Goal

- Give you some advice that will be useful for your MoPS presentations (and for your presentations in general)

- Will use some slides from earlier student presentations in my grad courses to demonstrate possibilities for improvement
General Advice - Preparation

- Concentrate on (some) important points
  - Don’t present every single detail
  - Look at presentation review form

- Target your talk at your audience
  - Maybe present additional background information
  - Give guidance (e.g., motivation/overview slides)

- Practice your talk
  - Especially if you are a non-native English speaker
  - At least twice, but don’t over practice
  - Memorize first few slides
General Advice – During the Talk

- Face your audience and use feedback from it
  - Are people looking confused?
  - Are they falling asleep?
- Repeat questions
  - You can delay a question till later
  - Unless it’s a clarification question
- Don’t read off slides
- Don’t mumble
- Watch your hands
- Watch the clock
Preserving Privacy in Environments with Location–Based Applications

Ginger Myles, University of Arizona

Adrian Friday, Lancaster University

Nigel Davies, University of Arizona and Lancaster University
Identify Yourself

- Give your name on the title side
  - Emphasize it if multiple authors (not relevant for MoPS)
  - You want your audience to remember you!

- Examples:
  - Alice, Bob, and Carol
  - Alice
    - Collaboration with Bob and Carol

- Maybe repeat your name on each slide
  - Not necessarily in MoPS, but maybe at a conference
An Analysis of Private Browsing Modes in Modern Browsers

Gaurav Aggarwal  Elie Bursztein  Collin Jackson  Dan Boneh

USENIX Security 2010

Presented by: Rob Smits

David R. Cheriton School of Computer Science
University of Waterloo
200 University Ave W
Waterloo, Ontario, Canada
N2L 3G1

Rob Smits  2010-10-07
Information on Title Side

☐ Yes: Title, name, affiliation
   In MoPS, names are the authors of the papers; in addition, you should give your own name

☐ Maybe: Venue (e.g., “USENIX Security 2013”), useful mainly if you make available your conference presentation on the web, university and/or group logos

☐ No: Date, sponsorship logos, address
Outline

- Introduction
- Backgrounds
- Motivation
- Privacy-Preserving
  - Edit Distance
  - Smith-Waterman
- Evaluation
- Conclusion
- Remarks
- Questions
1. Introduction
   - Concepts and Definition

2. Description of Security Games
   - Total Effort
   - Weakest-link
   - Best Shot
   - Weakest-target without Mitigation
   - Weakest-target with Mitigation

3. Nash Equilibrium Analysis

4. Identification of Social Optima

5. Conclusions and Discussion
Be Careful About Outline Slide

- At the beginning of your talk, you want your audience to become excited about what is coming next.
- You don’t want to put it asleep while going through a lengthy outline slide that is full of technical terms.
- Consider having short motivation/introduction (“attention grabber”) after title slide, followed by outline slide.
- Keep outline slide short and understandable, wherever you place it.
Outline

• Introduction
• Related work
• Threat
• Data Collected
• Theories
  • Possible explanations?
• Analysis
• Conclusions
Agenda

- Introduction
- Key management
- Implementation
- Evaluation
- Conclusion
Agenda

• Background & motivation
• Research questions
• Research methods
• Case study
• Analysis & implication
• Conclusion
• Discussion
Outline Slide (cont.)

- Don’t have a generic outline slide, make it interesting!
- Outline slide is not strictly required but useful if you are an unexperienced speaker or if your talk is long (45 mins)
- If you have an outline slide, consider repeating it throughout the talk (emphasize topic to be discussed next)
Security Issues

- Security issues of wireless networking
  - Availability
  - Authenticity
  - Integrity
  - Confidentiality
- A concrete example of a thermometer
Put Page Numbers on Slides

- Makes it easier for your audience to write down and ask questions
Authentication by Certificate Chain

Certificate chain (hashes, application data, public keys) May also send a certificate from its software vendor
Use Large Fonts

- People sitting in the last row should still be able to read the text on your slides
- Use fonts of size at least 20 points
Security Objective

**Uniqueness**
Use a unique password for each site.

**Resistance**
Resist offline dictionary attacks on user-chosen secrets.

**Adaptive**
Adapt to the development of faster computers.

**Computed Password**
Avoid storing passwords in long-term storage.

**No centralized dependency.**
Avoid introducing a centralized dependency.

**Phishing resistance**
Resist attacks based on fake website login forms

**Websites identification**
Help the user reliably identify websites

**Resist attacks based on imitating the browser UI**
Resist attacks based on imitating the browser UI.
Limit Number of Lines

- Don’t crowd your slides
- About 10-12 lines of text
  - Goes along with font size
Result
Each Slide Needs a Message

- Don’t expect your audience to find message by itself
- This is especially important for slides showing graphs
- For example, give message in the title  
  - “Algorithm Foo improves latency by 10%” is much more useful than “Results”
- Also, make sure to explain graphs thoroughly
Thank You
Final Slide

- Avoid final slides with no useful information
  - “Thank you”
  - “Questions?”
- The final slide is the slide that your audience likely will spend the most time looking at
- Put a few take-home messages on it
  - “Conclusions”
  - E.g., problem, approach, evaluation summary
Privacy: Canada

- Personal Information Protection and Electronic Documents Act
  - Very much as EU Directive
  - Requires consent of the subject
  - Supply a person with a product/service even in the case of refusing

- Implementation:
  - 2001 – applied to federally regulated industries (airlines, banking, broadcasting)
  - 2002 – health sector
  - 2004 – any organization that collects personal info
Use Fonts Without Serifs

