LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing Wearable Device Security

OVERALL CLASSIFICATION IS TLP:WHITE

March 19, 2020

Agenda

- Overview
- Wearables in Healthcare
- Threats to Wearable Devices
- Sywentooth
- Wearable Data Path
- Wearable Device Vulnerabilities Examples
- Application Vulnerabilities – Walkie Talkie
- Application Vulnerabilities - MyFitnessPal
- Wearable Device Best Practices
- References
- Conclusion

Slides Key:

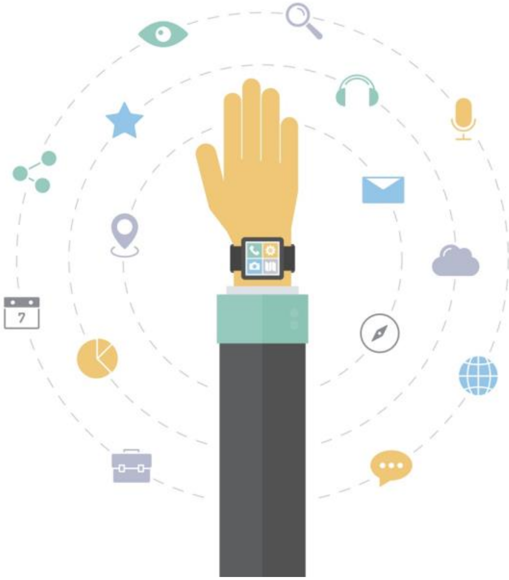
Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

Wearable Technology (Wearable devices, wearables): electronic technologies or computers that are incorporated into items of clothing and accessories with can be comfortably worn on the body

- Can perform many of the same computing tasks as mobile phones and computers
- Considered part of Internet of Things (IoT) technology
- Often provides sensory and scanning features, such as biofeedback and tracking of physiological function
  - Features makes wearable technology particularly useful for health related activity
- Examples of wearable devices include watches, glasses, contact lenses, e-textiles and smart fabrics, headbands, beanies and caps, jewelry such as rings, bracelets, and hearing aid-like devices that are designed to look like earrings.



Wearable Technology Statistics

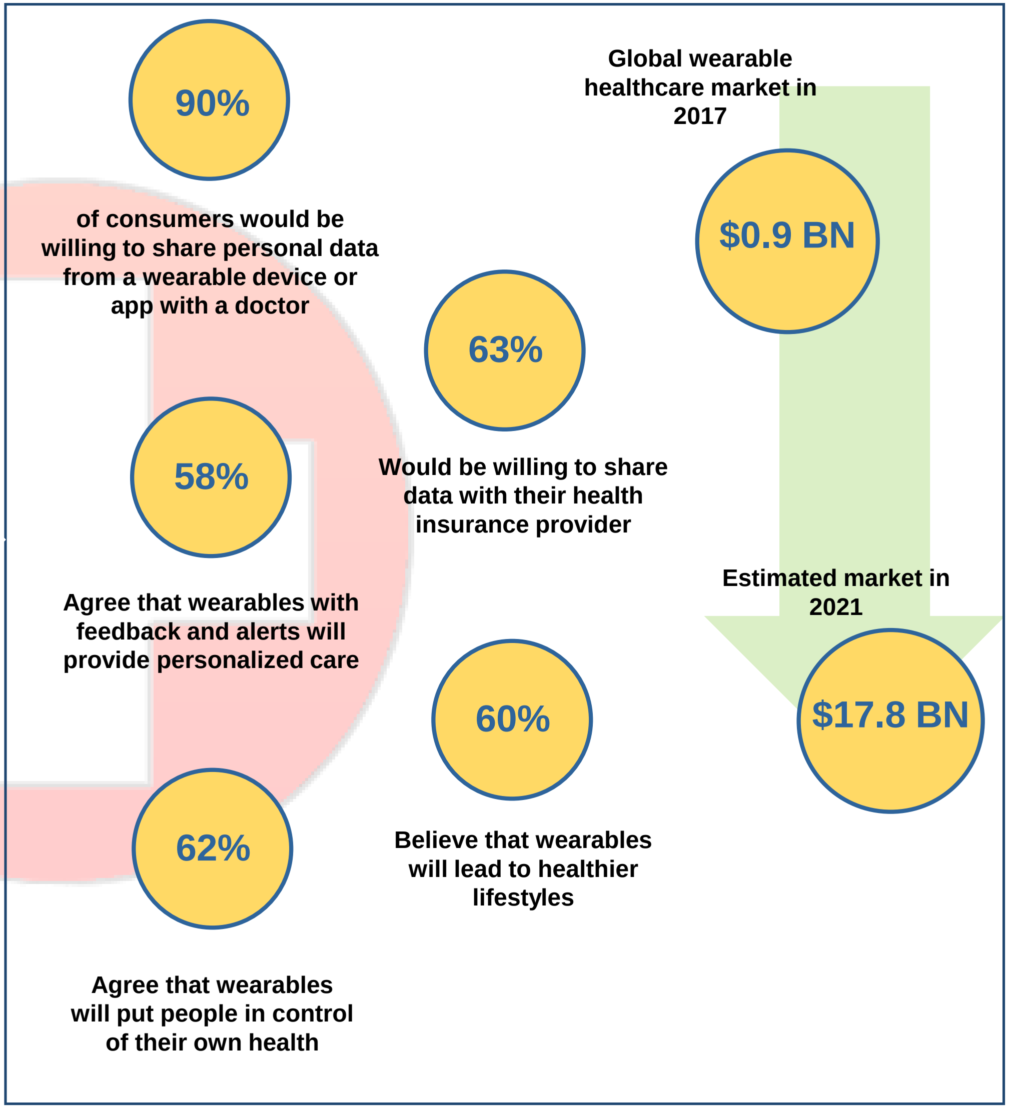
- ➢ Wearable technology and the health app market grew 84 million units in 2015 to 245 million units in 2019
- ➢ Revenue in the Wearables segment amounts to US$15,376m in 2020.
- ➢ Revenue is expected to show an annual growth rate (CAGR 2020-2024) of 3.8%, resulting in a market volume of US$17,856m by 2024.
- ➢ The average revenue per user (ARPU) currently amounts to US$43.09.
- ➢ In global comparison, most revenue is generated in China (US$4,800m in 2020).

