Juho Vesanen

“I know when you brush your teeth” - Cyber Security on Personal Medical Devices

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Thesis

30.1.2019

Metropolia

Author(s) Title Number of Pages Date	Juho Vesanen “I know when you brush your teeth” - Cyber Security on Personal Medical Devices 50 pages 30 January 2019
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Lecturer Sami Sainio, D.Sc. (Tech)

This thesis addresses the cyber security issues on personal medical devices. Such devices are for example electric toothbrush, blood glucose monitors and personal scales.

Cyber security can be defined as information security with potential impact on the society. One individual blood glucose monitor or a smart thermometer and their information security does not have any significance in the big picture. However, all the smart features, wireless interfaces and connectivity options, and various cloud-based services may significantly increase the number of potential targets and may put the data of very large user base at risk.

In addition to general introduction on the field of cyber security this thesis addresses the common cyber security testing methods used, and the cyber security in medical devices in general. This thesis also presents a security assessment process that can be used for assessing personal medical devices. The presented process is the first technical testing guideline for technical testing of personal medical devices from information security point of view.

The security assessment process is applied to assess the technical security of selected common personal medical devices. A general observation drawn is that on assessed devices the wireless interfaces have such vulnerabilities that may leak personal data to outsiders, and which may be exploited to assist in other attacks.

The key finding is that there should be special attention on cyber security on personal medical devices. All medical devices for consumer use should be assessed properly before releasing into market.

Keywords	Cyber Security, Personal Medical Device

Table of Contents


Metropolia

Abbreviations

ASVS	Application Security Verification Standard. Provided by OWASP
BLE	Bluetooth Low Energy. Also known as Bluetooth Smart. Very low energy operating mode supported by Bluetooth 4.0
CERT	Computer Emergency Response Team. Referring to national authorities.
CIA	Confidentiality, Integrity, Availability. Widely recognized information security concept
CVSS	The Common Vulnerability Scoring System
CVE	Common Vulnerabilities and Exposures. Reference for publicly known vulnerabilities and security issues. Operated by Mitre Corporation
DPIA	Data Protection Impact Assessment
EMS	Electronic Muscle Stimulation
FICORA	Finnish Communications Regulatory Authority
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol. Used primarily to transport web pages.
JTAG	Joint Test Action Group. Commonly used for technology for debugging microprocessors and microcontrollers
KATAKRI	Kansallinen turvallisuusauditointikriteeristö, Information security auditing tool for authorities
MDD	Medical Device Directive
MITM	Man In The Middle. A technical attack where attacker can both eavesdrop and modify the data.
NFC	Near-Field Communication. Contactless very short distance communication system. Commonly also known incorrectly as RFID
NIST	National Institute of Standards and Technology

OSSTMM	Open Source Security Testing Methodology Manual
OWASP	The Open Web Application Security Project
PDFA	Personal Data Flow Analysis
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PCI	Payment Card Industry. Regulates and coordinates the credit card payments and related technology.
PCI DSS	Payment Card Industry Data Security Standard
RFID	Radio-Frequency Identification. Wireless technology used to identify tags. Typically very short distance
TENS	Transcutaneous Electric Nerve stimulation
TLS	Transport Layer Security. Standard that supersedes SSL. Used for encrypted HTTP traffic

1 Introduction

Personal medical devices are commonly used in modern households. This includes various devices from electronic thermometers to blood pressure monitors. The number of features on these devices is on a constant rise along with add-on services offered using smart phones and cloud-based systems. Due to their wide spread use and abundance, personal medical devices have the potential to impact on the daily life of very large user group.

Cyber security risks arise when there is a potential method to have an impact on very large user base using electronic means. Cloud-based services are already targeted by attackers and criminals. As the technology on individual devices advances, makes this also the personal medical devices a potential target. The topic of this thesis is no longer only science fiction. It is justified to focus on the cyber security issues on the current generation of personal medical devices that utilize various communication technologies and services, and that may put users, or their data, at risk.

The end goal of this thesis is to demonstrate whether cyber security issues are relevant by performing technical security assessment on a selection of common personal medical devices. Secondary goal is to propose a process applicable for security assessment of personal medical devices that yields non-obvious results.

This thesis is organized as follows. Chapter 2 covers security in general, existing processes, general documents and tools for security assessments. The aim is to set the scene for chapter 3 that covers the security issues in medical devices along with related governmental regulation. Chapter 4 describes a proposed process for security assessments of personal medical devices. Chapter 5 contains brief results of multiple security assessments carried out for this thesis. Conclusions are drawn in chapter 6.

2 Introduction to Security

The traditional concept of security in computing or information technology refers to *information* security. E.g. protecting the information from being accessed, disclosed, modified etc. without authorization.

The ISO/IEC in standard 27000:2009 [1] defines information security as

> *preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.*

The principles confidentiality, integrity and availability are commonly known as the CIA triad or CIA model [2] which is the cornerstone of modern concepts in information security. Confidentiality covers protecting the information from being accessed without authorization. Integrity means ensuring that processed information stays intact and that it cannot be modified without authorization. Availability simply means that the information must be available when needed. The CIA model it is one of the most widely recognized concepts within information security. It can be applied on nearly anything within the information security domain where data is processed, including communication channels, computing hardware and software.

The CIA model lacks some key principles and has been extended further when needed. As an example, in [3] three additional principles are proposed: possession or control, authenticity and utility. Possession or control refers to physical losing control. Through proper authenticity the data source can be correctly identified. More abstract concept of utility refers to data usefulness. I.e. properly encrypted data without the encryption keys is not useful at all.

In the end, security - when applied to computing in general, networked devices or embedded systems - can be seen as an attempt to prevent service disruption and theft of or damage to the hardware, to the information or to system users or general public.

In addition to introducing this very basic concept of security this chapter aims in the following to further broaden the understanding of *cyber security*, introduce numerous methods how it can be quantified, measured, assessed and ensured.

2.1 Cyber security

The term *cyber security* has become part of common language during the 2010's. Data from Google Trends shown in Figure 1 reveals that the term popularity has been increasing 20% per annum for the past five years. However, even though the word *cyber* is now commonly used, there is still no common and universal definition for the term.

Figure 1 - Popularity of the term "Cyber Security" in Google Trends

In the Finland's Cyber Security Strategy [4] the *cyber security* is defined as a *desired state* where the cyberspace can be trusted and where its operations are secured. The cyberspace in turn is defined as the environment consisting of one or multiple IT-systems processing electronic information. While the actual definitions are vague, more insight is in the three main points of the desired cyber security vision: Finland can protect critical functions against cyber threats; People and organizations can utilize the secure cyberspace and the skillset that protects it; By 2016 Finland is in the spearhead of preparing against cyber threats and managing the related interrupts.

The National Defence University [5] approaches the term definition through warfare where *cyber battle* refers to hostile actions against a nation, and its critical infrastructure that are carried out in *cyberspace.* The cyberspace is in turn defined as the entire environment consisting of software, hardware, information systems, people and social interaction using computer networks.

Outside the military domain, there are numerous Finnish companies[1] offering *cyber security services*. While the company service offerings slightly differ, it can be clearly seen that the focus is in securing systems by finding weaknesses in products or security functions in general. Another common service offered detects breaches in IT systems as they happen. Also, more high-level services are offered that deal with processes instead of

[1] Companies such as F-Secure, KPMG, Nixu, Silverskin.

systems, and services where companies can utilize outsourced information security professionals even for high level managemental tasks.

By using a generic Google search for then term cyber security, it becomes obvious that most organizations use the term interchangeably for generic IT security. Security of applications, information, and backend systems all play critical part in the cyber security. In some occasions disaster recovery is also included. While the term seems to cover practically speaking all aspects of modern IT systems, the consensus appears to rule out anything that is not caused by an active attacker. For example, natural disasters are not considered a cyber threat, even if these would have a significant impact on the IT systems and on public.

Periodically breaches on various online services make their way into headlines and are described as “cyber attacks”. To illustrate the nature of typical events and the possible extent a breach may have, the most notable recent breaches from early 2018 are listed in the following:

- Under Armour / MyFitnessPal breach [6]
    - User names, email addresses and encrypted passwords. By decrypting the password gives also access to personal fitness related data.
    - Breach affects 150 million users.
- FedEx data exposed [7]
    - Scanned highly sensitive documents such as driving licenses, passports, personal details, home addresses and phone numbers left on publicly accessible server without any protection.
    - Data leak affects 119 000 users.
- Liiketoimintasuunnitelma.com breach [8]
    - Usernames, clear text passwords and business plans.
    - Affects 130 000 Finnish citizens.

Two last of the shown examples were discovered not by the company operating the service, but independent 3rd party information security organizations or teams. On the Liiketoimintasuunnitelma.com breach the most alarming detail is the usage of clear text passwords as storing passwords in clear text is an indication of lax information security in system design. These three examples alone demonstrate that the size of the company providing the service, or nature of the stored data, is no guarantee of security.

The information leak attacks also open new business opportunities for cyber criminals. So far on the black market most of the information sold has been credit card details and personal information. However, since 2014 the personal medical record has actually been worth more than credit card details in the black market [9]. There is a definite market of stolen health data [10]. Due to the increasing interest in personal medical data, the cyber security issues of connected personal medical devices should be taken seriously. Cloud-based service collecting personal medical devices of a very large user base is a tempting target for modern cyber criminals.

Based on this it can be argued that cyber security refers to the security of computer-based systems that process information where exploitable security issues and events may have a great impact on society either through the large user base, or through the significance of the system.

In the context of this thesis, cyber security threats are relevant on personal medical devices. Due to the abundance of these devices, private information of *very large* user base may be accessible, and any vulnerabilities may have significant impact on society if, for example, the data is stored on a cloud-based service and leaks or is modified by the attacker. Also, as these devices are widely used, certain vulnerabilities may simplify target selection for cyber crimes, and provide information that can used in further attacks.

2.2 Security assessments and penetration testing

A security assessment attempts to define the security posture of the target by focusing on vulnerabilities and on possible impact exploitation could have. The aim is to find vulnerabilities and to determine the current level of security. While commonly mixed, a security assessment differs from a security audit, where the target is assessed against a standard to check for compliance. [11]

A security assessment can be carried out by multiple methods including analysis of architecture or source code, passive analysis of application operation, feeding the application with non-valid data, attempting to use the application against valid used-cases. Typically, a combination of multiple methods is used. Together the findings represent issues affecting the security posture of the system.

