Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff

Docket No. FDA-2015-D-5105

Comments of Electronic Frontier Foundation

April 21, 2016

Submitted by:
Cory Doctorow
Corynne McSherry
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
cory@eff.org
corynne@eff.org

Failing Gracefully: Protecting Against Unintended Barriers to Safety and Security

The Electronic Frontier Foundation (EFF) is grateful for this chance to comment on cybersecurity for medical devices and systems. EFF is a member-supported 501(c)3 nonprofit, which has spent the past 25 years campaigning to ensure that the protections that we all enjoy in the "real" world remain with us into the electronic, information age. EFF participates in standards and treaty negotiations, works with regulators and governments around the world, and is actively involved in litigation on key questions of electronic security and safety.

EFF submits these comments to assist the FDA in its efforts to ensure the safety of medical devices, specifically those that include embedded software. Improving the safety and efficacy of embedded systems – including systems embedded in medical devices – is a complex and difficult task that breaks down into two equally important parts: first, improving the quality of the code and systems that are introduced to the market; and second, ensuring that defects in shipping products are quickly discovered and remediated. Part one can be described as "working well." Part two is all about "failing well" – meaning "failing" in such a way that defects can be disclosed, fixed, and avoided in the future. Unfortunately, practical and legal barriers may impede the discovery and disclosure of device flaws. As explained below, we urge the FDA to use its regulatory power to diffuse those barriers by encouraging companies to adopt specific policies that will encourage timely discovery and disclosure of defects.

The case for paying attention to failure

Pre-market testing, no matter how robust and exacting, cannot ever fully secure a system against unsafe failure modes. As cryptographer Bruce Schneier says, "Security is a process, not a product" because "anyone can design a security system that works so well that he himself can't figure out a way around it."[1] It's only when systems are tested by other creative intellects, with different strengths and points of view, that the oversights in the designer's assumptions, which give rise to dangerous failure modes, can be surfaced.

[1] *Schneier's Law*, Bruce Schneier, https://www.schneier.com/blog/archives/2011/04/schneiers_law.html

If you don't care how a system fails, it is comparatively easy to make it work well. The FDA could (and should) continue its rigorous pre-market testing program for medical implants, to determine whether they perform their stated roles adequately under a reasonable test period under simulated field conditions – but a device that passes this test might still be unsafe: for example, it could permanently cease to function if its clock is set to January 1, 1970,[2] it could be vulnerable to lethal remote attacks[3] or it could be designed to allow third parties to covertly access it and change its configuration and read its data.[4]

Disclosure is key

Discovering a problem is not enough – disclosure is also essential. Security experts understand that disclosure is as vital to the remediation of defects and continuous improvement of security. Unfortunately, manufacturers aren't always happy when researchers (including those retained by their customers) examine their products for defects.[5] They insist that disclosure harms more than it helps, by alerting "bad guys" to exploitable vulnerabilities before countermeasures are in place. As a result, efforts to raise concerns quietly before going public may be met with silence or denial, or worse, threats of legal action[6] and even arrests[7]. The dangers to the users of these systems remain, because "bad guys" independently discover the same flaws and exploit them, and the users of the systems rely on them because they are in the dark about those flaws.

Merely knowing about flaws – even ones that have no immediate fix – can improve safety. If you know your car's brakes are faulty, you can increase your following distance and decrease your speed until you can get them serviced. If you don't know about their faults, you're liable to find out in the hardest way possible, when they fail with insufficient braking room between you and an obstacle.

Disclosure is a best practice engineering

Virtually every engineering student must study the Therac-25 disasters,[8] in which a defectively designed medical device administered lethal doses of radiation to patients. The manufacturer might not have wanted the public to know the details of why the Therac-25 machines killed people (or even that it happened at all – even apart from any legal liability, events like these the company's reputation). Nonetheless, the ability of future engineers to understand what went wrong is making them better and more careful, so it is not just beneficial for regulators to have this kind of information, but for the whole engineering community to have access to it.

