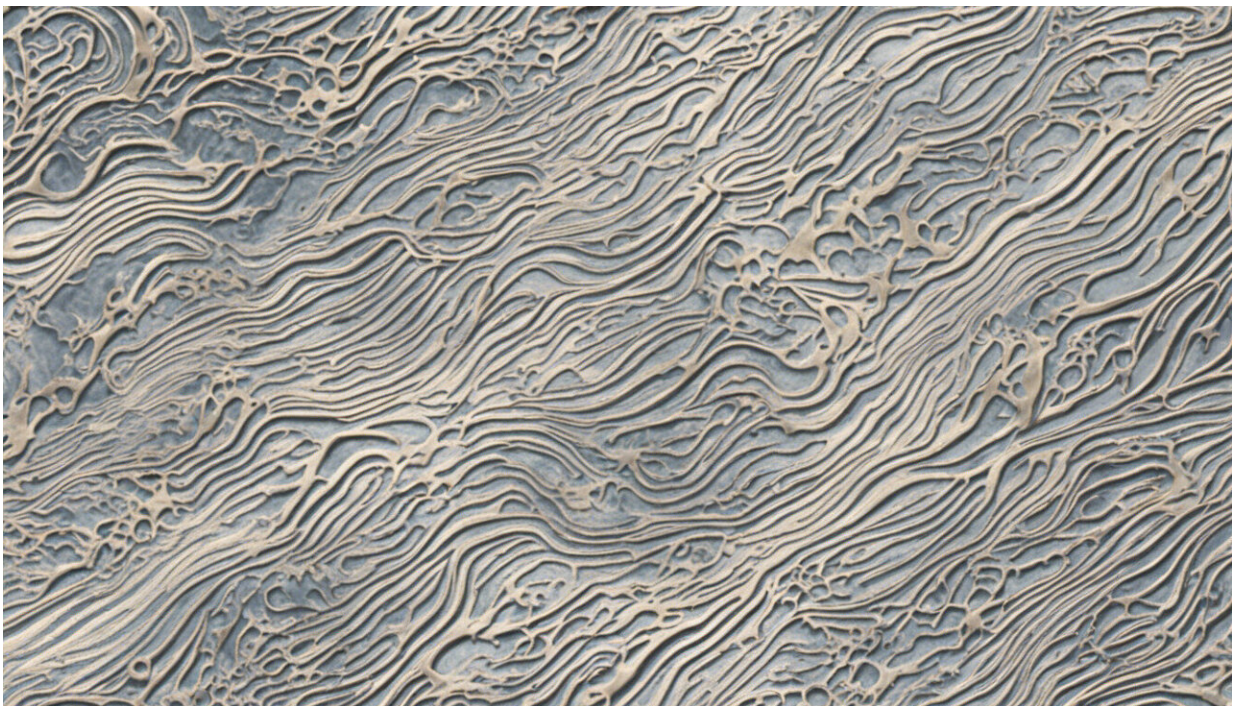


# Opinion: When Chrome, YouTube and Firefox drop it like it's hot, Flash is a dead plugin walking

July 20 2015, by Neil Smith

---



Credit: AI-generated image ([disclaimer](#))

After more than 20 years making the web a slightly more interesting and interactive place, albeit one that pandered to designers' worst excesses and (in pre-broadband days) led to interminable download waiting times, the word on the net is that Adobe Flash Must Die.

The ironic hack of Hacking Team, the controversial security and surveillance software firm, exposed yet another brace of security flaws and vulnerabilities in Flash, the hugely popular multimedia animation plugin for web browsers. This may be the final straw: Mozilla has [disabled Flash by default in its Firefox browser](#), and Facebook's chief of security has called for Adobe to set a date when the program will be [taken behind the shed and shot](#).

## **Why hate Flash?**

The software and services that Hacking Team sells provide the means for its government and law enforcement clients to break into and even control computers remotely through the internet. The huge leak of the firm's company data also revealed details of previously unknown vulnerabilities in software that could be exploited to provide ways of hacking computers – known as [zero-day vulnerabilities](#) because the software's manufacturer has no time to fix the problem.

Zero-day vulnerabilities are great news for criminals. Three of these vulnerabilities were in Flash, and some of those revealed in the leaked documents appeared in attack kits available online within hours – faster than the developers of the affected programs could fix the holes, let alone distribute the updates to millions of users worldwide.

The Flash plugin is notorious for being riddled with security flaws and other shortcomings. Yet it's also one of the most popular pieces of software on the planet. So what will it take to kill it?