In Finland an official and recognized security audit may only be performed by very limited number of inspection bodies accredited by the FICORA – The Finnish Communications

Regulatory authority [12]. On spring 2018 only three organizations are accredited for the following competence areas: Protective level III and IV, ISO/IEC 27001:2013, KATAKRI II or KATAKRI 2015. The protective levels and KATAKRI refer to information security for authorities.

The term penetration testing is commonly seen to be interchangeable for security assessment. A penetration test may successfully identify problems or security related bugs in the target, or concrete vulnerabilities. However, as opposed to a complete security assessment that correctly defines the security posture, a penetration test can only identify a small representative sample of security risks in the system. Penetration testing, despite the name, is not simply “hacking” and attempting to break the target without any kind of detailed plan. Instead it must be structured according to perceived risk in the target and must be based on all findings tracked from the beginning of software life cycle and requirement and risk analysis. [13]

2.2.1 Vulnerability classification and disclosure

When a security assessment has identified vulnerabilities the severity of each vulnerability is classified using a scoring method. The most common method is The Common Vulnerability Scoring System (CVSS) [14]. The CVSS v3 numeric score is expressed from 0 to 10 with one decimal. A critical-level finding is given the score of 9 – 10 and high, medium and low-level findings are given lower scores. The CVSS scoring takes in account the possible impact, exploitation requirements and several other factors.

The base metric is calculated by analyzing the impact on confidentiality, integrity and availability, and the requirements and difficulty of the exploitation. On each of the metrics, there are only a few possible options; for example, none-low-high for the impact metrics, and low-high for attack complexity metric. The base metrics can be modified through optional temporal and environmental metrics. Various tools[2] exist to quickly calculate the score and identify the overall severity of a vulnerability.

As an example, on the Key Reinstallation Attack (KRACK) [15] against WiFi networks published during fall 2017, the numerous contributing vulnerabilities have the CVSS v3

[2] NIST (National Institute of Standards and Technology) and FIRST (Forum of Incident Response and Security Teams) CVSS score calculators are available at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator and https://www.first.org/cvss/calculator/3.0, respectively.

base score of 6.8 – medium. Despite the total compromise of confidentiality and integrity, the attack is relatively complex which reduces the severity. The Meltdown and Spectre [16] vulnerabilities disclosed on January 2018 are a result of three vulnerabilities – each ranked as 5.6 – medium. Despite the impact and the publicity or these issues, the attacks cannot be carried out remotely without user interaction and have high complexity.

If the findings made during a security assessment are made public, the vulnerabilities are typically disclosed though various online services. The most common service is MITRE CVE (Common Vulnerabilities and Exposures) database that is sponsored by US-CERT, accessible at https://cve.mitre.org/cve/. For security analysts the CVE provides a comprehensive list of known vulnerabilities in various products. It's a common practice, that the findings are publicly disclosed after a period from 3 to 12 months after the initial discovery giving vendor time to prepare and release a patch.

2.3 Existing well-known standards & guidelines

Multiple organizations publish security related standards, methodologies and guidelines. Depending on the task at hand, these documents may provide valuable insight in ensuring that all aspects are covered and therefore effectively reduce the risk of failure. In the following several guidelines and methodologies are described.

2.3.1 Open Source Security Testing Methodology Manual

The Open Source Security Testing Methodology Manual (OSSTMM) [17] is a peer-reviewed methodology for performing security tests. The test cases described by the methodology test items such as computer networks, information and data controls, but also personnel security awareness levels and physical security assess controls.

A security assessment that follows the OSSTMM is executed in four phases that contain numerous testing modules. The modules and the full process is illustrated in Figure 2 where phases are color coded.

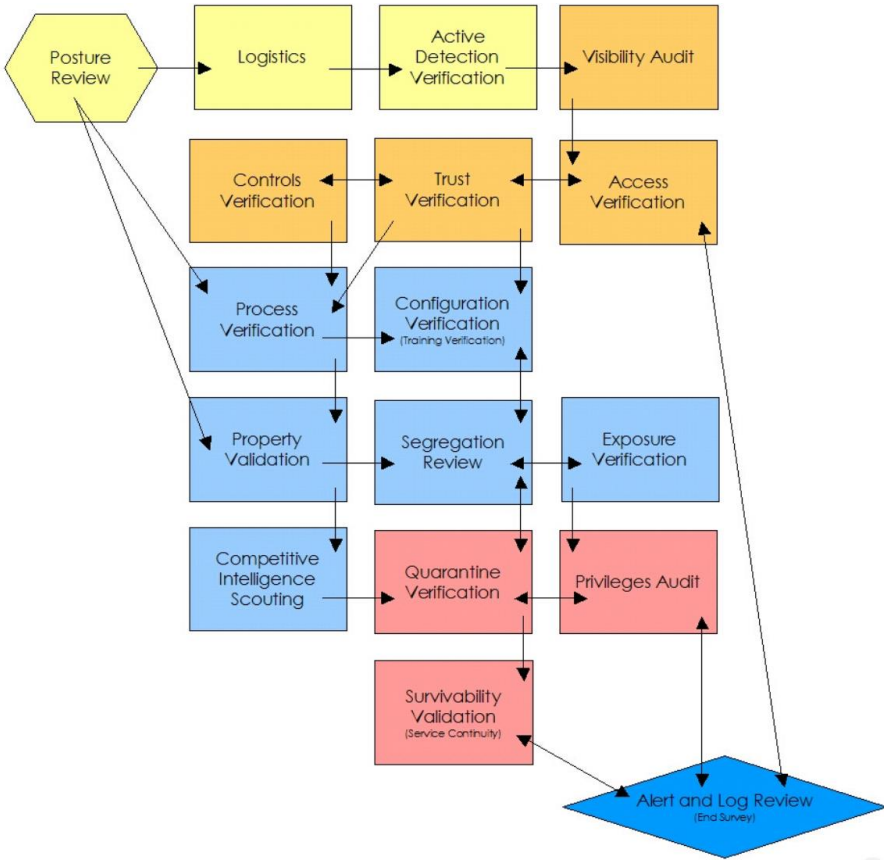

Figure 2 - Full OSSTMM process [17]

Each of the modules contain tests performed in five different channels. These are used to address and possibly to limit the scope of the assessment. The classes defined by the OSSTM are: Human Security, Physical Security, Wireless Security, Telecommunications Security and Data Networks Security. As an example, the Logistics module contains tests related to Time. Depending on which classes are included, the testing may take various approaches as illustrated the following three examples:

- Human Security Testing: *Test for the timezone, holidays, and work schedules for various roles and jobs within the scope including partners, resellers, and influential customers interacting with the scope.*
- Physical Security Testing: *Determine if decreased mobility or visibility during time of day, week, month, or season (day or night, fog, rain, or snow) will have an impact upon operations at the target.*
- Wireless Security Testing: *Test for the time frame of equipment operation. For example, is a wireless access point (AP) available 24/7 or just during normal business hours?*

While some of the tests are not highly technical and attempt to be technology-agnostic, the OSSTMM in Data Networks Security class takes very detailed approach to ensure the entire target is covered. As an example, the Network Surveying step in Visibility Audit module:

> *(i) Trace the route of ICMP packets to all targets.*
> *(j) Trace the route of TCP packets to all targets for ports SSH, SMTP, HTTP, and HTTPS ports.*
> *(k) Trace the route of UDP packets to all targets for DNS and SNMP ports.*
> *(l) Identify TCP ISN sequence number predictability for all targets.*
> *(m) Verify IPID increments from responses for all targets*

In short, the OSSTMM is a highly comprehensive methodology that aims to cover all aspects of security. As such it may not be suitable for limited-scope security assessments. Following the OSSTMM ensures "*the most thorough and efficient test possible*".

2.3.2 OWASP ASVS

Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) [18] is a widely recognized document helping organizations to develop and maintain secure applications. Also, the ASVS is to be used to align requirements and offerings with a common standard. It can be used as a metric for developers and application owners, as a guidance for developers and during procurement for specifying desired requirements.

The ASVS format resembles a checklist of requirements organized in multiple categories ranging for example from authentication to session management and from generic cryptography to HTTP security configuration. It defines three different verification levels that are to be used depending on the target security level. Level 1 should be applied on all network accessible applications, but levels 2 and 3 depending on the possible impact a compromise would have. The most optimal way to use the ASVS is to create a tailored blueprint specific to the application.

To illustrate the nature of the ASVS, selected excerpts are shown in the following from a few categories:

- Category 5 - Malicious input handling, requirement 5.1

Levels 1-3: *Verify that the runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.*

- Category 7 – Cryptography at Rest, Requirement 7.7

  Levels 1-3: *Verify that cryptographic algorithms used by the application have been validated against FIPS 140-2 or an equivalent standard.*

- Category 7 – Cryptography at Rest, Requirement 7.15

  Level 3: *Verify that random numbers are created with proper entropy even when the application is under heavy load, or that the application degrades gracefully in such circumstances.*

- Category 10 - Communications security, Requirement 10.10

  Levels 2 & 3: *Verify that TLS certificate public key pinning (HPKP) is implemented with production and backup public keys.*

- Category 17 - Mobile applications, Requirement 17.10
  - Levels 2 & 3: *Verify that sensitive information maintained in memory is overwritten with zeros as soon as it no longer required, to mitigate memory dumping attacks.*

Based on the examples shown earlier, it can be argued that carrying out an extensive test requires high level of skills and knowledge – and access to the application source code or to the developers.

2.3.3 Payment Card Industry Data Security Standard

Payment Card Industry (PCI) Security Standards Council provides multiple security standards that specify how credit and debit card payments are to be handled. The most well-known is the Data Security Standard [19], which is simply known as PCI DSS. The most recent, the PCI DSS 3.2, applies to all entities involved with the credit card or card holder data processing including but not limited to merchants, issuers, and service provides. For all entities, to process credit cards PCI compliance must be achieved and maintained during yearly audits.

