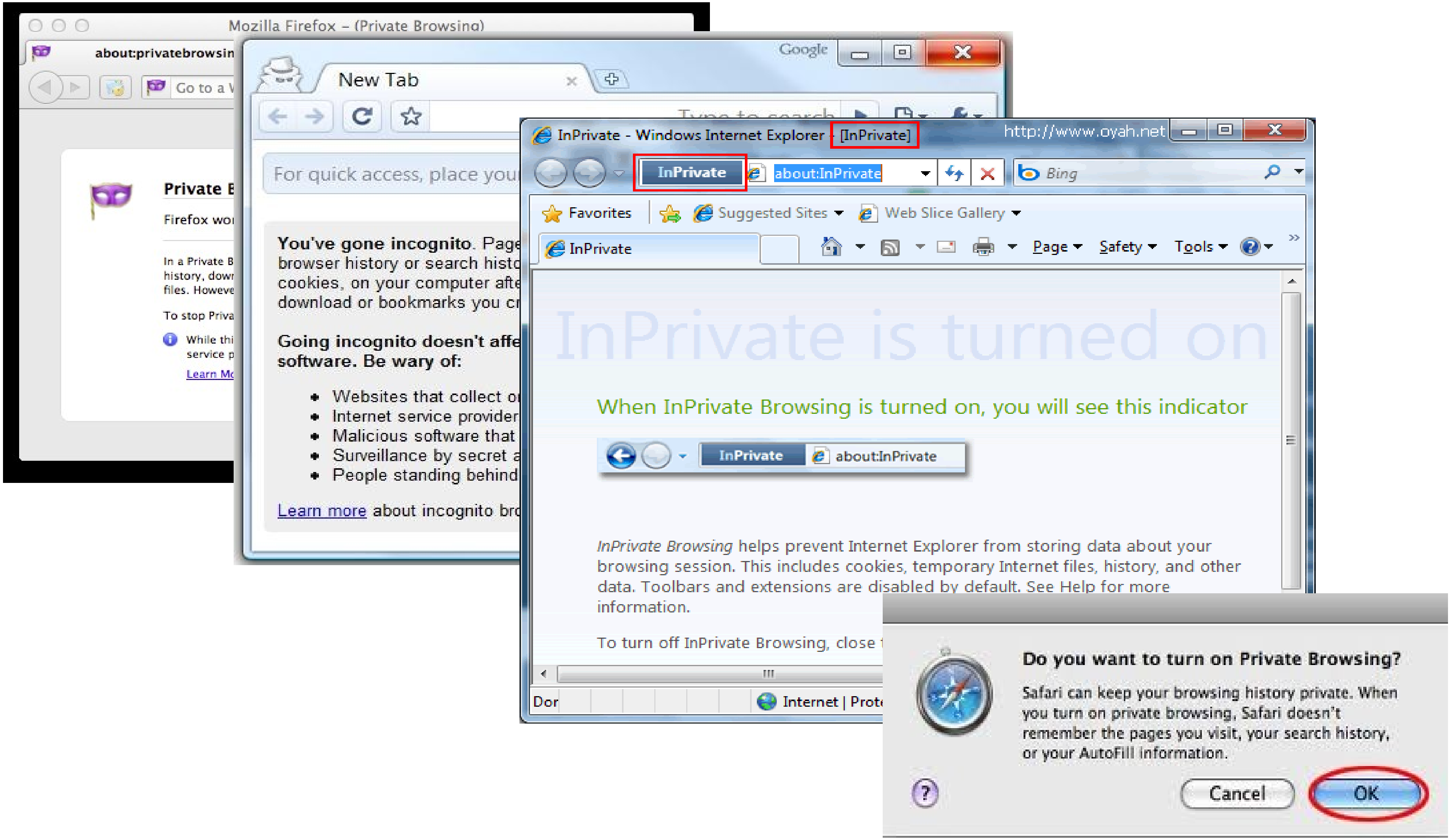
Gone, But Not Forgotten: The Current State of Private Computing

Aseem Rastogi[*] Jun Yuan[†] Rob Johnson[†]

[*]University of Maryland, College Park
[†]Stony Brook University

Web browser private mode



Firefox wo

In a Private B
history, dow
files. Howeve

To stop Priva

While thi
service p
Learn Mo

For quick access, place you

You've gone incognito. Page
browser history or search histo
cookies, on your computer afte
download or bookmarks you c

Going incognito doesn't affe
software. Be wary of:

- Websites that collect o
- Internet service provider
- Malicious software that
- Surveillance by secret a
- People standing behind

Learn more about incognito bro

InPrivate is turned on

When InPrivate Browsing is turned on, you will see this indicator

InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.

To turn off InPrivate Browsing, close t

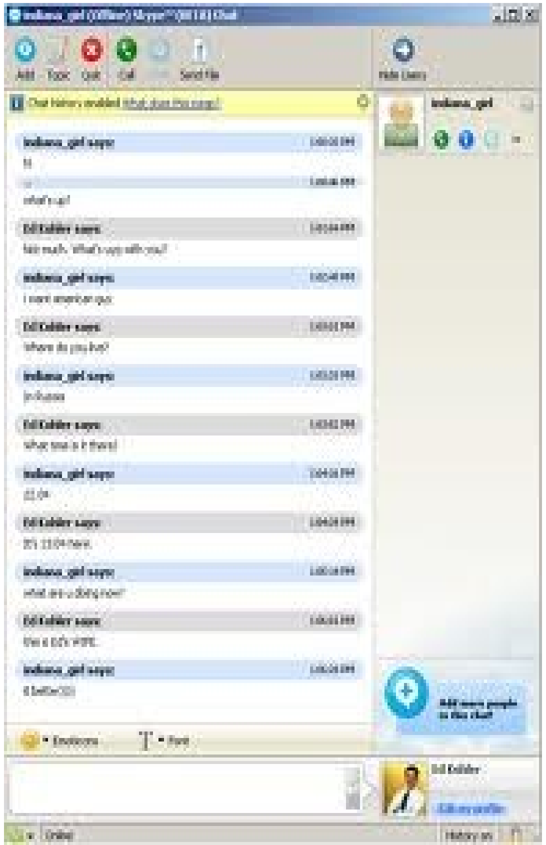
Do you want to turn on Private Browsing?

Safari can keep your browsing history private. When you turn on private browsing, Safari doesn't remember the pages you visit, your search history, or your AutoFill information.

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.

More...



indiana_girl says:

hi

what's up?

Ed Kohler says:

Not much. What's up with you?

indiana_girl says:

i want american guy

Ed Kohler says:

Where do you live?

indiana_girl says:

in Russia

Ed Kohler says:

What time is it there?

indiana_girl says:

22:04

Ed Kohler says:

It's 15:04 here.

indiana_girl says:

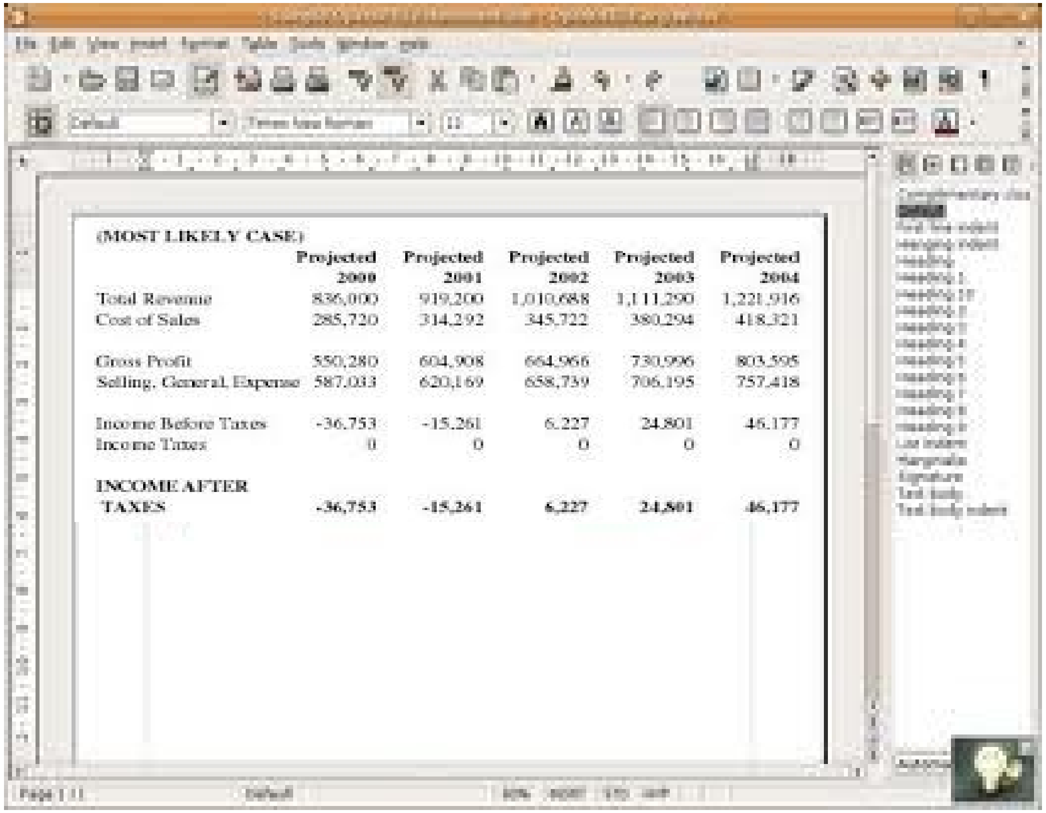
what are u doing now?

