

60001224078.txt

Please, Please, Please, (Three Pleases) do not implement rules that take away the ability of users to examine and correct the universally faulty software that wireless devices are shipped with. As much as testing of devices can identify problems, a vast array of problems, particularly security problems, cannot be identified by FCC pre-manufacture testing. Locking down software so that it cannot be effectively repaired after manufacture renders the American public powerless against security attacks.

<p>

Without having the public availability of wireless firmware that is open to examination and correction, research into improved devices will be severely impaired. There hasn't been a single commercial device yet provided for which the originally provided software hasn't been faulty - it's the general nature of low-level software development that faulty software is universal. It is only by allowing many researchers to examine the software that any assurance of security and proper operation can be accomplished. Closed-source devices can be researched, but only at high cost, as the source code is much more accessible and usable than the binary code. In addition, the use of digital signature or other technological means to avoid the use of modified software makes it impossible for anyone but the original manufacturer to test and deploy improved software - this must not be permitted to be an obstacle to fixing and improving devices.

<p>

The American public need the ability to fix security holes in their devices when the manufacturer chooses to not do so. In this day where individual and state-supported security attacks are commonplace, it would be a crying shame to lay our country's wireless infrastructure wide open for exploitation by terrorists and enemy government action - the next security failure would be on the FCC's shoulders and hung around the FCC's neck.

<p>

It is often the case that manufacturers fail to fix devices for which they have already received their maximum profit, leaving the wireless spectrum full of devices with serious bugs and security failures. I personally have purchased devices that were subject to serious security exploits that the manufacturers never fixed, and relied upon Open Software firmware to repair these devices. Without such repair, these devices would have had to have been scrapped and replaced at significant cost, and the manufacturers were unavailing and unwilling to shoulder the cost of replacement, as warranties were unreasonably short in the face of security failures that render the device completely unsuitable for continued use.

<p>

The FCC needs to understand that once an exploit has been discovered, unless the software can be repaired, an exploitable device is rendered worthless. This represents a catastrophic failure of the entire production volume of a device unless the software can be promptly replaced. Even a few days of delay in repairing the software can permanently devalue a wireless device, as it must be promptly replaced if it is not repaired. This can result in literal billions of dollars of monetary losses to individuals and businesses of the American public.

<p>

Open Software has generally run far ahead of manufacturers, which have attempted to divide the market for maximum confusion and profit. Open Software focuses on continuing support for wireless devices that have gained some success in the marketplace but the original manufacturer has failed to fully exploit the capabilities of the device. Because many manufacturers use similar hardware components, Open Software has been able to support a great variety of devices that manufacturers have provided less capable or downright faulty software.

<p>

In the alternative, the FCC would have to require that devices have continuing support from manufacturers for any problems that can be identified in the future. I'd envision requirement that (1) devices retain software support for at least a five-year period and preferably a ten-year period, and (2) that identified problems be fixed promptly, within a 30-day period of public availability of exploits, and (3) that failures to provide effective software updates subject the manufacturer to full liability for such problems. In addition, (4) any such devices which are no longer supported with such a required period would be subject to mandatory return and refund of the full original purchase price. Failing such alternative requirements for closed-source devices, manufacturers could escape liability by (5) promptly providing the full source code for any devices.

<p>

If the FCC promulgates a closing of the availability of open software for wireless devices, it will be demonstrating a true failure of regulation of the public airwaves for benefit of the public. Again, triple please, reconsider this ill-considered regulation.