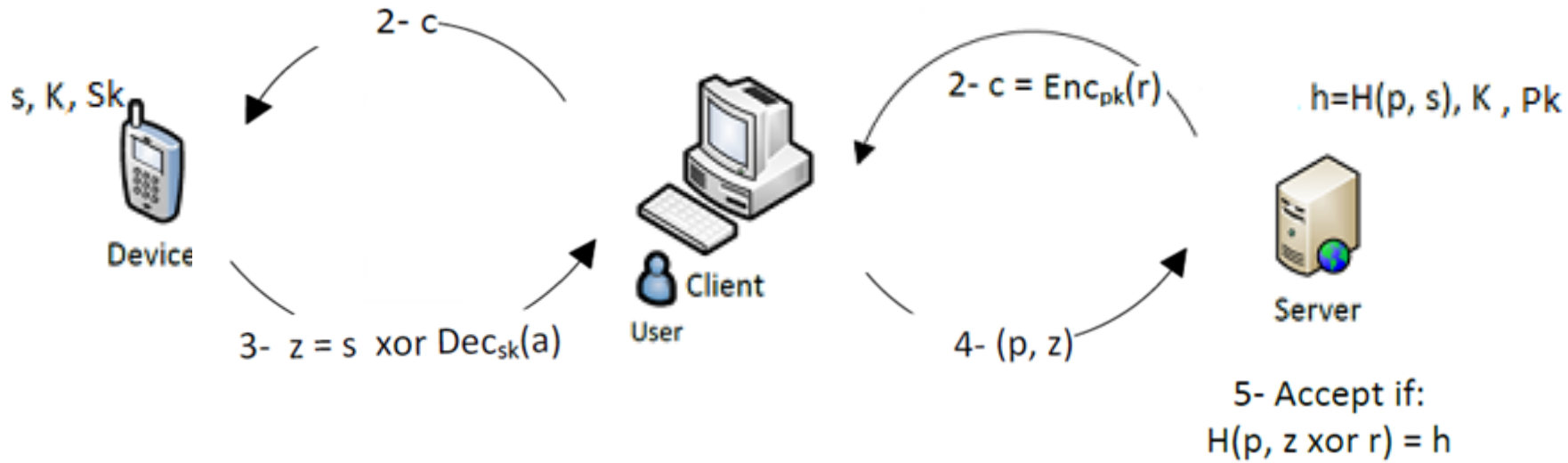
Time-Based TFA Protocol



Symmetric-Key TFA Protocol



Public-Key TFA Protocol



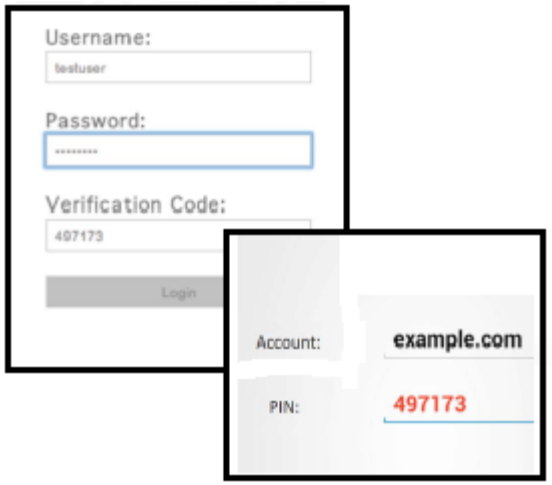
Security of the Protocols

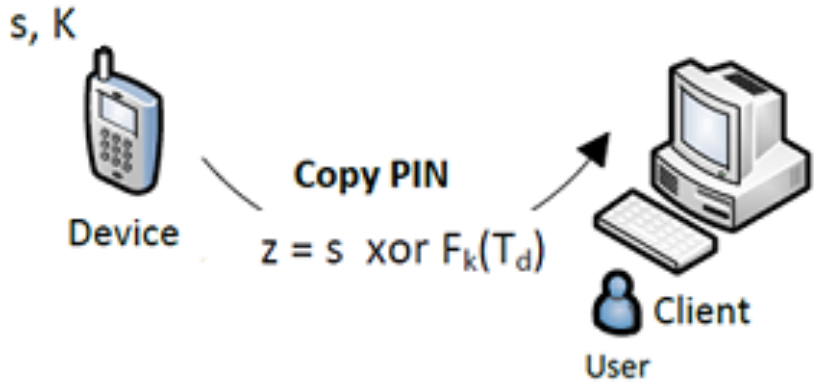
In case of:	**Desired:**
On-line guessing	Probability of (1/|D| x 1/2^t) instead of 1/|D|
Offline Dictionary attack	Complexity of O(|D| x 2^t) instead of O(|D|)
Lunch time attack/ C-D communication	Shouldn't affect above
Adversary breaks into the user's device	security degrades to password-only
Adversary learns the user's password	security degrades to the device-only

