Lecture 12.2: User-Enabled Device Authentication II

CS 436/636/736
Spring 2012

Nitesh Saxena
Course Admin

- HW3 graded
  - Solution provided
  - Stats to be posted
- HW4 Posted
  - Problem 1 and 2: due Apr 26, 11am (individually assigned)
  - Problem 3: demo due 11am May 7 (can be teams of 2)
    - Please sign-up for demo slots – sheet being circulated
Course Admin

- Final Exam – **May 3 (Thursday)**
  - 10:45 to 1:15
  - Venue – CH 430 (our regular lecture room)
- Covers everything (cumulative)
  - 35% -- pre mid-term material
  - 65% -- post mid-term material
- Again, close-book, just like the mid-term
- Exam Review on May 1
Challenges

- Comparative Usability!
Many Mechanisms Exist

- See survey: [Kumar, et al. @ Percom’09]
  - Manual Comparison or Transfer:
    - Numbers [Uzun, et al. @ USEC’06]
    - Spoken/Displayed Phrases: Loud & Clear [Goodrich, et al. @ ICDCS’06]
    - Images: [Goldberg’96][Perrig-Song’99][Ellison-Dohrman @ TISSEC’03]
    - Button-enabled data transfer (BEDA) [Soriente, et al. @ IWSSI’07]
    - Synchronized Patterns [Saxena et al. @ ACNS’08 & SOUPS’08]
  - Automated:
    - Seeing-is-Believing (SiB) [McCune, et al. @ S&P’05]
    - Blinking Lights [Saxena, et al. @ S&P’06]
    - Audio Transfer [Soriente, et al. @ ISC’08]
A Comparative Usability Study

- How do these mechanisms compare with one another in terms of usability?
  - Timing; error rates; user preferences
- Needed a formal usability study

- Automated testing framework
- 20 participants; over a 2 month long period

- Surprise:
  - Users don’t like automated methods: handling cameras not easy
TESTED METHODS (1/5)

- Number Comparison
  “65473” =? “75853”

- Phrase Comparison
  “Alice buys jackets” =? “John likes elephants”

- Image Comparison
Tested Methods (2/5)

- Audiovisual synchronization methods
  - Beep-Blink
    - [Audio Symbol] [Audio Symbol] [Audio Symbol] → [Eye Symbol] ← [Eye Symbol] [Eye Symbol] [Eye Symbol] [Eye Symbol]
  - Blink-Blink
    - [Eye Symbol] [Eye Symbol] [Eye Symbol] → [Eye Symbol] ← [Eye Symbol] [Eye Symbol] [Eye Symbol] [Eye Symbol]
Tested Methods (3/5)

- Button enabled (BEDA) methods
  - LED-Button
  - Vibrate-Button
  - Button-Button
TESTED METHODS (4/5)

- **Loud and Clear (L&C) variants**
  - Speaker-Speaker
    
  - Display-Speaker
Tested Methods (5/5)

- Seeing is Believing (SiB)
- Blinking Lights
- HAPADEP Variant
Comparative Usability Study: Time

![Graph showing completion time in seconds for different tasks. The graph compares tasks such as Image Comparison, Number Comparison, etc., and shows the variance in completion times.]
Comparative Usability Study: Ease-of-Use

Answers given as "Very Hard", "Hard", "Easy" or "Very Easy" on a 4 point scale.
Conclusions from the study

- Both devices have a display
  - Numeric Comparison

- One device does not have a display but an audio interface
  - L&C Display-Speaker
    - if one has a display and the other has a speaker
  - Audio Transfer
    - if microphone is available on one, and speaker on the other

- Interface constraint device(s)
  - BEDA Vibrate-Button, if possible
  - BEDA LED-Button otherwise
Challenges

- Multiple devices – scalability
Secure Group Association

- Small groups (> 2) of users + devices
  - phones, PDAs, laptops
- Common use-cases:
  - Share content as part of an ad hoc meeting
  - Multiplayer games
  - Multimedia streaming
- Two user tasks:
  - Comparison of SAS strings
  - **Verification of group size**
### SAS-based Group Key Agreement

