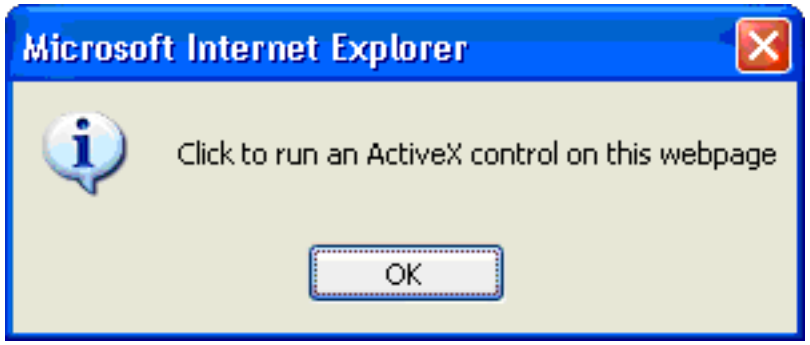
Google Native Client (NaCl)

B4M36BSY

Filip Klimeš
Pavel Štíbal

Run performant native code in a web browser

~~ActiveX~~


Microsoft Internet Explorer
Click to run an ActiveX control on this webpage
OK

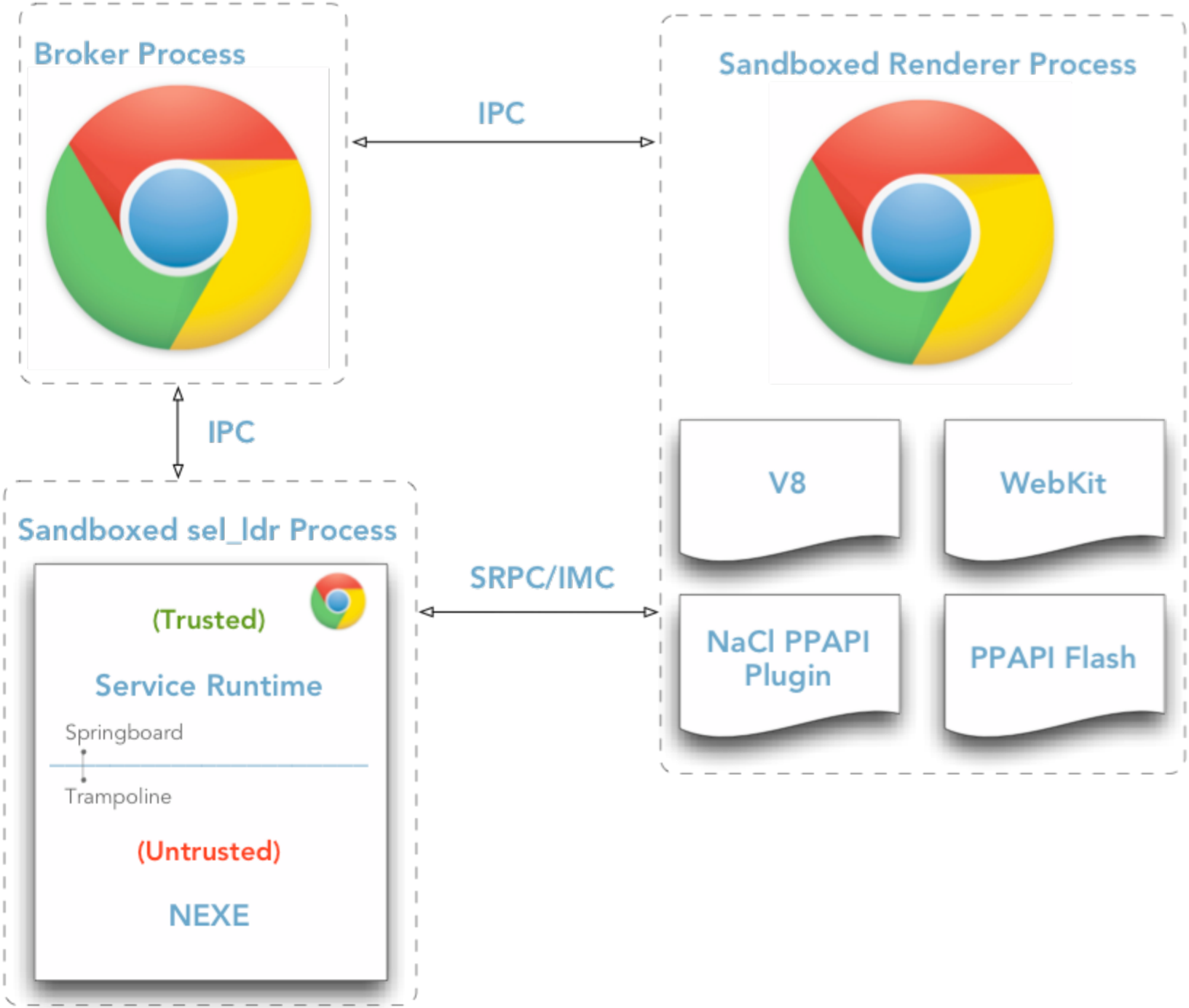
Native Client offers comparable safety with JavaScript

User installs NaCl plugin, which runs the native code.
No pop-ups. Instead, it checks the code automagically.

Security through Sandboxing

Software Fault Isolation (SFI)

You can run compiled C and C++ code and use advanced CPU operations, including multi-threading, in a browser.


