Securing Mediated Trace Access Using Black-box Permutation Analysis

Prateek Mittal (UIUC), Vern Paxson (UCB/ICSI), Robin Sommer (ICSI/LBNL), Mark Winterrowd(UCB)
Thirst for Data

- Need real world network traffic traces
- Traces are sensitive

Institutions reluctant to release anonymized data

Community needs a new approach
Mediated Trace Access

- Bring the experiment to the data

  Analysis Program

  Researcher

  Results

- Often used on an *ad hoc* basis
  - Requires great deal of trust
  - **Key Challenge**: detect information leaks
Black-box Permutation Analysis

- Key observation: Run program multiple times on different inputs and observe the program's behavior

- Black-box approach
  - Nearly arbitrary programs
  - Deterministic, no Internet connectivity

- Key Issues:
  - How to permute?
  - How many times?
  - Output Comparison?

For node sending largest number of bytes: print IP

\[ \text{diff}(\text{output1}, \text{output2}) \]
Policy Driven Permutation

- Providers determine their *privacy policy*
  - Hard problem
- Partial ordering of use cases based on risk
  - Permute IP addresses of all packets, or keep them consistent within flows, or even per-host across flows
Number of Permutation Experiments

- 2 permutation experiments not sufficient

\[
\text{If } (IP \in \{0/8,127/8\}) \{\text{output} = 0\}
\]
\[
\text{elseIf } (IP \in \{128/8,255/8\}) \{\text{output} = 1\}
\]

- Output remains same if

\[
\begin{cases} 
(IP \in \{0/8,127/8\}) & \& (IP' \in \{0/8,127/8\}) \\
(IP \in \{128/8,255/8\}) & \& (IP' \in \{128/8,255/8\})
\end{cases}
\]

- Our approach: detect leaks in a probabilistic fashion
  - Including estimate of information leak
Analytic Model

- Analysis program is a mapping from the input to the output
  - Output may reveal some information about the input
- Program induces a set of input equivalence classes
  - All inputs within a particular equivalence class $R_i$ yield the same output
  - Output $o$ reduces attacker’s uncertainty to the members of the corresponding equivalence class, which we denote as $R_i(o)$
  - $H(I|o) = \log_2 |R_i(o)|$. 

![Diagram of Analytic Model](image-url)
Analytic Model

- Bayesian inference model 1: Based on $x_1, m$

  - Assumption: Equivalence classes of uniform size
    - Good adversarial strategy given no prior information
    - Bayesian inference model 2: Based on $(x_1, x_2, \ldots x_k)$, $m$

  $m = \# \text{ permutation experiments}, \ x_i = \# \text{ permuted outputs equal to } \text{Output}_i$
Output Canonicalization

- **diff** typically not sufficient
  - Output might need processing

- TCPTTrace output

```
1 arg remaining, starting with 'bro-1.2.4.MV.test-input.trace'
Ostermann's tcptrace -- version 6.6.7 -- Thu Nov  4, 2004

139 packets seen, 139 TCP packets traced
elapsed wallclock time: 0:00:00.002607, 53317 pkts/sec analyzed
trace file elapsed time: 6:39:55.727366
TCP connection info:
  1: 75-27-223-38:64840 -128.3.98.148:135 (a2b) 1> 0< (unidirectional)
  2: 222.68.193.70:64840 - 128.3.97.0:23 (c2d) 138> 0< (reset) (unidirectional)
```
Output Templates

- **Output Template**: Researcher supplies an output template that describes an output’s layout in a simple format.
Output Canonicalization

- Ordering within output may change on permutation
- GraphSplicer Output

<table>
<thead>
<tr>
<th></th>
<th>.33</th>
<th>0</th>
<th>.33</th>
<th>.33</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>.66</td>
<td>.16</td>
<td>.16</td>
<td>.16</td>
</tr>
<tr>
<td>.16</td>
<td>.25</td>
<td>.41</td>
<td>.16</td>
<td>.16</td>
</tr>
<tr>
<td>.16</td>
<td>.25</td>
<td>.16</td>
<td>.41</td>
<td>.16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>.41</th>
<th>.16</th>
<th>.16</th>
<th>.25</th>
</tr>
</thead>
<tbody>
<tr>
<td>.16</td>
<td>.41</td>
<td>.16</td>
<td>.25</td>
<td>.25</td>
</tr>
<tr>
<td>.33</td>
<td>.33</td>
<td>.33</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>.16</td>
<td>.16</td>
<td>0</td>
<td>.66</td>
<td>.66</td>
</tr>
</tbody>
</table>