Ed Kohler says:

[illegible]

indiana_girl says:

[illegible]



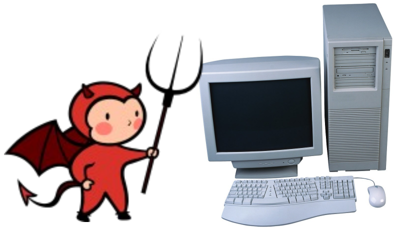
(MOST LIKELY CASE)

	Projected 2000	Projected 2001	Projected 2002	Projected 2003	Projected 2004
Total Revenue	836,000	919,200	1,010,688	1,111,290	1,221,916
Cost of Sales	285,720	314,292	345,722	380,294	418,321
Gross Profit	550,280	604,908	664,966	730,996	803,595
Selling, General, Expense	587,033	620,169	658,739	706,195	757,418
Income Before Taxes	-36,753	-15,261	6,227	24,801	46,177
Income Taxes	0	0	0	0	0
INCOME AFTER TAXES	**-36,753**	**-15,261**	**6,227**	**24,801**	**46,177**

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.

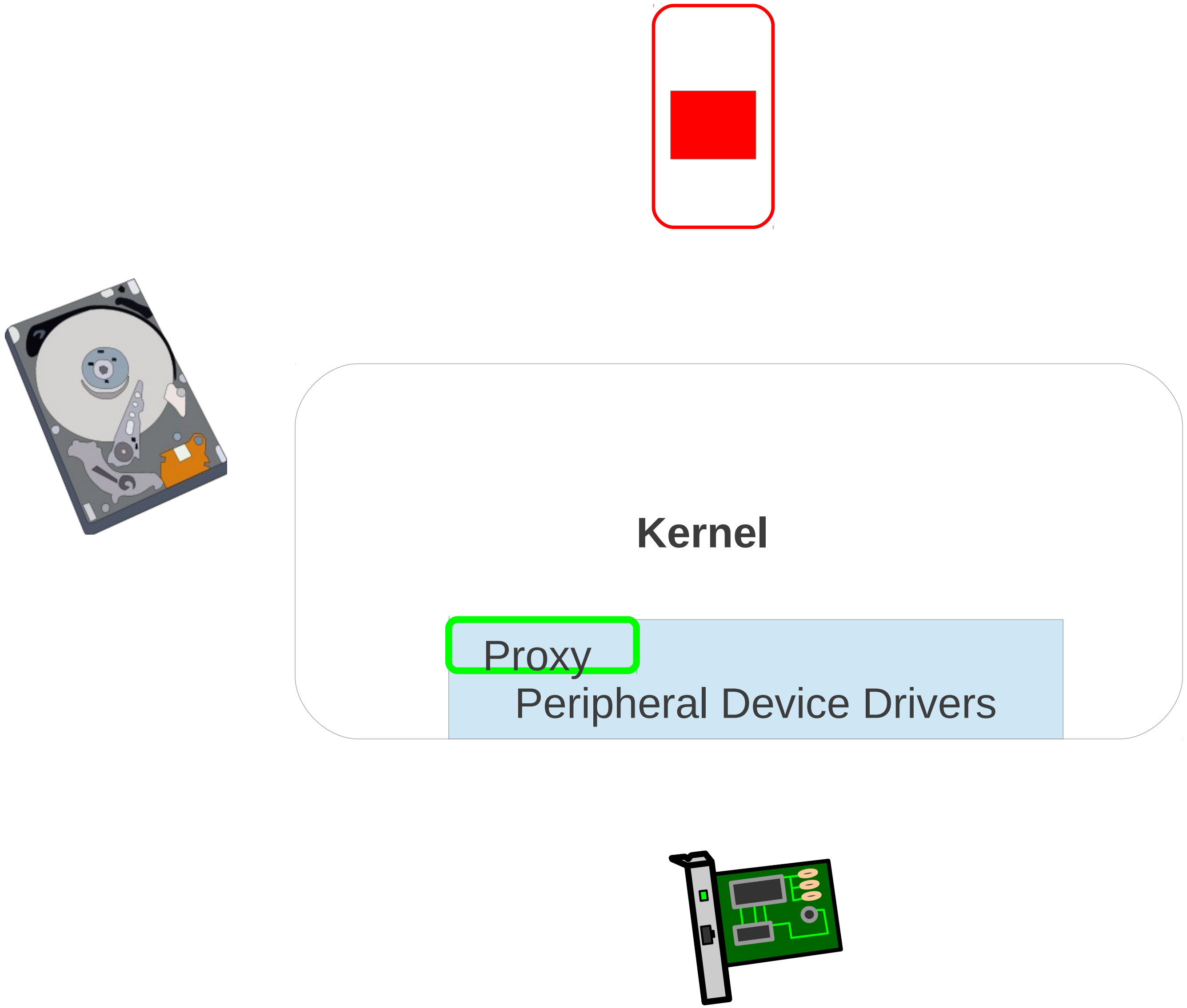
