Security Levels for Web Authentication Using Mobile Phones

Anna Vapen and Nahid Shahmehri

Linköping University – IDA/ADIT
PrimeLife Summer School 2010

LiU

Agenda

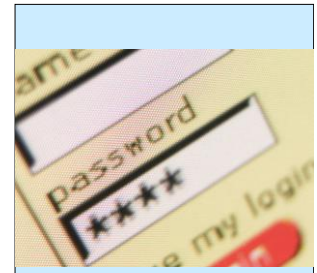
- Problems with web authentication
- Mobile phones in authentication
- Security levels

- Our approach: Using security levels for evaluation and design of mobile phone authentication
- Conclusions and future work

LiU

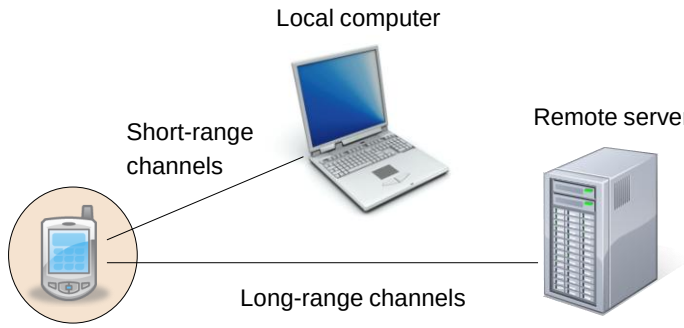
Problems with Web Authentication

- Passwords are insecure
  - Eavesdropping
  - Key loggers
- Passwords are valuable
- Hardware devices for strong authentication
  - Distribution
  - Availability
- The mobile phone – a non-dedicated device



LiU

Mobile Phones in Authentication



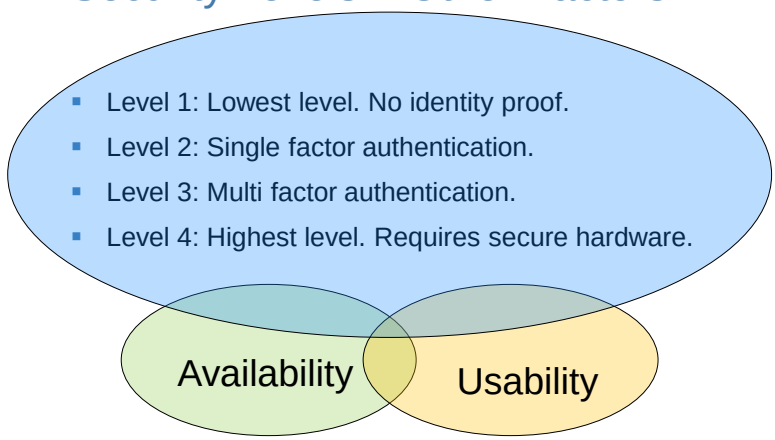
LiU

NIST Security Levels for Authentication

- Level 1: Lowest level. No identity proof.
- Level 2: Single factor authentication.
  - No replay attacks
  - No eavesdropping
- Level 3: Multi factor authentication.
  - No MiTM attacks
  - Possible to lock the device
- Level 4: Highest level. Requires secure hardware.

LiU

Security Levels + Other Factors



LiU

Design and Evaluation Method

Design: Start with a security level

Evaluation: Start with a solution

1. Authentication methods
2. Locking methods
3. Eavesdropping
4. Man-in-the-Middle-attacks
5. Other factors
6. Conclusion: Solution or level

Conclusions and Future Work

- Evaluation and design method for web authentication with mobile phones

- Future work:
  - Include protocols and hardware modules
  - Add new factors
  - Adapt the method for different services
  - Let the user switch security level

Any questions?