[2] *Why 1/1/1970 Bricks Your iPhone*, Mark Frauenfelder, Boing Boing, http://boingboing.net/2016/02/16/why-111970-bricks-your-iphon.html

[3] *Dick Cheney Feared Assassination by Cardio Device Hack, Had Docs Turn Defibrillator's Wireless Off*, Xeni Jardin, Boing Boing, http://boingboing.net/2013/10/19/dick-cheney-feared-assassinati.html

[4] *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*," Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Landau, Susan; Neumann, Peter G.; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael; Weitzner, Daniel J., https://dspace.mit.edu/handle/1721.1/97690

[5] *Oracle's CSO Demands an End to Customers Checking Oracle Products for Defects*, Cory Doctorow, Boing Boing, http://boingboing.net/2015/08/11/oracles-cso-demands-an-end-t.html

[6] *Michael Lynn's Controversial Cisco Security Presentation*, Cory Doctorow, Boing Boing, http://boingboing.net/2005/07/29/michael-lynns-contro.html

[7] *US v. ElcomSoft-Sklyarov*, EFF, https://www.eff.org/cases/us-v-elcomsoft-sklyarov

[8] *Therac-25*, Wikipedia, https://en.wikipedia.org/wiki/Therac-25

Engineering, and safety engineering in particular, has a strong tradition of convening post-mortems, accident investigations, root cause analyses, etc. When there's a plane crash, the National Traffic Safety Board figures out what went wrong, and tells the public in great technical detail so that others can learn from the errors and figure out how to make aviation safer in the future. When there were Space Shuttle crashes, the government launched independent investigatory boards to figure out why the Shuttles failed and share that information. ¶

These kinds of analyses can be embarrassing to companies. But in information security, practitioners have a lot of powerful expertise and a willingness to bring that expertise to bear investigating problems and sharing what they learn. Things like Google's Project Zero (and the incredible range of research that has appeared at conferences year after year) show that you don't have to be officially chartered to advance the state of the art in security engineering: you just have to be smart, motivated and willing to tell the public what you find out. Regulators wouldn't have the resources to do all that on their own, and vendors lack both the resources and the incentive to let the public know the results.

Removing barriers to disclosure

Given the importance of research and disclosure to improving safety, our legal system should not punish those who engage in it. Unfortunately, a law that was intended for a very different purpose, can be used to do exactly that. Specifically, research and disclosure can be subject to legal threat if that research required interfering with or circumventing digital locks on software embedded in a device. In 1998, Congress passed the Digital Millennium Copyright Act, which included language that prohibits breaking a "digital lock" that forms "an effective means of access control" to a copyrighted work, even if the lock is being removed for an otherwise lawful purpose.

The DMCA was intended to update America's entertainment industry regulations for the digital era. Because it applies to technological protections on all kinds of software, however, it affects safety testing for all kinds of devices, including medical devices. The DMCA has been used to threaten and prosecute researchers who come forward with information about vulnerabilities[9] on the grounds that these disclosures would facilitate copyright infringement. Significantly, researchers who discovered critical vulnerabilities in medical devices, including implanted devices, were discouraged from coming forward with their revelations,[10] leaving their users in the dark about their own safety, and leaving the vulnerabilities intact to be exploited by unscrupulous parties, from malicious "pranksters" to organized criminals.

The DMCA has no place in the medical device world

Fortunately, the FDA has a simple remedy for this state of affairs: it can require that vendors covenant, as a condition of approval of their devices for field use, to abstain from the use of DMCA 1201 for causes of action related to security research. Vendors could opt out of the covenant, but would have to demonstrating that they had a policy to compensate for the delays and omissions in vulnerability reporting that their products would face as a result.

[9] *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Comments, Proposed Class 25: Software – security research*, US Copyright Office, http://copyright.gov/1201/2015/comments-020615/

[10] *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Comments, Proposed Class 27: Software – networked medical devices*, US Copyright Office, http://copyright.gov/1201/2015/comments-020615/

The covenant is deliberately narrow

The covenant is designed to be narrow. In essence vendors are simply promising not to use copyright law to prevent security or safety research. It says nothing about a vendor's other rights (e.g. patent, trade secrets, contracts), leaving intact all the traditional mechanisms that Congress has granted to companies to protect their investments.

In an analysis of 50 court cases that invoked Section 1201 of the DMCA,[11] we found that 47 of the complaints invoked a legal theory other than anti-circumvention liability; of the remaining three, two were criminal complaints and one was dismissed. In other words, 100 percent of the substantive civil complaints under the DMCA could continue under a different legal theory; the covenant only covers "bare circumvention" without any additional conduct that gives rise to a complaint. This covenant would limit only those very unusual claims.

Ensuring security research improves failure modes

It would be irresponsible to plan a national medical device policy on the assumption that everything will go right. The post-market reporting of mistakes and prevention of market abuses are every bit as important to public safety as ensuring that things work well in the first place. By safeguarding patients, users, competitors and security researchers through post-market reporting procedures, the FDA will complement its commitment to excellence in initial manufacture with an equally important commitment to excellence in graceful failure modes.

Respectfully submitted,

Cory Doctorow
Corynne McSherry
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
cory@eff.org
corynne@eff.org

[11] https://www.eff.org/document/list-1201-threats