July 31, 2018

TLP White

We start with a new/not so new vulnerability in Bluetooth and then spend some time talking about some government initiatives in Australia and elsewhere focused on citizen healthcare data. We conclude with an interesting update from the recently reported SingHealth breach. Welcome back to *Hacking Healthcare:*

Authors Note: I had the pleasure of attending the inaugural NH-ISAC's Blended Threat Exercise in Maple Grove, MN last week. I want to thank the great people at Boston Scientific for hosting the event, and for the great work NH-ISAC staff and members clearly put into developing the exercise. There are four more planned over the next few months, and we'll keep you updated in our ***Conferences, Webinars, and Summits*** section below. These types of exercises are an excellent way to test your knowledge and your organization's ability to respond when faced with complex incidents. I highly recommend that you make time to attend.

Hot Links –

1. ***Bluetooth Vulnerability.*** From our "Ok, but how bad is it really?" department, we report on a recently disclosed vulnerability in the Bluetooth protocol. Last week, US-CERT issued an advisory[1] regarding the vulnerability and reports since then have followed the typical cycle of hype->counter-hype->actual risk. Here is what we know:

   Bluetooth is a widely (to put it mildly) implemented wireless protocol for creating communications between two or more devices. For most users, it is the means by which you connect your headphones, speakers, mouse, keyboard or other types of accessories to your laptop, PC, or mobile device. It's effective, reliable and other than having to authorize an initial pairing request, requires little user interaction.

   That pairing request is the essential security mechanism that prevents random devices from connecting to each other without the user's knowledge, and is also where this particular vulnerability was found. In this case, the vulnerability is the "result of a missing check on keys during the process of encrypting data sent over Bluetooth

[1] https://www.kb.cert.org/vuls/id/304725

connections. More specifically, it was a missing validation contained in the method of encryption used in Bluetooth, a standard known as the 'Diffie-Hellman key exchange.'"[2]

If wireless protocol security isn't your thing, all you need to know is for vulnerable devices, an attacker could intercept the messages between the two devices, which could be anything from the music you are listening to, to multi-factor authentication codes that could enable the attacker to create more harm.

For its part, the Bluetooth SIG, which oversees the development of the standard, issued a statement bringing some clarity to the situation and is providing guidance for manufacturers in the development of patches.[3]

2. ***Healthcare Down Under (And Beyond).*** Coming to Australia in mid-October this year is the *My Health Record* initiative. The government program "…is intended to provide details of a patient's medical history easily to doctors who have not previously treated them..."[4]

   That sounds pretty useful and it "has the backing of all of Australia's peak health bodies, including the Australian Medical Association, the Royal Australian College of GPs and the Pharmacy Guild of Australia." What could go wrong?

   You might recall that last week, we talked about the incident in Singapore where health information on nearly 1/3rd of the population was exposed. That is one of the things that can go wrong.

   Unsurprisingly, privacy advocates have pointed out that the information in this database could be used for discriminatory practices, or for purposes not directly related to a person's health.

   They point to a similar program that was attempted in the UK a few years ago, and that didn't end well. After about two years, the program was abandoned "…after an investigation found that drug and insurance companies were able to buy information on patients' mental health conditions, diseases and smoking habits."[5] Many have noted that the privacy framework for *My Health Record* is essentially identical to the one used in the UK program, and in fact was developed in part by the same person.

---

[2] https://www.forbes.com/sites/thomasbrewster/2018/07/24/bluetooth-hack-warning-for-iphone-android-and-windows/#78d41da77d73

[3] https://www.bluetooth.com/news/unknown/2018/07/bluetooth-sig-security-update

[4] https://www.theguardian.com/australia-news/2018/jul/22/my-health-record-identical-to-failed-uk-scheme-privacy-expert-says

[5] https://www.theguardian.com/australia-news/2018/jul/22/my-health-record-identical-to-failed-uk-scheme-privacy-expert-says

We will be watching this issue closely and will provide additional discussion as it evolves. Stay tuned.

3. ***Third-Party Risk May Help Explain Singapore Breach.*** As we reported last week and mentioned above, Singapore recently experienced the largest data breach in its history, resulting in the unauthorized access and theft of health records belonging to 1.5 million Singaporeans. Over the weekend, Trustwave's SpiderLabs published a blog post providing an analytical perspective on the SingHealth breach.[6]

The post provides an analysis of two files published by unknown actors on Pastebin, a code and text storage website.[7] Researchers suspect that the files found on Pastebin are linked to the SingHealth breach, including an exception log from a Java server that was posted on Pastebin on May 24th. The log shows a query for delegating access to a SingHealth database to an IT contractor. Researchers believe that the hacker was able to access the SingHealth database by taking over the contractor's user account. Researchers also discovered that several SQL queries targeting SingHealth medical data had been uploaded to Pastebin, indicating that the individual executing the queries was in search of sensitive information. While the investigation is still underway in the SingHealth breach, researchers noted that the combination of events occurring within the attack window are highly suspicious.