Broker Process
IPC
Sandboxed Renderer Process
IPC
V8
WebKit
Sandboxed sel_ldr Process
SRPC/IMC
(Trusted)
Service Runtime
Springboard
Trampoline
(Untrusted)
NEXE
NaCl PPAPI Plugin
PPAPI Flash

Unlike obsolete NPAPI, the PPAPI is not scriptable and it provides only a minimalistic API to minimize attack surface.

There is an SDK for NaCl providing a special compiler, which produces secured executable code in .nexe format.

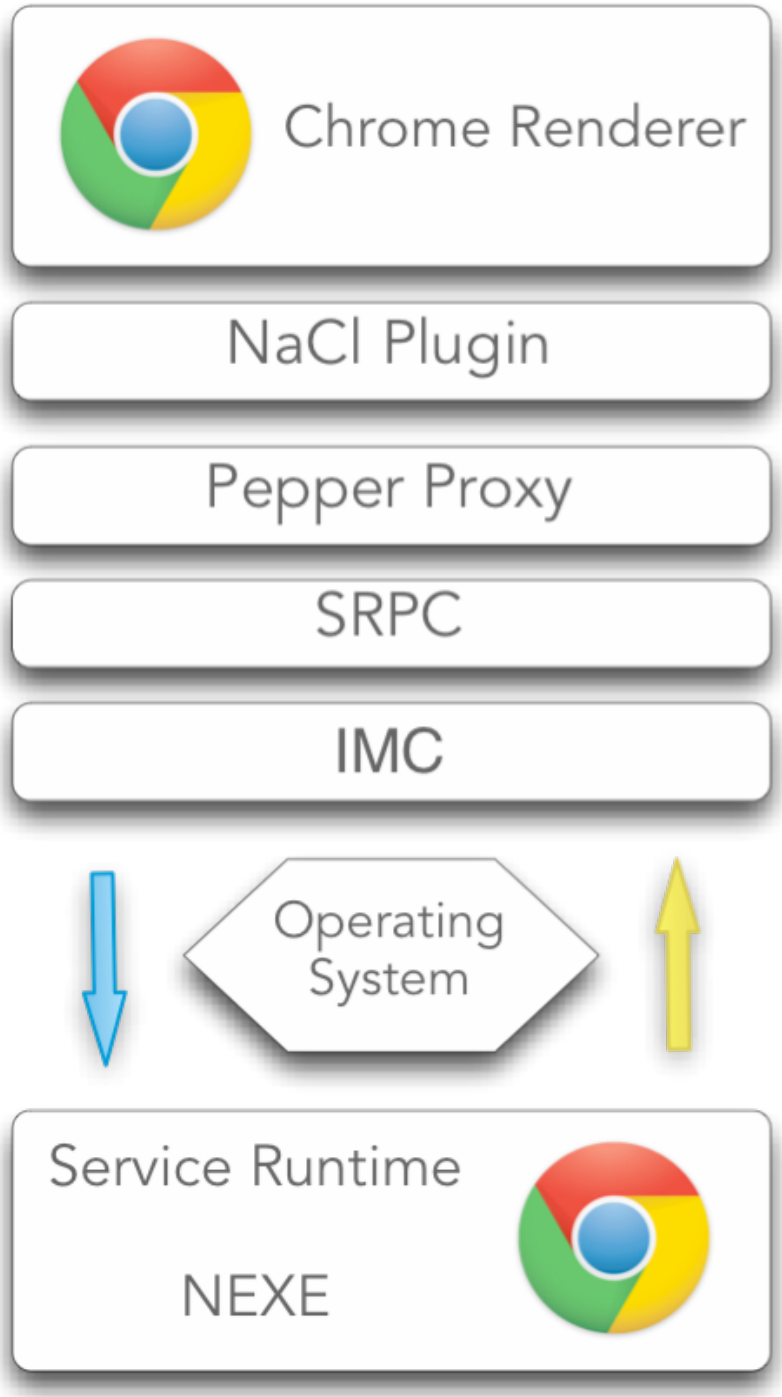
The sandbox statically analyses the binary code and enforces constraints, which provide basic level of safety.

C1	Once loaded into the memory, the binary is not writable, enforced by OS-level protection mechanisms during execution.
C2	The binary is statically linked at a start address of zero, with the first byte of text at 64K.
C3	All indirect control transfers use a `nacljmp` pseudo-instruction (defined below).
C4	The binary is padded up to the nearest page with at least one `hlt` instruction (0xf4).
C5	The binary contains no instructions or pseudo-instructions overlapping a 32-byte boundary.
C6	All *valid* instruction addresses are reachable by a fall-through disassembly that starts at the load (base) address.
C7	All direct control transfers target valid instructions.

Table 1: Constraints for NaCl binaries.

NaCl identifies trusted and untrusted modules.
The downloaded code is never trusted.

NaCl modules can communicate with other modules through Inter Module Communication (IMS).


Chrome Renderer
NaCl Plugin
Pepper Proxy
SRPC
IMC
Operating System
Service Runtime
NEXE

The communication among processes goes through the pepper proxy.

NaCl runtime provides basic system services such as memory mapping or POSIX thread interface.

NaCl Security evaluation

In order to escape the sandbox, you need to breach two levels of sandboxes – the NEXE runtime and then the Chrome renderer process.

The most vulnerable attack surface are the trusted modules.

Thank you for your attention :)