ERNW RESEARCH
pursuing knowledge.

ERNW WHITE PAPER 69

SAFETY IMPACT OF VULNERABILITIES IN INSULIN PUMPS

Version:	1.0
Date:	September 10, 2020
Classification:	Public
Author(s):	Julian Suleder

Federal Office for Information Security

Julian Suleder

Digital unterschrieben von Julian Suleder
Datum: 2020.09.10 15:16:28 +02'00'

ERNW RESEARCH
pursuing knowledge.

Table of Content

ERNW RESEARCH
pursuing knowledge.

List of Abbreviations

APS	Artificial Pancreas System
BfArM	German Federal Institute for Drugs and Medical Devices
BLE	Bluetooth Low Energy
BSI	German Federal Office for Information Security
CGM	Continuous Glucose Monitor
CSII	Continuous Subcutaneous Insulin Infusion
CT	Computer Tomography
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposure
DDG	German Diabetes Association
FSCA	Field Safety Corrective Action
FSN	Field Safety Notice
GKV	German Statutory Health Insurance
ICS	Industrial Control System
ICSMA	ICS Medical Advisory
IFU	Instructions for Use
ManiMed	Manipulation of Medical Devices
MDK	Medical Service of German Statutory Health Insurance providers
MRI	Magnetic Resonance Imaging
PIN	Personal Identification Number
SHI	Statutory Health Insurance

List of Figures

ERNW RESEARCH
pursuing knowledge.

1 Project ManiMed - Manipulation of Medical Devices

Digital networking is already widespread in many areas of life. In the healthcare industry, a clear trend towards networked devices is noticeable, so that the number of high-tech medical devices in the health sector (hospitals, care institutions, doctor's offices, home care, etc.) is steadily increasing. In clinical settings, these include, e.g., infusion pumps, implants, or large medical equipment, such as CT and MRI. Notably, in a clinical environment, highly complex devices are used for vital applications. This is usually accompanied by extensive usage over a prolonged service life and can cause severe problems because security measures are often missing or ineffective. A defective or manipulated device can pose a potential threat to patients' lives.

The German Federal Office for Information Security (BSI), in its role as the Federal Cyber Security Authority in Germany, aims to sensitize manufacturers and the public regarding security risks of networked medical devices. In response to the often fatal security reports and press releases of networked medical devices, the BSI initiated the project *Manipulation of Medical Devices (ManiMed)* in 2019. In this project, a security analysis of selected products is carried out through security assessments.

The project aims to assess the current cybersecurity state of medical devices and further to bring security researcher, manufacturers and authorities to a table. Five different device categories, namely ventilators, patient monitors, ICDs and their environment, infusion pumps, and insulin pumps are selected for a market research as shown in Figure 1.

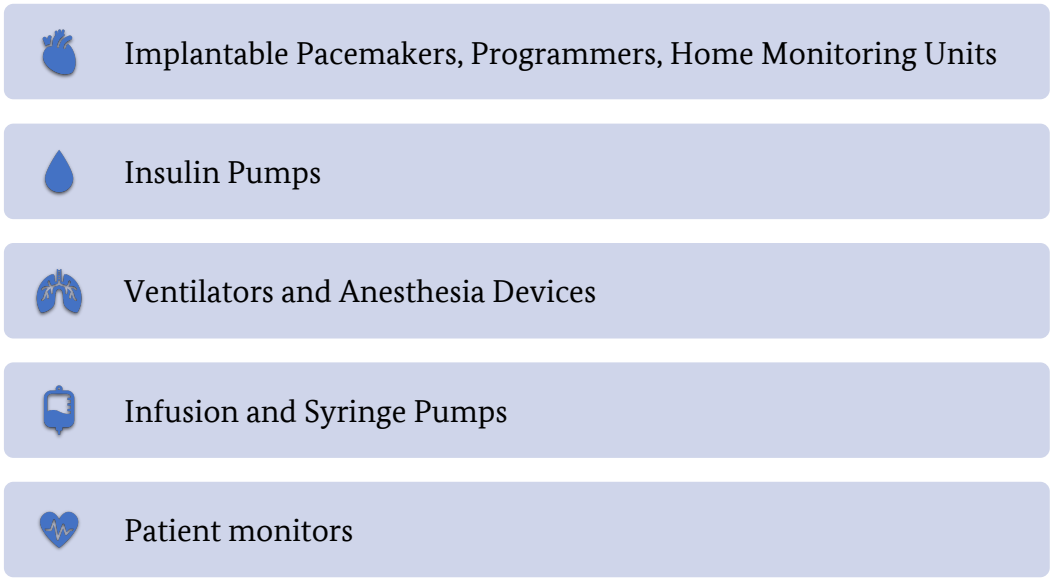

Figure 1: Devices from the categories of ventilators, patient monitors, ICDs and their environment, infusion pumps, and insulin pumps are selected for a market research.

Out of each category two devices are assed within the scope of the project. To further restrict the market research, additional requirements had to be met. The devices had to be put on the German market after January 1, 2014 and should be highly connected, having as many interfaces as possible (appropriate attack surface) as shown in Figure 2.