Notes on System Design and Implementation

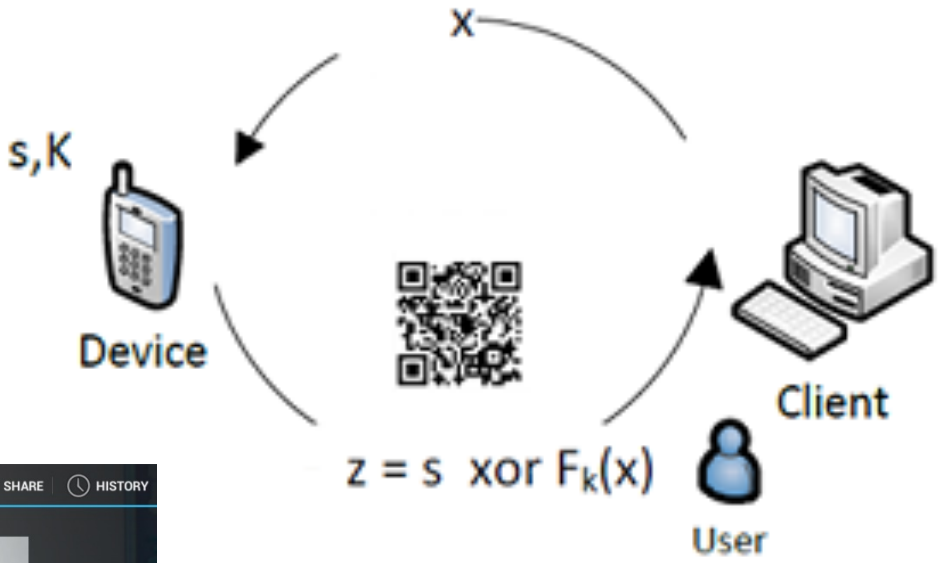
- Total 13 TFA mechanisms categorized based on:
  - The underlying protocol
  - The underlying device type
  - The underlying Device - Client channel – PIN, QR, BT, WiFi
    - PIN: 6 digits, manual entry
    - QR: The QR code encoding and decoding ZXing library, HTML5 Server codes and a plain browser on the Client
    - BT: Android application listening on a RFCOMM socket, Client runs a browser extension (Bluetooth API)
    - WF: Virtual WiFi between Client and Device, Client runs a browser extension (chrome.socket API)