SingHealth may be the latest, but is certainly not the only example of compromised third-party vendor credentials leading to serious breach exposure. The 2013 Target breach, which exposed credit card and personal data belonging to more than 110 million consumers, was traced back to network credentials issued to an HVAC firm with whom Target had contracted, and were later stolen in an email malware attack.[8] Earlier this year, Hancock Health paid hackers 4 bitcoin (or $47,000) to unlock its network following a SamSam ransomware attack in which hackers compromised a third-party vendor's administrative account to the hospital's remote-access portal.[9] The Petya ransomware outbreak also relied on account credentials to effectuate the attack.[10]

Breaches like the SingHealth breach and others involving third-party risk have compelled us at NH-ISAC to support the Third-Party Risk Governance ("TPRG") Summit. NH-ISAC and its member organizations, in partnership with the Global Resilience Federation ("GRF"), created a cross-sector summit to include members and vendors across eight different information sharing communities with the common goal of increasing security across industries. Summit attendees will have the opportunity to participate in training, education and networking on critical cyber and physical security issues facing

---

[6] https://www.trustwave.com/Resources/SpiderLabs-Blog/SingHealth-Data-Breach-%E2%80%93-An-Analytical-Perspective/?page=1&year=0&month=0&LangType=1033

[7] https://www.securityweek.com/massive-singapore-healthcare-breach-possibly-involved-contractor

[8] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[9] https://www.healthcareitnews.com/news/hancock-health-pays-47000-ransom-unlock-patient-data

[10] https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/

organizations, vendors, and the intersection of the two. For more information about the GRF Summit on Third-Party Risk, please visit: https://www.grfederation.org/2018-Summit-Overview.

Congress –

Tuesday, July 31:
--Hearing to examine reducing health care costs, focusing on decreasing administrative spending (Senate Committee on Health, Education, Labor, and Pensions).[11]
--Hearing to examine internet and digital communications, focusing on the impact of global internet governance (Senate Subcommittee on Communications, Technology, Innovation, and the Internet).[12]

Wednesday, August 1:
-- Hearing to examine foreign influence operations and their use of social media platforms (Senate Committee on Intelligence).[13]

Thursday, August 2:
--No relevant hearings

Conferences, Webinars, and Summits –

--Basic Best Practices in Cybersecurity – Abilene, TX (7/31) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas-2/>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA– Washington, DC (8/9) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--NH-ISAC Blended Threats Exercise Series – CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Biotech/Pharma Security Workshop at Gilead Sciences – Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>
--Biotech/Pharma Security Workshop at Amgen – Tokyo, Japan (8/29) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-at-amgen-tokyo/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

[11] https://www.senate.gov/committees/hearings_meetings.htm
[12] https://www.senate.gov/committees/hearings_meetings.htm
[13] https://www.senate.gov/committees/hearings_meetings.htm

--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC & Cleveland Clinic Medical Device Security Workshop – Breachwood, OH (10/17-18) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-cleveland-clinic-beachwood-oh/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Demployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**Election Security Problems Go Beyond 2018**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/07/30/election-security-problems-go-beyond-2018-300204>
--**Trump convenes election security meeting as hacking looms**
<https://www.reuters.com/article/us-usa-election-security/trump-convenes-election-security-meeting-as-hacking-looms-idUSKBN1KH1O4>
--**Jailhouse Tablets Allow Inmates to Steal Thousands of Dollars in Credits**
< https://threatpost.com/jailhouse-tablets-allow-inmates-to-steal-thousands-of-dollars-in-credits/134527/>
--**Mozilla to Remove Support for Built-In Feed Reader From Firefox**
<https://www.bleepingcomputer.com/news/software/mozilla-to-remove-support-for-built-in-feed-reader-from-firefox/>
--**DOD to Move All Websites to HTTPS by the End of the Year**
<https://www.bleepingcomputer.com/news/government/dod-to-move-all-websites-to-https-by-the-end-of-the-year/>
--**Windows 10 Maps App Updated With Several New Features for Insiders**
<https://www.bleepingcomputer.com/news/microsoft/windows-10-maps-app-updated-with-several-new-features-for-insiders/>
--**Fighting Chinese cyber-espionage could cost U.S. 5G dominance**
< https://www.cyberscoop.com/5g-network-huawei-zte-us-telecom/>

July 31, 2018

--**NetSpectre attack can exploit CPUs to leak information remotely, researchers say**
<https://www.cyberscoop.com/netspectre-spectre-variant-remote-hack/>
--**The Law of Military Cyber Operations and the New NDAA**
<https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa>
--**How a Bunch of Lava Lamps Protect Us from Hackers**
<https://www.wired.com/story/cloudflare-lava-lamps-protect-from-hackers>

Contact us: follow @NHISAC and email at contact@nhisac.org