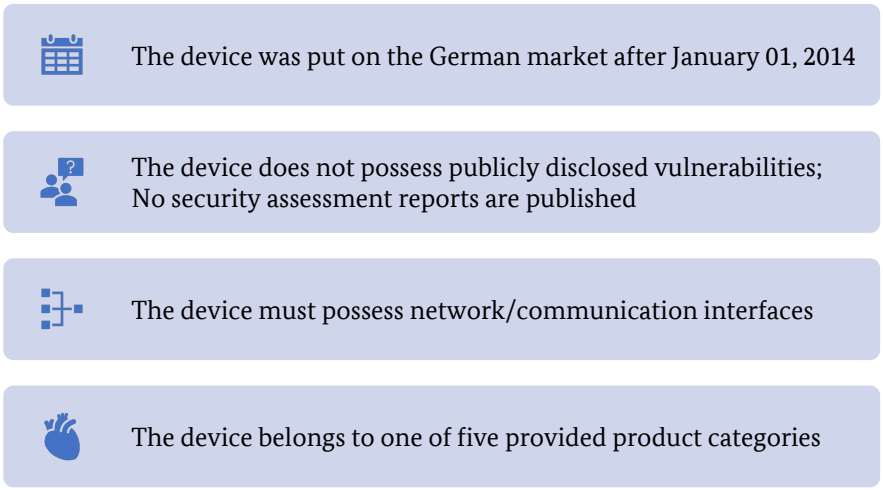

Figure 2: Medical Device Selection Criteria in project ManiMed.

Prior to the assessment, the BSI got in contact with the top manufacturers found in the market research and explained the intention of the project to pentest the respective devices. Ideally a testing contract is signed. With this, the manufacturers provide the respective medical devices and lab environments and receive exclusive knowledge about the cybersecurity state of the system in return. More precisely, the manufacturers are provided with detailed reports about all findings and proposed mitigation strategies and a subsequent Coordinated Vulnerability Disclosure (CVD) process is initiated. All findings are published as soon as the vulnerabilities are fixed and it is recommended to use advisories, e.g., an ICS Medical Advisory (ICSMA) and to assign Common Vulnerabilities and Exposures (CVEs) to each vulnerability or group of vulnerabilities.

After completing the project, specific statements can be made about the security level of the examined products. These project results will be published in a security review for networked medical devices on the BSI website in December 2020. Ideally, the project results will have an impact on standardization and facilitate devising technical guidelines in that field. The intention is to improve cybersecurity without finger pointing and to transparently communicate barriers everyone might face in the field of network-connected medical devices. The project aims to increase transparency and awareness with regard to medical device cybersecurity. The trustful communication and cooperation among all stakeholders throughout the project is essential to maintain and improve on cybersecurity in medical devices. There have never been any projects of this nature, neither on a national nor on an international level, which means that the results may be groundbreaking for the health care sector.

2 Management Summary

In the context of the BSI project ManiMed (Section 1), severe vulnerabilities were identified during the assessment of the DANA Diabecare RS system. In this section, the scope of the security assessment (Section 2.1), as well as multiple vulnerabilities (Section 2.2) are described. The impact of the identified vulnerabilities is depicted in Section 2.3.

2.1 Scope

The inspected components were the communication protocol of the SOOIL DANA Diabecare RS insulin pump with its AnyDANA mobile apps via Bluetooth Low Energy (BLE). The testing method was a black box penetration test without source code insight. Two insulin pumps were available for testing, voluntarily provided by the manufacturer, and publicly available documentation such as a user manual.

2.2 Results

The device's manual recommends using a weak device keypad lock PIN to easily disable the device lock (Section 4.1.2). Moreover, all pumps have a default PIN `1234` as described in Section 4.1.1. Additionally, the device PIN is disclosed without authentication via BLE (Section 4.3.4). An attacker with physical access to the pump and being in possession of the PIN can unlock a locked pump, change the pump's configuration, and administer an insulin bolus, which may lead to serious patient harm. Further, the physician PIN for gaining access to the pump's physician menu is the same for all pumps and cannot be changed without contacting the support. An attacker with access to this PIN and physical access to a pump can change the pump's configuration, such as the maximum daily insulin dose (Section 4.1.3).

Furthermore, multiple controls that were only implemented on the client side and not on the pump have been identified. The device keypad lock PIN is validated by mobile applications instead of being confirmed by the pump. An attacker can omit the check when communicating with the pump (Section 4.2).

All cryptographic keys and their key material used for the application-layer encryption of BLE messages are generated deterministically, e.g., depending on the insulin pump's hardware clock (Section 4.3.3) and transmitted via clear text BLE messages (Section 4.3.5).

Further, the authentication of the communicating party only relies on the possession of the pairing key (Section 4.3.6).

Additionally, the protocol implemented on top of BLE has no replay protection measures as described in Section 4.3.8.

2.3 Impact

The combination of the identified vulnerabilities empowers an attacker to hijack the DANA Diabecare RS insulin pump via Bluetooth Low Energy (BLE) using the sniffed pairing key which may lead to serious patient harm. To perform an attack, an attacker needs to be in proximity to the pump and sniff a single handshake between a pump and a paired mobile application. Afterward, the attacker can use all functionalities that are utilizable via BLE. This may lead to serious patient harm.

