Resurrecting Duckling

Imprinting on Mother:
  Device shares key on 1\textsuperscript{st} contact with controller

Metempsychosis:
  Upon death, soul progresses to a new body

Reverse metempsychosis:
  Upon death, new soul can enter the body

Resistance to assassination:
  Only mother can kill her ducklings

Escrowed seppuku:
  Manufacturer can kill too
Cashier-as-a-Service (CAAS)

Ecommerce workflow:
1. Shopper surfs Merchant’s site
2. Shopper sends over …/place_order.html
3. Merchant sends back redir. to CAAS.com
4. Shopper interacts with CAAS
5. CAAS interacts with Merchant
6. CAAS redirects shopper back to Merchant
CAAS Attack #1

S→M: place_order.html
   [M inserts ID and price into database; status=PENDING]

M→S→C: get_payment?orderID=X&price=Y
   [C records payment info, generates transaction # T]

C→S→M: finish?transID=T
   [M contacts C for identifier X associated w/ T]
   [M retrieves orderID=X from database;
    if order status = PENDING → mark as PAID; ship X]
CAAS Attack #2

S→M: place_order.html
   [M inserts ID and price into database; status=PENDING]

M→S→C: get_payment?SIGN_M(ID=X,price=Y)
   [C verifies signature; records payment info, generates # T]

C→S→M: finish?SIGN_C(ID=X,price=Y,PAID)
   [M verifies signature and PAID is indicated]
   [M retrieves orderID=X from database;
     if order status = PENDING → mark as PAID; ship X]
CAAS Attack #2

S→M: place_order.html

[M inserts ID and price into database; status=PENDING]

M→S→C: get_payment?SIGN_{M}(ID=X, price=Y)

[C verifies signature; records payment info, generates # T]

C→S→M: finish?SIGN_{C}(ID=X, price=Y, PAID)

[M verifies signature and PAID is indicated]

[M retrieves orderID=X from database;
   if order status = PENDING → mark as PAID; ship X]
Fix for CAAS Attack #2

S→M: place_order.html
   \([M \text{ inserts } ID \text{ and price into database; status=}\text{PENDING}\]\)

M→S→C: get_payment?
   \(\text{SIGN}_M(ID=X, price=Y, merch=M)\)
   \([C \text{ verifies signature; records payment info, generates } \# T]\)

C→S→M: finish?
   \(\text{SIGN}_C(ID=X, price=Y, merch=M, PAID}\)
   \([M \text{ verifies signature and PAID is indicated, etc.}]\)
   \([M \text{ retrieves orderID}=X \text{ from database; if order status = PENDING } \rightarrow \text{ mark as PAID; ship X}]\)
Better Fix for CAAS Attack #2

S→M:  place_order.html
      [M inserts ID and price into database; status=PENDING]

M→S→C:  get_payment?
         SIGN_M(ID=X,price=Y,merch=M,shop=S)
         [C verifies signature; records payment info, generates # T]

C→S→M:  finish?
         SIGN_C(ID=X,price=Y,merch=M,shop=S,PAID)
         [M verifies signature and PAID is indicated, etc.]
         [M retrieves orderID=X from database;
           if order status = PENDING → mark as PAID; ship X]
CAAS Attack #3

...  
S→M: checkout?ID=X&price=Y
  [M sets session_status[S] ←
   confirm_with_C(shop=S,ID=X,price=Y)]

M→S→M: update_status?SIGN_M(ID=X)
  [M validates signature;
   if session_status[S]=CONFIRMED →
   session_status[S]=PAID; ship X]
CAAS Attack #3

S→M: checkout?ID=\(X_1\)\&price=\(Y_1\)

\[M \text{ sets } session\_status[S] \leftarrow \]
\[\text{confirm\_with\_C}(\ldots,X_1,Y_1) \leftarrow \text{FAILED}\]

M→S: update\_status?SIGN_M(ID=\(X_1\))
CAAS Attack #3

S→M: checkout?ID=X_1&price=Y_1

[M sets session_status[S] ←
confirm_with_C(...,X_1,Y_1)←FAILED]

M→S: update_status?SIGN_M(ID=X_1)

S→M: checkout?ID=X_2&price=Y_2 \ Y_2 \ll Y_1

[M sets session_status[S] ←
confirm_with_C(...,X_2,Y_2)←CONFIRMED]
CAAS Attack #3

S→M: checkout?ID=X₁&price=Y₁

[M sets session_status[S] ←
   confirm_with_C(...,X₁,Y₁)←FAILED]

M→S: update_status?SIGNₘ(ID=X₁)

S→M: checkout?ID=X₂&price=Y₂  Y₂ ≪ Y₁

[M sets session_status[S] ←
   confirm_with_C(...,X₂,Y₂)←CONFIRMED]

S→M: update_status?SIGNₘ(ID=X₁)

[M validates signature;
   if session_status[S] = CONFIRMED →
   session_status[S] = PAID; ship X₁]
Figure 2: Difficult but correctly transcribed examples from the internal street numbers dataset.
Figure 3: Examples of incorrectly transcribed street numbers from the large internal dataset.
Figure 4: Examples of images from the hard CAPTCHA puzzles dataset.
Asirra

Asirra is a human interactive proof that asks users to identify photos of cats and dogs. It's powered by over two million photos from our unique partnership with Petfinder.com. Protect your web site with Asirra — free!