☐ This is difficult to read (Times New Roman)

☐ This is easier to read (Verdana)

☐ But don’t use Comic Sans MS
  - Some people really hate it, and you don’t want to annoy your audience
Important Tenets of CAPTCHAs

- Code and database public.
- Randomness unknown.
- Some humans probability of success very high.
- AI problem “hard” < human success.
- Humans can take as long as they like; programs have time limits.
Watch Punctuation

- Only complete sentences have full stop at the end

- If you don’t want to worry about punctuation, just leave it away entirely
  - But be consistent
## List of Sites

<table>
<thead>
<tr>
<th>Website</th>
<th>Real or Spoof</th>
<th>Phishing or Security Tactic Used (Partial List)</th>
<th>% Right (avg conf)</th>
<th>% Wrong (avg conf)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of the West</td>
<td>Spoof</td>
<td>URL (bankofthewest.com), padlock in content, Verisign logo and certificate validation seal, consumer alert warning</td>
<td>9 (3.0)</td>
<td>91 (4.2)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Spoof</td>
<td>Uses Mozilla XML User Interface Language (XUL) to simulate browser chrome w/ fake address bar, status bar and SSL indicators</td>
<td>18 (3.0)</td>
<td>81 (4.5)</td>
</tr>
<tr>
<td>Etrade</td>
<td>Real</td>
<td>3rd party URL (etradetruetrust.com), SSL, simple design, no graphics for mobile users</td>
<td>23 (4.6)</td>
<td>77 (4.2)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Spoof</td>
<td>URL (paypal-signin03.com), padlock in content</td>
<td>41 (4.0)</td>
<td>59 (3.7)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Spoof</td>
<td>URL (IP address), padlock in content</td>
<td>41 (3.9)</td>
<td>59 (4.5)</td>
</tr>
<tr>
<td>Capital One</td>
<td>Real</td>
<td>3rd party URL (capitalonebanking.com), SSL, dedicated login page, simple design</td>
<td>50 (3.9)</td>
<td>50 (3.5)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Spoof</td>
<td>Screenshot of legitimate SSL protected Paypal page within a rogue webpage</td>
<td>50 (4.7)</td>
<td>50 (4.3)</td>
</tr>
<tr>
<td>Ameritrade</td>
<td>Spoof</td>
<td>URL (ameritrading.com)</td>
<td>50 (4.2)</td>
<td>50 (3.9)</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Spoof</td>
<td>Rogue popup window on top of legitimate BOFA homepage, padlock in content</td>
<td>64 (4.2)</td>
<td>36 (4.4)</td>
</tr>
<tr>
<td>Bank of the West</td>
<td>Spoof</td>
<td>URL (IP address), urgent anti-fraud warnings (requests large amount of personal data)</td>
<td>68 (4.8)</td>
<td>32 (4.4)</td>
</tr>
<tr>
<td>USBank</td>
<td>Spoof</td>
<td>URL (IP address), padlock in content, security warnings, identity verification (requests large amount of personal data)</td>
<td>68 (4.1)</td>
<td>32 (4.3)</td>
</tr>
<tr>
<td>Ebay</td>
<td>Spoof</td>
<td>URL (IP address), account verification (requests large amount of personal data)</td>
<td>68 (4.4)</td>
<td>32 (4.0)</td>
</tr>
<tr>
<td>Yahoo</td>
<td>Spoof</td>
<td>URL (center.yahoo-security.net), account verification (requests large amount of personal data)</td>
<td>77 (3.0)</td>
<td>23 (4.2)</td>
</tr>
<tr>
<td>NCUA</td>
<td>Spoof</td>
<td>URL (IP address), padlock in content, account verification (requests large amount of personal data)</td>
<td>82 (4.5)</td>
<td>18 (4.3)</td>
</tr>
<tr>
<td>Ebay</td>
<td>Real</td>
<td>SSL protected login page, TRUSTe logo</td>
<td>86 (4.4)</td>
<td>14 (4.0)</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Real</td>
<td>Login page on non-SSL homepage, padlock in content</td>
<td>86 (4.4)</td>
<td>14 (3.3)</td>
</tr>
<tr>
<td>Tele-Bears</td>
<td>Real</td>
<td>SSL protected login page</td>
<td>91 (4.7)</td>
<td>9 (4.5)</td>
</tr>
<tr>
<td>(Student Accounts)</td>
<td></td>
<td>Login page on non-SSL homepage, padlock in content</td>
<td>91 (4.6)</td>
<td>9 (3.0)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Real</td>
<td>Login page on non-SSL homepage, padlock in content</td>
<td>100 (4.0)</td>
<td>0 (N/A)</td>
</tr>
</tbody>
</table>

Table 2: Security or spoofing strategy employed by each site (spoof sites shown with white background, real sites gray).
Don’t Use Filler Slides

- Don’t present slides that you don’t expect your audience to read anyway
- What’s the point?
The Results of Wish-list Attacks

- Neutral Information Toolbar: 45%
- SSL Verification Toolbar: 38%
- System Decision Toolbar: 32%
Miscellaneous

- Don’t use 3D if there is no need
- Use consistent way for emphasizing
  - This finding is important, so is this one and that one
- A picture often explains a concept more easily than many words
- Be careful about color schemes, animations,…
- Spell check your slides, check your grammar
- Ideally, your slides do not need your spoken part to be understandable
Miscellaneous (cont.)

- Be polite
  - “Thank you for your attention.”
  - “That’s a good point. Bla bla...”