Even if PCI DSS takes a very strong stance on protecting the sensitive data, it does give a lot of freedom to decide how the required mechanisms or controls are implemented. Also, the concept of compensating controls is well understood (e.g. a firewall is not necessary for disconnected networks). For illustrative purposes, a sample of requirements from [19] are listed in the following:

> *1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment*
>
> *2.3 Encrypt all non-console administrative access using strong cryptography*
>
> *3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.*
>
> *6.5.9 Cross-site request forgery (CSRF)*
>
> > *Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.*
>
> *9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines*

By a quick look on the requirements, most of these seem obvious to IT professionals. However, implementing the requirements in practice may be far from trivial. For example, fulfilling the requirement 3.2 requires overwriting all memory locations and hard disk sectors where sensitive authentication data has been even temporarily stored. With modern and complex IT system and various components such as SSD hard-drives this becomes rather non-trivial task.

While PCI DSS is the governing standard only within the payment card industry, it does nevertheless provide a proven set of requirements that can be selectively applied in nearly any application when certain data is to be kept safe.

In addition to the rather generic information and requirement in the PCI DSS, there is also a novel method presented by the PCI Security Standards Council to specify the difficulty of attacks a device must be able to withstand. For example, a hardware security module (HSM) is a system processing the most sensitive information during credit card payment. Hardware Security Module Security Requirements in [20] state the following requirement:

> *There is no feasible way to determine any sensitive information … without an attack potential of at least 25 for identification and initial exploitation*

The Derived Test Requirements [21] defines numerous test procedures, which may be usable for assessment of various electronic devices that must be tamper evident of tamper proof, and a Physical Attack Potential Formula. The formula first breaks the attack in two phases: identification and exploitation phase. In the first phase the vulnerabilities are identified and in the second phase the target is initially exploited.

For both phases various parameters are evaluated: attack time, expertise, knowledge on the devices, access to target devices, equipment required and requirements for specific parts. To derive the total attack potential, scores of both phases and all parameters are put together to find the total attack potential. A sample calculation illustrates the nature of the formula:

- Identifying a vulnerability:
    - More than 160 hours of work - 7.5
    - Expert level attacker - 4
    - Restricted for public knowledge - 0
    - Only mechanical samples available - 1
    - Specialized equipment required - 3
    - Using only standard parts - 1
- Attacking a target system using discovered vulnerability
    - Attack time with physical access to the target less than 8 hours - 3
    - Skilled attacker - 1
    - No special knowledge on the device - 0
    - Attacker has physical access to a device with working keys and software - 4
    - Standard equipment - 1
    - Using only standard parts - 1

This example has the total attack potential of 26.5. In other words, HSM device is not required to withstand this kind of an attack what requires more than a month to prepare, and a full working day with a device that is in operational condition.

What is interesting in this approach of attack difficulty specification is that it allows substituting skills, tools, parts, equipment and time which is often the case in real life. Also, the approach accurately reflects the concept where the vulnerability discovery if separated from the exploitation. By using a lot of resources, it may be possible to discover such vulnerabilities that can be exploited with minimal effort.

2.3.4 NIST Guide to Bluetooth Security

National Institute of Standards and Technology (NIST) publishes a variety of widely recognized guidelines, recommendations and reference material on cyber security related topics[3]. Guide to Bluetooth Security [22] is a general document describing the Bluetooth

[3] A full list of NIST Computer Security Division Special Publications, is available at http://csrc.nist.gov/publications/PubsSPs.html

operation, security features, weaknesses and threats. The latest release is from 2017 and it covers all, even the most recent Bluetooth protocol version 4.2.

The guide explains in detail the operation of all security features and provides a 37-item checklist that covers management, technical and operational domains. Each is classified either as a recommended practice or as something that should be considered during implementation and usage of Bluetooth technology. For illustrative purposes, two of the recommendations from the checklist are shown in the following:

- Technical recommendation 23:

  Configure encryption key sizes to the maximum allowable.
- Operational recommendation 30:

  A BR/EDR service-level security mode (i.e., Security Mode 2 or 4) should only be used in a controlled and well-understood environment.

Sections where Bluetooth vulnerabilities and threats are listed and described along with affected protocol versions provides a comprehensive outlook that can be used to gain an overview of possible threats on specific product. I.e. Bluetooth being susceptible to Denial of Service attacks may not be a threat if the product is not expected to provide service in all situations.

It's worth noting that some of the details in Bluetooth device operation cannot be trivially verified as the consumer grade devices are not equipped with debugging interfaces. This applies specially to low-level functionalities including pairing and encryption. Nevertheless, when assessing systems that utilize Bluetooth the described NIST guideline provides a solid structure for identifying possible security issues in the wireless connectivity and should be used as guideline to ensure that any aspects are not overlooked.

2.4 Threat modeling

Threat modeling is a process for software development to optimize security of a target by identifying threats and vulnerabilities; and defining measures to mitigate identified issues. It is not clearly defined process but adapted to the system under modeling. Typically, the process first identifies the protected assets and all entry points within a component, then the threats are identified in a threat modeling session, and finally the follow-up guarantees mitigation and documentation. [23]

The current software products may be very complex. Therefore, to reduce the complexity of the threat modeling the scope should not cover the entire system or application, but instead the process is performed a smaller subset of functionality – a component – at a time. Most significant phase in the process prior to the threat modeling session is documenting the module, usually using some sort of a data-flow diagram. The component internal workings are irrelevant, but effect inputs have on the outputs has to be identified. [23]

The actual threat modeling session requires participation from personnel who has up-to-date knowledge on the system. This includes at least architects, developers and software testers. The session resembles in a way a brainstorming session, where the data-flow diagram is analyzed for all different possible threat types. The purpose of the session is to use the provided information of assets and information flow to *identify* possible threats. Every identified threat is documented – even the ones already resolved, and the opinions of people or current operation of the application or component are not used to suppress anything. [23]

To identify the possible impact of identified threats, and to list possible threat types, two common classification methods are used: DREAD [24] and STRIDE [25]. In the DREAD model, each vulnerability is given a numeric rating based on the sum of points in categories damage, reproducibility, exploitability, number of affected users and discoverability. In the STRIDE model the threats are classified based on possibility to spoof user identify, data tampering, repudiation, information disclosure, denial of service and elevation of privilege. STRIDE is not only a classification method but is used to also help reasoning and finding the threats against a system.

Any threats identified during the threat modeling must be resolved. All the documented threats are classified based on the current mitigation status: already mitigated – not mitigated, which component is responsible for mitigation and whether mitigation is required or not. Each of the threats may have different resolution process, but all identified threats must be tracked down. Any documentation created during the threat modeling is important reference for future software development. [23]

2.5 Privacy Impact Assessment

In addition to a technical security assessment, a privacy impact assessment or PIA can be conducted to identify possible issues and risks with data collection and processing of personally identifiable information (PII). Carrying out the PIA focuses on analyzing the data flows and interviewing the relevant personnel involved in the process. The PIA rarely is a simple technical process, but instead relies heavily on the “soft” side: data collection through the interviews, questionnaires and data analysis. [26]

In the core of a PIA are data flow analysis and privacy analysis. The goal of the data flow analysis is to identify all systems and subsystems, processes, and interfaces that are used to collected, process and transport the PII. Based on this, it’s possible to create diagrams that accurately describe the flow and processing of PII. The privacy analysis is basically an interview of all relevant personnel that attempts to identify the data being processed and collected, the attributes of the data and practices for sharing the data. [26]

2.6 Typical tools for a security assessment

For a technical security assessment, number of tools are used to gain understanding of the security posture of the target system or device. Selection of suitable tools always depends on the target. In certain cases, highly specialized custom build hardware is required, while for rather basic website security assessment some automated tools can give an overview of the most severe security issues. In the following a brief overview of most common tool categories and tools is given.

For typical web application security testing [27] tools such as Burp Suite [28] and OWASP Zed Attack Proxy [29] are the most common. This helps analyzing the communication between the server and the browser but are also able to perform requests for resources on their own. In automatic mode, they can analyze every single resource for multiple different types of vulnerabilities.

Network based vulnerability scanning [30] attempts to discover possible issues in different server software running on the target. The scanning software communicates with the target using TCP and/or UDP, and can identify services provided, disclosed vulnerabilities and unsafe configuration. Testing is fully automatic, and is usually carried out with tools such as Nessus [31] and OpenVAS [32].

For communication analysis variety of methods are used. Wireshark [33] is most common network traffic analyzer for TCP/IP and related application protocols. For analyzing Bluetooth connectivity, there are some Bluetooth sniffers such as Ellisys Bluetooth Explorer [34], but most Android smart phones support capturing the Bluetooth data [35], which can be later analyzed using the Wireshark.

Fuzzing [36] is process for testing for unknown weaknesses in the system by feeding the system under test with large number of variable, and incorrect input. The input is typically derived from a working sample input and is then modified in numerous ways using dedicated tools. This method can be applied against application, protocols, file formats, electronic interfaces etc. Radamsa [37] is commonly used tool for creating fuzzed input data sets. Peach Fuzzer [38] is an example of a fully featured fuzzing platform supporting a very large variety of different targets.

When security testing is performed, it's also common to implement tools by using suitable programming languages and libraries. For example Python with Scapy [39] is a powerful combination for network traffic modification. When this is combined further with Radamsa, a highly customizable network traffic fuzzer can be realized.

For RFID and NFC technologies the most common tool for research and development is Proxmark 3 [40]. It can interface with nearly any kind of RFID or NFC system that uses 125 kHz, 135 kHz or 13.56 MHz frequencies as it provides a very low-level interface and supports creating custom operations. Furthermore, it can emulate nearly any type token. In a security assessment the Proxmark 3 can be used in various scenarios from brute-forcing the keys to eavesdropping the data between the reader and the token [41]. For non-offensive security testing the tool can be simply used to explore the NFC attack surface [42].

When assessing the possible RF emanations devices create the testing is usually carried out using a spectrum analyzer and RF-shielding chamber or room. More specific equipment that can be used to assess the actual contents of the RF transmissions include various software-defined radios that can be used to interface with non-standard radio transmissions. These devices may also be used to transmit arbitrary data to the device under test.