**BD GKA**

<table>
<thead>
<tr>
<th>Step 1:</th>
<th>Step 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i \rightarrow G$:</td>
<td>$U_i \rightarrow G$:</td>
</tr>
<tr>
<td>$PK_i = g^{s_i}$</td>
<td>$X_i = \left( \frac{PK_{i+1}}{PK_{i-1}} \right)^{s_i}$</td>
</tr>
</tbody>
</table>

**Key Computation**

- $K_i = \left[ g^{s_{i}^{x_1} + \cdots + s_{i}^{x_n}} \right] = (PK_{i-1})^a X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2}^1$
Usability Evaluation of Group Methods

- Usability evaluation of FIVE simple methods geared for small groups (4-6 members)
  - Three leader-based
  - Two peer-based
Study Goals

- How well do users perform the two tasks when multiple devices and users are involved:
  - Comparison/Transfer of SAS strings?
  - Counting number of group members?
Leader-Based Methods (1/3)

- **Leader-VerifySize-VerifySAS (L-VS-VS):** Leader announces 5-digit SAS, group members verify the displayed SAS and the group size.

  - The Verification Code is 39715
  - Group size is 4
  - Verification code is 39715
  - Accepted or Rejected

  1. Enter the group size
  2. Enter the verification code
  3. Accepted or Rejected
Leader-Based Methods (2/3)

- Leader-VerifySize-CopySAS (L-VS-CS): Leader announces SAS, members enter it to their devices and verify group size.
Leader-Based Methods (3/3)

- **Leader-VerifySize-AudioSAS (L-VS-AS):** Leader’s device broadcasts SAS (over audio), other devices record & verify. Users only verify group size.
Peer-Based Methods (1/2)

- Peer-VerifySize-VerifySAS (P-VS-VS): Each peer verifies group size and compares SAS with left-hand peer.
Peer-Based Methods (2/2)

- **Peer-InputSize-VerifySAS (P-IS-VS):** Each peer enters group size and compares SAS with left-hand peer.

  1. Identify Group Size: 4
  2. Your code is 38715
  3. Does it match with the code of the person next to you?
  4. Accept or Reused
The gender split was 58% male and 42% female. Most participants were university students resulting in a fairly young (80% aged 18–29), well-educated and technology-savvy group.

Phone model N95
Pairwise t-tests (paired) revealed that L-VS-CS is significantly ($p < 0.05$) slower than L-VS-VS and P-IS-VS for both group sizes.

In terms of average completion times, the fastest method is P-IS-VS (27.57 sec.) for smaller groups and L-VS-VS (31.33 secs.) for larger groups.

L-VS-CS yields the most safe errors for both group sizes.

Pairwise t-tests (paired) revealed that SUS scores for P-IS-VS were significantly higher ($p < 0.01$) than those for all other leader–based methods. This seems to indicate that, for small groups, peer-based methods are generally more acceptable than leader-based ones.

There is also evidence ($p < 0.054$) suggesting that P-IS-VS is perceived as more usable than P-VS-VS.
In particular, L-VS-CS appears vulnerable to this attack, since at least one group member accepted the pairing in almost half of attack cases, irrespective of group size.

In contrast, P-VS-VS seems to be the most resilient, as only one of thirteen groups had a member who erroneously accepted a tainted pairing.

Larger groups are more susceptible to evil twin attacks.
Combined Usability Metrics

- Interesting result: peer based methods performed better in general
Summary of results

- Peer-based methods generally better than Leader-based ones
- P-IS-VS has the best overall usability
- L-VS-CS has the worst
- L-VS-VS and L-VS-AS are natural choices if peer-based methods are not suitable
  - L-VS-VS > L-VS-AS
- Over-counting unlikely in small groups
- Entering group size is better than verifying it
Other open questions

- Rushing user behavior (Saxena-Uddin [ACNS’09])
- Hawthorne effect
- Security priming
- More usability tests
References

- Many of them on my publications page