Web browser private mode

- 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

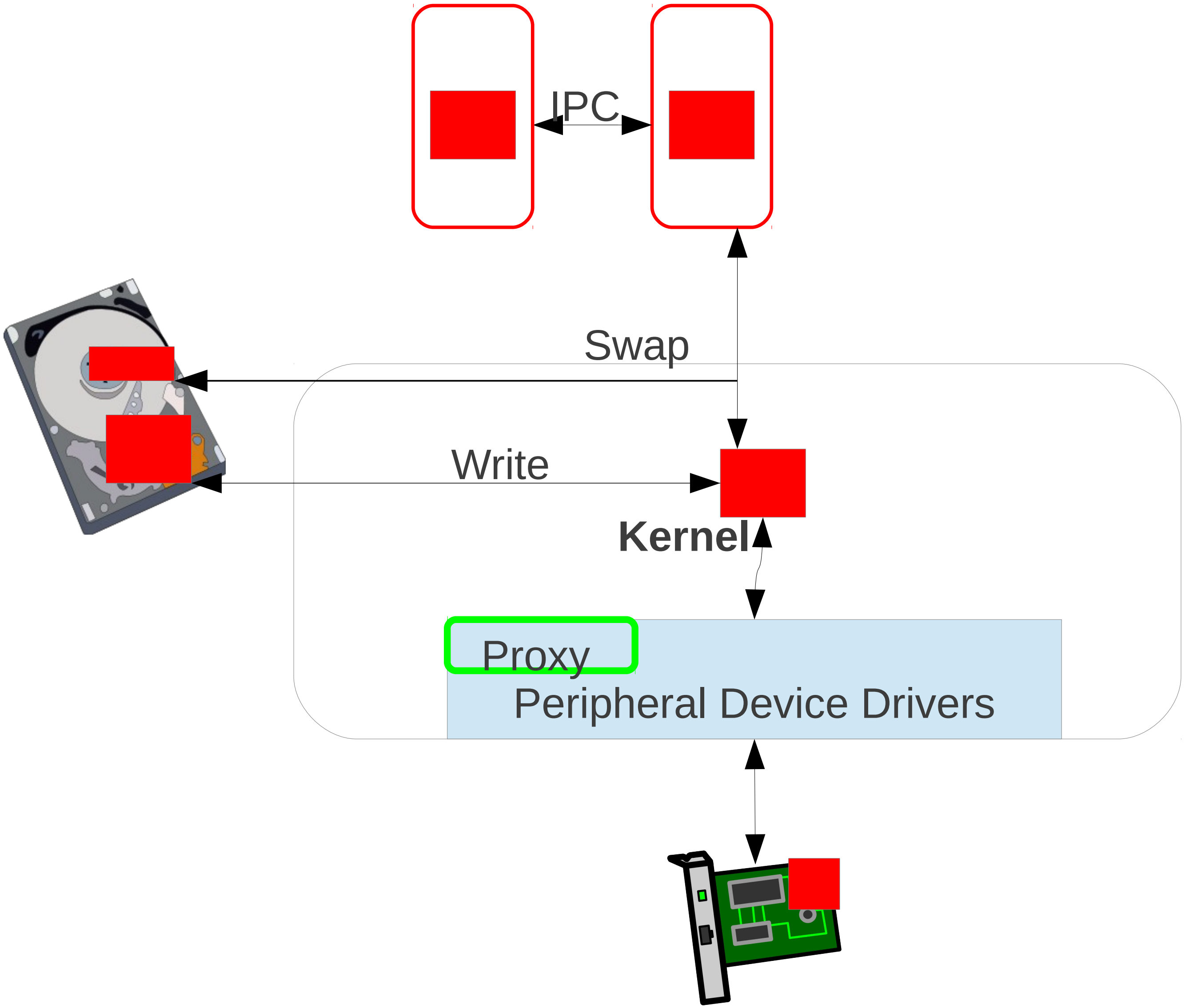
🟥 private data



Kernel

Proxy

Peripheral Device Drivers



IPC

Swap

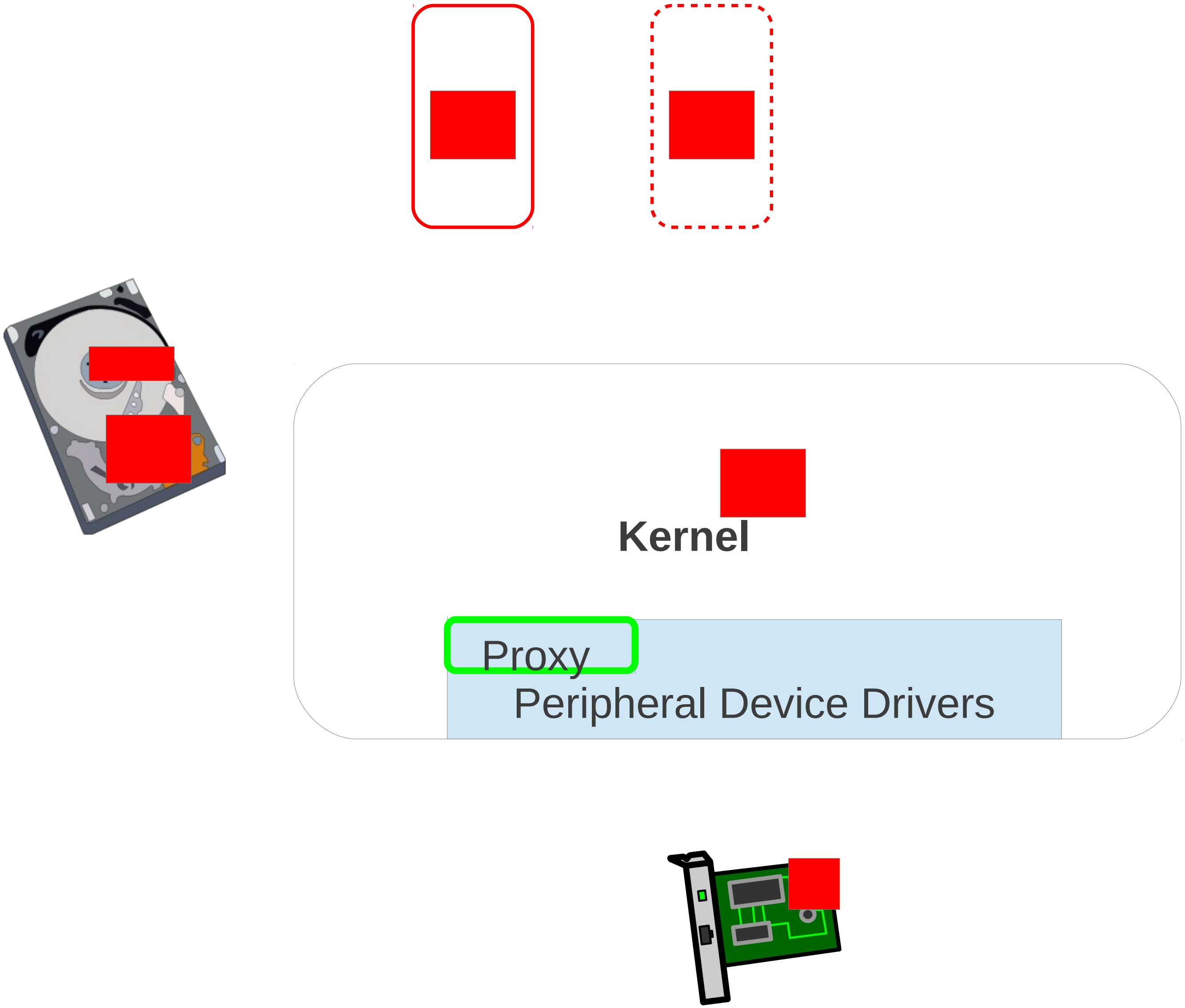
Write

Kernel

Proxy

Peripheral Device Drivers

- After the process exits, there are still many spots left with private data



Kernel

Proxy

Peripheral Device Drivers

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

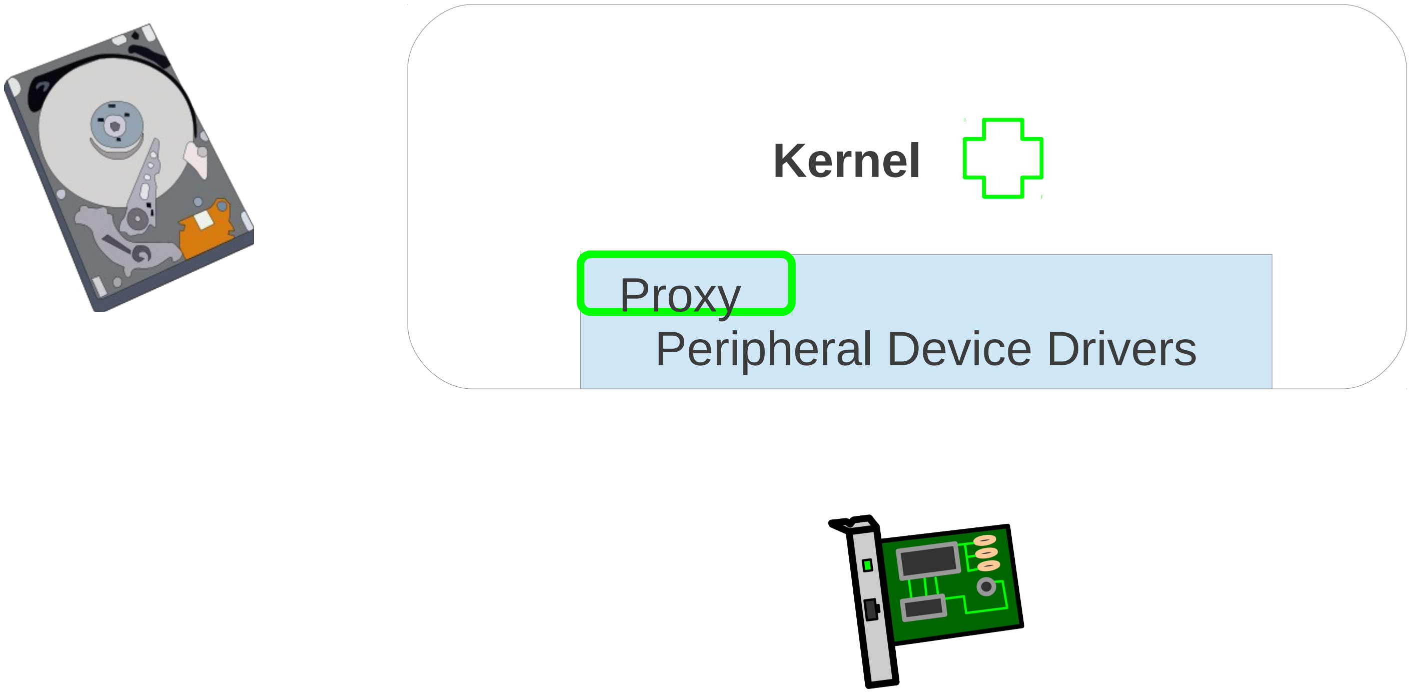
- Private computing should not impact user experience

  The bookmarks in the public mode should be accessible in the private browser mode.

- Private computing should support a variety of applications.