Source: Statista, Wearabledevices, smartercx

Healthcare

The convenience and real-time data that wearable technology provides allows many medical industry, insurers, providers, and technology companies to incorporate them into their processes.

- Wearables store and transmit PHI-related data that is covered under HIPAA
- Despite security concerns, support for wearable usage in healthcare is overwhelmingly positive:



90% of consumers would be willing to share personal data from a wearable device or app with a doctor

63% Would be willing to share data with their health insurance provider

58% Agree that wearables with feedback and alerts will provide personalized care

60% Believe that wearables will lead to healthier lifestyles

62% Agree that wearables will put people in control of their own health

Global wearable healthcare market in 2017: $0.9 BN

Estimated market in 2021: $17.8 BN

Source: Medicaldevice-network, Businessinsider, wearable technologies, raconteur

Healthcare

Wearable benefits in Healthcare

Personalization. The doctor, with the help of a software can quickly create a program based on the needs of the patient

Early diagnosis. Precise medical parameters in the wearable devices allow early detection of symptoms

Remote patient monitoring. Healthcare professionals can monitor patients remotely and in real-time through the use of wearable devices

Adherence to medication. Wearable devices help patient to take medications on time and even inform medical professionals if the patient fails to adhere to medications

Information registry. The data are stored in real-time, allowing a more exhaustive analysis of the information. Results in a more complete and precise report on the patient's medical history, which can be shared with other medical specialists.

Optimum decision by the doctor. The doctor is able to compare and analyze data to make a sharper clinical decision to enhance the patient's quality of life.

Saving healthcare cost. Remote healthcare via wearable devices mean saving time and mobility, as it removes the need for the patient to be continuously transferred to the medical center.

Health related wearable technology examples:

Fitness Tracker – tracks physical activities and heart rate

Electrocardiogram (ECG) monitors – records electric signals in the heart to monitor heart disease, anxiety, etc.

Blood pressure monitors – can measure blood pressure and daily activity

Wearable biosensors (skin patches) – self-adhesive patch that collects data on movement, heart rate, respiratory rate, and temperature

Smart glasses – eyeglass that incorporate first person imaging, facial recognition, enhanced turn-wise directions, healthsensing, etc.

Hearables – hearing aids that incorporate functions such as sleep monitoring, brain wave analysis, and virtual assistant support

SweynTooth

Wireless/Bluetooth Weaknesses: Technology such is Bluetooth is often used to connect wearable devices to phones and other devices, however, many of these technologies are insufficient at securing against simple threats such as a brute force attack.

- Researchers disclosed the existence of 12 potentially severe security vulnerabilities, collectively named **SweynTooth**.
  - The vulnerabilities specifically impacts Bluetooth-enabled devices.
    - Caused by poor implementation of Bluetooth Low Energy technology on devices.
      - Used on 480 distinct products from vendors including blood glucose meters and MRIs
      - Consumer goods affected include consumer electronics, smart home devices, and **wearables**
        - Many used in the healthcare industry
  - According to the report, hackers in close physical proximity to vulnerable devices can abuse this vulnerability to remotely trigger deadlocks, crashes, and even bypass security in BLE products, allowing them to arbitrary read or write access to device's functions that are otherwise only allowed to be accessed by an authorized user.

List of SweynTooth vulnerabilities

•**Link Layer Length Overflow (CVE-2019-16336, CVE-2019-17519)** — These allow attackers in radio range to trigger a buffer overflow by manipulating the LL Length Field, primarily leading to a denial of service attacks.

•**Link Layer LLID deadlock (CVE-2019-17061, CVE-2019-17060)** — These trigger deadlock state when a device receives a packet with the LLID field cleared.

•**Truncated L2CAP (CVE-2019-17517)** — This flaw results due to a lack of checks while processing an L2CAP packet, causing a denial of service and crash of the device.

•**Silent Length Overflow (CVE-2019-17518)** — A buffer overflow occurs when a certain packet payload with higher than expected LL Length is sent, the peripheral crashes.

•**Invalid Connection Request (CVE-2019-19195)** — When devices do not properly handle some connection parameters while the central attempts a connection to the peripheral, they could lead to Deadlock state.

•**Unexpected Public Key Crash (CVE-2019-17520)** — This bug is present in the implementation of the legacy pairing procedure, which is handled by the Secure Manager Protocol (SMP) implementation and can be used to perform DoS and possibly restart products.

•**Sequential ATT Deadlock (CVE-2019-19192)** — This flaw lets attackers deadlock the peripheral by sending just two consecutive ATT request packets in each connection event.

•**Invalid L2CAP fragment (CVE-2019-19195)** — improper handling of the PDU size of the packets can lead to deadlock behavior.

•**Key Size Overflow (CVE-2019-19196)** — This overflow in the device memory issue is a combination of multiple bugs found during the pairing procedure of devices, resulting in a crash.

