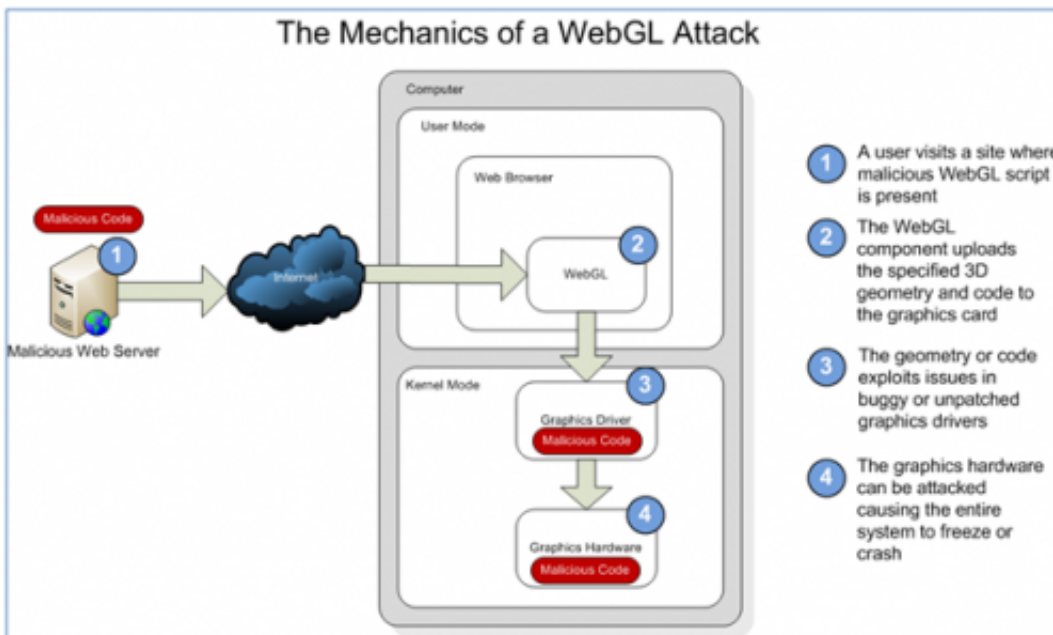# Security flaws found in the WebGL standard

May 13 2011, by Katie Gatto

(PhysOrg.com) -- Researchers at Context Information Security have issued a warning about the WebGL standard. The warning states that this standard has the potential to undermine the security concepts that are practiced by current operating system versions and provide a new set of opportunities for attacks on a variety of system.

The standard, which is designed to enabled the rendering of 3D animations, executes the shader code directly on the system's graphics card. While this may make graphics rendering simpler, it does however make a space for the exploitation. If the graphics card has any vulnerability in it the system could be breached. This level of vulnerability is something that the Khronos Group, who are the creators of the WebGL standard, have acknowledged the possibility of in the WebGL specifications.

How serious are the potential vulnerabilities? Well, the researchers at Context Information Security say that they have been able to create the blue screen of death by using an exploitation that targets the overloading of a graphics card. While some of the current operating systems do have a fail-safe that rests an overloaded graphics card after a few seconds, the blue screen of death can be reached after a certain number of resets.

The Mechanics of a WebGL Attack

Computer

User Mode

Web Browser

Malicious Code

Malicious Web Server

Internet

WebGL

Kernel Mode

Graphics Driver
Malicious Code

Graphics Hardware
Malicious Code

1. A user visits a site where malicious WebGL script is present
2. The WebGL component uploads the specified 3D geometry and code to the graphics card
3. The geometry or code exploits issues in buggy or unpatched graphics drivers
4. The graphics hardware can be attacked causing the entire system to freeze or crash

The flaw could also, according to the researchers, be used to not just create the blue screen of death, but to inject malicious code onto the system.

There is no word yet as to whether or not the standard will be changed, or when any changes to the standard would be implemented. Since the problem is already known and published in the standard it may not change at all.

More information: Report: www.contextis.com/resources/blog/webgl/

Citation: Security flaws found in the WebGL standard (2011, May 13) retrieved 26 June 2024 from https://phys.org/news/2011-05-flaws-webgl-standard.html