Design of PCM

The kernel is patched to erase the kernel buffers, Kernel stack, kernel heap upon recycling

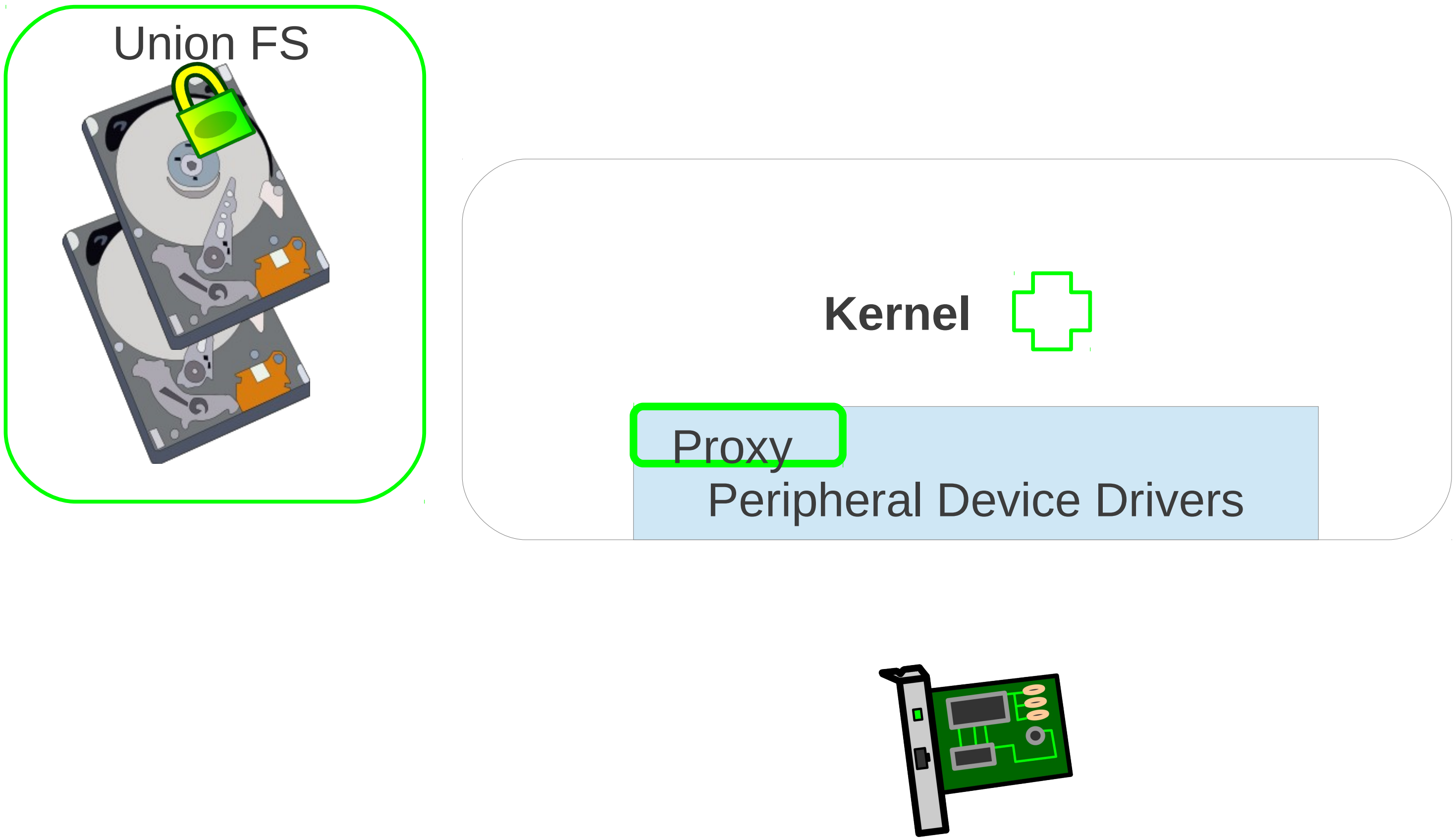


Kernel

Proxy

Peripheral Device Drivers

Design of PCM