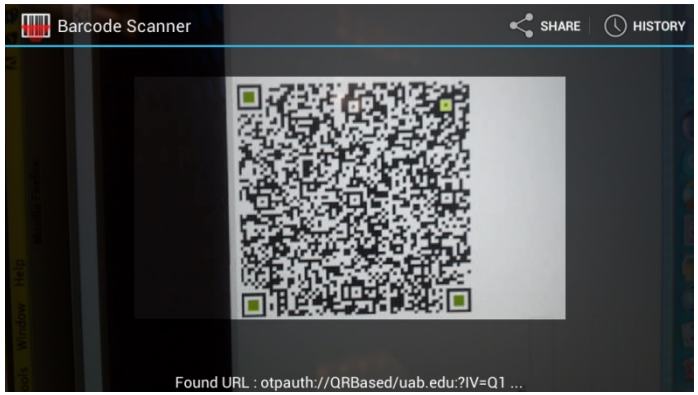
LBD Authentication Phase



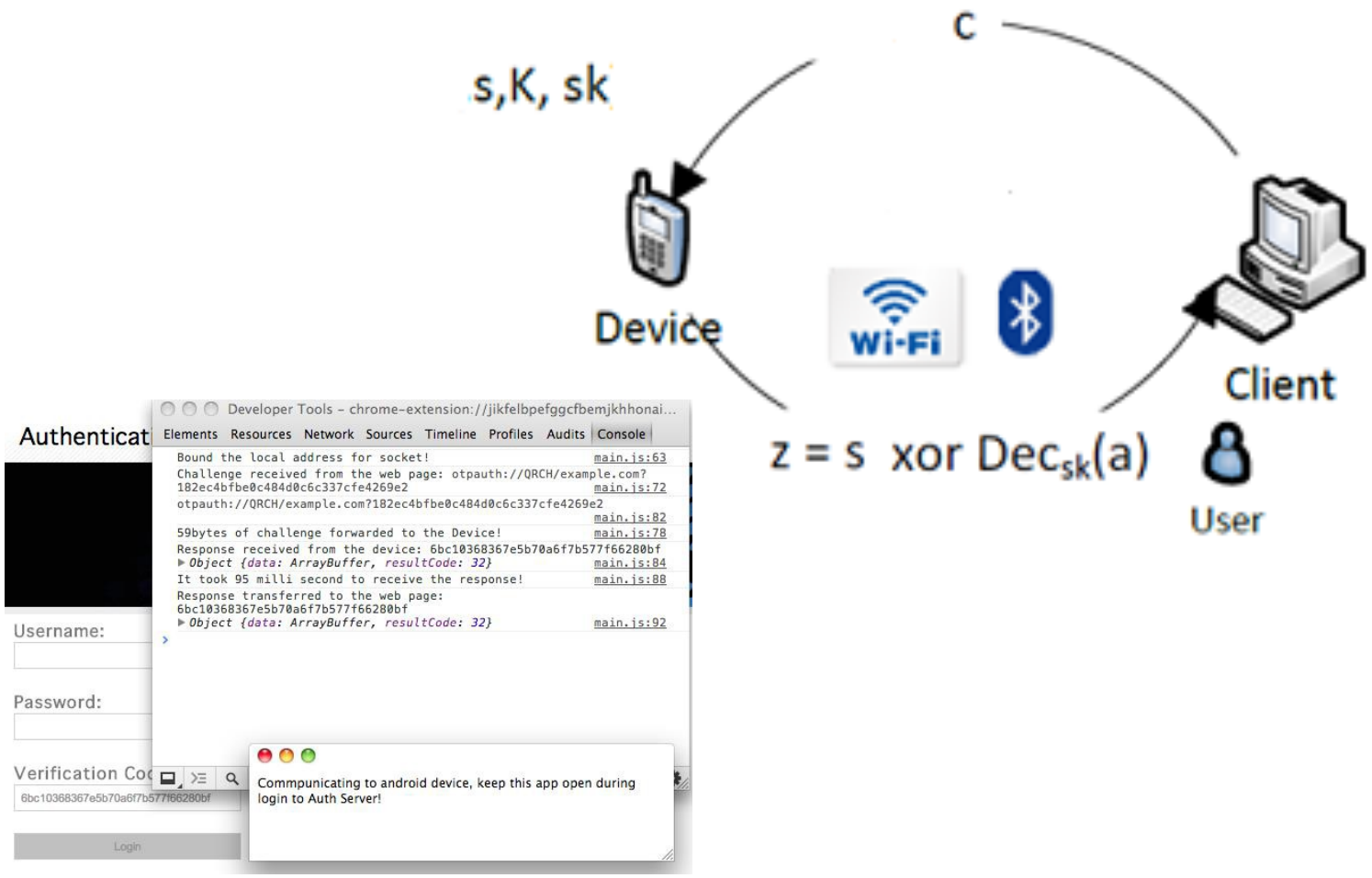


MBD Authentication Phase





FBD Authentication Phase



Discussion and Conclusion

- **Security**:
  - All mechanism provide improved resilience to offline dictionary attacks and online attacks.
  - Challenge-Response protocols are secure against a lunch-time attacker.
  - FBD mechanisms are more secure against online attacks.
- **Usability**:
  - There is no time synchronization requirement in Challenge Response mechanisms.
  - In high bandwidth channels user does not need to manually transfer the PIN.
- **Deployability**:
  - Traditional and LBD work with a plain browser and no special hardware.

Thank you!

Questions?