IBOS:Trust and Protection in the Illinois Browser Operating System

Insecure Web browser

- “Monolithic” Browser jams everything in one address space.
- Extremely unsafe, things are in your trusted computing base
- **Browser Kernel**: Google chrome, even though isolates untrusted computing base, it still has a huge amount of code in part of their trusted computing base.

Microkernel solve the problem ?

Secure Web browser

- Even if a components get compromised in browser, we can still browser it safely

IBos: Illinois Browser Operating System

- A whole new OS to make the web browser more secure
- Makes browser abstractions as first-class OS abstractions, they separate each web instance as process and lift all components(TCP/IP,drivers) up, and nest a software to monitor interactions between them. Even if any those components broken, user still can browse safely.

Result

			Chrome	IBOS
Category	**Example**	**Num.**	**Contained**	**Contained or eliminated**
Memory exploitation	A bug in layout engine leads to remote code execution	82	71 (86%)	79 (96%)
XSS	XSS issue due to the lack of support for ISO-2022-KR	14	12 (87%)	14 (100%)
SOP circumvention	XMLHttpRequest allows loading from another origin	21	0 (0%)	21 (100%)
Sandbox bypassing	Sandbox bypassing due to directory traversal	12	0 (0%)	12 (100%)
Interface spoofing	Two pages merge together in certain situation	6	0 (0%)	6 (100%)
UI design flaw	Plain-text information leak due to autosuggest	17	0 (0%)	0 (0%)
Misc	Geolocation events fire after document deletion	22	0 (0%)	3 (14%)
Overall		175	83 (46%)	135 (77%)

IBos pro and cons

Pros:

Cons:

Why IBOS isn’t mainstream?

How does making browser abstraction first class-OS affect other OS abstractions in IBOS?

Will this adversely affect the whole OS performance?