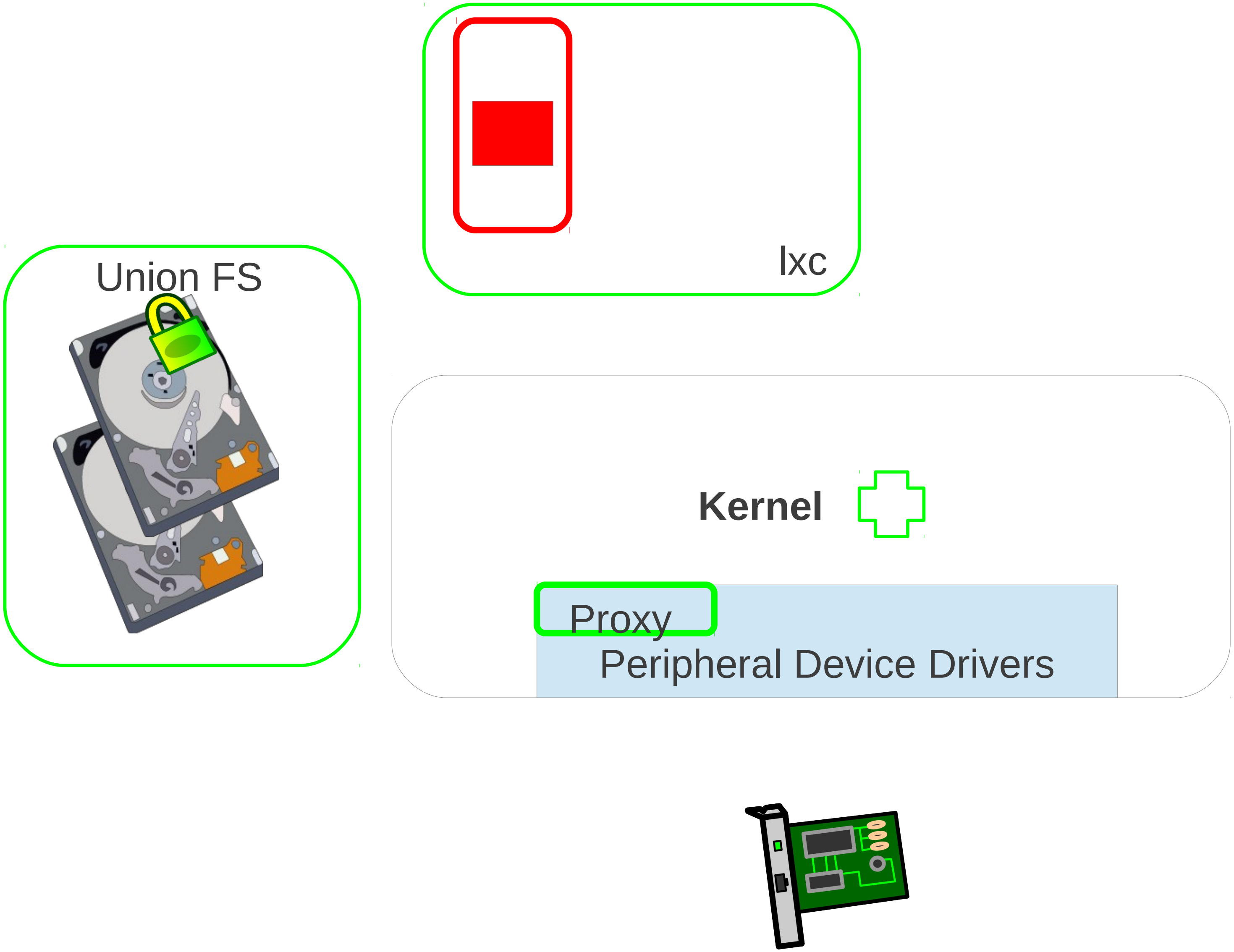
Union FS

Kernel

Proxy

Peripheral Device Drivers

Design of PCM



Union FS

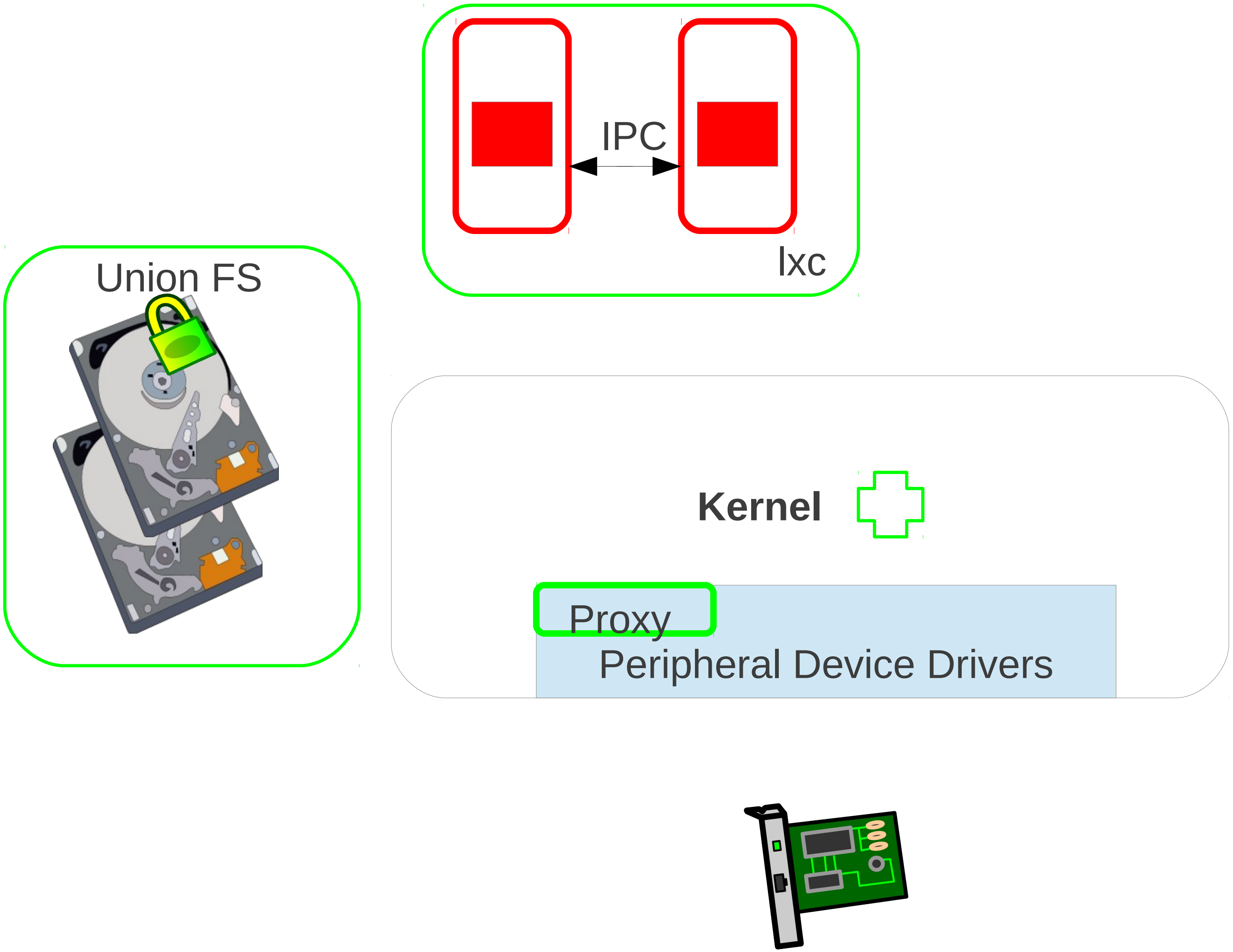
lxc

Kernel

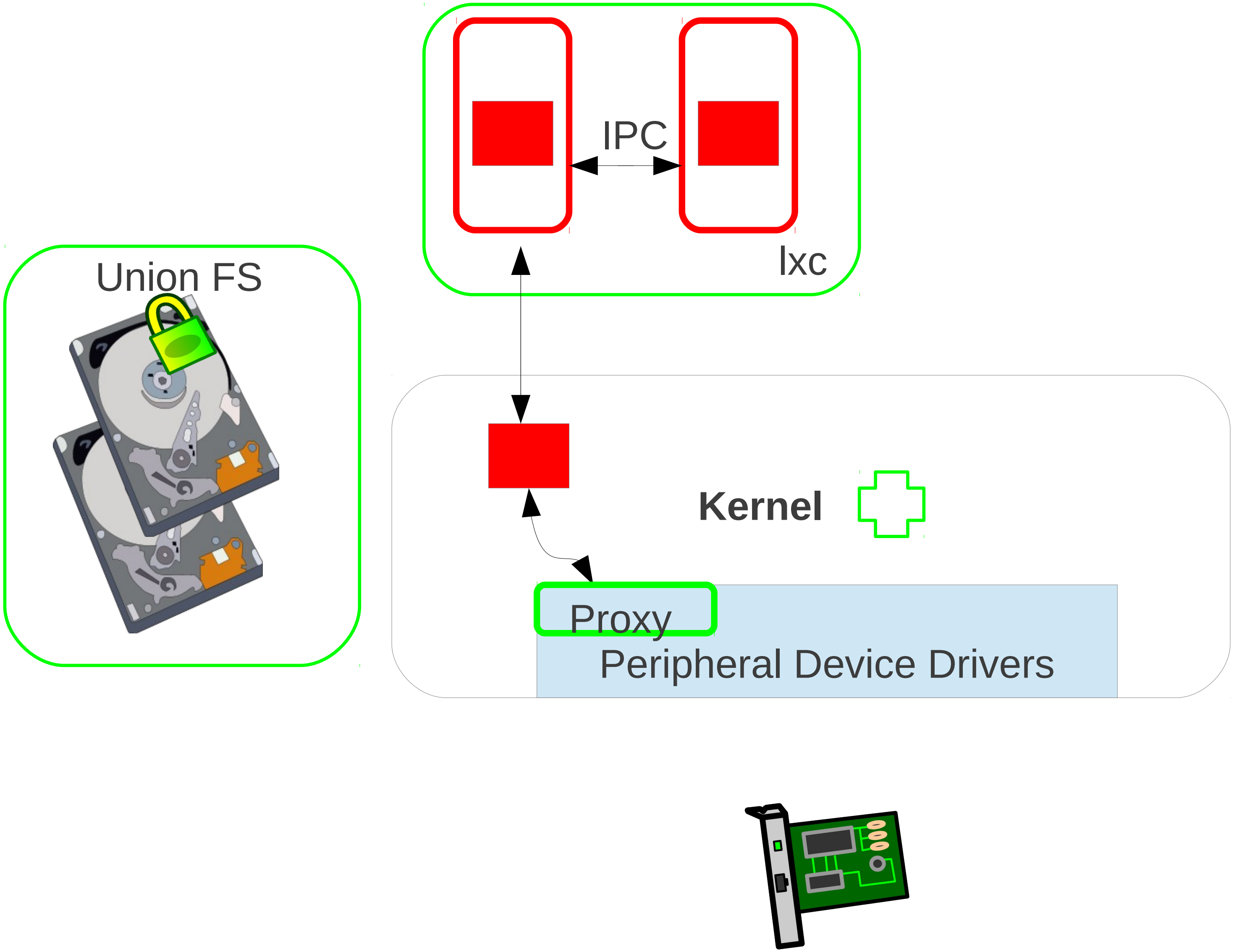