When assessing embedded systems with very limited input and output interfaces low-level electronic analysis tools are used. This includes devices such as oscilloscopes and logic analyzer. Using such devices, the contents of individual communication buses can

be exposed which may give out otherwise unknown details of device operation. However, it's worth noting that if an attacker can gain such low-level access, all system defense mechanism may be bypassed. Therefore, this approach is usually used only to gain information on the device operation, not to test the low-level defense mechanism.

3 Cyber security in medical devices

Medical devices are no longer single units but offer – and often require – connectivity. The amount of software and computerization is on a constant rise. This progress leads to new challenges in securing the devices and ensuring that no harm is inflicted on the patients. The common impression on security with medical devices revolves around the idea of “stopping a pacemaker” or “the surgical robot attacking the patient”. These, in fact, *are* recognized threats that are taken into account and are recently reviewed in e.g. [43] and [44].

The field of computerized devices covers at minimum diagnostic systems (e.g. MRI, CT scanners), monitoring systems (e.g. oxygen saturation, blood pressure, ECG, EKG), treatment devices (e.g. infusion pumps, medical lasers, surgical equipment) and life support (e.g. ventilators, anesthetic and dialysis machines). The number of different devices types is very large, there are numerous use-cases and various threat scenarios. All in all, the entire medial cyber security environment is very complex, and the problem is quite multifaceted [45].

In addition to the movie-plot threats earlier described, also the patient data is at risk. Quite often the software used by medical professionals is lacking modern security controls. This has been demonstrated numerous times on various occasions. Latest publications being from cyber security company McAfee. In [46] McAfee researchers discover poor security that exposes medical data. In [47] researchers explain how cyberattacks are now targeting the entire healthcare industry. Researches make also an interesting point that with for example credit card number leaks it’s relatively simple to cancel a credit card – while medical data breaches the records cannot be simply cancelled. According to the researchers, cybercrime-as-a-service is now a viable business model also in the healthcare industry.

It can also be speculated how far this can go in real life. Are the next steps physical attacks against patients, or simply just extortion on those who will undergo treatments using connected systems? If stolen medical data has now a viable market as is shown in [10], will the cyber criminals soon offer also services to *alter* your medical history for lower insurance premiums? In any case, the cyber security of all kinds of medical devices and data must be taken seriously.

3.1 Personal medical devices

The term “personal medical device” is widely used and recognized, but still lacks a clear definition. In this thesis the term refers to devices that are used by individuals for self-care or diagnosis, are sold over the counter to end users, and rarely used by medical professionals. While there are not necessarily any threat scenarios that would include killing individual patients, or other similar threats with significant consequences as described earlier in chapter 3, the large user-base and possible connectivity options increase the potential target group and attack surface. This in turn increases the potential gain a widespread attack may have. Also, as the personal medical devices get more common, there is also an option to use these devices as information source used in another types of attacks. Therefore, it’s relevant to treat abundant personal medical devices as a class of their own.

The group of personal medical devices includes but is not limited to: body mass composition monitors, blood glucose level meters, heart rate monitors, pulse oximeters, transcutaneous electric nerve stimulation (TENS) devices, temperature meters, toothbrush, weight scales and other similar devices.

3.2 Threats against personal medical devices or device users

The personal medical devices are not used for critical tasks, but mainly for personal comfort and/or self-diagnosis. Therefore, the most severe of the possible threats briefly described earlier in chapter 3 (i.e. stopping a pacemaker) do not directly apply. There are, nevertheless, numerous other possible threats that apply when using such devices. Also, a successful attack may not have as great impact on one single patient or user, but due to the widespread distribution and usage, the overall impact may be quite significant.

A realistic set of possible threats can be modelled through for example the CIA model earlier introduced in chapter 2 with the additional principles introduced by [3]. While this approach is primarily applicable for information security, it can also be applied on physical devices. In the following the identifying individual threats on confidentiality, integrity, availability, possession or control, authenticity and utility are listed. The following listing is based on the typical features and use-cases of personal medical devices.

Possible threats in personal medical devices:

- Confidentiality
    - Eavesdropping or capturing the data collected and/or processed by the device. Including the data transmission from the personal medical device to a smart phone.
    - Identifying the use of the device. Examples:
        - Usage of a blood glucose level meter may be an indication of diabetes.
        - Repeated use of a thermometer may indicate a person is having fever, common cold or influenza.
        - Detecting toothbrush usage may be used to deduct times when person is waking up or going to bed.
    - Identifying the device operational parameters. Examples:
        - Toothbrush operational mode (normal vs. sensitive) may indicate a person is suffering from gingivitis.
        - A TENS device operational mode and power level may indicate a person is having sore muscles
- Integrity
    - Modification of measured and/or processed data at any point.
    - Altering device operational mode without authorization. Example:
        - Changing the parameters (age, height) on a body composition monitor may result in incorrect body composition measurements.
- Availability
    - Rendering the device permanently unusable.
    - Impacting on the device in such a way that it *appears* to be broken. Example:
        - Altering the toothbrush operational mode and parameters while the device is in use may result in target assuming the device is broken.
    - Impacting on the collected and/or processed data in such a way that it becomes not available.
- Possession or control
    - Losing the device and stored data by mistake of theft.
    - Using the lost device to attack smartphone the device was paired with.

    - Using the lost device to attack on the collected data set stored in cloud-based services.
- Authenticity
    - Providing falsified information from alternate sources to a smartphone or other similar system collecting and analyzing the data.

While this list is not necessarily full and complete, we can use it to derive the actual requirements a personal medical device should fulfill to be secured against threats. The following requirements effectively address all types of identified issues:

- The data collected by the device must be accessible and modifiable only by authorized parties.
- The operation may not be interfered with or the operational parameters may not be modified or revealed without authorization.
- The use of the device must remain private and not be possible to detect by outsiders.
- The device may not store personal data of its user in the event of losing the device.
- Should the device be lost, any trust relationships must be broken with smart phones or other similar devices.
- Providing falsified information to users' smartphone or similar data collecting device must either be detected or prevented.

For devices that do not have any wireless connectivity issues, analyzing whether any of these threats are relevant is rather straightforward technical process. Devices with connectivity to cloud or smart phones require special attention and focus on the radio and cloud interfaces. More details on a proposed methodology for identifying security weaknesses are described on chapter 4.2.

In addition, there are some other security threats that might be used against users. I.e. if an attacker gains physical access to a target device, the internal electronics and/or firmware can be modified. This kind of attacks are not specific to personal medical devices, require physical access to the device thus limiting the potential extent of a successful attack and require relatively high amount of resources. As this thesis focuses on *cyber* security, this kind of attacks are excluded.

3.3 Regulation of medical devices

Within the European Union, medical devices are currently regulated by several different directives, regulations and decisions. The current legislation covers multiple aspects from in vitro diagnostics to implants, but the one applying in the scope of this thesis is Medical Device Directive (MDD) 93/42/EEC [48] that applies to medical devices in general. Since the initial publication, there have been numerous amendments to the MDD. By 2020 a Medical Device Regulation (MDR) should be fully applicable instead of MDD.

The currently effective directive 93/42/EEC [48] defines medical devices as follows:

> *"medical device" means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:*
>
> *— diagnosis, prevention, monitoring, treatment or alleviation of disease,*
>
> *— diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*
>
> *— investigation, replacement or modification of the anatomy or of a physiological process,*
>
> *— control of conception,*
>
> *and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means;*

This definition alone of medical devices can be interpreted in such a way that all commonly available personal medical devices from toothbrush to body temperature monitors and blood glucose level meters are covered by the directive.

The MDD specifies various risk-classes that define the exact requirements for the device. For high risk-class devices the evaluation is required to be performed by a Notified Body. The interpretation of the MDD in this thesis is that the personal medical devices fall into such risk-class where the manufacturer may itself assess whether the product meets the MDD requirements.

Software, information or cyber security is not directly referred in the MDD. Instead, the Directive concentrates on minimizing the potential generic risks that could compromise the safety and health of patients and users. MDD Annex I provides essential requirements all medical devices must meet. To illustrate the nature of these requirements, in the following are some selected excerpts from the MDD Annex I [48] that are related to the scope of this thesis:

> *The devices must be designed and manufactured in such a way that they can be used safely with the materials, substances and gases with which they enter into contact during their normal use or during routine procedures*
>
> *Devices with a measuring function must be designed and manufactured in such a way as to provide sufficient accuracy and stability within appropriate limits of accuracy and taking account of the intended purpose of the device.*
>
> *Devices incorporating electronic programmable systems must be designed to ensure the repeatability, reliability and performance of these systems according to the intended use.*
>
> *Devices intended to monitor one or more clinical parameters of a patient must be equipped with appropriate alarm systems to alert the user of situations which could lead to death or severe deterioration of the patient's state of health.*
>
> *Terminals and connectors to the electricity, gas or hydraulic and pneumatic energy supplies which the user has to handle must be designed and constructed in such a way as to minimize all possible risks.*

Even if the Medical Device Directive does not directly take a stand in software, information or cyber security, the European-harmonized standard IEC 62304 on Medical device software applies. It requires that security is handled by general quality and risk management that must be incorporated into software design processes.

European-harmonized standard IEC 60601-1-11 [49] instead directly covers home healthcare devices. It recognizes the fact that devices used for healthcare may be used outside clinical environments and that device users are non-professionals. There are requirements i.e. for electrical isolation and EM interference. In addition to obvious engineering requirements (such as mechanical strength requirements or addressing children inhaling or swallowing small parts) there are also requirements for preventing confusion of operation modes, and changes of control. This standard also is not taking a direct stand on cyber security, but certain requirements are protecting users from remote threats.

It is worth pointing out that the entire medical device regulation field is *very* complex, and no interpretations should be drawn based on this short introduction. Readers are encouraged to address the full list of Harmonized Standards for Medical Devices by the European Commission at https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en which lists close to 1000 standards. The bottom line is that devices should be safe to use in varying conditions and environments.

3.4 Regulation of personal data

Within the European Union, protection of personal data was regulated by 95/46/EC directive on data protection until spring 2018. In May this was replaced by General Data Protection Regulation (GDPR) 2016/679 [50] which will be fully applicable throughout the European Union. However, on fall 2018 not all members of the European Union have yet ratified the regulation. In the public, the most discussed feature of the GDRP is the requirement to report any breaches of personal data, and the possible fines for breach of private date ranging up to 4% of revenue.