The manufacturer prepared an update for the insulin pump, thereby fixing all identified vulnerabilities. The firmware update can be applied to a Dana Diabecare RS insulin pump with the help of the respective local distributor. To temporarily reduce the risk of potential patient harm, it is recommended to disable the insulin pump's BLE functionality by putting it in airplane mode. Being in airplane mode[1], the insulin pump's therapeutic purpose can be preserved as it is optional to control the device via mobile applications. Furthermore, it must be noted that the device implements safety features such as a maximum daily dose or bolus block. These settings can only be configured on the pump and, therefore, not be circumvented by an attacker nearby.

[1] *German Federal Institute for Drugs and Medical Devices. Field Safety Notice. Dringende Sicherheitsinformation zu Insulinpumpe DANA Diabecare RS;mobilen Anwendung AnyDANA von SOOIL Development Co. Ltd. May 08, 2020. Accessed: August 05, 2020. Online: https://www.bfarm.de/SharedDocs/Kundeninfos/DE/07/2020/17203-19_kundeninfo_de.html.*

ERNW RESEARCH
pursuing knowledge.

3 Introduction

The object under Investigation in this white paper is the SOOIL DANA Diabecare RS insulin pump with its mobile apps. The following sections describe the architecture und medical purpose of the insulin pump as well as the procurement process and scope of the security assessment.

3.1 Medical Purpose

An insulin pump is an active medical device used for the administration of insulin in the treatment of diabetes mellitus (type 1 diabetes). Diabetes mellitus is an autoimmune disease and based on a lack of insulin as a result of the destruction of the insulin-producing beta cells in the Langerhans islets of the pancreas. An insulin pump is a less invasive alternative to multiple daily injections of insulin and allows for flexible insulin therapy. The Continuous Subcutaneous Insulin Infusion (CSII) therapy with insulin pumps aims to enable automated and on-demand delivery of insulin via thin tubings subcutaneously without the need for injections. According to the the German Diabetes Association (DDG) publication *German health report - Diabetes 2020*[2], estimated 32,000 children and adolescents and 340,000 adults with type 1 diabetes live in Germany. It is estimated that about 45,000 people in Germany use an insulin pump, but no reliable sources for this number exist.

3.2 Architecture

The DANA Diabecare RS insulin pump is the central component of the therapy system and can be controlled with an application for the mobile operating systems Android and iOS via a Bluetooth Low Energy (BLE) interface. The interface also allows the transfer of therapy data to a PC software called DANA Monitor. The manufacturer intends neither the use of remote control nor the use of a Continuous Glucose Monitor (CGM) device to build a closed-loop system.

A closed-loop system combines the sensor data from a CGM with individual diabetes management properties such as basal rate and insulin sensitivity factor. Some central unit calculates treatment suggestions and administers small insulin boluses to keep the blood glucose within the target range using an insulin pump. The aim is to keep blood sugar levels within healthy limits by using automated insulin dosing, building an Artificial Pancreas System (APS). At the moment, no commercial APS system is available but patient-driven open-source mobile application projects such as OpenAPS[3] and AndroidAPS[4] exist. Especially, AndroidAPS features the use of the DANA Diabecare RS insulin pump for an APS[5].

[2] *Deutsche Diabetes Gesellschaft. Deutscher Gesundheitsbericht Diabetes 2020. Accessed: August 05, 2020. Online: https://www.deutsche-diabetes-gesellschaft.de/fileadmin/user_upload/06_Gesundheitspolitik/03_Veroeffentlichungen/05_Gesundheitsbericht/2020_Gesundheitsbericht_2020.pdf.*

[3] *https://openaps.org/. Archived: January 5, 2020*

[4] *https://androidaps.readthedocs.io/en/latest/EN/. Archived: January 5, 2020*

[5] *https://androidaps.readthedocs.io/en/latest/EN/Getting-Started/ClosedLoop.html. Archived: January 5, 2020*

3.3 Procurement Process

Insulin pumps and their accessories are listed as application aids in the aid register of the German Statutory Health Insurance (GKV) and therefore are to be regarded as prescribable at the expense of the GKV. An examination of the requirements for the cost reimbursement by the GKV is conducted, including the so-called Medical Service of German Statutory Health Insurance providers (MDK). In the legal mandate, the MDK supports the GKV and statutory nursing insurance in medical and nursing questions. Correspondingly, insulin pumps are not publicly sold in Germany without a doctor's prescription and approval by the MDK supporting the health insurers.

4 Technical Analysis

In this section, the technical analysis of the insulin pump is presented. First, some vulnerabilities concerning the use or recommendation of weak PINs and client-side controls in the mobile applications are described (Sections 4.1 and 4.2). Second, the vulnerabilities in the communication protocol are elucidated (Section 4.3).

4.1 Weak PINs

The following three sections describe vulnerabilities concerning the use or recommendation of weak PINs.

4.1.1 Vulnerability: Weak Default Device Keypad Lock PIN

All pumps have the default PIN `1234` as shown in the device instructions for use (IFU)[6]. The PIN is needed to unlock a device that has been locked by the user, for the derivation of key material for BLE messages and user authentication with mobile applications. An attacker with physical access to an insulin pump with the default PIN may administer an insulin bolus or change other insulin pump configurations. Changing the PIN is only enforced when an official AnyDANA mobile application is used as described in the client-side controls finding in Section 4.2.

