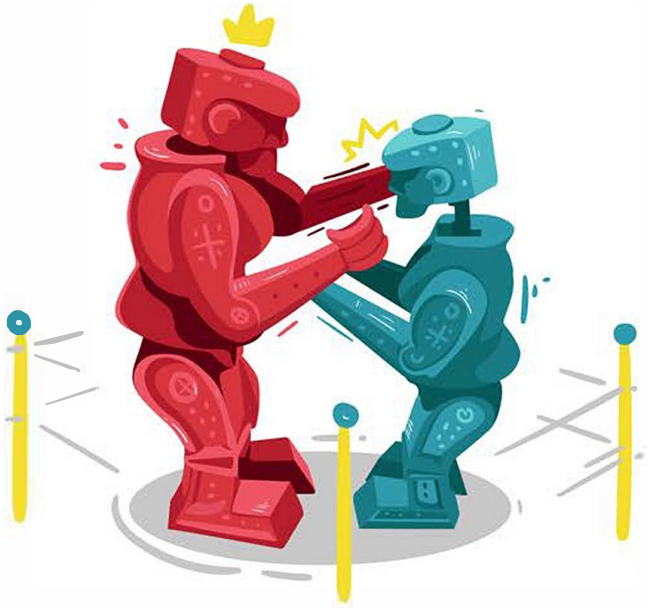
LOCKDOWN BROWSER® VS. LOCKED BROWSER PLUGINS



A BARE-KNUCKLE CAGE FIGHT

This isn't really a bare-knuckle cage fight Its a straight comparison between LockDown Browser and the various browser plugins that refer to themselves as a "locked browser".

Let's start with the **similarities between Lock Down Browser and the "locked browser" plugins:**

- The browser runs full-screen and cannot be minimized
- Users cannot open a new tab or go to another website
- Certain keyboard functions, keystroke combinations, and mouse menus are disabled (e g .printing, copy and paste, task switching)

This is where most locked browser plugins end It's better than nothing, but it's like constructing a wall around 70% of the city - it looks formidable from cer-tain vantage points, but the gaping hole leaves it open to attack.

Lock Down Browser isn't a browser plugin It's a custom browser - a native application - for Windows, Mac, and iOS. Why is that important? Because native applications have direct access to the operating system and the computing device (essential for stopping many types of exploits) whereas a plugin is blocked from accessing key areas of the OS.

Here are some **basic exploits possible with a "locked browser" plugin, but NOT with Respondus Lock Down Browser:**

- Virtual Machine and Safe Mode exploits
- Remote desktop & screenshare
- Extended desktop, multiple monitor, and screencast exploits
- Undesirable applications running in the background (IM, video recording)
- Applications launched with a timer, an incoming message/alert, or a keystroke combination (e g Shift +@)
- Programmable and extended mouse buttons 2)
- Browser cache and JavaScript injection exploits
- Task switching swipes

Not only is a native application like LockDown Browser better able to control the device and OS, it has the benefit of 12 years of heavy-duty use in the field Over 1,500 educational institutions use LockDown Browser to protect 60 million exams delivered within their LMS each year Through an SDK program, LockDown Browser is additionally licensed by dozens of the largest publishers, testing centers, certification organizations, and assessment platforms throughout the world

Implications for Automated Proctoring

Respondus pioneered "automated proctoring" seven years ago, with the introduction of Respondus Monitor. Respondus Monitor is a companion application to LockDown Browser that uses webcam and video analytics to deter cheating during **non-proctored,** online exams. Suspicious behaviors are automatically flagged for instructors, and exam sessions are ranked in terms of overall risk

More recently, "live proctoring" companies have begun offering automated proctoring services. We'll save the comparison between Respondus Monitor and other automated proctoring systems for another time. But a critical piece of automated proctoring is ensuring that the student doesn't use the computer itself to cheat during the exam.

Other companies attempt to counter this concern by recording the student's computer screen during the exam. This has two problems First, the instructor is now tasked with reviewing this video to determine if cheating has occurred Second, many exploits aren't visible with a recording of a student's desktop For example, if a video capture application is running prior to the start of the exam, this won't be visible to the instructor. Likewise, screen capture applications can save images to a file without anything appearing on the screen. Remote desktop applications can be used, extended desktops allow applications to be run outside of the desktop recording, and on and on. The bottom line there's no point analyzing videos of students smiling broadly into their webcams, while they take advantage of countless exploits on the computer itself.

So, if you're thinking of using automated proctoring for your students' online exams (and we hope you are), be sure it includes the protection of LockDown Browser. Because a locked browser plugin that safeguards only 70% of the online testing environment just doesn't cut it.