The key terms related to this thesis and the GDPR are 'personal data', 'processing' and 'data concerning health'. These are defined as follows:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
>
> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
>
> *'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;*

Based on these definitions alone it can be argued that a personal medical device that collects and stores *data concerning health*, such as a smart thermometer, may not in fact be covered by the GDPR if the collected personal data cannot possibly be linked to the subject person. However, when smart phones or cloud-based services are used to process the personal data, it becomes clear that the natural person is identifiable. Thus, in these cases the processing of data originating from personal medical devices does fall under the GDPR.

The key in processing any kind of personal data is consent given by the data subject. Explicit consent is required when processing personal data in certain special categories,

such as racial, religion, sexual orientation and data concerning health. The GDPR defines consent as follows:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

When personal data, including data concerning health, is collected or processed within European Union a consent is required. On request, or when the consent is withdrawn, the personal data must be erased ("right to be forgotten"). The personal data can be processed within the EU, but export outside is permissible only with adequate level of protection. Significant number of cloud-based services operate in the United States. Exporting personal data to US is governed by EU-US Privacy Shield. The key is that only certain US organizations are approved to handle personal data of European Citizens.

In addition to strengthening of individual data subjects' rights the GDPR also poses requirements for organizations processing personal data. Data protection impact assessment (DPIA) is mandatory when data processing may result in a high risk. The DPIA can be considered as a limited Privacy Impact Assessment described in chapter 2.4. Processing data concerning health requires always a DPIA.

It should be noted that this chapter is a layman's interpretation on the GDPR and should not be taken as a legal statement.

4 Proposed security assessment process

Personal medical devices do not have any common technologies or interfaces, and the use-cases and possible threats differ significantly from device to device. While there are numerous processes and guidelines for security assessments, some described on chapter 2.3, none of these are directly applicable for testing personal medical devices. Therefore, it is reasonable to derive a new process that ensures everything is covered during security assessments of personal medical devices. The fundamental concept of the derived process is to ensure covering possible security threats identified in chapter 3.2.

In the very core of the derived security assessment process is an ordinary technical penetration test. To ensure that all features and functions are properly assessed there are additional phases that cover threat modeling and privacy issues described in chapters 2.4 and 2.5, respectively. The derived process also forces the assessor to ensure compliance with all identified issues with current regulation described in chapters 3.3 ja 3.4. The fundamental three cornerstones of the derived process are keeping users safe, keeping users' data safe and ensuring compliance.

For possible marketing and other purposes, the security assessment process could be illustrated graphically as described in Figure 3. The figure illustrates how the cyber security on personal medical devices depends on all three cornerstones and how the cyber security is not purely a set of technical requirements and operational parameters.

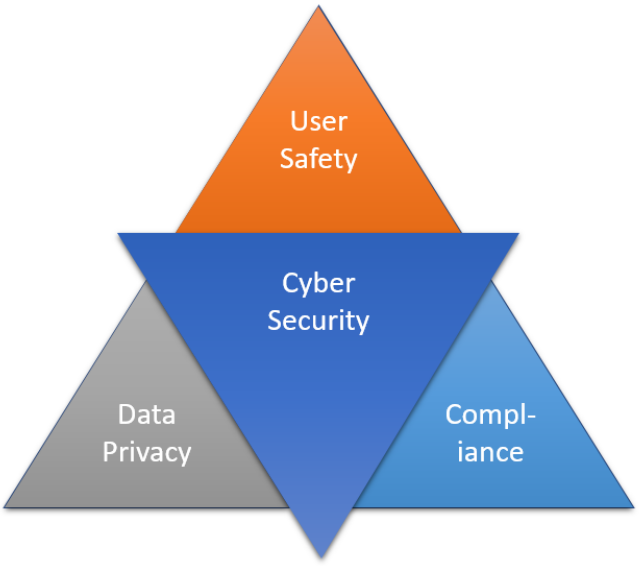

Figure 3 – Graphical illustration of the derived process

4.1 Security assessment process

The actual process for security assessment covering the three cornerstones consists of five major steps: Scoping, PDFA (Personal Data Flow Analysis), Penetration Test, Compliance Check, Analysis/Reporting. The order of the steps and the flow is illustrated in the following Figure 4.

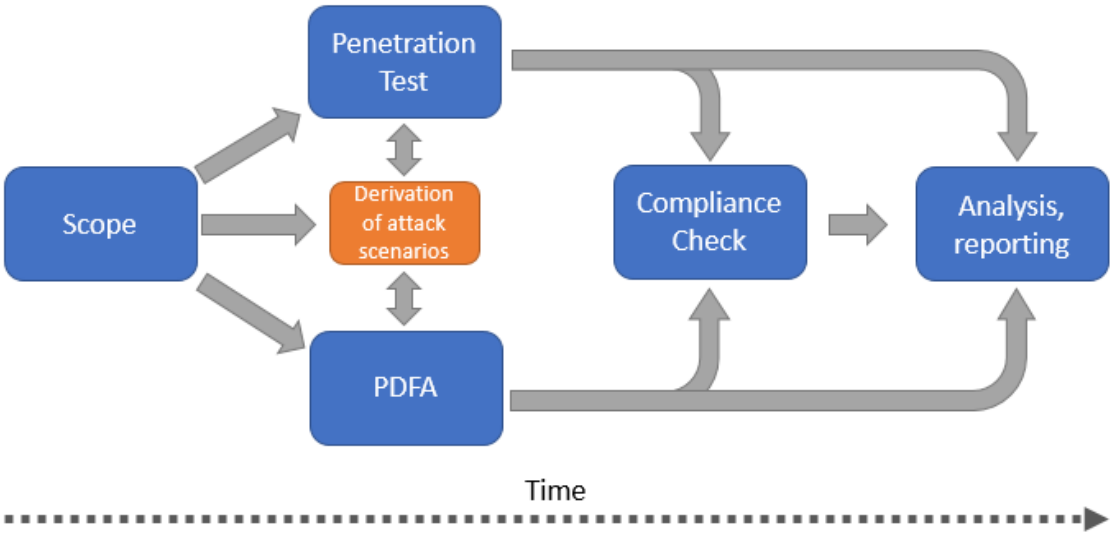

Figure 4 - Security assessment process flow

Scope – A Preliminary study aiming to decide the target and the extent of testing. Attention is needed in ensuring that enough time is reserved for the assessment, and that the scope covers the target. Usually the most interesting security findings are made at the edge, or right outside of the scope as certain things may be considered to be irrelevant.

Derivation of attack scenarios – Analysis of potential threats against the target system that are drafted originally based of the scope. If development team and the key personnel is available, perform threat modeling. During the assessment this step takes input from PDFA (Personal Data Flow Analysis) and Penetration Test to keep an up-to-date list of possible scenarios and guarantees the PDFA will address the Penetration Test findings and vice versa. Use chapter 3.2 as a basis.

PDFA – Personal Data Flow Analysis for identifying the privacy issues. Focus on what kind of data the devices collect, and all systems, interfaces and technologies used to transmit and process the data. Feed the findings to the attack scenario derivation, and include possible targets on the Penetration Test.

Penetration test – Discovering possible technical weaknesses and vulnerabilities. Analyzing the feasibility of attack scenarios. Standards and guidelines such as the ones described in chapter 2.3 and others should be used if applicable to ensure that the assessment does not overlook anything. Also, utilize the checklist in chapter 4.2 that is created for assessing personal medical devices. Most of the focus is on the following:

- Can the device be influenced through any of the provided interfaces without authorization? Including, but not limited to remote and wireless access.
- Does the device leak any information about its presence or use?
- In case the device itself collects data, can the data be accessed without authorization?

Compliance check – Assessing whether the target is compliant with relevant governmental regulations based on the findings of the PDFA and the Penetration Test. Note that regulations on cloud-based services may vary based on the country where services are provided from.

Analysis/reporting – Analyzing the results, creating a security assessment report that contains at least the following:

- The scope
- Relevant attack scenarios
- Functions and features that were tested and that were *not tested*
- Identified vulnerabilities and security issues during Penetration Test and PDFA. Each identified issue includes severity level and description of the finding. Also issues that are against regulations are documented as security issues.
- Conclusion of the current security level

It is worth noting that the security assessment is *not* an audit, it cannot prove a system is secure without any vulnerabilities and – without suitable accreditation – cannot state that a system follows governmental regulation or standard. Therefore, all issues affecting on the security are simply listed, and no audit-report like statements are given.

The current security level of the system is based on the severity levels of discovered vulnerabilities as described in the following Table 1.

Most severe finding	Overall security level
Critical	Low
High	Low
Medium	Medium
Low	High

Table 1 - Most severe finding vs. Overall security level

4.2 Technical and privacy checklist for penetration test

Checklists are commonly used to guarantee following the defined processes thoroughly and to prevent overlooking anything. A security assessment can be carried out against multiple types of devices, in various environments, and as in the process defined in chapter 4.1, the scope may vary from assessment to assessment. Defining a universal checklist with low abstraction level items is not feasible. To ensure that no technical details are overlooked, the following high-level checklist is created.

The created checklist aims to cover all technical weaknesses and issues in relatively high abstraction level. This cannot be universally broken down to individual technical tests and requires a highly skilled professional to ensure that each item is adequately tested. Furthermore, it is critical to understand that and by answering ‘yes’ on any of the items on the checklist does not necessarily identify a vulnerable system. It merely means that the particular feature needs to be properly assessed for any weaknesses that could be used against the user. For technical details on any item, there are numerous other checklists, for example the NIST Guide for Bluetooth security as explained on chapter 2.3.

1 Identifying existing security vulnerabilities

Numerous organizations and individuals perform security assessments on various devices and software. It may be possible that a security assessment has been performed already on a device or a part of its software and that security issues have been discovered.

1.1 Are there any publicly disclosed vulnerabilities on the target device or related software? Check at least CVE by Mitre[4] and SecurityFocus Bugtraq[5].

