Act for Affordable Data Care

Saikat Guha, Srikanth Kandula

Microsoft Research

HotNets-XI
Data Breaches Today

- July 2012: Yahoo! — 400K passwords
- June 2012: LinkedIn — 6M passwords
- May 2011: Sony — 100M+ passwords, CC#
Data Breaches Today

Data source: Privacy Rights Clearinghouse

Saikat Guha, Srikanth Kandula Act for Affordable Data Care
Data Breaches Today

Data source: Privacy Rights Clearinghouse

Saikat Guha, Srikanth Kandula  
Act for Affordable Data Care
User Behavior Today

**Credit and Debit Cards**
C1 Online transactions (monthly)
C2 Sites credit-card saved at
C3 Monthly statements checked (yearly)

**Data Protection**
D1 Sites persistently logged into
D2 Public devices used (monthly)
D3 Identity document emailed (last year)
D4 Sensitive number emailed (last year)

**Loss**
L1 Fraudulent transactions (last two years)
L2 Transactions above resulting in money loss

**Password Security**
P1 Bank passwords changed (last year)
P2 Banks with same password
P3 Non-bank sites with bank password
P4 Email passwords changed (last year)
P5 Non-email sites with email password

**Physical Security**
H1 Device left unlocked and unattended (last year)
H2 Phones lost or misplaced (last year)
H3 Laptop/tablet lost or misplaced (last year)
H4 Wallet/keys lost or misplaced (last year)
H5 Items above that weren’t recovered

Saikat Guha, Srikanth Kandula  
Act for Affordable Data Care
Data Breaches Today

New technology is NOT the solution

- Cryptographic hashing: 30y+ old
- Salting hashes: 30y+ old
- Encrypted FS: commercialized 12y+ ago
- Single-use CC#: commercialized 12y+ ago
- Password managers: freeware 5y+ ago

New policies or regulation is NOT the solution

- Yahoo!, LinkedIn, Sony have good policies
- Past regulation ineffective (spam, cookies, . . . )
What are we Missing?
What are we Missing?

Money
Crazy Idea: Data-Breach Insurance

- **Underwrite damages** for a small premium
  - Users: fraudulent charges, ID-theft monitoring, ...
  - Enterprises: lawsuits, cleanup, ...
  - *Safety-net.* No changes needed.

- **Create an incentive to improve**
  - Lower premiums for good behavior
  - Data driven. *Individualized.*
Crazy Idea: Data-Breach Insurance

- **Underwrite damages** for a small premium
  - Users: fraudulent charges, ID-theft monitoring, ...
  - Enterprises: lawsuits, cleanup, ...
  - *Safety-net.* No changes needed.

- **Create an incentive to improve**
  - Lower premiums for good behavior
  - Data driven. *Individualized.*
Insurance 101

- **Scale**: Many prospective clients
- **Non-Catastrophic**: No hurricane Katrina
- **Loss**: Large enough to justify premium
- **Premium**: Low enough that clients pay
- **Incident**: Loss event can be identified
- **Accident**: Outside of client’s control
- **Risk-Assess**: Loss probability and magnitude
Insurance 101

- **Scale**: Many prospective clients
- **Non-Catastrophic**: No hurricane Katrina
- **Loss**: Large enough to justify premium
- **Premium**: Low enough that clients pay
- **Incident**: Loss event can be identified
- **Accident**: Outside of client’s control
- **Risk-Assess**: Loss probability and magnitude
<table>
<thead>
<tr>
<th>Response</th>
<th>all</th>
<th>victims (Δ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1: Online transactions (monthly) ≥ 4</td>
<td>48%</td>
<td>67% (+18%)</td>
</tr>
<tr>
<td>H4: Wallet/keys lost or misplaced (last year) &gt; 0</td>
<td>18%</td>
<td>31% (+12%)</td>
</tr>
<tr>
<td>C2: Sites credit-card saved at ≥ 4</td>
<td>30%</td>
<td>42% (+12%)</td>
</tr>
<tr>
<td>D1: Sites persistently logged into &gt; 0</td>
<td>75%</td>
<td>87% (+11%)</td>
</tr>
<tr>
<td>D3: Identity document emailed (last year) &gt; 0</td>
<td>29%</td>
<td>40% (+11%)</td>
</tr>
<tr>
<td>H5: Items above that weren’t recovered &gt; 0</td>
<td>12%</td>
<td>20% (+8%)</td>
</tr>
<tr>
<td>P5: Non-email sites with email password ≥ 4</td>
<td>21%</td>
<td>28% (+7%)</td>
</tr>
<tr>
<td>C3: Monthly statements checked (yearly) ≥ 4</td>
<td>78%</td>
<td>85% (+6%)</td>
</tr>
<tr>
<td>D4: Sensitive number emailed (last year) is 1–3</td>
<td>16%</td>
<td>23% (+6%)</td>
</tr>
<tr>
<td>D2: Public devices used (monthly) &gt; 0</td>
<td>32%</td>
<td>37% (+5%)</td>
</tr>
<tr>
<td>P4: Email passwords changed (last year) is 1–3</td>
<td>50%</td>
<td>55% (+5%)</td>
</tr>
<tr>
<td>P1: Bank passwords changed (last year) is 0</td>
<td>43%</td>
<td>37% (-5%)</td>
</tr>
<tr>
<td>P2: Banks with same password &gt; 0</td>
<td>24%</td>
<td>30% (+5%)</td>
</tr>
</tbody>
</table>
Correlating User Behavior with Loss

Physical Security
- H4: Wallet/keys lost or misplaced (last year)

Credit and Debit Cards
- C1: Online transactions (monthly)
- C3: Monthly statements checked (yearly)

Data Protection
- D1: Sites persistently logged into
- D2: Public devices used (monthly)
- D3: Identity document emailed (last year)

Loss
- L1: Fraudulent transactions (last two years)
Would users pay? 77% say they would
How much? $20 per year (median)
Profitable for insurance company? Likely
Behavior change? 94% want to
Fraud, Moral hazard? Existing mechanisms
Adverse selection? Also, advantageous
Other mechanisms? Complementary
Make users *act* for data safety
  - Data safety linked directly to money

One crazy idea: **Data Breach Insurance**
  - but is it crazy enough to work?

Technology: *individualized risk-assessment*
  - Immediate feedback for bad behavior
  - Ongoing work
Putting Money Where Mouth Is

- **Monitor user behavior** *privacy-preserving; in-browser*
  - Track password re-use
  - Opening unknown attachments
  - Not locking computer

- **Offer different incentives to change**
  - Gentle nudge
  - Gamification
  - Social incentives
  - Financial

- **Real data** *from few thousand users*
  - A/B testing
  - Success metric: *change user behavior*