Proxy

Peripheral Device Drivers

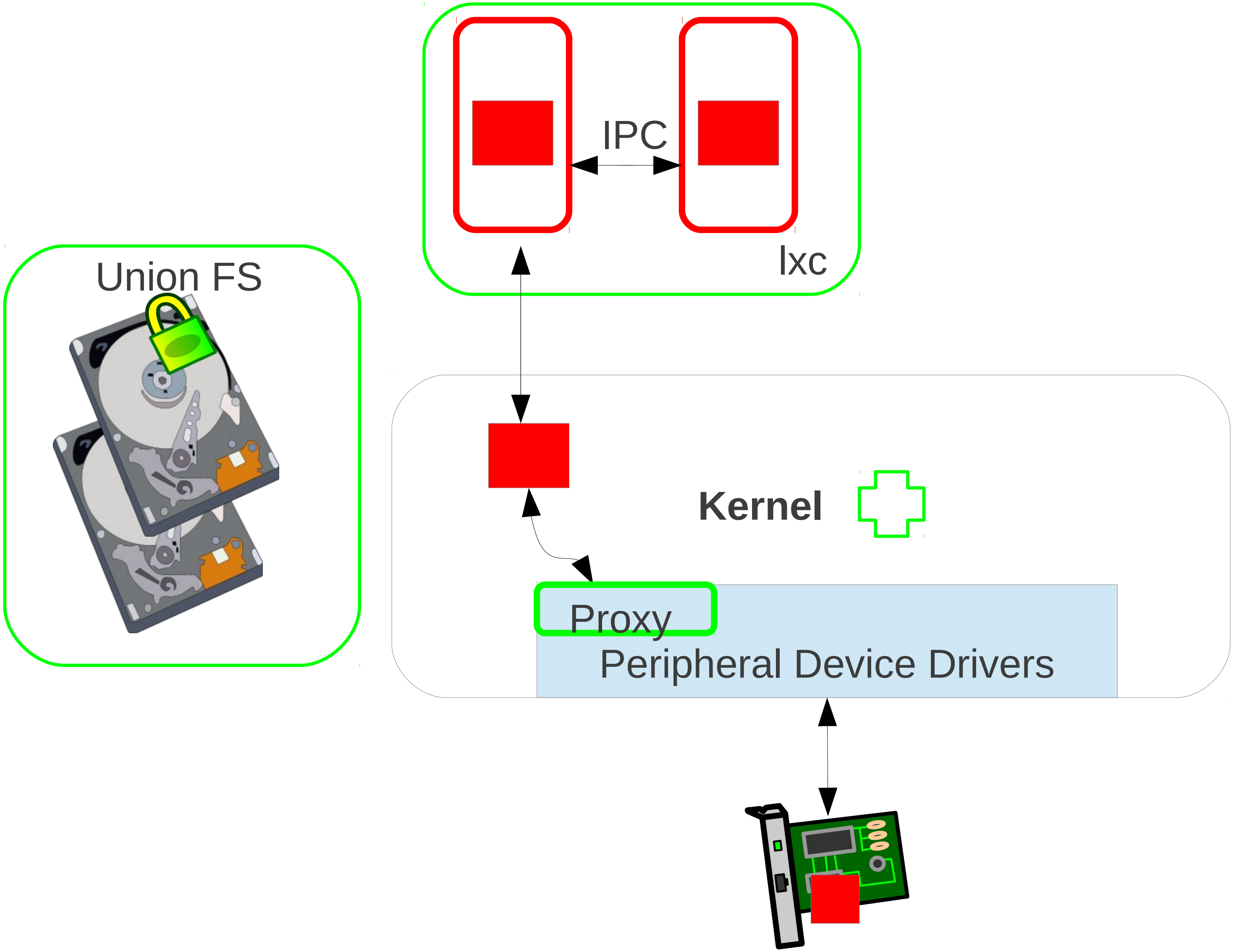
Design of PCM



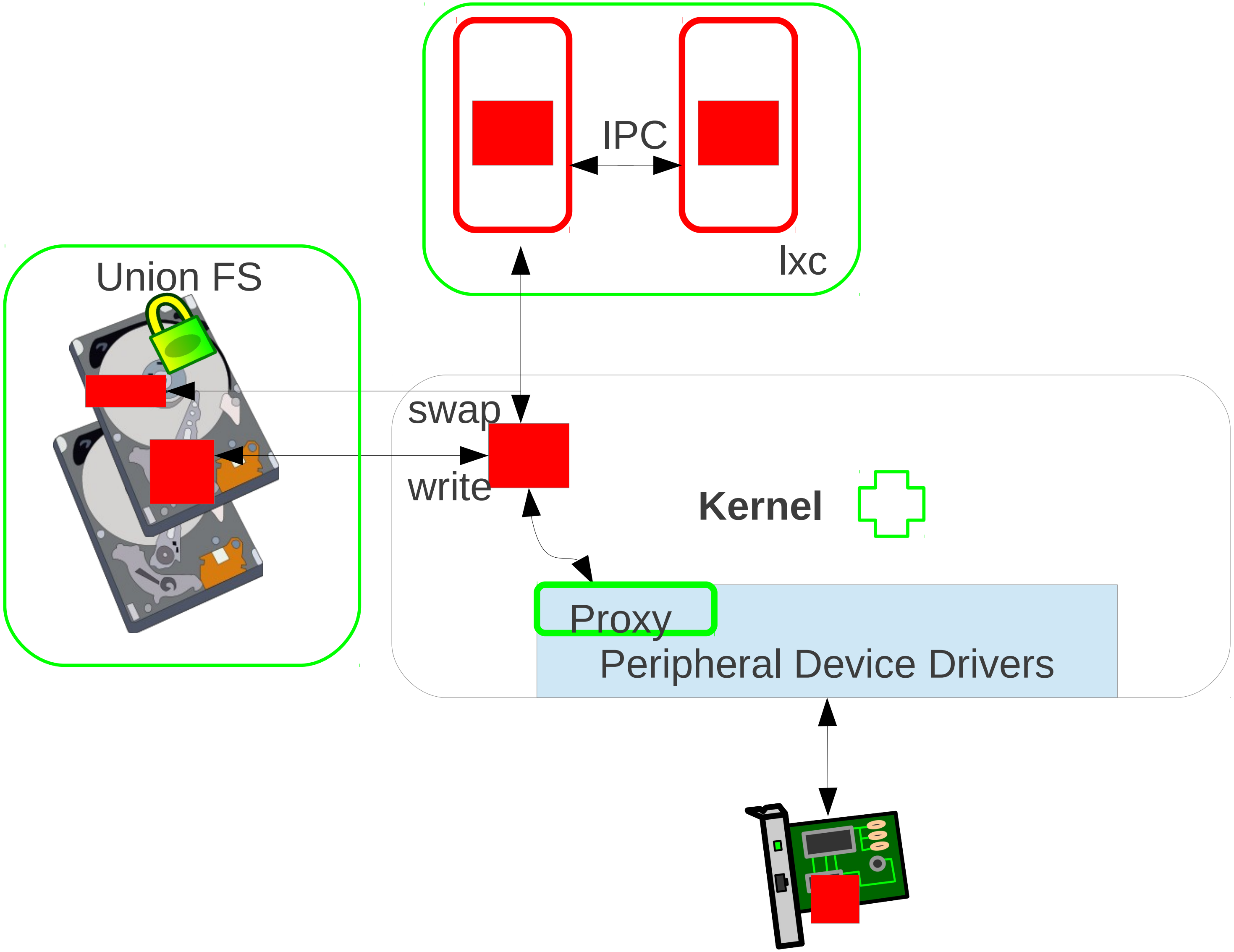
Design of PCM



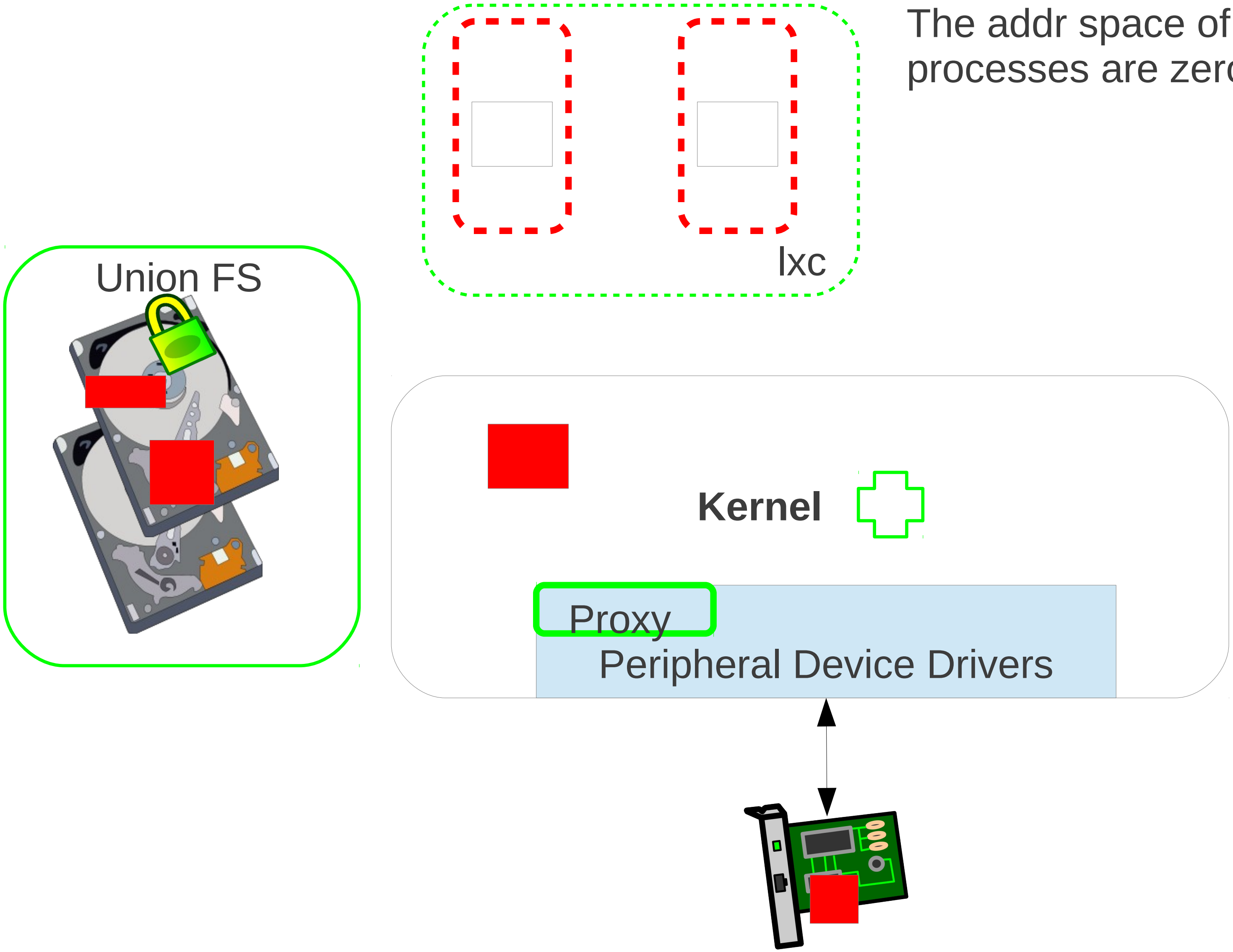
