Gone, But Not Forgotten: The Current State of Private Computing

Aseem Rastogi∗ Jun Yuan† Rob Johnson†

∗University of Maryland, College Park
†Stony Brook University
Web browser private mode
Why is the private mode desirable for web browsers?

- People can use web browser private mode to surf online without leaving a trace on their computers.
(MOST LIKELY CASE)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Revenue</td>
<td>830,000</td>
<td>910,200</td>
<td>1,010,000</td>
<td>1,110,200</td>
<td>1,215,000</td>
</tr>
<tr>
<td>Cost of Sales</td>
<td>285,720</td>
<td>314,292</td>
<td>345,722</td>
<td>380,204</td>
<td>418,321</td>
</tr>
<tr>
<td>Gross Profit</td>
<td>540,289</td>
<td>595,908</td>
<td>664,278</td>
<td>730,796</td>
<td>803,675</td>
</tr>
<tr>
<td>Selling, General, Expense</td>
<td>587,033</td>
<td>620,169</td>
<td>658,759</td>
<td>705,195</td>
<td>757,418</td>
</tr>
<tr>
<td>Income Before Taxes</td>
<td>-36,753</td>
<td>-15,261</td>
<td>6,227</td>
<td>24,801</td>
<td>46,177</td>
</tr>
<tr>
<td>Income Taxed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>INCOME AFTER TAXES</td>
<td>-36,753</td>
<td>-15,261</td>
<td>6,227</td>
<td>24,801</td>
<td>46,177</td>
</tr>
</tbody>
</table>
Major Themes

• Opinion #1: Private computing should be implemented as a OS service.

• Opinion #2: Private computing should be efficient, usable and complete.

• Opinion #3: Modern OS features and organization will make it practical to make such a private computing service.
Threat Model

Passive attacker with Local privilege

Can inspect before and after

Can inspect every component of the system

No key-logger and malicious app: Out of the scope
Web browser private mode

• The current issues of web browser private mode

  For the local attack,

  ➢ Software engineering difficulty. Complete mediation by manual code review is hard to achieve.
Web browser private mode

• The current issues of web browser private mode

For the local attack,

➢ Software engineering difficulty. Complete mediation by manual code review is hard to achieve.

➢ The traces left in swap, browser memory, kernel buffers and IPC
• After the process exits, there are still many spots left with private data
Web browser private mode

• The current issues of web browser private mode

  For the local attack,

  ➢ Software engineering difficulty. Complete mediation by manual code review is hard to achieve.

  ➢ The traces left in swap, browser memory, kernel buffers and IPC

  ✔ Extensions and plugins undermines the private mode.
Goals

- Private computing should offer strong assurance of privacy
- Private computing should be lightweight and pay-as-go
- Private computing should not impact user experience
  The bookmarks in the public mode should be accessible in the private browser mode.
- Private computing should support a variety of applications.
The kernel is patched to erase the kernel buffers, Kernel stack, kernel heap upon recycling
Design of PCM

Union FS

Kernel

Proxy
Peripheral Device Drivers
Design of PCM

- Union FS
- lxc
- Proxy
- Peripheral Device Drivers
Design of PCM

Union FS

Kernel

Proxy

Peripheral Device Drivers

IPC
Design of PCM

- Kernel
- Peripheral Device Drivers
- Proxy
- IPC
- lxc
- Union FS
Design of PCM

Union FS

IPC

lxc

Kernel

Proxy

Peripheral Device Drivers
Design of PCM

- Union FS
- lxc
- Peripheral Device Drivers
- Proxy
- IPC
- swap
- write
- Kernel
Upon the exit of the container

The addr space of contained processes are zero-ed.
Upon the exit of the container, kernel buffers are zero-ed.
Upon the exit of the container

The to-be-retained data decided by policy engine is written to underlying fs
The swap which lies in encrypted loop device and to-be-discarded write are automatically discarded once the encryption key is destroyed.
Upon the exit of the container

The proxy of peripheral device
(1) zero while unmapping
(2) dummy output to overwrite the finite buffer
Related work

- Lacuna[2]
- PrivExec[3]


Private computing should be implemented as an OS service.

Private computing should be efficient, usable and complete.

Modern OS features and organization will make it practical to make such a private computing service.