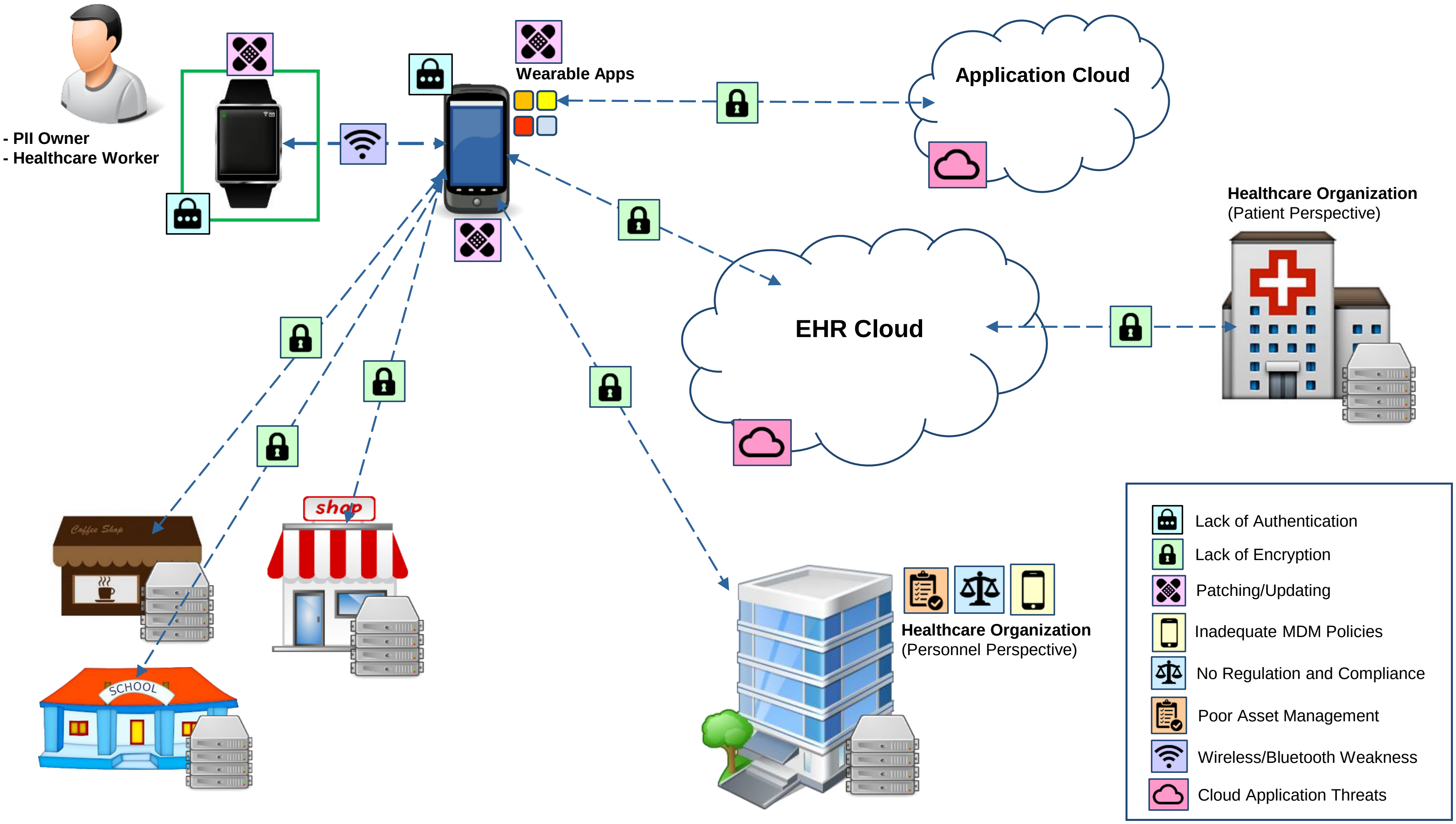
•**Zero LTK Installation (CVE-2019-19194)** — This critical vulnerability is a variation of one of the Key Size Overflow. It affects all products using Telink SMP implementation with support for secure connection enabled.

"The most critical devices that could be severely impacted by SweynTooth are the medical products. VivaCheck Laboratories, which manufacture Blood Glucose Meters, has many products listed to use DA14580,“ - Singapore University of Technology and Design Report

Hacker News, Singapore University of Technology and Design

TLP:WHITE

Wearable Devices Data Path



- PII Owner
- Healthcare Worker

Wearable Apps

Application Cloud

EHR Cloud

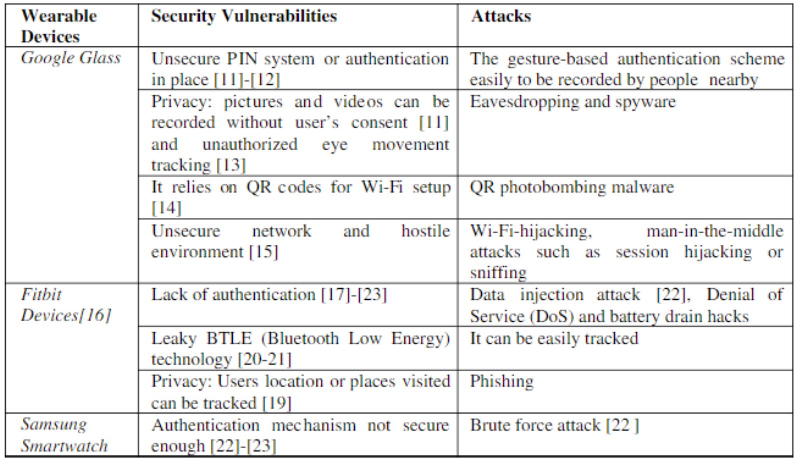
Healthcare Organization
(Patient Perspective)

Healthcare Organization
(Personnel Perspective)

- Lack of Authentication
- Lack of Encryption
- Patching/Updating
- Inadequate MDM Policies
- No Regulation and Compliance
- Poor Asset Management
- Wireless/Bluetooth Weakness
- Cloud Application Threats

Wearable Device Vulnerability Examples

Summary of Security Vulnerabilities and Security Attacks Found in Popular Wearable Devices (2017)



Wearable Devices	Security Vulnerabilities	Attacks
Google Glass	Unsecure PIN system or authentication in place [11]-[12]	The gesture-based authentication scheme easily to be recorded by people nearby
	Privacy: pictures and videos can be recorded without user's consent [11] and unauthorized eye movement tracking [13]	Eavesdropping and spyware
	It relies on QR codes for Wi-Fi setup [14]	QR photobombing malware
	Unsecure network and hostile environment [15]	Wi-Fi-hijacking, man-in-the-middle attacks such as session hijacking or sniffing
Fitbit Devices[16]	Lack of authentication [17]-[23]	Data injection attack [22], Denial of Service (DoS) and battery drain hacks
	Leaky BTLE (Bluetooth Low Energy) technology [20-21]	It can be easily tracked
	Privacy: Users location or places visited can be tracked [19]	Phishing
Samsung Smartwatch	Authentication mechanism not secure enough [22]-[23]	Brute force attack [22]

Source: Semantic Scholar, Researchgate, VPN Mentor

Vulnerabilities found on medical wearable devices (2018)

Digitsole Warm Insoles

Vulnerabilities found:

- Exposes personal information
- Accesses location even when turned off
- Collects data about your Facebook profile.