Design of PCM



Design of PCM

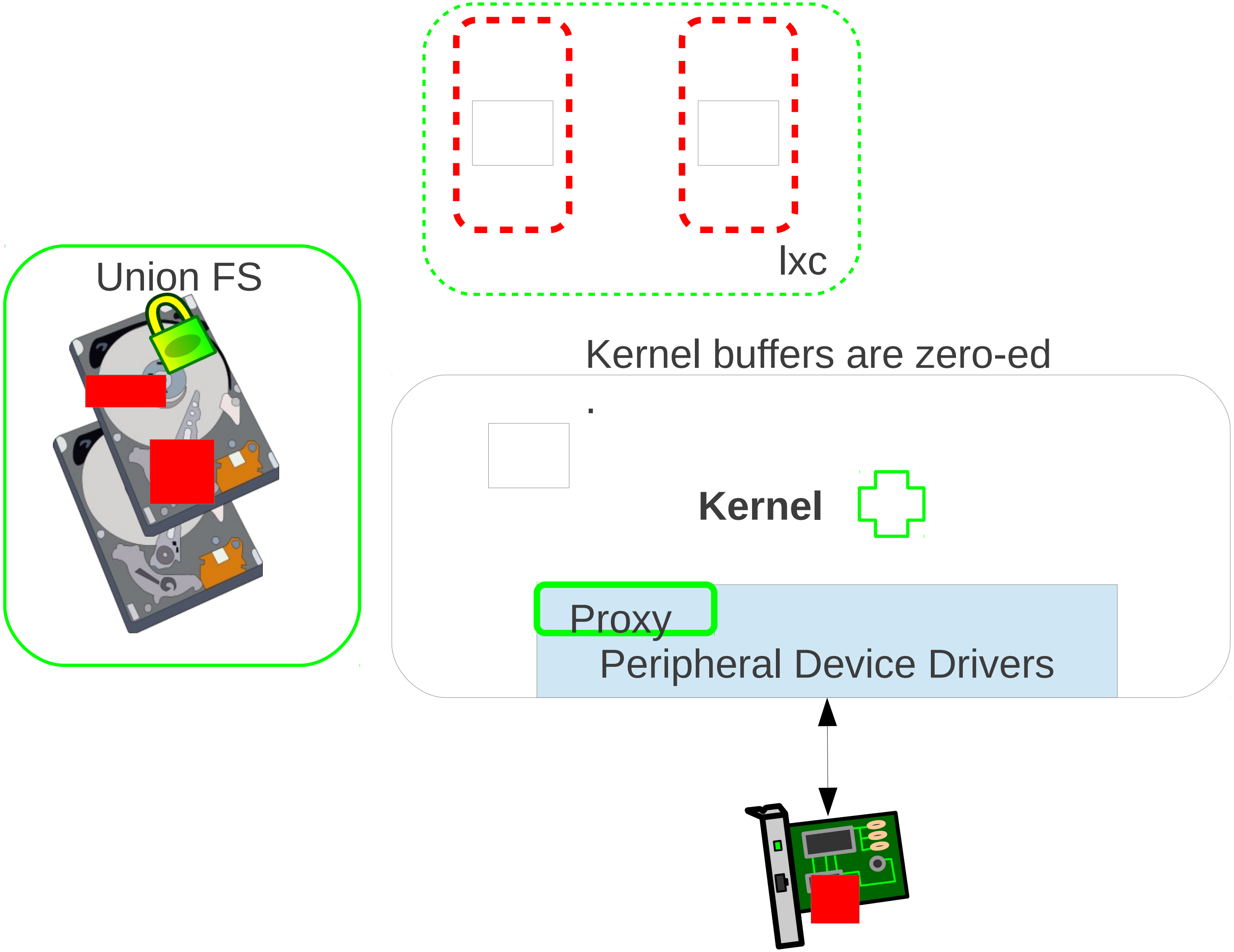


Upon the exit of the container

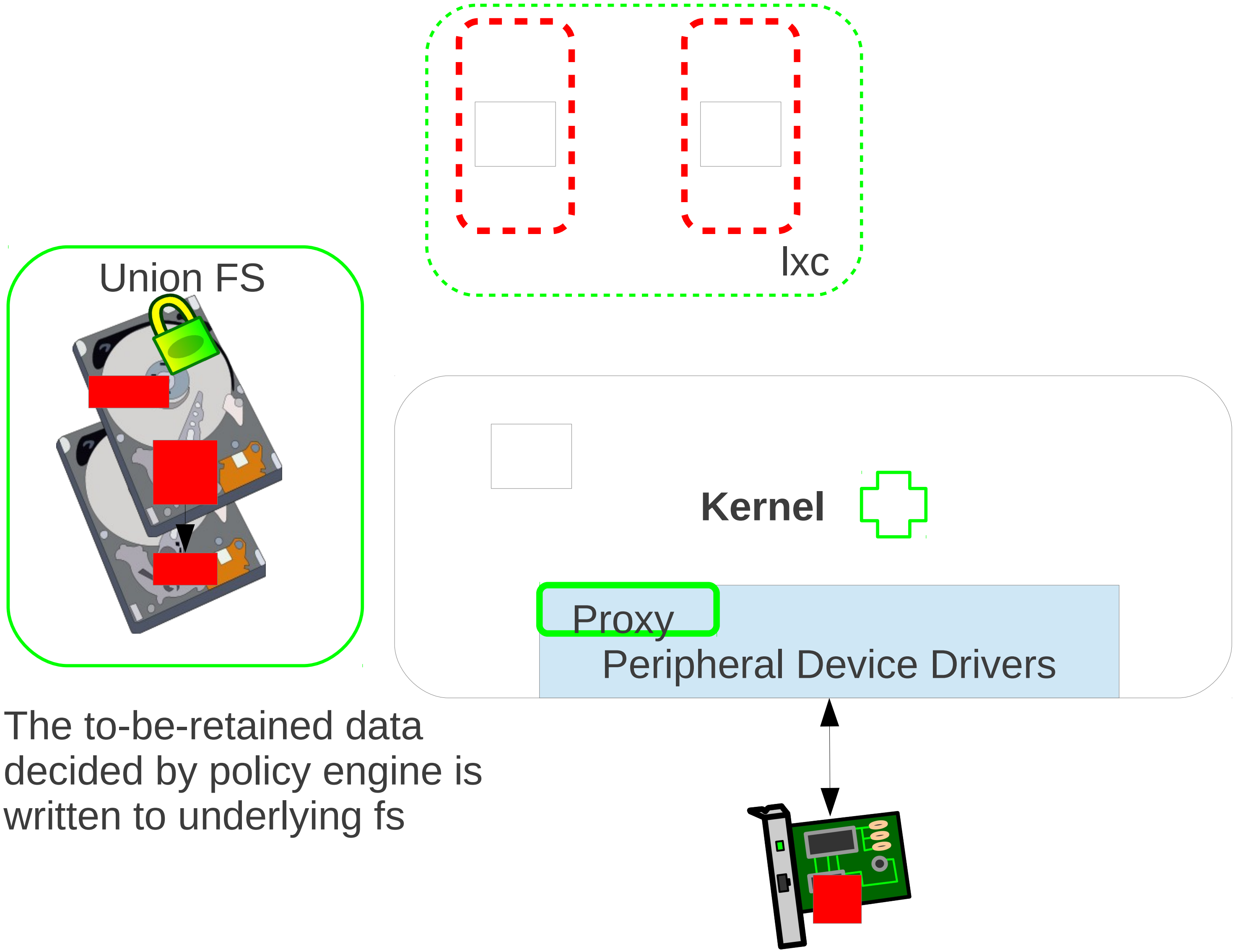


The addr space of contained processes are zero-ed.