## **It seemed like a good idea at the time**

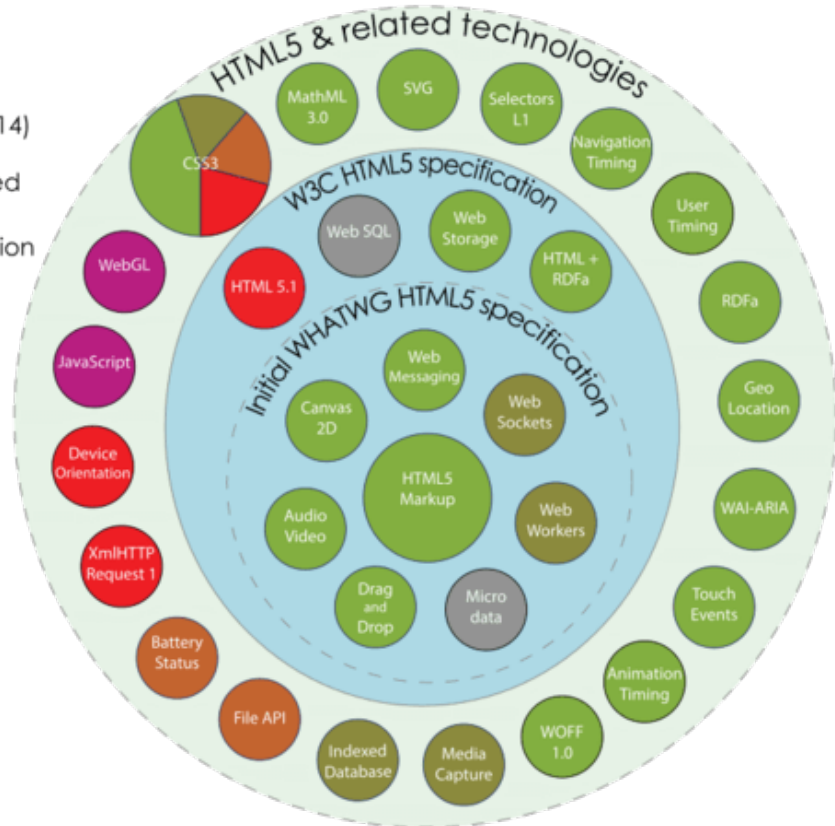
Back in the web's dim and distant past (the 1990s), [web pages](#) were static, unyielding things with just text and images and occasionally a

[dumb animated GIF](#) that everyone but the designer hated.

# HTML5

Taxonomy & Status (October 2014)

- Recommendation/Proposed
- Candidate Recommendation
- Last Call
- Working Draft
- Non-W3C Specifications
- Deprecated or inactive



Inside, HTML 5 supports a lot of technologies such as audio/video now, with more to come. Credit: Sergey Mavrody, CC BY-SA

But we wanted more: interactivity, responsiveness, perhaps even a little bit of bling. Flash made this happen, and animators and designers could create all the interactivity they wanted and wrap it up in a file that was inserted into the web page and downloaded on request.

The web is a hostile place for browsers, however, and the more functionality exposed to the web, the larger the surface exposed to

attack. Flash offers a large attack surface, and because animation is often computationally demanding, Flash needed deep access to many aspects of the computer to work well, making any flaw potentially serious.

Security isn't the only problem with Flash. For example it wasn't security but Flash's demanding processor and battery consumption that caused [Steve Jobs to banish Flash from the iPhone and iPad](#). On a device with such limited resources as a smartphone or tablet, Flash just doesn't fit.

While these drawbacks could be tackled, Flash's proprietor Adobe seems uninterested in doing so, having not released an update to Flash Player on mobile [since 2012](#).

## **Flash forward to the future**

Yet Flash endures, mainly on account of the last 20 years in which websites have been created using it and the plugin has been installed in billions of browsers. There have been attempts at alternatives: Microsoft's Silverlight was Windows-specific and never caught on, and even the company itself [urges people not to use it](#); Java applets have even worse problems than Flash, and have already been [deprecated or removed from modern browsers](#).

The best hope for the elimination of Flash is HTML 5. The latest version of HTML, the markup language in which web pages are written, finally includes support for directly embedding video and audio in a web page. In combination with JavaScript, web pages can now offer all the interactivity and animated bling that anyone could want. Having previously been without a doubt the largest user of Flash, YouTube [now uses an HTML 5-based player as default](#) for its video content. Google's Chrome browser dropped support for Adobe Flash some time ago, and uses only its own version.

HTML 5 has two major advantages over Flash. As a much more modern technology (2014 versus 1995) it delivers better results with fewer resources, making it better suited to mobile devices. But more importantly it requires no plugin, which means the surface open to attack by hackers doesn't expand just because you want to watch a video, or because some site wants to display an animated advert.

Of course there are still sites that use Flash extensively, and these will have to be redesigned in HTML 5. While these sites still exist and people wish to use them, the Flash problem will not go away.

## **It's more than just Flash**

Flash's problems make it an easy target, but it's just one place where security failures occur. Of the zero-day exploits discovered so far in the Hacking Team leak, three relate to Flash, [one to Java](#), one to a [font processor for Windows](#) (also made by Adobe), and one to Microsoft's Internet Explorer 11 browser. But security is hard, no software is invulnerable, and breaches like this will continue to happen. Even if Flash is somehow secured – or disappears entirely – [security flaws](#) will still be found and exploited in other software. Security is an ongoing journey, not a destination.

The bigger problem is how the exploits originate. Hacking Team didn't discover most of these exploits – they [bought them from hackers who found them](#), keeping them secret for use in their products. Perhaps this is why a security firm such as Hacking Team becomes a tempting target for criminals, as a concentrated source of zero-day exploits.

As governments and intelligence agencies collect more information, they will also become more valuable targets. If Britain's GCHQ is able to bypass all encryption, as prime minister David Cameron [has suggested](#), then all our data could be vulnerable to anyone who can find the slightest

crack in GCHQ's armour.

*This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Opinion: When Chrome, YouTube and Firefox drop it like it's hot, Flash is a dead plugin walking (2015, July 20) retrieved 28 April 2024 from <https://phys.org/news/2015-07-opinion-chrome-youtube-firefox-hot.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.