Hackers could connect to the Insoles via Bluetooth and change the heat on the insoles to a hot temperature

Modius Headband

Vulnerabilities found:

- Accesses location and fingerprint
- Reveals personal information about your body

Hackers could control the device to alter the electric current, causing nausea and general sickness

Ivy Health Kid's Thermometer

Vulnerabilities found:

- Exposes personal information
- Stores this information over insecure HTTP
- Collects data about names, data of birth, gender, temperature, etc.

Hackers could find and expose information about relationship of each child's family.

Application Vulnerabilities – Walkie-Talkie App

In 2019 Web application security experts reported the presence of a vulnerability in the Apple Watch

- if exploited, allowed threat actors to spy on users of iPhone devices.
- The vulnerability was exploitable through Walkie-Talkie, an app installed on Apple Watch; due to this flaw, people could listen to calls on other users' iPhone.
  - The **Walkie-Talkie app** allows two users to send and receive short audio messages; you need to accept an invitation before receiving the messages.
  - Apple disclosed that a user reported a vulnerability that allowed other users to listen through other people's iPhone without their consent or knowledge

When discovered, Apple disabled the function then released a security update to fix this issue.

- Apple also stated it was not aware of any use of the vulnerably against a customer and specific conditions and sequences of events were required to exploit it.

10:10
WALKIE-TALKIE
John Voorhees wants to talk with you over Walkie-Talkie.
Always Allow
John
10:21
TALK
10:08
Walkie-Talkie
Talk with friends Apple Watch to Apple Watch. Contacts you add can talk to

Source: Threatpost, Security Newspaper

Application Vulnerabilities – MyFitnessPal

- In 2018, data of more than 150 million users of the MyFitnessPal app were stolen by hackers.
  - MyFitnessPal is advertised as an app that tracks diet and exercise.
  - The breached data includes usernames, email addresses, and hashed passwords.
    - It is still unknown who the breach is attributed to
  - Under Armour, the owner of the app, claims no user financial information was compromised due to the breach.
    - The company also assesses the damage of the breach as moderate, as the app/company does not collect any government-issued identifiers.
  - A year later, it was reported that the stolen credentials from the breach were showing up for sale on the darkweb.
    - The entirety of the breaches data along with along with stolen data from other websites was offered for sale.
      - Hacker’s price for all the data: Less than $20,000 in bitcoin

Source: Csonline, Fortune

Mitigation Practices: Wearable Devices

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate vulnerabilities in wearable devices.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Implement and maintain/update endpoint protection systems.	[2.S.A], [2.M.A], [2.L.A],
Automate provisioning of endpoints and maintain mobile device management program.	[2.L.B]
Develop/maintain asset management program to include initial procurement through decommissioning.	[5.S.A - C], 5.M.A – D]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement automated device discovery/maintenance program along with network access control.	[5.L.A - B]
Implement/maintain intrusion detection/incident response program covering wearable devices when possible	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Implement medical device specific security endpoint protection and network access management program.	[9.S.A], [9.M.A and E]

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

References

- Statista – Wearable Worldwide Statistics
  https://www.statista.com/outlook/319/100/wearables/worldwide
- Wearable Technology and Wearable Devices: Everything you need to know
  http://www.wearabledevices.com/what-is-a-wearable-device/
- Top Wearable Technology Trends and Health Apps to Look for in 2020
  https://smartercx.com/top-wearable-technology-trends-and-health-apps-to-look-for-in-2020/
- Wearable Technology in Healthcare: What are the Leading Tech Themes Driving Change?
  https://www.medicaldevice-network.com/comment/wearable-technology-in-healthcare-what-are-the-leading-tech-themes-driving-change/
- Latest trends in medical monitoring devices and wearable health technology
  https://www.businessinsider.com/wearable-technology-healthcare-medical-devices
- The State of Wearable Technology in Healthcare: Current and Future
  https://www.wearable-technologies.com/2018/10/the-state-of-wearable-technology-in-healthcare-current-and-future
- Wearable Healthcare Tech
  https://res.cloudinary.com/yumyoshojin/image/upload/v1/pdf/future-healthcare-2018.pdf
- Electronic Pickpocket: Security Risks of Wearable Devices
  https://www.eidebailly.com/insights/articles/2018/4/security-risks-wearable-devices

References

- 7 Potential Security Concerns for Wearables
  https://www.csoonline.com/article/3054584/7-potential-security-concerns-for-wearables.html

- 8 Security Threats Wearables Pose to Companies and Individuals
  https://www.vipre.com/blog/8-security-threats-wearables-pose-companies-individuals/

- A Dozen Vulnerabilities Affect Millions of Bluetooth LE Powered Devices
  https://thehackernews.com/2020/02/hacking-bluetooth-vulnerabilities.html

- SweynTooth: Unleashing Mayhem over Bluetooth Low Energy
  https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf

- Assessment of Security Vulnerabilities in Wearable Devices
  https://pdfs.semanticscholar.org/c96a/9f626ef760ed2abe108a0ba8b020722cace5.pdf

- Wearable Technology Devices Security and Privacy Vulnerability Analysis
  https://www.researchgate.net/publication/303870892_Wearable_Technology_Devices_Security_and_Privacy_Vulnerability_Analysis

- Security and Privacy Flaws Discovered on Popular Wearable Devices
  https://www.vpnmentor.com/blog/security-and-privacy-flaws-discovered-on-popular-wearable-devices/

- Apple Disables Walkie-Talkie App Due to Eavesdropping Flaw
  https://threatpost.com/apple-disables-walkie-talkie-app-due-to-eavesdropping-flaw/146410/

References

- Apple Watch Vulnerability Allows You To Spy On Your Friend’s iPhone
  https://www.securitynewspaper.com/2019/07/11/apple-watch-vulnerability-allows-you-to-spy-on-your-friends-iphone/
- 150 Million MyFitnessPal Accounts compromised by a massive data breach
  https://www.csoonline.com/article/3505179/150-million-myfitnesspal-accounts-compromised-by-a-massive-data-breach.html
- Hacked MyFitnessPal Data Goes on Sale on the Dark Web – One Year After the Breach
  https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/
- HHS 405d Program Health Industry Cybersecurity Practices
  https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing
“SweynTooth” Devices in the Medical Environment