Upon the exit of the container

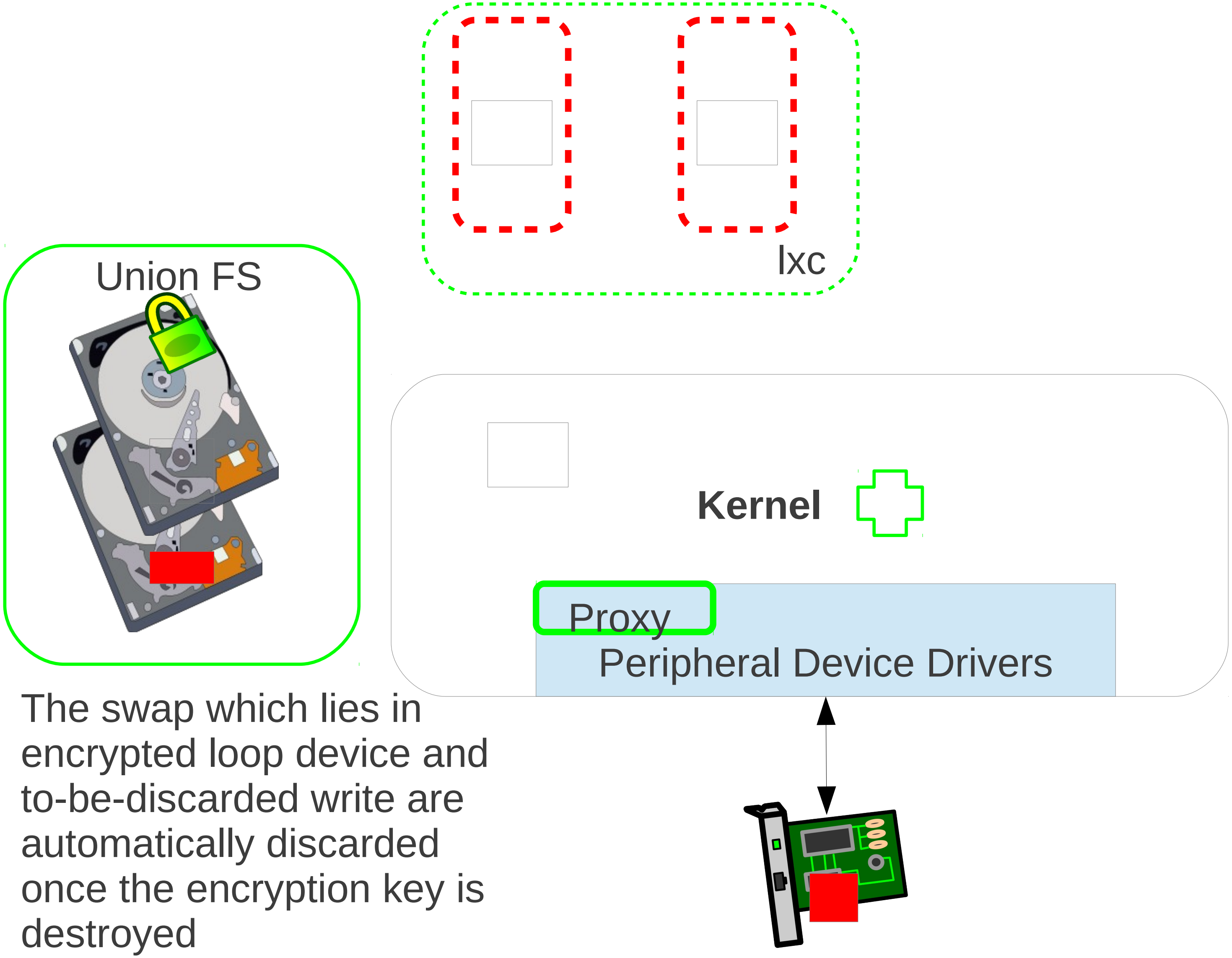


Upon the exit of the container



The to-be-retained data decided by policy engine is written to underlying fs

Upon the exit of the container



Union FS

lxc

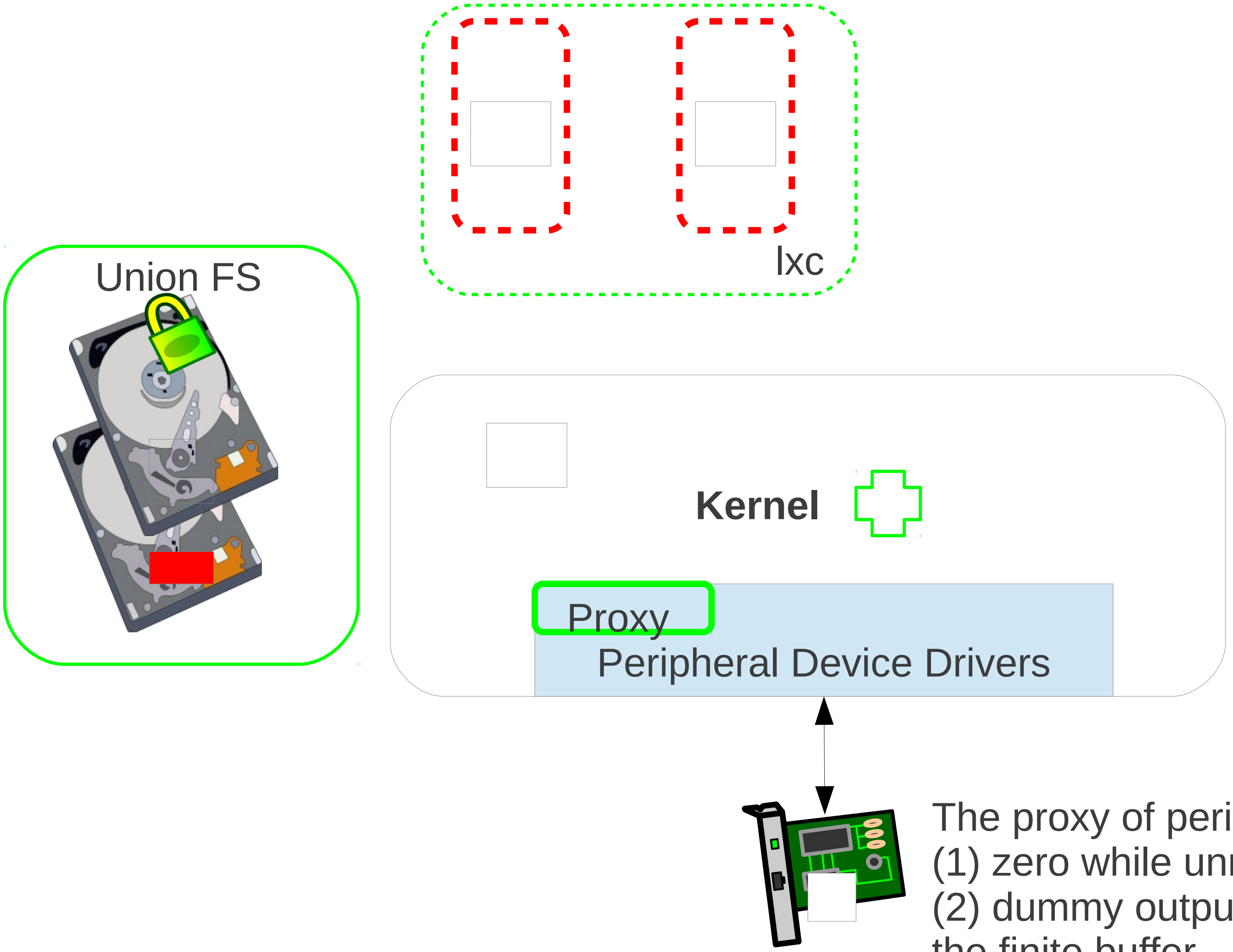
Kernel

Proxy

Peripheral Device Drivers

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]

Reference

[1] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh. An analysis of private browsing modes in modern browsers. In USENIX, 2010.

[2] A. M. Dunn, M. Z. Lee, S. Jana, S. Kim, M. Silberstein, Y. Xu,
V. Shmatikov, and E. Witchel. Eternal sunshine of the spotless machine: protecting privacy with ephemeral channels. In OSDI, 2012.

[3]Kaan Onarlioglu, Collin Mulliner, William Robertson, Engin Kirda
PrivExec: Private Execution as an Operating System Service
In Proceedings of the IEEE Symposium on Security and Privacy (S&P)

[4] J. Chow, B. Pfaff, T. Garfinkel, and M. Rosenblum. Shredding your garbage: reducing data lifetime through secure deallocation. In USENIX, 2005.

- Private computing should be implemented as a 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.