PHISHING

Ingredients for phishing

1. Users conditioned to enter passwords
2. A convincing spoof of the user interface
PHISHING RISK

1. When are users conditioned to enter their passwords or payment information?
2. Can those scenarios be convincingly spoofed?
THREAT MODEL

• Sender ⇒ Target

• **Direct attack:** false control transfer

• **Man-in-the-middle attack:** subverted control transfer
MOBILE PHISHING

- Phones lack trustworthy security indicators
- Interaction between web & mobile apps
- Mobile login screens are simple
OUR APPROACH

1. Survey how applications condition users
   - 50 most popular Android & iOS apps
   - 85 popular web sites on Android, iOS

2. Evaluate avenues for spoofing
   - Direct
   - Man-in-the-middle
CONTROL TRANSFERS

- Mobile sender ➔ Mobile target
- Mobile sender ➔ Web target
- Web sender ➔ Mobile target
- Web sender ➔ Web target
MOBILE ⇒ MOBILE

- Social sharing
- Upgrades via store
- Music purchases
- Game credits (iOS)
### MOBILE ⇒ MOBILE

<table>
<thead>
<tr>
<th>Target</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile app</td>
<td>56%</td>
<td>72%</td>
</tr>
<tr>
<td>Password-protected</td>
<td>36%</td>
<td>60%</td>
</tr>
<tr>
<td>Payment</td>
<td>10%</td>
<td>34%</td>
</tr>
</tbody>
</table>
M ⇒ M: DIRECT ATTACK

Attack App

Spoof Page

Real Page

W2SP 2011 - Phishing on Mobile Devices
M ⇒ M: MITM ATTACK

- Scheme squatting
  - Register for another app’s URI scheme
  - Weak: detectable by user, reviewers

- Task interception
  - Poll task list, pop up when target opens
  - Unnoticeable by users
CONTROL TRANSFERS

- Mobile sender ⇒ Mobile target
- Mobile sender ⇒ Web target
- Web sender ⇒ Mobile target
- Web sender ⇒ Web target
MOBILE ⇒ WEB

- Mechanisms
  - Links to the browser
  - Embedded web content
- Reasons
  - Social sharing
  - Not much payment
## MOBILE ⇒ WEB

<table>
<thead>
<tr>
<th></th>
<th>Browser target</th>
<th></th>
<th>Embedded target</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td><strong>Android</strong></td>
<td><strong>iOS</strong></td>
<td><strong>Target</strong></td>
<td><strong>Android</strong></td>
</tr>
<tr>
<td>Web site</td>
<td>30%</td>
<td>18%</td>
<td>Web site</td>
<td>16%</td>
</tr>
<tr>
<td>Password-protected</td>
<td>3%</td>
<td>4%</td>
<td>Password-protected</td>
<td>8%</td>
</tr>
<tr>
<td>Payment</td>
<td>2%</td>
<td>-</td>
<td>Payment</td>
<td>2%</td>
</tr>
</tbody>
</table>
M ⇒ W: DIRECT ATTACK

- Link to web browser
- Send the user to a fake browser
- Open in real browser, hide/fake URL bar
- Embedded content
- Eavesdrop on credentials given to embedded content
M ⇒ W: DIRECT ATTACK

Real Browser

Spoof Browser

W2SP 2011 - Phishing on Mobile Devices
M ⇒ W: MITM ATTACK

- **Attack**: alter target of form on HTTP page
- **Defense**: forms only on HTTPS pages
- **Attack**: alter links to HTTPS pages
CONTROL TRANSFERS

- Mobile sender $\Rightarrow$ Mobile target
- Mobile sender $\Rightarrow$ Web target
- Web sender $\Rightarrow$ Mobile target
- Web sender $\Rightarrow$ Web target
WEB ⇒ MOBILE

- **Mechanisms**
  - tel://18005555555
  - market://details?id=123

- **Reasons**
  - mailto, Twitter
  - Install the app version
### WEB ⇒ MOBILE

#### Core mobile apps

<table>
<thead>
<tr>
<th>Target</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core mobile application</td>
<td>38%</td>
<td>47%</td>
</tr>
<tr>
<td>Password-protected</td>
<td>22%</td>
<td>41%</td>
</tr>
<tr>
<td>Payment</td>
<td>6%</td>
<td>25%</td>
</tr>
</tbody>
</table>

#### Any mobile apps

<table>
<thead>
<tr>
<th>Target</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any mobile application</td>
<td>49%</td>
<td>48%</td>
</tr>
<tr>
<td>Password-protected</td>
<td>38%</td>
<td>42%</td>
</tr>
<tr>
<td>Payment</td>
<td>6%</td>
<td>25%</td>
</tr>
</tbody>
</table>

W2SP 2011 - Phishing on Mobile Devices
W $\Rightarrow$ M: DIRECT ATTACK

- Hide the browser chrome and mimic app
  - In Android, only detectable if user hits the “Menu” button
  - Not possible in iOS unless user has “installed” the page
**W ⇒ M: DIRECT ATTACK**

Real App

Spoof App (In Browser)
W ⇒ M: MITM ATTACK

- Scheme squatting
- Task interception
CONTROL TRANSFERS

- Mobile sender \(\Rightarrow\) Mobile target
- Mobile sender \(\Rightarrow\) Web target
- Web sender \(\Rightarrow\) Mobile target
- Web sender \(\Rightarrow\) Web target
WEB ⇒ WEB: DIRECT

- Spoof or hide the URL bar [Niu et al.]
- Eased how it scrolls
- Reduced URL loading/rendering time
WEB ⇒ WEB: MITM

- Subvert all HTTP pages so that links to HTTPS are never trustworthy
- User won’t be warned by the URL bar
PREVENTION

- Permanently application identity indicator
- Embedded web content still a problem
- Trusted password entry mechanism
- Usability?
- Adoption?
Questions?

apf@cs.berkeley.edu