FPSelect: Low-Cost Browser Fingerprints for Mitigating Dictionary Attacks against Web Authentication Mechanisms

ACSAC 2020, December 11, 2020

Nampoina Andriamilanto, Tristan Allard, Gaëtan Le Guelvouit
Context
Passwords suffer from flaws
  - Dictionary attacks: common passwords [6] or reuse [16]
  - Phishing attacks: 12.4 million stolen credentials [12]

Other authentication factors reduces usability [3]
  - User must remember, possess, or do something
Browser fingerprinting [2, 11]
- Collection of browser attributes
- Depending on the web environment
**Issue of Attribute Selection**

- **Adding an attribute**
  - Helps distinguish browsers
  - Reduces usability

- **Hundreds of attributes are available [2, 11, 13]**
  - Collecting them all is unpractical (e.g., taking too long to collect)

- **Previous works**
  - Use the well-known attributes [2, 11, 15]
  - Iteratively pick attributes [7, 8, 9, 17]
  - Evaluate every possible set [4]
Attribute Selection Framework
The attacker knows a **fingerprint** distribution
- Submits the **β-most common** fingerprints

**Example**
- $β=2$
- $f_1$ and $f_2$ are submitted
- The sensitivity is of $4/7$

<table>
<thead>
<tr>
<th>$F$</th>
<th>PMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_1$</td>
<td>0.40</td>
</tr>
<tr>
<td>$f_2$</td>
<td>0.20</td>
</tr>
<tr>
<td>$f_3$</td>
<td>0.10</td>
</tr>
<tr>
<td>$f_4$</td>
<td>0.10</td>
</tr>
<tr>
<td>$f_5$</td>
<td>0.10</td>
</tr>
<tr>
<td>$f_6$</td>
<td>0.05</td>
</tr>
<tr>
<td>$f_7$</td>
<td>0.05</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$U$</th>
<th>$F$</th>
<th>Spoofed</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1$</td>
<td>$f_2$</td>
<td>●</td>
</tr>
<tr>
<td>$u_2$</td>
<td>$f_1$</td>
<td>●</td>
</tr>
<tr>
<td>$u_3$</td>
<td>$f_4$</td>
<td>○</td>
</tr>
<tr>
<td>$u_4$</td>
<td>$f_2$</td>
<td>●</td>
</tr>
<tr>
<td>$u_5$</td>
<td>$f_3$</td>
<td>○</td>
</tr>
<tr>
<td>$u_6$</td>
<td>$f_5$</td>
<td>○</td>
</tr>
<tr>
<td>$u_7$</td>
<td>$f_1$</td>
<td>●</td>
</tr>
</tbody>
</table>
Verifier has a set $A$ of candidate attributes

Verifier seeks the attribute set
- Satisfies a security level $\alpha$
- At the lowest cost

Attribute set $C \subseteq A$
- $c(C)$: its usability cost (strictly increasing)
- $s(C)$: its sensitivity (decreasing)

$$\arg \min_{C \subseteq A} \{c(C) : s(C) \leq \alpha\}$$
◆ **Greedy exploration algorithm**
  - Expands by adding one attribute
  - Holds $k$-nodes to expand
  - Partial solutions ordered by the usability gain/sensitivity ratio

◆ **Pruning methods**
  - Cost higher than the current minimum $c_{\text{min}}$ (1)
  - Superset of a node satisfying the threshold or (1)

![Lattice Model Diagram](image-url)
◆ **Execution with $k=2$ and $\alpha=0.15$**
  
  - $S$ starts with $k$-empty sets
  - $c_{\text{min}} = 20$ at stage 2
    - $\{2, 3\}$ is not expanded
  - $\{1, 2, 3\}$ is not added to $E$ as it is a superset of $\{1, 2\}$

<table>
<thead>
<tr>
<th>Stage</th>
<th>$E$</th>
<th>$T$</th>
<th>$S$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${{1}, {2}, {3}}$</td>
<td>${}$</td>
<td>${{1}, {3}}$</td>
</tr>
<tr>
<td>2</td>
<td>${{1, 2}, {1, 3}, {2, 3}}$</td>
<td>${{1, 2}}$</td>
<td>${{1, 3}}$</td>
</tr>
<tr>
<td>3</td>
<td>${}$</td>
<td>${{1, 2}}$</td>
<td>${}$</td>
</tr>
</tbody>
</table>
**Usability cost in points**
- Memory size (10 kilobytes = 10K points)
- Collection time (1 second = 10K points)
- Number of changing attributes (1 changing attribute = 10K points)

\[
\text{cost}(C, D) = \gamma \cdot [\text{mem}(C, D), \text{time}(C, D), \text{ins}(C, D)]^T
\]

\(C\) : attribute set
\(D\) : fingerprint dataset
\(\gamma\) : cost weights

**Sensitivity**
- Measured by the verifier
- Attacker knows the fingerprint distribution of the protected users
- Matching function between a submitted and a stored fingerprint
Results
Sample of 30 thousand fingerprints [20, 21]

Verifier and attacker instantiation
- Sensitivity thresholds: 0.001, 0.005, 0.015, 0.025 [1, 3, 14]
- Number of submissions: 1, 4, 16 [5, 18]
- Explored paths: 1 and 3

Matching function
\[ \sum_{a \in A} f[a] \approx^a g[a] > \theta \]

\( f, g \) : submitted and stored fingerprint
\( \approx^a \) : 1 if \( a \) is sufficiently similar between \( f \) and \( g \), else 0
\( \theta \) : matching threshold
\( A \) : the attributes used

Compare FPSelect results with the baselines
- Entropy [8, 9]
- Conditional entropy [7]
A solution for 9 among the 12 cases, due to unreachable sensitivity threshold.

The fingerprints are, on average, up to
- 97 times smaller
- 3,361 times faster to collect
- with 7.2 times fewer changing attributes
◆ ASF-1: three orders of magnitude more attribute sets than the baselines

◆ ASF3: three times more attribute sets than ASF-1
Conclusion
**FPSelect: attribute selection framework**  
- Possibility space as a lattice  
- Greedy exploration algorithm  
- Fingerprints of lower cost than the baselines  
- Higher computation cost

**Future works**  
- Attackers with targeted knowledge  
- Other experimental settings (browser population, measures)
Thank You

Any question ?

tompoariniaina.andriamilanto@irisa.fr
References