2 Identifying the use of the device

The presence and/or the use of device may give out sensitive information on health conditions depending on the device type and device detection accuracy. E.g. carrying a Bluetooth-enabled blood glucose meter identifies with high confidence the person as diabetic.

2.1 Is the device itself, or its use detectable from a distance?

2.1.1 By wireless connectivity features?

2.1.2 By other emanations including but not limited to RF?

3 Data processing

This section affects only devices that measure, collect and/or process any data that is originating from the user, including the usage history and pre-set parameters. There are numerous electronic personal medical devices that are outside of this category. However, special attention is needed when making the initial judgement on the internal workings of the device.

3.1 Does the device measure, collect and/or process any data? Does the device record usage history?

3.1.1 Are there secure mechanisms to erase the data?

3.1.2 Are there secure mechanisms to erase the usage history?

3.1.3 Does the device support transferring of personal data?

3.1.3.1 Is there a secure mechanism that ensures that data is not transferred or leaked to unauthorized parties during transmission?

[4] https://cve.mitre.org/cve/search_cve_list.html
[5] https://www.securityfocus.com/vulnerabilities

3.1.3.2 How does the receiving device identify the true source of the data? Is the data transfer protected against MITM-attacks?

3.1.3.3 Is the data sent further to a 3rd party i.e. a cloud-based service?

3.1.3.3.1 Does the cloud service operator comply with current legislation and regulations?

3.1.3.3.2 Is the data transfer over the internet secure by design and implementation?

4 Communication channels

Communication channels (e.g. WiFi, Bluetooth, USB etc.) may allow interfacing with the device. When there is no user interface limiting the communication, it may be possible to interact with the device in non-standard ways and supply it with data that may cause undesired behavior. This may be used against the device to extract data or to modify its internal working parameters.

4.1. Are there any service ports or interfaces?

4.1.1. Can the operational parameters be modified?

4.1.2. Is it possible to extract any sensitive data?

4.1.2. How does the device react on unexpected input?

4.2. Is there wireless connectivity?

4.2.1. Is communication secure by design and implementation?

4.2.2. Are unauthorized parties able to access the device or the data stored?

4.2.3. Are unauthorized parties able to modify operational parameters or data stored?

4.2.4. How does the device react on unexpected input?

5 Firmware upgrades

A firmware upgrade allows modifying the internal software of the device. If this is not implemented in a secure manner it provides a possible attack vector that can be used to influence with the internal workings of the device. Furthermore, if the firmware is provided in a non-encrypted package, it allows attackers to reverse engineer to software to find possible weak points and vulnerabilities

5.1 Can the device firmware be upgraded?

5.1.1 Is the firmware upgrade process secured against using software from unauthorized sources? If third party firmware is supported, it may open a new set of attack vectors.

5.1.2 Can the firmware upgrade be completed remotely without authorization and having physical access to the device? If possible, it may be possible to have the device execute arbitrary code which gives the attacker total control of the device.

5.1.3 Is firmware upgrade possible to older firmware version? If yes, device firmware can be downgraded to version that contains more vulnerabilities than the current one.

5.2 Is the device firmware accessible e.g. on a download page in the internet?

5.2.1 Is the firmware image encrypted and/or protected against reverse engineering?

5 Practical assessments

Series of practical assessments using the described process was carried out against common personal medical devices that are sold over the counter. The devices are:

- Oral-B SmartSeries 6200 toothbrush
- Philips Avent smart thermometer
- Medisana MediTouch 2 blood glucose meter
- GlucoRx Nexus blood glucose meter
- Beurer EM49 TENS device

This selection represents a realistic set of modern personal medical devices found commonly in households. Some of these are stand-alone systems with very limited connectivity options, and some utilize cloud connectivity and specialized smart phone apps to enhance the user experience. The potential impact should for example a blood glucose meter be compromised could be severe.

In short, the assessments carried out demonstrated that the current state of cyber security on personal medical devices is relatively high. No serious issues were discovered in any of the devices that could be used to directly inflict physical damage on users. However, numerous minor issues were identified that can be used impact of the Bluetooth communication. Most significant issues identified were information leakage that could provide unauthorized parties with sensitive data.

Certain constraints limited the scope of the practical assessments. While some of the devices can be connected to cloud-based systems, these systems were declared to be out of scope and no assessment on the cloud functionalities was performed. There was no permission from the companies to perform penetration test on their environments.

Also, the extent of the actual penetration tests was reduced for testing various communication interfaces. Testing how the interfaces react using fuzz testing requires specialized, and in some cases tailored physical equipment that was not available during the assessments. Tests carried out were performed using ordinary PC-compatible computers and standard tools.

As the companies and/or the developers of the devices and applications were not participating in this thesis, also the Personal Data Flow Analysis could not be performed. Due to the limitations, in the following not full reports are provided, but the technical findings each assessed device.

5.1 Oral-B SmartSeries 6200 toothbrush

Oral-B SmartSeries 6200 [51] represents a premium electric toothbrush with multiple additional features and connectivity options. A typical setup consists of a cordless toothbrush, a charging station and a SmartGuide display unit. The SmartSeries toothbrushes may also be connected to a mobile phone to be used with Oral-B application. Figure 5 illustrates the typical components of the setup.

Figure 5 - Oral-B SmartSeries 6200 [51]

The numerous connectivity options the toothbrush has are reflected in the attack scenarios. In addition to simple technical vulnerabilities also processing of private data had to be analyzed. The attack scenarios assessed were there following:

- Denial of service scenarios
- Modifying the operation of the toothbrush to inflict discomfort
- Modifying the displayed data from a distance
- Accessing brushing details (time, duration, mode)
- Accessing users' personal data
- Detecting the use of the device

In addition to Bluetooth connectivity there are no user serviceable parts, sockets, or other interfaces. The only buttons and input functions on the toothbrush are for starting and stopping, and for changing the brushing mode. On the SmartGuide unit there are buttons for setting the current time. This effectively limits the potential interfaces an attacker may utilize practically only to Bluetooth connectivity.

When the toothbrush is activated it will constantly broadcast over Bluetooth Low Energy the current mode of operation and the duration of the current brushing session. There appears to be no secure mechanism to prevent eavesdropping of the data. Physical location can be estimated using radio direction finding techniques. The SmartGuide unit will display the duration and mode based on the information on these broadcasts without authenticating the data source.

The Oral-B app on smart phones may download the data of the last 20 brushing sessions from the toothbrush. The app can also be used to modify the operational modes of the toothbrush. I.e. the brush can be programmed to pause the brushing for a brief moment at specific intervals, and limit which operational modes can be selected on the toothbrush.

There is virtually no protection against accessing the internal activity history of the device using any generic Bluetooth device. Furthermore, when the device is active, it will broadcast information about current operational mode and the length of the current session. Attackers may utilize this for accessing users' information. Furthermore, the operational mode of the toothbrush may reveal if users are suffering from for example gingivitis and reveal the daily rhythm of users'.

Based on the information collected it appears that potential attackers may transmit custom Bluetooth Low Energy frames to make the SmartGuide unit display arbitrary data. Also, the operational mode of the toothbrush may be modified from a distance that users may interpret as device failure.

The Oral-B smart phone app does not relay information on the usage of the toothbrush to the Oral-B, however it does report the physical location when the app is started. This appears to be used to provide weather forecasts. On the reports user's phone model, current IP-address and other details are sent that can be used to identify the user.

In the current state the device has the following vulnerabilities:

- Possibility to alter device operational parameters and retrieve history data without authorization. CVSS score 4.6 (Medium)
- Possibility to detect device usage, brush mode and brushing duration by passive eavesdropping from a distance. CVSS score 3.5 (Low)
- Possibility to inject incorrect data to the SmartGuide display. CVSS score 3.5 (Low)
- Leakage of users' location and identifiable data. (Undefined)

Based on the findings, the security level of the Oral-B SmartSeries 6200 toothbrush is medium.

5.2 Philips Avent smart ear thermometer

The Philips Avent smart ear thermometer [52] measures the body temperature from the ear within a few seconds. It's part of uGrow family of connected products that contains multiple devices to monitor health of babies and newborn. The ear thermometer does not have any age limitations. The device has Bluetooth connectivity and supports data transfer to uGrow smart phone application. Figure 6 illustrates the device.

Figure 6 - Philips Avent smart ear thermometer [52]

The attack scenarios assessed were there following:

- Denial of service
- Accessing measurement data without authorization
- Modifying the measurement results from a distance
- Detecting the use of the device

The device provides wireless connectivity to smart phones using Bluetooth Low Energy technology. When temperature is being measured the device broadcasts its identity using BLE advertisement. During a 30 second time window it is possible to communicate with the thermometer using the BLE technology and extract measurement data. Measured values appear to be protected in such a way that the first smart device to access certain value gains exclusive rights to it.

An attacker may identify the use of the Philips Avent ear thermometer simply by listening to the BLE advertisements. Physical location can be estimated using radio direction finding techniques. The pace of BLE advertisements a particular device is transmitting may be used to deduct information on the current health conditions. I.e. a person suspecting or suffering from a fever most likely measures the body temperature more often than one feeling healthy.

The current measurement can be downloaded by an attacker simply by initiating the data download faster than the victim. Should the victim not use any smart devices and uses the Philips Avent as a simple ear thermometer without a smart phone, an attacker may download the entire measurement history.

Use of the smart features require the use of a smart phone and uGrow software by Philips. The app itself highlights privacy issues and asks for permissions prior to execution of tasks that process personal medical data. On the first software start-up the app opens multiple connections to various destinations. These, however, seem to comply with provided agreement that is required to use cloud-based services. Nevertheless, the language in these agreements is English, which may be problematic in non-English speaking countries.

Should the victim use smart phone and the uGrow app, there appear to be no mechanisms to prevent the attacker from sending falsified information to the smart phone. This could not be verified due to the lack of testing hardware, and is based on packet analysis.

The uGrow software communicates with multiple servers and service providers using TLS protected HTTP. On closer analysis the TLS is adequately configured for all servers. There are minor variations, but none of the servers suffers from higher level vulnerabilities. There is, however, on various servers support for TLS 1.0 and 1.1, and for weak encryption algorithms, but this is most likely required due to the large variation of customer devices.