OVERALL CLASSIFICATION IS

TLP:WHITE

3/19/2020

Agenda

- Overview
- HC3 Assesment
- Types of Devices Affected by “SweynTooth”
- Manufacturers Affected by “SweynTooth”
- 12 CVEs Disclosed by ASSET Researchers
- What Can Hackers do if Exploited?
- Other BLE Devices in Health Care Facilities
- Assessment / Mitigation
- References
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

Researchers at the Singapore University of Technology and Design identified over 12 vulnerabilities associated with Bluetooth Low Energy (BLE) devices:

- Some CVEs are undisclosed because of non-disclosure agreements
- Collectively referred to as the “SweynTooth” vulnerabilities
- Estimated that “millions” of logistics, medical, consumer electronic, smart home, and wearable BLE devices affected
- The vulnerabilities affect BLE wireless communication software development kits for 7 system-on-a-chip (SoC) manufacturers
- Exploitation → Crash and/or Deadlock and/or Security Bypass
- BLE devices are used for various functions in the day-to-day operations of a health care facility

HC3 Assessment

HC3 Assessment – High Risk

- HC3 analysts assess with high confidence that there are devices affected by “SweynTooth” in most medical settings.

- Bluetooth devices that do not have an external power source and are designed for ‘prolonged battery life’ (rechargeable) likely use BLE SoCs that could potentially be affected by “SweynTooth”.

- **A mitigation is to turn Bluetooth off on devices if the functionality is not needed.**

- **If available by the manufacturer, the application of available patches for affected devices is the only known remediation for “SweynTooth”.**

TLP:WHITE

Types of Devices Affected by “SweynTooth”

The vulnerabilities affect Bluetooth Low Energy (BLE) wireless communication software development kits, commonly used in devices such as “logistics, medical, consumer electronics, smart home, wearables”:

- Fitness Bands
- Hearing Aids
- Bluetooth Headsets
- Bluetooth Trackers
- Remote Controls
- Virtual Reality
- Human Interface Device Profile (HID)
- Apple HomeKit
- Other rechargeable devices

(a) FitBit Inspire

(b) Eve Energy

(c) August Smart Lock

(d) CubiTag

(e) eGeeTouch

For more resources about medical device cybersecurity visit FDA.gov. Or contact the Division of Industry and Consumer Education or CyberMed@fda.hhs.gov.

Manufacturers Affected by “SweynTooth”

The researchers identified 480 vulnerable devices—the total number of affected devices is estimated to be in the millions—that use chips produced by seven system-on-a-chip (SoC) vendors:

1. Cypress
2. NXP
3. Dialog Semiconductors
4. Texas Instruments
5. Microchip
6. Telink Semiconductor
7. STMicroelectronics

TLP:WHITE

12 CVEs Disclosed by ASSET Researchers

The 12 vulnerabilities disclosed were classified into three different “vulnerability types” by the researchers:

Type	Vulnerability Name	Affected Vendors	CVE
Crash	Link Layer Length Overflow	Cypress, NXP	CVE-2019-16336 CVE-2019-17519
	Truncated L2CAP	Dialog Semiconductors	CVE-2019-17517
	Silent Length Overflow	Dialog Semiconductors	CVE-2019-17518
	Public Key Crash	Texas Instruments	CVE-2019-17520
	Invalid L2CAP Fragment	Microchip	CVE-2019-19195
	Key Size Overflow	Telink Semiconductor	CVE-2019-19196
Deadlock	LLID Deadlock	Cypress, NXP	CVE-2019-17061 CVE-2019-17060
	Sequential ATT Deadlock	STMicroelectronics	CVE-2019-19192
	Invalid Connection Request	Texas Instruments	CVE-2019-19193
Security Bypass	Zero LTK Installation	Telink Semiconductor	CVE-2019-19194

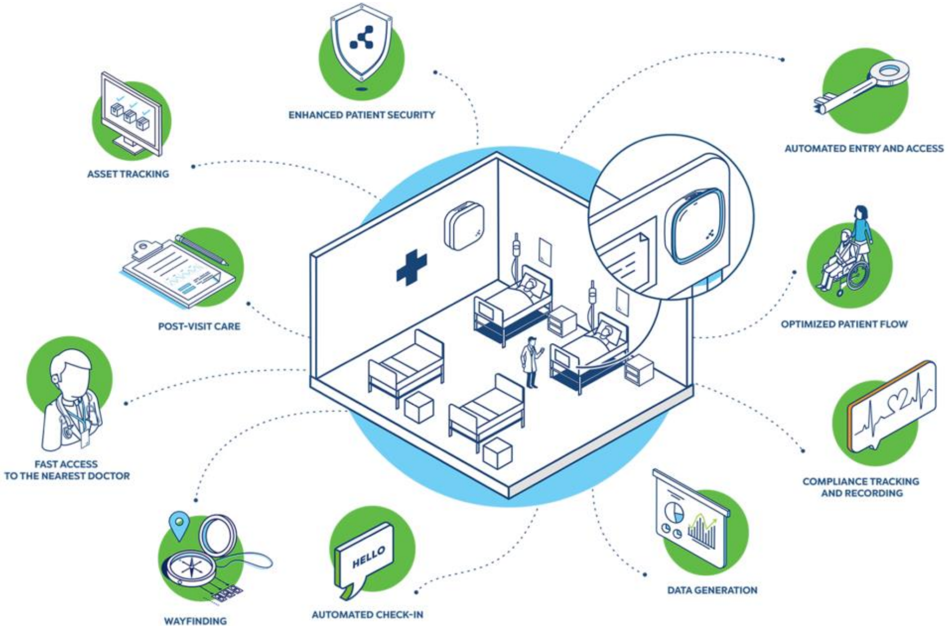
What Can Hackers do if Exploited?