- Audit Trail: Program generates an audit trail that records meta-information about the processing
Output Canonicalization using Audit Trail

Output with Secret data

<table>
<thead>
<tr>
<th>IP1:IP1</th>
<th>IP1:IP2</th>
<th>IP1:IP3</th>
<th>IP1:IP4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP2:IP1</td>
<td>IP2:IP2</td>
<td>IP2:IP3</td>
<td>IP2:IP4</td>
</tr>
<tr>
<td>IP4:IP1</td>
<td>IP4:IP2</td>
<td>IP4:IP3</td>
<td>IP4:IP4</td>
</tr>
</tbody>
</table>

Output with Permuted data

<table>
<thead>
<tr>
<th>IP3':IP3'</th>
<th>IP3':IP4'</th>
<th>IP3':IP1'</th>
<th>IP3':IP2'</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP4':IP3'</td>
<td>IP4':IP4'</td>
<td>IP4':IP1'</td>
<td>IP4':IP2'</td>
</tr>
<tr>
<td>IP1':IP3'</td>
<td>IP1':IP4'</td>
<td>IP1':IP1'</td>
<td>IP1':IP2'</td>
</tr>
<tr>
<td>IP2':IP3'</td>
<td>IP2':IP4'</td>
<td>IP2':IP1'</td>
<td>IP2':IP2'</td>
</tr>
</tbody>
</table>

Audit Trail with Secret data

<table>
<thead>
<tr>
<th>.33</th>
<th>0</th>
<th>.33</th>
<th>.33</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>.66</td>
<td>.16</td>
<td>.16</td>
</tr>
<tr>
<td>.16</td>
<td>.25</td>
<td>.41</td>
<td>.16</td>
</tr>
<tr>
<td>.16</td>
<td>.25</td>
<td>.16</td>
<td>.41</td>
</tr>
</tbody>
</table>

Audit Trail with Permuted data

<table>
<thead>
<tr>
<th>.41</th>
<th>.16</th>
<th>.16</th>
<th>.25</th>
</tr>
</thead>
<tbody>
<tr>
<td>.16</td>
<td>.41</td>
<td>.16</td>
<td>.25</td>
</tr>
<tr>
<td>.33</td>
<td>.33</td>
<td>.33</td>
<td>0</td>
</tr>
<tr>
<td>.16</td>
<td>.16</td>
<td>0</td>
<td>.66</td>
</tr>
</tbody>
</table>
Additional Concerns:

- Covert channels in variable order output
- If privacy policy is satisfied
  - Take an input that lies in the same equivalence class as secret input
  - Ship its output to the researcher
Validating Canonicalization

- Position of trace provider, IP address is sensitive
- LBNL trace (4169 IP addresses, 2.2 million packets)

Analysis Tools
- Honest GraphSplicer
- Modified GraphSplicer

Results (m=50)

<table>
<thead>
<tr>
<th>GraphSplicer version</th>
<th>Honest</th>
<th>Modified (i)</th>
<th>Modified (ii)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equivalent outputs</td>
<td>50</td>
<td>0</td>
<td>26</td>
</tr>
</tbody>
</table>

For node sending largest number of bytes, Print IP
For node sending largest number of bytes, Print 0 if IP lies in 0/8, 127/8 and 1 otherwise
Validating Analytic Model

m=50 (model 1) sufficient for small values of actual leakage

For an actual leakage of 10 bits, m=100 (model 2) predicts 10.2 bits
Summary: Blackbox Permutation Analysis

- Permute sensitive fields in the input trace and analyze resulting changes in the output
  - Nearly arbitrary analysis programs
  - Expressive privacy policies
  - Few permutation rounds
  - Output templates and audit trails
Backup Slides
Incentives for Data Providers?

- Network operators interested to support scientific progress.
- Concrete interest in the outcome of research.
  - Netflix, AOL, Microsoft
- Researchers as data providers
  - Reciprocal access
  - Stronger publications, ACM IMC
- Inclusion in author list
- Trace mediation as a service that is purchased
Advantages over anonymizing a sensitive field

- Greater transparency to data provider
  - Partial declassification of data
  - Expressive fine grained policies
- Feedback to researchers/ catch cheaters
- Infer privacy policy of program / certify programs as non-malicious
Extension to multiple sensitive fields

- **Independent Fields**
  - IP addresses vs packet-capture timestamps
  - A permutation to one field first, keeping the other fixed, and then vice versa.
  - Number of experiments increases only linearly

- **Dependent Fields**
  - TCP timestamp option vs corresponding echo reply
  - IP address vs IP checksum
  - If specified by privacy policy, permute other to maintain semantics