4.1.2 Vulnerability: Recommending Weak Device Keypad Lock PINs

The pump's instructions for use (IFU)[6] recommends to use device PINs near `0000` such as `1000` to easily disable the device lock. The Instructions for Use (IFU) says that the PIN `0000` can be used to unlock the device easily. The PIN is needed to unlock a device that has been locked by the user, for the derivation of key material for BLE messages and user authentication with mobile applications. It also states that using `0000` simplifies the unlocking procedure as only the `OK` button needs to be pressed. An attacker may brute-force the PIN much faster, trying the easily guessable PINs first.

An attacker with physical access to an insulin pump with a weak PIN may administer an insulin bolus or change other insulin pump configurations.

4.1.3 Vulnerability: Default Physician PIN

The physician PIN for gaining access to the pump's physician menu is the same for all pumps and cannot be changed without contacting the support. An attacker with access to this PIN and physical access to the pump can change the pump's configuration, such as the maximum daily insulin dose, which may lead to patient harm. The pump's physician manual[7] states that the PIN `3022` is the insulin pump's physician menu PIN and that it is possible to change the PIN.

[6] *https://www.ime-dc.de/sites/default/files/p_506_400_en_xx_01_01_en_01_x_web.pdf, archived: January 5, 2020*
[7] *https://www.ime-dc.de/sites/default/files/p_506_401_de_xx_01_02_de_00_x_web.pdf, archived: January 5, 2020*

4.2 Client-Side Controls

The device keypad lock PIN is validated by the mobile application instead of being confirmed by the pump.

4.2.1 Client-Side Keypad Lock PIN Validation

During the handshake via BLE with a pump, mobile applications ask users for the correct device keypad lock PIN, although the pump does not require this PIN to establish a connection. As this check is performed on the client-side, an attacker may omit it when communicating with the pump. Furthermore, the client-side check implies the disclosure of the PIN as described in Section 4.3.4.

4.2.2 Denying access with PIN 1234

The following screenshot of the AnyDANA iOS App shows that the application denies the connection to the insulin pump when the pump is configured with the PIN `1234`.

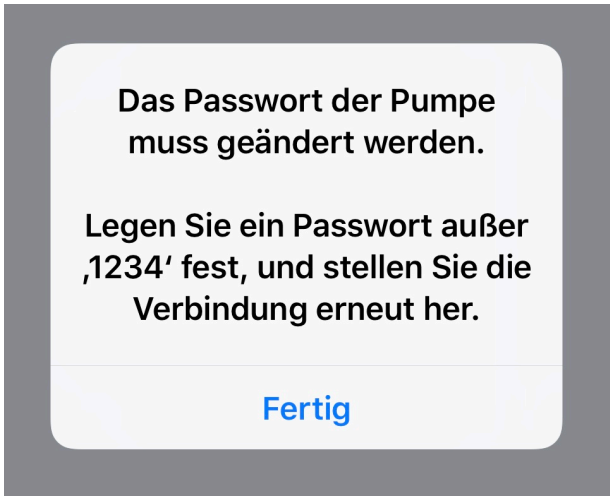

Figure 3: The AnyDANA iOS App refuses to connect to a pump with the PIN 1234.

The following communication sequence proves that an attacker can communicate with an insulin pump with the keypad lock PIN `1234`. This proves that the check for the PIN is performed in the mobile application and not on the pump itself.

```
[*] Device [Name=<redacted> BD=<redacted>]
[DEBUG] Connected to Device.
[*] 0x0100
[DEBUG] C >>: 0100<SERIAL-REDACTED>
[DEBUG] C <<: 02004F4B
[*] 0x01D1
[DEBUG] C >>: 01D1
[DEBUG] C <<: 02D100
[*] 0x0101
[DEBUG] C >>: 0101
[DEBUG] C <<: 02D20E42
[+] P_Key: 0E42
[DEBUG] C <<: 020113081B0E2702B31F
[+] PIN: 0x1234
[+] S_Key: 0x2b
```

Listing 1: The script output proves that an attacker can communicate with an insulin pump with the keypad lock PIN 1234.

4.3 Weak Communication Protocol

This section describes the application-layer communication protocol of the DANA Diabecare RS system.

4.3.1 Application-Layer Pairing

The following diagram shows that three keys are used during the application-layer pairing of a DANA Diabecare RS insulin pump and the respective mobile applications, the `D_KEY` (3 bytes), a pairing key `P_KEY` (2 bytes) and a session key `S_KEY` (1 byte). These keys will be described in the Sections 4.3.3.1, 4.3.3.2 and 4.3.3.3.

Every communication attempt, starts with the signaling bytes `\x01\x00` followed by the insulin pump's serial number (character-wise converted to hex) as shown in Figure 4. The pump's response indicates that the serial number is matching.

The second message initiated by the mobile application (`\x01\xD1`) requests the pairing. This is confirmed by the insulin pump with the response `\x02\xD1\x00`.

After this, the user needs to manually confirm the pairing request shown on the pump's display. With this confirmation, a `\x02\xD2\x38\x37` message is sent to the mobile application where the two additional bytes after the signaling bytes represent the pairing key (`P_KEY`).

Subsequently, the third request (`\x01\x01`) requests a session key (`S_KEY`) that changes with every new BLE connection between the insulin pump and mobile applications.

With all three keys, the mobile application can initiate higher-privileged requests.