Type	Vulnerability Name	Impact
Crash CVEs: **CVE-2019-16336** **CVE-2019-17519** **CVE-2019-17517** **CVE-2019-17518** **CVE-2019-17520** **CVE-2019-19195** **CVE-2019-19196**	Link Layer Length Overflow	- Trigger a buffer overflow (Denial of Service) - Cause the device to restart - Possible remote execution - Force user to restart device (remove “deadlock” state of device) - Bypass encryption and leak user information
	Truncated L2CAP	
	Silent Length Overflow	
	Public Key Crash	
	Invalid L2CAP Fragment	
	Key Size Overflow	
Deadlock CVEs: **CVE-2019-17061** **CVE-2019-17060** **CVE-2019-19192** **CVE-2019-19193**	LLID Deadlock	- Deny/disrupt the BLE connection - Cause the device to restart - Force user to restart device (remove “deadlock” state of device)
	Sequential ATT Deadlock	
	Invalid Connection Request	
Security Bypass CVE: **CVE-2019-19194**	Zero LTK Installation	- Give the attacker read/write access to the victims device

Other BLE Devices in Health Care Facilities

BLE-enabled devices in the medical environment could be devices that transmit data from the device—such as stethoscopes glucose monitors, scales, and pulse readers—to smartphones or tablets. Beyond individual devices used for patient assessments, Bluetooth devices are used for various functions in the day-to-day operations of a health care facility for: *

- Asset Management
- Automated Check-In
- Automated Physical Entry and Access
- Blood Transport Tracking
- Compliance Tracking and Recording
- Data generation
- Patient Security/Doctor Response
- Environmental Monitoring
- Optimized Patient Flow


ENHANCED PATIENT SECURITY
ASSET TRACKING
AUTOMATED ENTRY AND ACCESS
POST-VISIT CARE
OPTIMIZED PATIENT FLOW
FAST ACCESS TO THE NEAREST DOCTOR
COMPLIANCE TRACKING AND RECORDING
HELLO
WAYFINDING
AUTOMATED CHECK-IN
DATA GENERATION

Smart Hospital with Bluetooth Beacons

* Non-Exhaustive List

Assessment / Mitigation

Assessment – High Risk

- HC3 analysts assess with high confidence that there are devices affected by “SweynTooth” in most medical settings.
- Because researchers have not yet disclosed the additional vulnerable SoCs and some security companies have placed the number of devices in the millions, there is a high likelihood of an affected device being present in most medical environments.
- Individual organization’s risk depends on the device(s) targeted:
  - PII or Patient Medical Device?

Mitigation

- Identification of Devices Potentially Affected by “SweynTooth”
  - Bluetooth devices that do not have an external power source and are designed for ‘prolonged battery life’ (rechargable) likely use BLE SoCs.
- Identification of the SoCs used by those BLE devices
  - Necessary to determine the risk posed to the user’s organization
- If available by the manufacturer, the application of available patches for affected devices is the only known mitigation for “SweynTooth”.
  - SoC manufacturers Cypress, NXP, Texas Instruments, and Telink have released patches for affected devices. By the end of March, Dialog will have patches available for affected devices.

Mitigation Practices: “SweynTooth” Devices

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate:

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities	**[1.L.A]**
Implement pre-procurement security requirements for vendors	**[9.L.C]**
Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested	**[9.M.B]**
Establish and maintain communication with medical device manufacturer’s product security teams.	**[9.L.A]**

- FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy
  - https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0
- ICS Alert (ICS-ALERT-20-063-01) SweynTooth Vulnerabilities
  - https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

References

- ASSET Research: Unleashing Mayhem over Bluetooth Low Energy
  - https://asset-group.github.io/disclosures/sweyntooth/
- Dialog Semiconductor: Wearables
  - https://www.dialog-semiconductor.com/products/connectivity/bluetooth-low-energy/applications/wearable
- Bitdefender: Millions of Bluetooth Devices Affected by SWEYNTOOTH Vulnerabilities
  - https://www.bitdefender.com/box/blog/iot-news/millions-bluetooth-devices-affected-sweyntooth-vulnerabilities/
- Orthogonal: The Growing Significance of Bluetooth BTLE in Healthcare
  - https://orthogonal.io/insights/the-growing-significance-of-bluetooth-btle-in-healthcare-html/
- Kontakt.io: 15 Top Bluetooth-Based IoT Uses in Healthcare
  - https://kontakt.io/blog/10-top-bluetooth-tag-uses-in-healthcare/
- Medical Device Cybersecurity: What You Need to Know
  - https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

Questions

Upcoming Briefs

- May 16th – Topic TBD
  - *Pending*

Product Evaluations

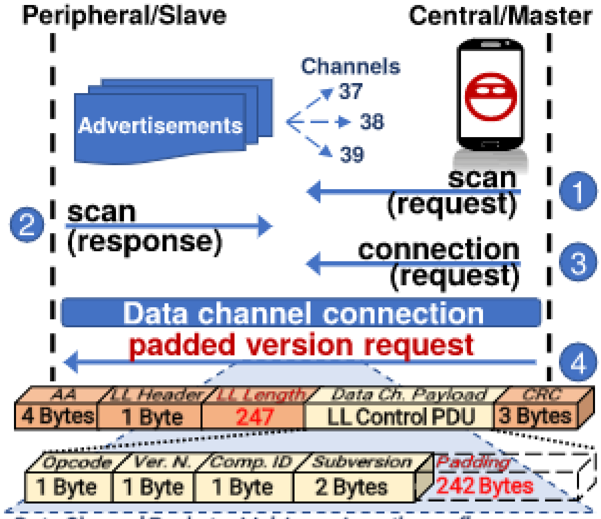
Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Appendix

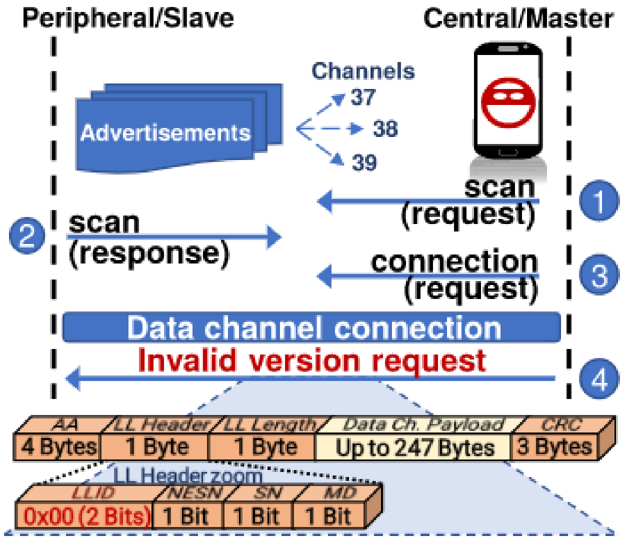
What Can Hackers do if Exploited? (cont.)