In the current state the device clearly has the following vulnerabilities:

- Possibility to access measured data without authorization. CVSS score 4.6 (Medium)
- Possibility to detect the use of the device from a distance. CVSS score 3.5 (Low)
- Tentative possibility to spoof measurement data retrieved on the smart device. CVSS score 3.5 (Low)
- Minor SSL configuration weaknesses with cloud backend, all low.

Based on the findings the security level of the Philips Avent ear thermometer is medium.

5.3 Medisana MediTouch 2

Medisana MediTouch 2 [53] is a blood glucose meter with very limited functionalities. In a typical use case the user first inserts a test strip, then touches it with a drop of blood and reads the blood glucose level. The historical values can be read from the display. User may also install VitaDock+ app for Android and iOS to store all recorded values on a mobile device and VitaDock cloud. The Medisana MediTouch 2 is shown in Figure 7,

Figure 7 - Medisana MediTouch 2 [53]

The attack scenarios assessed were there following:

- Denial of service
- Detecting the use of the device
- Accessing measurement data on the device without authorization
- Modifying the measurement results and/or accuracy from a distance

After a measurement is complete the MediTouch 2 attempts to discover a mobile device running the VitaDock+ application. This is implemented by Bluetooth Low Energy advertisements. An attacker at a vicinity of the device may receive these advertisements, use radio direction finding techniques and identify the person using the blood glucose meter. These BLE advertisements do clearly identify the device as MediTouch 2 without attempting to hide the device type. These advertisements do not contain the measurement data.

While there was no equipment at hand to fully analyze the Bluetooth operation and all its possible weaknesses, it appears that for a user who does not utilize the wireless functionality, the sensitive data stored on the device can be accessed by unauthorized parties.

During the technical assessment it was observed on several occasions that the device ran out of power. The device has two CR2032 batteries, but it can also be supplied with

smaller capacity batteries such as. CR2025 and CR2016. On all of the occasions the event happened during Bluetooth communication. This, while not fully confirmed, suggests that an attacker may be able to cause a denial of service on the target device by intense communication thus depleting the batteries.

The VitaDock+ application communicates with Vitadock server using TLS protected HTTP. On closer analysis the TLS is adequately configured. There is, however, support for TLS 1.0 and 1.1, and for weak encryption algorithms, but this is required due to the large variation of customer devices. Also, it's worth noting that the site is using a wildcard certificate that includes such alternative names that do not exist. While this is not a security risk, it implies lacking system or certificate magement.

In the current state the device has the following vulnerabilities:

- Tentative Denial of Service through battery exhaustion by extensive Bluetooth usage. CVSS score 5.7 (Medium)
- Possibility to access measured data without authorization. CVSS score 4.6 (Medium)
- Possibility to detect the use of the device from a distance. CVSS score 3.5 (Low)
- Minor SSL configuration weaknesses with cloud backend, all low.

Based on the observations the security level of the Medisana MediTouch 2 is medium.

5.4 GlucoRx Nexus blood glucose meter

GlucoRx Nexus [54] is a blood glucose meter with very limited functionalities. In a typical use case the user first inserts a test strip, then touches it with a drop of blood and reads the blood glucose level. The historical values can be read from the display using the only button device has. User may download GlucoRx HealthCare Management System for Windows-based computers. This can be used to transfer data from the meter to a PC using USB connection. The software offers very limited functions and is limited only for displaying the data. No cloud connectivity is supported. The GlucoRx Nexus is shown in Figure 8.

Figure 8 - GlucoRx Nexus blood glucose meter [54]

The attack scenarios assessed were there following:

- Denial of service
- Detecting the use of the device
- Accessing measurement data on the device without authorization
- Modifying the measurement results and/or accuracy from a distance

Internally it is obvious that the manufacturer of the device is Taiwanese Taidoc Corp. and that is has been rebranded as GlucoRx Nexus based on the markings on the main circuit board. Internal observations did not reveal any hidden functionalities, including RF communication subsystems. The main printed circuit board does have connectors that resemble JTAG interfaces that may be used to extract the device firmware and modify the operational parameters.

There is a possibility for an attacker to modify the device operation in case the device is physically compromised, this however cannot be seen a as cyber security issue. Whether the USB interface can be used to modify the internal workings of the device was not assessed, as it provides very little value to a possible attacker while there are JTAG connector available.

The USB interface does provide a way to transfer measured data to a personal computer. Should the meter be lost or stolen, there is a possibility that historical values may end on unauthorized hands. There however are no personally identifiable details on the device, so there is no method to identify the actual user of the device. Losing the device is equivalent to losing hand-written notes.

Based on the observations the security level of the GlucoRx Nexus is high.

5.5 Beurer EM49 TENS device

Beurer EM49 TENS device [55] is small device intended for electronic muscle stimulation (EMS) and transcutaneous electrical nerve stimulation (TENS). EMS is for muscle training and regeneration, and TENS for pain relief and massage. To use the device four self-adhesive electrodes are placed on the skin. These are used to excite the muscles by utilizing very brief voltage pulses. Beurer EM49 does not collect or store any data, and it does not have any communication interfaces. It does not have any interfaces other than the electrode connectors. The device is shown in Figure 9.

Figure 9 - Beurer EM49 TENS device [55]

The attack scenarios assessed were there following:

- Detecting the use of the device from a distance
- Inflicting damage or intense pain by modifying the device operation without authorization

When the device is operating the individual pulses delivered are in the range of 10 Volts. This along with the relatively low frequency of the pulses effectively limits the radiated energy. Based on the measurements the use of the device can be detected from a very, very short distance. This is not a feasible attack to leak information on device users from a distance of multiple meters. Furthermore, as the use cases for the EM49 device include not only TENS, but also for EMS, even if the use of the device could be detected, the information leaked on medical conditions is not full accurate.

Based on the observations made from the device main circuit board, increasing the output power to harmful levels is not possible. The output power is limited first by the power supply (3x AAA battery), then by the pulse forming circuitry and finally by the inductance of coils used to create the voltage pulses. Furthermore, people with heart conditions are discouraged using the device, and the manual prohibits placing the electrodes in such a way that the current would flow through the heart or spinal cord. Therefore, small increases on the output power, which are possible, are most likely not to cause any permanent damage.

While the device electrically is able to provide output power levels that would cause discomfort, enabling such operation is not feasible. The device does not appear to use any commonly available microcontrollers, and is on the circuit board lacking any interfaces, including JTAG and similar. Therefore, modifying the operation of the device is not a trivial task, and practically impossible from a distance.

Based on the observations the cyber security level of the GlucoRx Nexus is high.

5.6 Discussion

On devices without any communication interfaces no technical vulnerabilities were discovered. This may seem an obvious and expected result, but when considering that even detecting the use of the device through RF radiations was assessed, this result is relevant. Personal data identifying users' medical conditions cannot be easily detected from a distance.

On Bluetooth-based attacks it can be argued that Bluetooth technology is a short-range communication system, with very limited communication range of approximately 10 meters. And as such, the Bluetooth based attacks would not pose a real risk. While the Bluetooth is a short-range communication protocol, there are multiple device classes with range up to 100 meters. Also, for attacking Bluetooth based systems range-extension techniques are available [56]. With Bluetooth Low Energy the range is quadrupled [57] – before using the range-extenders.

The devices with wireless connectivity features did contain multiple vulnerabilities that could be used on practical attacks. While the impact on the society directly by discovered vulnerabilities is rather minimal, the results should not be taken lightly as the vulnerabilities can be used as a part of another attacks. As an example, an attacker could use the Bluetooth information leakage on a toothbrush to identify the daily routines of a target household. When these routines change, it will give the attacker an edge to carry out a physical attack. The information leakage on a thermometer leaks highly sensitive data on medical conditions which is not something device users would expect.

The fact that these wireless devices can be accessed from a large distance with equipment that can be carried easily without being detected makes searching for potential targets and collecting data from a large area quite an easy task. Therefore, the discovered weaknesses may have an impact of large user base and are *cyber* threats.

For this thesis, the cloud-based services, APIs and other related interfaces were *not* assessed. Systems may contain vulnerabilities that would enable attackers to breach the systems hosting the private data. Considering the few examples of recent data breaches briefly addressed in chapter 2.1, it can be argued that the personal data is not necessarily safe on service providers' servers.

The mobile applications that utilize cloud-based services do provide user information on storing the data on the service providers' servers. However, the information provided is

not easily understandable, and is written in “legalese”. Individual users may not fully understand the agreements, and the associated risks of using cloud-based services. Furthermore, there might be issues related to the current privacy legislation, the GDPR. The compliance should therefore be assessed together with subject matter experts.

The proposed security assessment process itself was identified to have some shortcomings. When performing as assessment on target without support from the manufacturer, the visibility on the low-level system operations is very much limited. For example, ensuring that the Bluetooth connectivity is implemented in a secure manner by verifying it against the NIST Guide to Bluetooth Security described in chapter 2.3.4 is practically impossible using only the interfaces provided to the consumer. The limited visibility also applies to general software running on the device. Any public application programming interfaces and cloud-based systems could technically be assessed with black box testing[6], but this was not carried out as there was no permission from the device manufacturer.

Due to the limited visibility on low-level operation of various communication channels, software itself and cloud-based services it’s possible that there are several other security issues that could not be detected. Also, the actual paths of the personal data could not be assessed as this was not adequately documented, and the manufacturers’ key personnel was not available.

Despite the shortcomings, the proposed model is valid, but it was nevertheless discovered that performing a security assessment on a real target requires more than just the target device. All key actors should be available, and permission should be granted to assess the online services. To form a very detailed view on the security posture of a personal medical device, also the source code for the internal software and mobile applications should be available to ensure all aspects are covered.

[6] In black box testing the internal workings of the target at not known, and the target is assessed only through interfaces it provides with the knowledge that can be obtained from these interfaces.

6 Conclusions

The cyber security field is constantly evolving. Due to the connectivity options, more and more devices are being accessed remotely, and share their data with cloud-based services. Traditional information security issues become cyber security issues when the vulnerabilities, or the potential impact may have an influence on larger group of people. With modern, connected devices even a minor security vulnerability can have an impact on a very large user base.