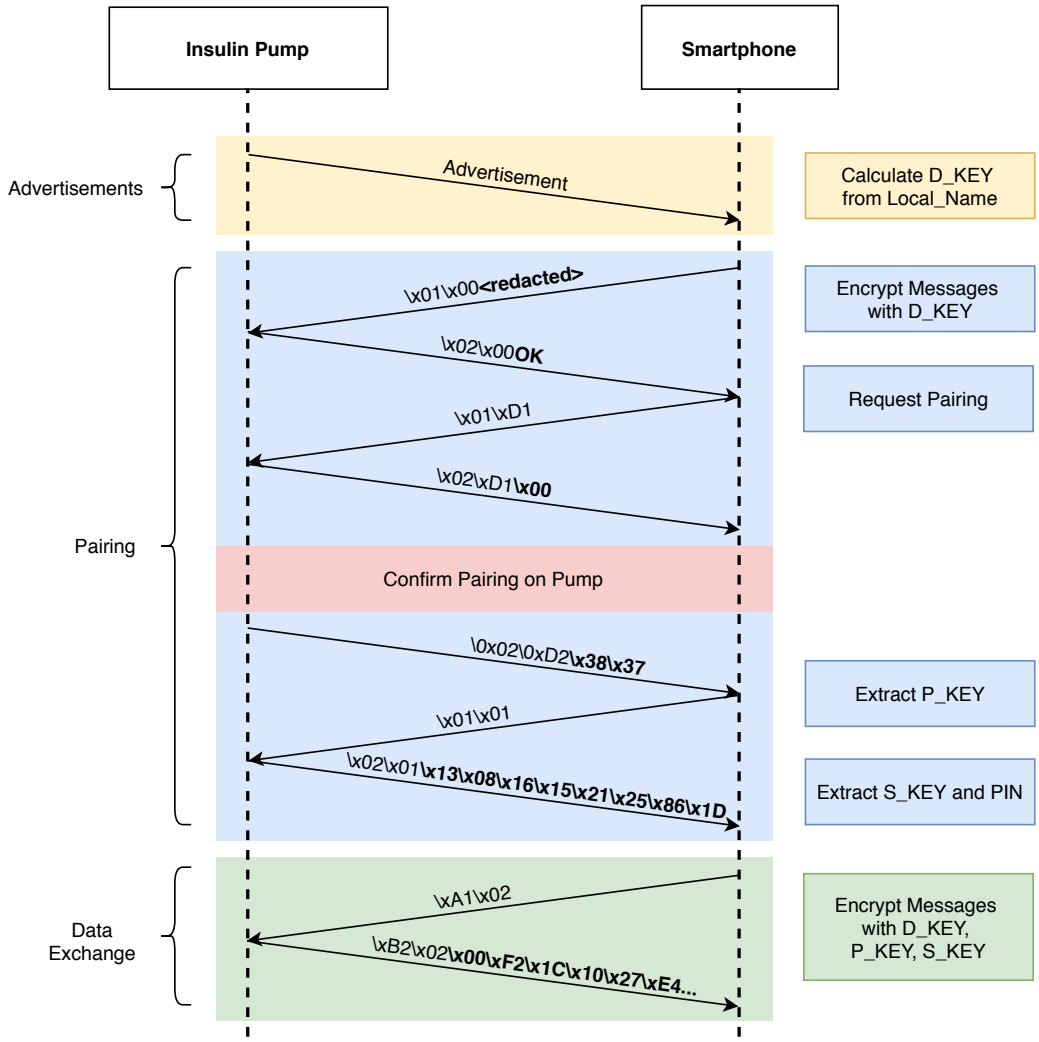

Figure 4: Pairing of a DANA Diabecare RS insulin pump and the respective mobile application.

4.3.2 Paired Communication

The following Figure 5 shows the communication between the insulin pump and mobile applications after the application-layer pairing.

After an initial pairing and exchange of the `P_KEY`, no new pairing needs to be performed between the insulin pump and mobile applications. Instead, the `P_KEY` is transmitted after the initial `\x01\x00` message appended to `\x01\xD0` signaling bytes. Afterward, the session key `S_KEY` is requested to finish the handshake and to be able to exchange higher-privileged messages.