Data Channel Packet – Link Layer Length overflow

Link Layer Length Overflow - CVE-2019-16336, CVE-2019-17519

- Allows attackers in radio range to trigger a **buffer overflow** by manipulating the LL Length Field, primarily leading to a **denial of service attacks**.



Data Channel Packet – Deadlock attack

Link Layer LLID deadlock - CVE-2019-17061, CVE-2019-17060

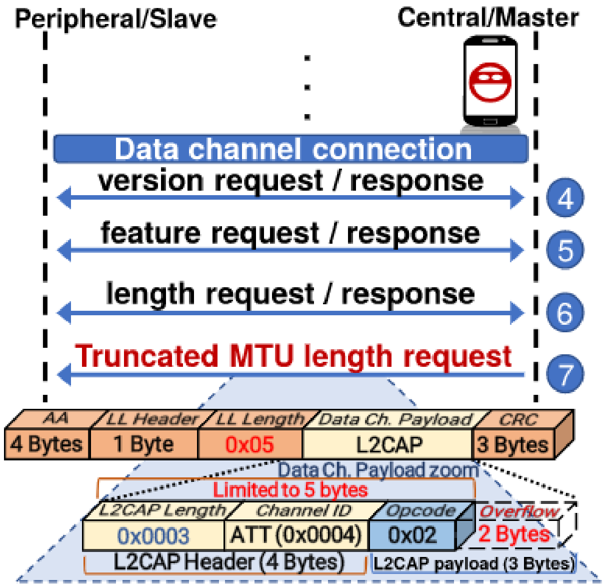
- These **trigger deadlock state** when a device receives a packet with the LLID field cleared.

TLP:WHITE

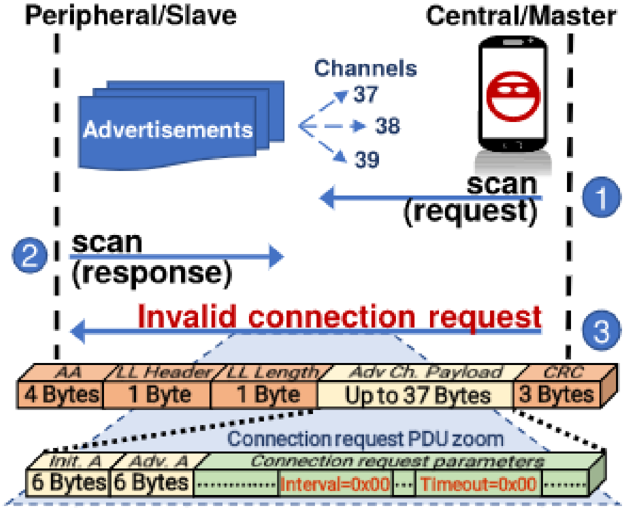
What Can Hackers do if Exploited? (cont.)

Truncated L2CAP - CVE-2019-17517

- This flaw results due to a lack of checks while processing an L2CAP packet, causing a **denial of service and crash** of the device.



Data Channel Packet – Truncated L2CAP Overflow



Data Channel Packet – Connection request DoS attack

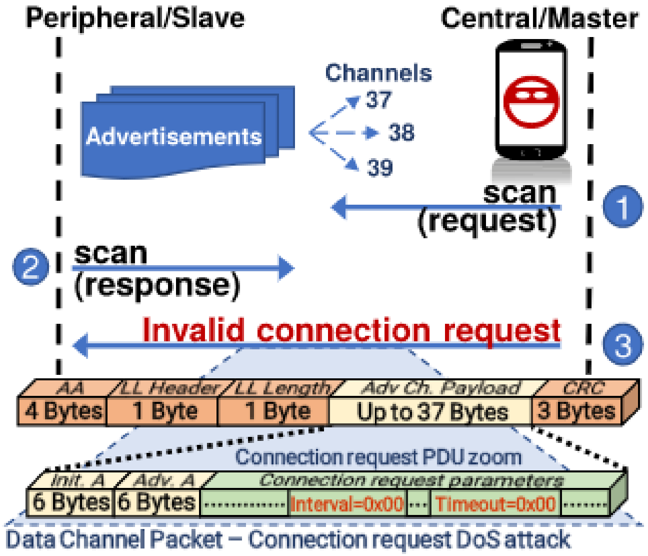
Silent Length Overflow CVE-2019-17518

- A **buffer overflow** occurs when a certain packet payload with higher than expected LL Length is sent, the **peripheral crashes**.

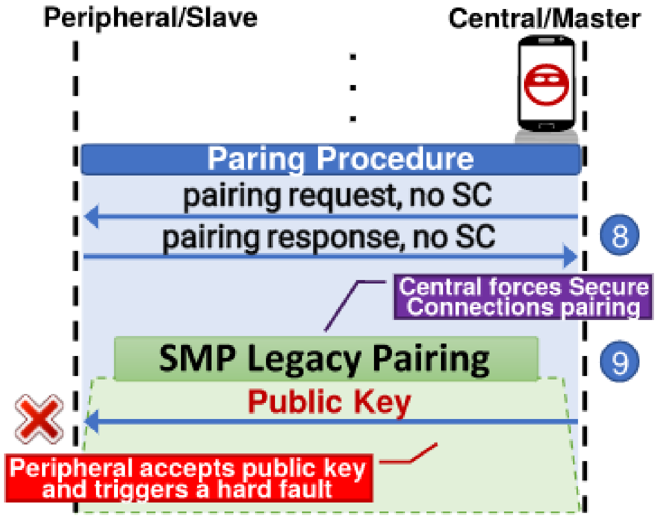
What Can Hackers do if Exploited? (cont.)

Invalid Connection Request - CVE-2019-19195

- When devices do not properly handle some connection parameters while the central attempts a connection to the peripheral, they could lead to **Deadlock state**.



