RAPID7

Comments to "*Cybersecurity Best Practices for Modern Vehicles*"

Docket ID: NHTSA-2016-0104

Nov. 28, 2016

Rapid7 submits these comments in response to the the National Highway Traffic Safety Administration's request for public comment on its draft Cybersecurity Best Practices for Modern Vehicles.[1]

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities, rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

We applaud the National Highway Traffic Safety Administration's (NHTSA) initiative in producing its draft Cybersecurity Best Practices for Modern Vehicles.[2] NHTSA has been a consistent advocate for driver safety for decades, and this mission remains critical as vehicles evolve to include more connectivity and digital features. The digital attack surface for vehicles is quickly growing larger, and action from the ecosystem – automakers, equipment manufacturers, drivers and regulators – will be needed to mitigate new risks.

NHTSA's draft best practices, which appear to generally reflect the Automotive ISAC's Automotive Cybersecurity Best Practices,[3] are a good step towards evolving with vehicle technology. Below are three recommendations to improve NHTSA's draft best practices.

I. Security updating should be a "fundamental vehicle cybersecurity protection."

NHTSA's draft best practices do not recommend security updates, though the draft notes that the "cybersecurity environment is dynamic and is expected to change continually."[4] Rapid7 views a

---

[1] National Highway Traffic Safety Administration, Request for public comment, 81 Fed. Reg. 75190, Oct. 28, 2016.
[2] National Highway Traffic Safety Administration, Cybersecurity Best Practices for Modern Vehicles, Oct. 2016, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.
[3] Automotive Information Sharing and Analysis Center, Automotive Cybersecurity Best Practices, Jul. 2016, https://www.automotiveisac.com/best-practices.
[4] National Highway Traffic Safety Administration, Cybersecurity Best Practices for Modern Vehicles, Oct. 2016, pg. 5, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

security update and advisory mechanism as a mandatory component of cybersecurity plans, and we do not believe technical challenges to updating vehicle software are insurmountable. NHTSA should urge the automotive industry to implement an update management program for vehicles, and encourage broad collaboration among manufacturers, mechanics and repair organizations, and security researchers to strengthen security and transparency across the supply chain.

While automakers may strive to "ensure that systems are designed free of unreasonable risks to motor vehicle safety,"[5] all software ships with exploitable bugs and implementation-based exposures. Vulnerabilities can arise through a variety of sources – vehicle system software or firmware, cloud-based features, proprietary infotainment interfaces, accessory devices or third party apps, the surrounding network, and other externalities. It will be impossible to protect these complex and diverse systems against every serious vulnerability before vehicles leave manufacturers' warehouses.

Cybersecurity vulnerabilities can surface more suddenly and affect a higher number of vehicles more quickly than mechanical part failures. While vehicle security patches may need time to roll out, a rapid (ideally over-the-air) update practice to critical exposures is important given the potential safety risks of inaction and the consumer engagement challenges associated with traditional recalls.[6] In addition, we believe companies should make plans to maintain patching capability beyond the typical lifetime or planned obsolescence of the vehicle, to protect end-users that rely on their vehicles for long periods.

NHTSA may choose to issue additional guidance to the auto industry, detailing mechanisms and approaches for issuing security updates, but the concept of security updating should be included in NHTSA's best practices as a "fundamental vehicle cybersecurity protection."[7]

II. Automakers should be transparent about cybersecurity features.

NHTSA's best practices should encourage automakers to be transparent to consumers – no later than at the point of sale – about vehicles' essential security features. Typically, vehicle buyers can already obtain granular, easy-to-understand information about the mechanical, physical safety, and performance features of specific vehicles. This practice should be extended to digital safety as well. Transparency will enable consumers to make informed choices and may prompt market competition for strong vehicle security.[8]

---

[5] *Id.*

[6] Jerry Hirsch, Many recalled vehicles do not get repaired, posing a safety risk, Los Angeles Times, Dec. 27, 2014, http://www.latimes.com/business/autos/la-fi-hy-record-recalls-20141228-story.html.

[7] National Highway Traffic Safety Administration, Cybersecurity Best Practices for Modern Vehicles, Oct. 2016, pg. 17, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[8] The National Telecommunications and Information Administration has begun an initiative on communicating security upgradability for Internet of Things devices. National Telecommunications and Information Administration, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, Oct. 24, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

Today, information about mechanical, physical safety, and performance features is often available at several degrees of detail: higher level summary information for casual consumers, greater detail for more sophisticated vehicle users, and very granular data for experts and practitioners. To maximize understanding, transparency regarding automotive cybersecurity features should follow the same pattern, with different levels of detail reaching a wide range of audiences. Two critical components that should be included at each level of disclosure are 1) Whether the automaker issues security updates for critical cybersecurity vulnerabilities, and whether those updates occur over-the-air or only through mechanics/dealers; and 2) The length of time for which the automaker provides security update support to the vehicle.

III. Vulnerability reporting/disclosure policies should be based on existing guidance.

Rapid7 supports NHTSA's inclusion of vulnerability reporting/disclosure policies as a component of the draft best practices.[9] Since cybersecurity vulnerabilities cannot be completely eliminated pre-market, companies must be prepared to discover, assess, and remediate cybersecurity flaws throughout the product lifecycle. Security vulnerabilities may be too voluminous or difficult for many companies' internal security teams to discover and assess alone. It is increasingly crucial to foster an environment where companies take disclosure of security issues from external sources – such as independent security researchers – seriously and openly, rather than with legal threats or avoidance. To do this effectively, it is critical for to have a plan and policy in place to receive and process vulnerability information from external sources.

NHTSA's draft best practices recommend that vulnerability reporting/disclosure policies should detail the company's expectations for the relationship between companies and researchers.[10] Yet the draft best practices give no additional guidance on what this relationship should look like to be most effective for consumer safety. Rapid7 has witnessed a wide range of responses in our experience researching and disclosing cybersecurity flaws to software vendors. There is a risk that some companies will use reporting/disclosure policies to place overbroad restrictions on research activity – such as accepting only vulnerabilities on a narrow set of products/features, or requiring researcher confidentiality for prolonged or indefinite terms beyond the safety needs of consumers even if the company is not developing a security patch. Such a restrictive approach may well backfire and fail to improve the broad coordination between researchers and companies that is needed.

We recommend that NHTSA's draft best practices encourage automakers to adopt vulnerability reporting/disclosure policies that are based on existing best practices for vulnerability disclosure and handling, such as ISO 29147 and ISO 30111.[11] The Dept. of Commerce's multistakeholder process

[9] National Highway Traffic Safety Administration, Cybersecurity Best Practices for Modern Vehicles, Oct. 2016, pg. 14, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.
[10] *Id.*
[11] ISO/IEC 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Feb. 15, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1,

on vulnerability disclosure, which Rapid7 supports, has also laid good groundwork for such policies.[12] Rapid7 generally believes vulnerability handling policies are made more effective as more software products can reasonably be included in such policies, and that researchers should be empowered to safely communicate their research to the public after an appropriate waiting period. Rapid7's own policies on vulnerability handling and disclosure – as a company that both receives and discloses software vulnerabilities – are available online.[13]

* * *

We appreciate the opportunity to share our views. If there are additional questions, or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at Harley_Geiger[at]Rapid7.com. Thank you.

END

2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[12] Multistakeholder Process: Cybersecurity Vulnerabilities, National Telecommunications and Information Administration, Apr. 08, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[13] Rapid7, Disclosure policy, https://www.rapid7.com/disclosure (last accessed Nov. 28, 2016).