With medical devices the common threat previously in the public has been “stopping a pacemaker” from a distance. While this, and other related to devices used for life support are in fact recognized, the improvement of the cyber security on medical technology has not yet covered personal medical devices.

Personal medical devices have previously been relatively simple apparatus. Currently the devices on the market have more advanced features. Devices have microcontrollers, they perform complex operations and store historical measurement data and offer variety of connectivity options. This enables the users to utilize smart phones and cloud-based services for additional use-cases.

This thesis proposed the first public security assessment process to assess the cyber security state of personal medical devices. Assessing personal medical devices is relevant as security risks have the potential to impact very large user base.

What was shown during technical security assessment on variety of devices is that some of the risks are real. Attackers may detect from a distance when you brush your teeth, or what is your body temperature if you are using vulnerable devices. The most common identified security issue is information leakage which may put users’ personal data on their medical conditions at risk. The proposed assessment process does have some weaknesses, and the key finding was that having only a target device may not be enough to perform a security assessment and that additional support from the device manufacturer is required.

As it was shown that personal medical devices *do* have vulnerabilities that put users’ data at risk, it is highly recommended to direct more focus on the field. This includes not just the security assessments of individual devices, but also system design during product development and education of public for possible issues and related risks.

References

[1] “ISO/IEC 27000:2014(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary.” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en. [Accessed: 17-Mar-2018].

[2] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*, Second edition. Amsterdam ; Boston: Elsevier/Syngress, Syngress is a imprint of Elsevier, 2014.

[3] D. B. Parker, *Fighting computer crime: a new framework for protecting information*. New York: Wiley, 1998.

[4] Turvallisuuskomitean sihteeristö, *Suomen kyberturvalliisuusstrategia*. Puolustusministeriö, 2013.

[5] T. Kuusisto, Ed., *Kybertaistelu 2020*. Maanpuolustuskorkeakoulu, 2014.

[6] “Under Armour says 150 million MyFitnessPal accounts breached,” *Reuters*, 30-Mar-2018.

[7] Iain Thomson in San Francisco 15 Feb 2018 at 21:29, “When it absolutely, positively needs to be leaked overnight: 120k FedEx customer files spill from AWS S3 silo.” [Online]. Available: https://www.theregister.co.uk/2018/02/15/fedex_aws_s3_leak/. [Accessed: 12-Apr-2018].

[8] Viestintävirasto, “Varoitus 01/2018: Suomalaisten selväkielisiä salasanoja paljastunut.” [Online]. Available: https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2018/varoitus-2018-01.html. [Accessed: 12-Apr-2018].

[9] “Your medical record is worth more to hackers than your credit card,” *Reuters*, 24-Sep-2014.

[10] “The Black Market For Stolen Health Care Data,” *NPR.org*. [Online]. Available: https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data. [Accessed: 12-Apr-2018].

[11] E. Fuller, *Network security evaluation: using the NSA IEM*. Rockland, Mass.: Syngress Pub., 2005.

[12] Viestintävirasto, “Accredited inspection bodies.” [Online]. Available: https://www.viestintavirasto.fi/en/cybersecurity/informationsecurityinspectionbodies/hyvaksytytarviointilaitokset_en.html. [Accessed: 13-Mar-2018].

[13] B. Arkin, S. Stender, and G. McGraw, “Software penetration testing,” *IEEE Secur. Priv.*, vol. 3, no. 1, pp. 84–87, Jan. 2005.

[14] P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system,” *IEEE Secur. Priv.*, vol. 4, no. 6, 2006.

[15] M. Vanhoef, “KRACK Attacks: Breaking WPA2.” [Online]. Available: https://www.krackattacks.com/. [Accessed: 21-Jan-2018].

[16] “Meltdown and Spectre.” [Online]. Available: https://meltdownattack.com/. [Accessed: 21-Jan-2018].

[17] P. Herzog, *OSSTMM 3 - The Open Source Security Testing Methodology Manual*. ISECOM, 2010.

[18] Manico et al., “Application Security Verification Standard 3.0.1.” OWASP - Open Web Application Security Project, 2016.

[19] PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures*. PCI Security Standards Council, 2016.

[20] PCI Security Standards Council, *Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements*. PCI Security Standards Council, 2009.

[21] PCI Security Standards Council, *Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) - Modular Derived Test Requirements*. PCI Security Standards Council, 2016.

[22] J. Padgette *et al.*, “Guide to bluetooth security,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-121r2, May 2017.

[23] P. Torr, “Demystifying the threat modeling process,” *IEEE Secur. Priv.*, vol. 3, no. 5, pp. 66–70, Sep. 2005.

[24] Microsoft, “Threat Modeling,” 2003. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff648644.aspx. [Accessed: 25-Feb-2018].

[25] Microsoft, “The STRIDE Threat Model,” 2005. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. [Accessed: 25-Feb-2018].

[26] D. Wright and P. De Hert, “Introduction to Privacy Impact Assessment,” in *Privacy Impact Assessment*, D. Wright and P. De Hert, Eds. Dordrecht: Springer Netherlands, 2012, pp. 3–32.

[27] G. Nájera-Gutiérrez, *Kali Linux Web Penetration Testing Cookbook*. Packt Publishing Ltd, 2016.

[28] “Burp Suite editions and features.” [Online]. Available: https://portswigger.net/burp. [Accessed: 30-Sep-2017].

[29] “OWASP Zed Attack Proxy Project - OWASP.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. [Accessed: 30-Sep-2017].

[30] W. Halton, B. Weaver, J. A. Ansari, S. R. Kotipalli, and M. A. Imran, *Penetration Testing: A Survival Guide*. Packt Publishing Ltd, 2017.

[31] “Nessus Vulnerability Scanner,” 18-Dec-2012. [Online]. Available: https://www.tenable.com/products/nessus-vulnerability-scanner. [Accessed: 30-Sep-2017].

[32] "OpenVAS - OpenVAS - Open Vulnerability Assessment System." [Online]. Available: http://www.openvas.org/. [Accessed: 30-Sep-2017].

[33] *Wireshark · Go Deep.* .

[34] Ellisys Inc., "Ellisys Bluetooth Explorer brochure." Ellisys Inc.

[35] P. Bai, K. Sheng, Y. Li, N. A. Yu', an Tan, and X. Yu, "Research on Bluetooth protocols based on Android kernel log," *Int. J. Comput. Sci. Math.*, vol. 6, no. 1, p. 78, 2015.

[36] M. Sutton, A. Greene, and P. Amini, *Fuzzing: Brute Force Vulnerability Discovery*. Pearson Education, 2007.

[37] A. Helin, *radamsa: a general-purpose fuzzer*. 2017.

[38] Peach tech, "Peach Fuzzer Overview." Peach tech.

[39] "Scapy." [Online]. Available: http://www.secdev.org/projects/scapy/. [Accessed: 30-Sep-2017].

[40] "Proxmark3 Kit - Rysc Corp." [Online]. Available: https://store.ryscc.com/products/new-proxmark3-kit.

[41] K. Rakesh, "RFID based Swiss Army Knife," *J. Adv. Technol. Eng.*, vol. 1, no. 1, pp. 1–4, 2012.

[42] C. Miller, "Exploring the NFC attack surface," *Proc. Blackhat*, 2012.

[43] B. Ransford *et al.*, "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists," *Pacing Clin. Electrophysiol.*, vol. 40, no. 8, pp. 913–917, Aug. 2017.

[44] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots," *ArXiv150404339 Cs*, Apr. 2015.

[45] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Med. Devices Auckl. NZ*, vol. 8, pp. 305–316, Jul. 2015.

[46] "McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals," *McAfee Blogs*, 11-Mar-2018. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/. [Accessed: 02-Apr-2018].

[47] C. Beek, C. McFarland, and R. Samani, "Health Warning Report." McAfee, 2018.

[48] Council of the European Union, "Council Directive 93/42/EEC of 14 June 1993 concerning medical devices," 1993.

[49] "A guide to meeting the IEC60601-1-11 standard in home healthcare devices," *Design World*, 17-Sep-2014. [Online]. Available: https://www.designworldonline.com/guide-meeting-iec60601-1-11-standard-home-healthcare-devices/. [Accessed: 18-Apr-2018].

[50] Parliament of the European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016,” 2016.

[51] “Amazon.com: Oral-B Electric Toothbrush Pro 6200 SmartGuide: Health & Personal Care.” [Online]. Available: https://www.amazon.com/Oral-B-Electric-Toothbrush-6200-SmartGuide/dp/B00LVUY4KU. [Accessed: 25-Mar-2018].

[52] “Amazon.com : Philips AVENT Smart Ear Thermometer : Baby.” [Online]. Available: https://www.amazon.com/Philips-AVENT-Smart-Ear-Thermometer/dp/B01M5DCJTK. [Accessed: 25-Mar-2018].

[53] “Amazon.com: Medisana MediTouch 2 Blood Glucose Device: Health & Personal Care.” [Online]. Available: https://www.amazon.com/Medisana-MediTouch-Blood-Glucose-Device/dp/B00G6R8B7A. [Accessed: 25-Mar-2018].

[54] “GlucoRx Nexus Blood Glucose Monitoring System Kit (Eligible for VAT relief in the UK): Amazon.co.uk: Health & Personal Care.” [Online]. Available: https://www.amazon.co.uk/GlucoRx-Glucose-Monitoring-System-Eligible/dp/B01LYKZ4ZU. [Accessed: 25-Mar-2018].

[55] “Beurer EM49 Handheld Digital TENS/EMS Device with LCD Electrode Positioning Indicator: Amazon.co.uk: Health & Personal Care.” [Online]. Available: https://www.amazon.co.uk/Beurer-Handheld-Electrode-Positioning-Indicator/dp/B01KUJ1VMG. [Accessed: 25-Mar-2018].

[56] J. P. Dunning, “Taming the Blue Beast: A Survey of Bluetooth Based Threats,” *IEEE Secur. Priv. Mag.*, vol. 8, no. 2, pp. 20–27, Mar. 2010.

[57] “Bluetooth® 5 Quadruples Range, Doubles Speed, Increases Data Broadcasting Capacity by 800% | Bluetooth Technology Website.” [Online]. Available: https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth-5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800. [Accessed: 31-Mar-2018].