Data Channel Packet – Connection request DoS attack



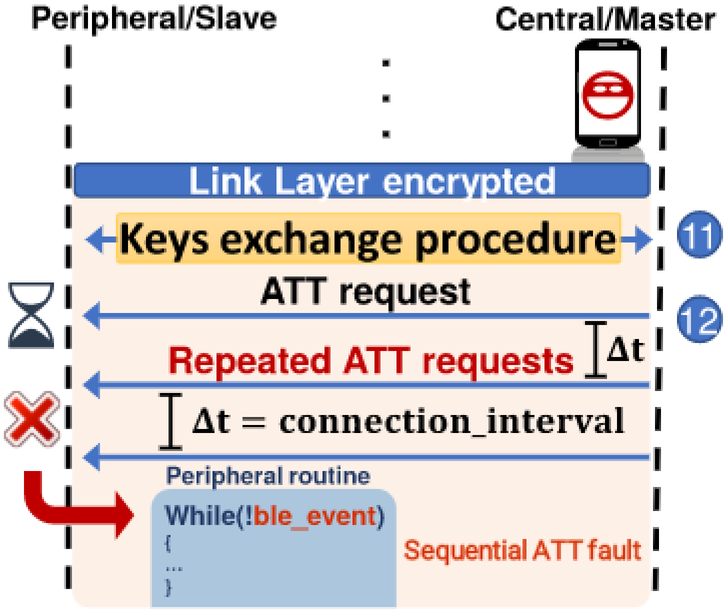
Unexpected Public Key Crash - CVE-2019-17520

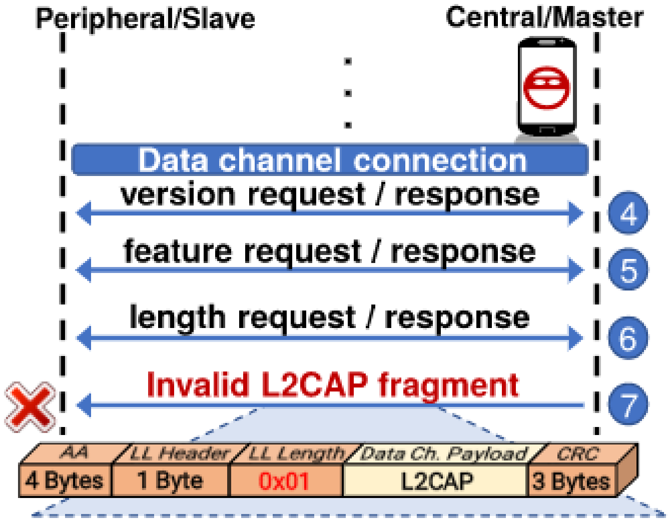
- This bug is present in the implementation of the legacy pairing procedure, which is handled by the Secure Manager Protocol (SMP) implementation and can be used to perform **DoS and possibly restart products**.

What Can Hackers do if Exploited? (cont.)

Sequential ATT Deadlock - CVE-2019-19192

- This flaw lets attackers **deadlock the peripheral** by sending just two consecutive ATT request packets in each connection event.





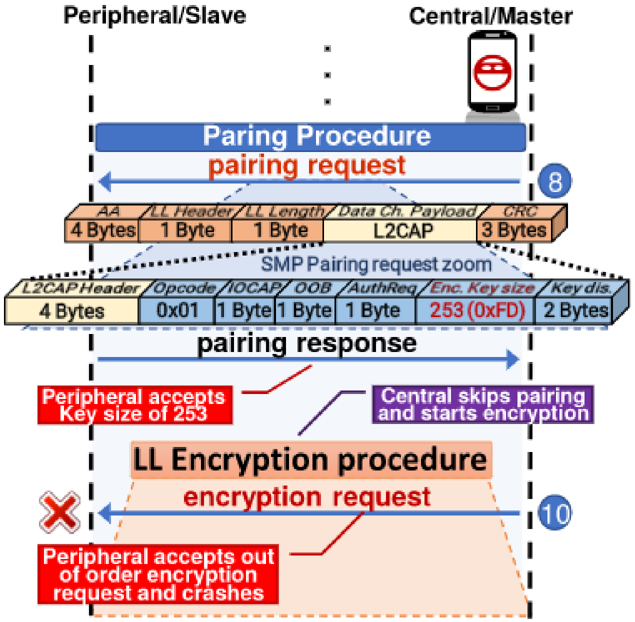
Invalid L2CAP fragment - CVE-2019-19195

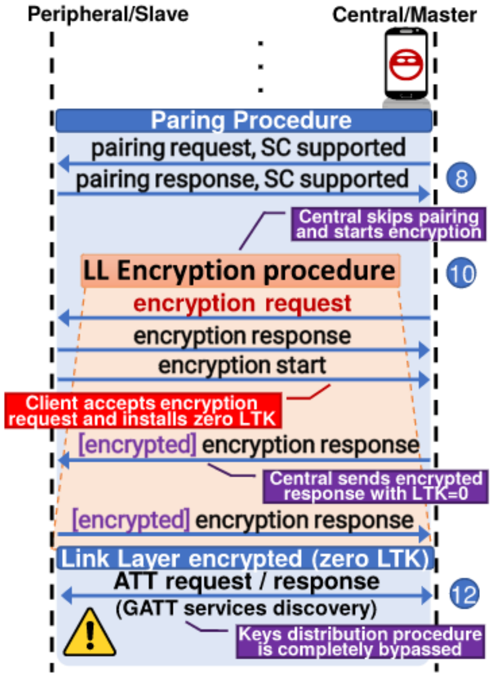
- Improper handling of the PDU size of the packets can lead to **deadlock behavior**.

What Can Hackers do if Exploited? (cont.)

Key Size Overflow - CVE-2019-19196

- This overflow in the device memory issue is a combination of multiple bugs found during the pairing procedure of devices, **resulting in a crash**.




Peripheral/Slave
Central/Master
Paring Procedure
pairing request, SC supported
pairing response, SC supported
8
Central skips pairing and starts encryption
LL Encryption procedure
10
encryption request
encryption response
encryption start
Client accepts encryption request and installs zero LTK
[encrypted] encryption response
Central sends encrypted response with LTK=0
[encrypted] encryption response
Link Layer encrypted (zero LTK)
ATT request / response
(GATT services discovery)
12
Keys distribution procedure is completely bypassed

Zero LTK Installation - CVE-2019-19194

- This critical vulnerability is a variation of one of the Key Size Overflow. It affects all products using Telink SMP implementation with support for secure connection enabled and can give an attacker **read/write access** to the victims device.