Please click on the images that show cats:

- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me
- adopt me

Score Test
Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business efficiency now!

Follow these steps:
- Register
- Login and follow the link inside to load funds to your account.
  Your request will be processed ASAP.

You pay for correctly recognized CAPTCHAs only
The price is $2 for 1000 CAPTCHAs. We accept payments from $10.

If you use a third-party software the price could be different, contact the software vendor for more information.

Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?
We have no restrictions about IP: with DeCaptcha you can bypass CAPTCHA from as many IPs as you need.

Hi. I need to crack captcha. Do you provide a captcha decoders?
DeCaptcha CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones
<table>
<thead>
<tr>
<th>Language</th>
<th>Example</th>
<th>AG</th>
<th>BC</th>
<th>BY</th>
<th>CB</th>
<th>DC</th>
<th>IT</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>one two three</td>
<td>51.1</td>
<td>37.6</td>
<td>4.76</td>
<td>40.6</td>
<td>39.0</td>
<td>62.0</td>
<td>39.2</td>
</tr>
<tr>
<td>Chinese (Simp.)</td>
<td></td>
<td>48.4</td>
<td>31.0</td>
<td>0.00</td>
<td>68.9</td>
<td>26.9</td>
<td>35.8</td>
<td>35.2</td>
</tr>
<tr>
<td>Chinese (Trad.)</td>
<td></td>
<td>52.9</td>
<td>24.4</td>
<td>0.00</td>
<td>63.8</td>
<td>30.2</td>
<td>33.0</td>
<td>34.1</td>
</tr>
<tr>
<td>Spanish</td>
<td>uno dos tres</td>
<td>1.81</td>
<td>13.8</td>
<td>0.00</td>
<td>2.90</td>
<td>7.78</td>
<td>56.8</td>
<td>13.9</td>
</tr>
<tr>
<td>Italian</td>
<td>uno due tre</td>
<td>3.65</td>
<td>8.45</td>
<td>0.00</td>
<td>4.65</td>
<td>5.44</td>
<td>57.1</td>
<td>13.2</td>
</tr>
<tr>
<td>Tagalog</td>
<td>isá dalawá tatló</td>
<td>0.00</td>
<td>5.79</td>
<td>0.00</td>
<td>0.00</td>
<td>7.84</td>
<td>57.2</td>
<td>11.8</td>
</tr>
<tr>
<td>Portuguese</td>
<td>um dois três</td>
<td>3.15</td>
<td>10.1</td>
<td>0.00</td>
<td>1.48</td>
<td>3.98</td>
<td>48.9</td>
<td>11.3</td>
</tr>
<tr>
<td>Russian</td>
<td>один два три</td>
<td>24.1</td>
<td>0.00</td>
<td>0.00</td>
<td>11.4</td>
<td>0.55</td>
<td>16.5</td>
<td>8.76</td>
</tr>
<tr>
<td>Tamil</td>
<td>ஒன் இரண்டு மூன்</td>
<td>2.26</td>
<td>21.1</td>
<td>3.26</td>
<td>0.74</td>
<td>12.1</td>
<td>5.36</td>
<td>7.47</td>
</tr>
<tr>
<td>Dutch</td>
<td>een twee drie</td>
<td>4.09</td>
<td>1.36</td>
<td>0.00</td>
<td>0.00</td>
<td>1.22</td>
<td>31.1</td>
<td>6.30</td>
</tr>
<tr>
<td>Hindi</td>
<td>एक दो तीन</td>
<td>10.5</td>
<td>5.38</td>
<td>2.47</td>
<td>1.52</td>
<td>6.30</td>
<td>9.49</td>
<td>5.94</td>
</tr>
<tr>
<td>German</td>
<td>eins zwei drei</td>
<td>3.62</td>
<td>0.72</td>
<td>0.00</td>
<td>1.46</td>
<td>0.58</td>
<td>29.1</td>
<td>5.91</td>
</tr>
<tr>
<td>Malay</td>
<td>satu dua tiga</td>
<td>0.00</td>
<td>1.42</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>29.4</td>
<td>5.23</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>molt hai ba</td>
<td>0.46</td>
<td>2.07</td>
<td>0.00</td>
<td>0.00</td>
<td>1.74</td>
<td>18.1</td>
<td>3.72</td>
</tr>
<tr>
<td>Korean</td>
<td>일 이 삼</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>20.2</td>
<td>3.37</td>
</tr>
<tr>
<td>Greek</td>
<td>ένα δύο τρία</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.5</td>
<td>2.65</td>
</tr>
<tr>
<td>Arabic</td>
<td>ثلاثة اثنين واحد</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.3</td>
<td>2.56</td>
</tr>
<tr>
<td>Bengali</td>
<td>এক দুই তিন</td>
<td>0.45</td>
<td>9.89</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.72</td>
</tr>
<tr>
<td>Kannada</td>
<td>ಒಂದು ಇೂರು ಇಪ್ಪತ್ತು</td>
<td>0.91</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>6.14</td>
<td>1.26</td>
</tr>
<tr>
<td>Klingon</td>
<td></td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.12</td>
<td>0.19</td>
<td>0.19</td>
</tr>
<tr>
<td>Farsi</td>
<td></td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.08</td>
</tr>
</tbody>
</table>

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.