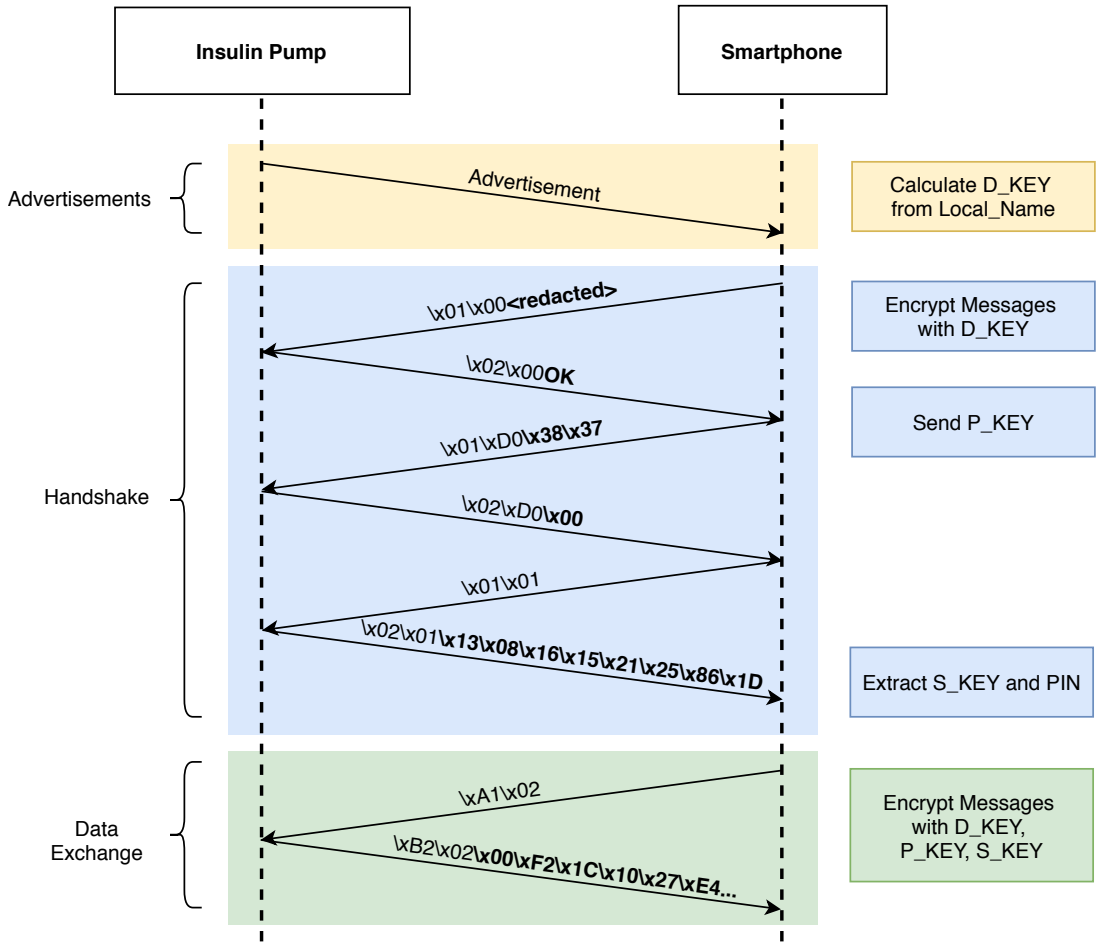

Figure 5: Handshake between the DANA Diabecare RS insulin pump and the respective mobile application.

4.3.3 Vulnerability: Weak Generation of Encryption Keys

As described in the Sections 4.3.1 and 4.3.2, all keys used to encrypt the BLE messages are generated deterministically dependent on the insulin pump's hardware clock, keypad lock PIN and serial number.

An attacker may brute-force the keys knowing the formulas to calculate them to limit the brute-force space and therefore does not need to try all of `2^24` combinations (we omitted the `D_KEY` in this calculation for reasons presented in Section 4.3.3.1).

An attacker in possession of these keys can eavesdrop the exchanged high-privileged messages, change the pump's configuration as well as administer an insulin bolus, which may lead to serious patient harm.

4.3.3.1 Device Key (D_KEY)

The device key has a length of three bytes derived from the serial number of the insulin pump. This key will never change as the calculation does not contain any randomizing element. The device serial number can be obtained from the BLE advertisements of the insulin pump.

4.3.3.2 Session Key (S_KEY)

The session key `S_KEY` is dependent on the device keypad lock PIN, which is chosen by patients and combined with the pump's time. This is the only key that changes between different connections to the device the `P_KEY` is fixed after pairing and as the `D_KEY` is fixed for every device.

The `S_KEY` is valid until the session is terminated. The session will be terminated either by the device after no messages are received within a dedicated time or with a connection termination message by the client.

The fact that the `S_KEY` is calculated from the pump's time also implies that `S_KEY` values can be calculated as an attacker can request the pump's time and keypad lock PIN without authentication being in close proximity. Also, an attacker can extract the information needed to calculate the `S_KEY` from session handshakes sniffed.

4.3.3.3 Pairing Key (P_KEY)

The following Listing 2 shows that the pairing key is dependent on the insulin pump's time as the same keys are obtained when pairing multiple times within a second.

```
[*] Device [Name=<redacted> BD=<redacted>]
[+] P_Key: 424B
2019-08-26 15:50:56.025675
[+] P_Key: 424B
2019-08-26 15:50:56.378260
[+] P_Key: 424B
2019-08-26 15:50:56.727121
```

Listing 2: Script output showing that the pairing key is dependent on the insulin pump's time.

4.3.4 Vulnerability: Unauthenticated Device Keypad Lock PIN Disclosure

The device keypad lock PIN is transmitted without establishing a privileged connection via BLE. An attacker with physical access to the insulin pump and in possession of the PIN can unlock a locked pump, change the pump's configuration, and administer an insulin bolus, which may lead to serious patient harm.

The following communication sequence shows that an attacker can retrieve information that can be used to calculate the device keypad lock PIN by only knowing the `D_KEY` to encode messages.

The message `\x01\x01` is intended to be sent after a successful pairing request or after the pairing key has been provided to exchange the `S_KEY` (see Section 4.3.2). An attacker can omit these pairing requests.

```
[*] Device [Name=<redacted> BD=<redacted>]
[*] Request 0x0100
[DEBUG] C >>: 0100<SERIAL-REDACTED>
[DEBUG] C <<: 02004F4B
[*] Request 0x0101
[DEBUG] C >>: 0101
[DEBUG] C <<: 020113081B0D2214861D
[+] PIN: 0x1001
```

Listing 3: An attacker can request the pump's time without authentication and calculate the device keypad lock PIN by only knowing the `D_KEY` to encode messages.

