January 21st, 2020

TLP White

In this edition of Hacking Healthcare, we begin with security researchers calling for a common language for hardware vulnerabilities. Next, we briefly detail how the European Commission is prepared to take drastic steps to curb misuse of facial recognition software. Additionally, we outline how Google's Dr. Feinberg is defending their partnership with Ascension. Finally, we quickly run through the topics that will be discussed at next week's H-ISAC Monthly Threat Brief. Welcome back to *Hacking Healthcare*.

1. **Hardware Vulnerabilities Need A Common Language.** According to a pair of Intel security researchers, hardware manufacturers are in desperate need of a standardized "language" to describe and classify the burgeoning list of hardware vulnerabilities. Intel's researchers state that there is no satisfactory method to understand "how these vulnerabilities get introduced into products, how they can be exploited, their associated risks, as well as best practices to prevent and identify them early on in the product development lifecycle."[1] As attacks become more sophisticated, often combining hardware and software vulnerabilities, a centralized trusted source that could inform researchers and developers on those questions would be invaluable.

   Intel's researchers propose that an ideal solution would be an overhaul of the current Common Weakness Enumeration ("CWE") system and Common Vulnerability and Exposures ("CVE") system. To quickly review, the CWE system is defined as a "formal list or dictionary of common software weaknesses that can occur in software's architecture, design, code or implementation that can lead to exploitable security vulnerabilities," while the CVE is a "list of common identifiers for publicly known cybersecurity vulnerabilities."[2, 3] Taken together, the CVE and CWE provide the go-to reference for software vulnerabilities. Rather than attempt to recreate a similar structure for hardware vulnerabilities, the researchers suggest that the CWE be revised to include "relevant entry points, common consequences, examples, countermeasures and detection methods from the specific hardware perspective."[4]

2. **European Commission Mulls Facial Recognition Ban.** As emerging technologies continue to forge ahead with unprecedented speed, legislative and regulatory bodies are struggling to keep up. While there is still some time to come to terms with how quantum computing will change the world, and even more before true AI is created, machine learning assisted facial recognition is already being used globally by social

media, law enforcement, and governments.[5, 6] Despite this, laws and regulations that seek to manage its use are few and far between.

In response to the lack of regulation and its growing use, the European Commission is considering a ban on the technology for up to five years as it attempts to assess the potential for misuse. The European Commission outlined its position in an 18-page draft report obtained by Euractiv.[7] The report set forth a number of proposed actions that could include "imposing obligations on both developers and users of artificial intelligence," as well as creating a new European authority to monitor any new rules established.[8] The report states its hope that a temporary ban would allow for the creation of "a sound methodology for assessing the impacts of this technology [as well as] possible risk management measures.[9] The report does state that should a ban be put in place, exceptions could be made for security and research purposes.

3. **Google Defends Ascension Partnership.** It was only several months ago that Google faced scathing criticism from the public, and even some raised eyebrows from Congress, when a whistleblower voiced concerns to journalists about the privacy concerns and potential HIPAA violations that may be occurring under their seemingly secretive partnership with the health system Ascension. The partnership gave Google access to millions of American's PHI without their consent or knowledge and little was known about how the data was being used. Last week, Google Health's VP Dr. David Feinberg attempted to set the record straight.

   Dr. Feinberg was adamant that the press was too quick to jump to conclusions by saying "This is not us mining somebody's records to sell ads," and that the Wall Street Journal grossly misrepresented the scale of the work they were doing at the time.[10] He continued by saying that the organization of Ascension's health records was limited to "Two hospitals, not three quarters of the United States like the Wall Street Journal said."[11] Furthermore, Dr. Feinberg reiterated that the goal of the partnership continues to be improving the ability of clinicians to access data and ultimately improve care for patients.[12] There was an open admission that patients whose data ended up being used were not told, but Dr. Feinberg defended the practice by pointing out that its routine for healthcare organizations to have business associate's arrangements with other parties and that this was no different.[13]

Congress –

Tuesday, January 21st:
- No relevant hearings

Wednesday, January 22nd:
- No relevant hearings

Thursday, January 23rd:
- No relevant hearings

January 21st, 2020

International Hearings/Meetings –
EU –
-No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
--Healthcare Cybersecurity Forum - Southern California – San Diego, CA (2/5/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/Southern_California
--Global Cyber Security in Healthcare & Pharma Summit - London, UK (2/6/2020)
http://www.global-engage.com/event/cybsec-health-summit/
--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Chennai, India (3/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-india/
--2020 APAC Summit – Singapore (3/31/2020-4/2/2020)
https://h-isac.org/summits/apac-summit-2020/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/14/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (4/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/

Sundries –
--FBI: Nation-state actors have breached two US municipalities
https://www.zdnet.com/article/fbi-nation-state-actors-have-breached-two-us-municipalities/
--Hackers Are Securing Citrix Servers, Backdoor Them for Access
https://www.bleepingcomputer.com/news/security/hackers-are-securing-citrix-servers-backdoor-them-for-access/

January 21st, 2020

--Microsoft: Application Inspector is now open source, so use it to test code security
https://www.zdnet.com/article/microsoft-application-inspector-is-now-open-source-so-use-it-to-test-code-security/
 --As Putin Schemes to Extend His Reign, Expect New Forms of Internet Repression
https://www.nextgov.com/policy/2020/01/putin-schemes-extend-his-reign-expect-new-forms-internet-repression/162490/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.helpnetsecurity.com/2020/01/13/common-weakness-enumeration-hardware/

[2] https://cwe.mitre.org/about/index.html

[3] https://cve.mitre.org/about/

[4] https://www.helpnetsecurity.com/2020/01/13/common-weakness-enumeration-hardware/

[5] https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html

[6] https://www.cnet.com/how-to/how-to-review-and-turn-off-facebooks-facial-recognition-feature/

[7] https://www.theguardian.com/technology/2020/jan/17/eu-eyes-temporary-ban-on-facial-recognition-in-public-places

[8] https://www.bbc.com/news/technology-51148501

[9] https://www.bbc.com/news/technology-51148501

[10] https://www.healthcareitnews.com/news/google-health-vp-ascension-partnership-press-has-made-something-its-not

[11] https://www.healthcareitnews.com/news/google-health-vp-ascension-partnership-press-has-made-something-its-not

[12] https://www.healthcareitnews.com/news/google-health-vp-ascension-partnership-press-has-made-something-its-not

[13] https://www.healthcareitnews.com/news/google-health-vp-ascension-partnership-press-has-made-something-its-not