The decoded response to the `\x01\x01` request is marked in red and has a length of 9 bytes. The insulin pump's keypad lock PIN can be calculated from the bytes and a magic number.

4.3.5 Vulnerability: Insecure Transmission of Cryptographic Keys

All key material and the cryptographic keys themselves used to encrypt or decrypt messages are transmitted in clear-text. An attacker with basic BLE sniffing hardware can eavesdrop the BLE communication and extract all keys or the information needed to calculate the keys. An attacker in possession of these keys can decrypt exchanged high-privileged messages and send requests to change the pump's configuration and administer an insulin bolus, which may lead to serious patient harm.

Having the three keys, an attacker can decode all exchanged high-privileged messages between the insulin pump and the mobile application.

Furthermore, an attacker can brute-force the `S_KEY` for other sniffed communication excerpts, where the handshake is missing. An attacker does not need to check all 256 possible keys as the `S_KEY` depends on the pump's time, as described in Section 4.3.3.2.

4.3.6 Vulnerability: Weak Authentication Mechanism

The authentication of the communicating party relies on the possession of the `P_KEY`, only. This key can be calculated from information transferred in unencrypted BLE messages, as described in Section 4.3.5. An attacker in possession of this key can eavesdrop the exchanged messages and change the pump's configuration as well as administer an insulin bolus, which may lead to serious patient harm.

4.3.7 Vulnerability: Spoofing the Pump's Identity

There is no active verification of the pump's identity. Mobile applications connect to the insulin pump based on the `Local_Name` advertised via BLE. An attacker sending respective advertisement messages can spoof the pump or perform Man-in-the-Middle (MitM) attacks on the communication system. An attacker in this position can eavesdrop the exchanged messages and change the pump's configuration as well as administer an insulin bolus, which may lead to serious patient harm.

4.3.8 Vulnerability: Missing Replay Protection

The protocol implemented on top of BLE has no replay protection measures. An attacker hijacking a BLE session between an application and the pump or in a MitM position can replay messages. An attacker that replays a sensitive message such as administering an insulin bolus may cause serious patient harm.

5 Mitigations and Retest Results

This section elucidates the recommended mitigations after the test. With the results of the retest, in brief, the measures taken by the manufacturer are described.

5.1 Weak PINs

The following section describes the recommended and taken measures concerning the findings in Section 4.1. SOOIL clarified that the purpose of the PIN is to prevent erroneous operation of the keypad and cannot be seen as an authorization mechanism. The pump is 24/7 close to the patient's body and, therefore, not easily physically accessible by an attacker.

5.1.1 Recommendation of using weak Device Keypad Lock PINs

It is recommended to remove the recommendation of using weak device PINs (Section 4.1.2) from the IFU. Instead, a recommendation of using strong PINs should be added.

SOOIL removes the recommendation from the IFU and will release an updated version.

5.1.2 Weak Default Device Keypad Lock PIN

It is recommended to enforce the change of the keypad lock PIN during the first use of the pump (Section 4.1.1). The insulin pump must enforce this measure.

The retest showed that the default keypad lock PIN 1234 was replaced with a device-specific PIN.

5.1.3 Default Physician PIN

It is recommended to set this PIN to a secure default by generating it randomly for each pump. As an alternative, a change functionality for the physician PIN without contacting the support may be implemented. This empowers to enforce a change of the physician PIN with the initial configuration of the pump.

The retest showed that the default physician PIN 3022 was removed.

5.2 Client-Side Controls

It is recommended to enforce the PIN verification on the pump or to remove the client-side check.

The retest of an updated firmware showed that the PIN dialog was removed in favor of a password dialog that utilizes a secret, which itself is stored and kept on the mobile device.

5.3 Weak Communication Protocol

The communication protocol has multiple vulnerabilities, as described in Section 4.3. In this section, the recommended mitigations and measures taken by the manufacturer, as well as complicating factors, are presented.

5.3.1 Vulnerability: Weak Generation of Encryption Keys

A cryptographically secure pseudorandom number generator should be used for generating keys. Since the pairing of a device will not occur frequently, it is feasible to use more calculating power for generating a secure, shared secret. Additionally, the BLE pairing and bonding mechanisms are recommended to be used to communicate via a secure channel. These mechanisms include the verification of the identity of the communicating party on the BLE protocol-level. Furthermore, using the BLE mechanisms may dispense the need for application-layer encryption.

The retest of an updated firmware revealed that no BLE mechanism is used. SOOIL states that the device does only support BLE 4.1 and that all recommended mechanisms require BLE 4.2. Therefore, the protocol was changed to require shared secrets that are generated on every pairing request. It is unclear how these secrets are generated and if they are cryptographically secure.

5.3.2 Vulnerability: Unauthenticated Device Keypad Lock PIN Disclosure

The device keypad lock PIN should neither leave the pump nor being transmitted via BLE. It is recommended to change the design of the communication protocol as the PIN is needed for client-side checks in the mobile application and to calculate the session key `S_KEY`.

The retest of an updated firmware showed that the protocol was changed to require shared secrets that are generated on every pairing request. The PIN is not transmitted via BLE anymore.

5.3.3 Vulnerability: Insecure Transmission of Cryptographic Keys

For the transmission of cryptographic keys, it is recommended to use established and security protocols and algorithms. All keys that are exchanged via insecure channels, as well as all the data encrypted with these keys, need to be seen as compromised and must not be trusted. The BLE pairing and bonding mechanisms are recommended to be used to communicate via a secure channel.

The retest of an updated firmware showed that no secure BLE pairing mechanism is used. The changed protocol requires two secrets that are displayed on the pump's screen. Users pairing the pump with a mobile application enter these secrets in the mobile app manually. The taken measure hinders an attacker from sniffing the keys, which renders the attack presented in Section 4.3.6 unpractical.

5.3.4 Vulnerability: Weak Authentication Mechanism

The BLE pairing and bonding mechanisms are recommended to be used to communicate via a secure channel. These pairing mechanisms include the verification of the identity of the communicating party on the communication protocol level.

The retest of an updated firmware revealed that no secure BLE pairing or bonding mechanism is used. The protocol was changed to require shared secrets that are generated on every pairing request. It could be determined that the secrets are not transmitted via insecure channels or calculated depending on any transmitted values.

5.3.5 Vulnerability: Spoofing the Pump's Identity

The BLE pairing and bonding mechanisms are recommended to be used to communicate via an encrypted channel. These pairing mechanisms include the verification of the identity of the communicating party on the communication protocol level.

The retest of an updated firmware revealed that no secure BLE pairing or bonding mechanism is used. It was determined that the identity of the pump is not authenticated explicitly other than being able to communicate with the exchanged secrets. An attacker spoofing the pump still requires to know the secrets. As long as these secrets cannot be obtained through exchanged messages or brute-forced, this finding can be seen as fixed.

5.3.6 Vulnerability: Missing Replay Protection

An attacker needs to sniff valid packages before being able to replay them. The design of the custom communication protocol needs to be changed to add application-layer replay protection. The BLE pairing and bonding mechanisms are recommended to be used to communicate via a secure channel that offers replay protection.

The retest of an updated firmware revealed that no secure BLE mechanism is used. The protocol was changed to require shared secrets generated on every pairing request and never transmitted via BLE. It could be determined that the secrets are not transmitted via insecure channels or calculated depending on any transmitted values. These secrets are used to encrypt the previously encrypted messages with an additional application-layer encryption scheme. Furthermore, the transmissions are protected by a random sync key and therefore replay protected.

5.4 Summary

The following Table 1 lists all vulnerabilities identified during the initial security assessment of the SOOIL DANA Diabecare RS communication system as well as the assessment of their status (i.e. *fixed* or *more information needed*).

Section	Finding	Status
4.1.1	Weak Default Device Keypad Lock PIN	Fixed
4.1.2	Recommending Weak Device Keypad Lock PINs	Fixed
4.1.3	Default Physician PIN	Fixed
4.2	Client-Side Controls	Fixed
4.3.3	Weak Generation of Encryption Keys	Fixed
4.3.4	Unauthenticated Device Keypad Lock PIN Disclosure	Fixed
4.3.5	Insecure Transmission of Cryptographic Keys	Fixed
4.3.6	Weak Authentication Mechanism	Fixed
4.3.7	Spoofing the Pump's Identity	Fixed
4.3.8	Missing Replay Protection	Fixed

Table 1: Retest Results

ERNW RESEARCH pursuing knowledge.

6 Disclosure

This section deals with the disclosure of the vulnerabilities to the manufacturer.

6.1 Involved Parties

Involved parties are ERNW Research GmbH (hereinafter called *ERNW*) in their role as security researchers performing the security assessment on behalf of the BSI. Furthermore, the German Federal Office for Information Security (BSI) is involved in the role of the ManiMed project initiator and owner of the assessment's results as well as SOOIL Developments Co., Ltd (hereinafter called *SOOIL*) in the role of the manufacturer of the medical device.

6.2 Limitations

The disclosure was managed by the ManiMed project team of the BSI and involved ERNW staff in a consultative capacity. As described in Section 1, the ManiMed project strives to identify vulnerabilities in medical devices for sustainable strengthening of consumer protection and patient safety. Therefore, a detailed disclosure of the results of the security assessment may only be performed if the publication of this information does not pose serious risks or harm to patients. Thus, a responsible disclosure process was chosen. A publication of this report does not pose serious risks or harm to patients as short-term measures or workarounds exist as described in Section 2.3.

6.3 Acknowledgment

The vulnerabilities shall be acknowledged to the following people:

- Julian Suleder, ERNW Research GmbH
- Birk Kauer, ERNW Research GmbH
- Nils Emmerich, ERNW Research GmbH
- Raphael Pavlidis, ERNW Research GmbH

6.4 Disclosure Timeline

The following table contains all important dates and events concerning the disclosure.

Date	Description
August 30, 2019	The BSI contacts SOOIL to inform about the vulnerabilities
October 22, 2019	SOOIL announces to ship an updated version of the insulin pump to Germany
November 2019	ERNW receives an updated insulin pump and performs a retest
January 2020	SOOIL provides source code of the updated Android application for a retest
March 3, 2020	The manufacturer's Field Safety Notice (FSN) is published by BfArM
April 2020	The firmware update is rolled out to first patients in Europe
May 8, 2020	Field Safety Corrective Action (FSCA) publicly announced by BfArM
September 2020	Public Disclosure of the vulnerabilities

Table 2: Disclosure Timeline