A Million Boluses: Discovery and Disclosure of Vulnerabilities in an Insulin Pump

Julian Suleder, Dr. Dina Truxius

About Us

- Julian Suleder
  - Security Analyst & Researcher
  - ERNW Research GmbH
  - jsuleder@ernw.de
  - Twitter: @jsuleder
- Dr. Dina C. Truxius
  - Section DI 24 - Cyber Security in the Public Health and Financial Services Sectors
  - Federal Office for Information Security (BSI)
  - dina.truxius@bsi.bund.de

Agenda

- Medical Device Security
- Testing Setup
- Technical Analysis
  - Communication Protocol
  - Vulnerabilities
- Impact & Temporary Measures
- Disclosure

ERNW RESEARCH
pursuing knowledge.

Disclaimer

- This talk focuses on security vulnerabilities identified in the DANA Diabecare RS insulin pump.
- The exemplifying vulnerabilities affected the pump's proprietary, Bluetooth Low Energy (BLE)-based communication and affected patient safety.
- Opinions expressed belong solely to the authors and not necessarily to the authors' employers or organizations.
- We want to thank SOOIL for participating in the project.

ERNW
providing security.

Part I: Medical Device Security

- What is a Medical Device?
- The Environment – Medical Devices
- The State of IT Security in Germany 2019
- Project ManiMed

ERNW RESEARCH
pursuing knowledge.

Medical Device Classification

- In the European Economic Area directives and legal regulations classify medical products
  - Depending on their use (primarily)
  - Possible harms to patients (secondary)
- Depending on the classification vendors must:
  - Implement processes for quality/risk management, SDL and usability for products including software
  - Get a needed certification

ERNW RESEARCH
pursuing knowledge.

Applies to the EU!

What is a medical device?

- Basically everything 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

See: Council Directive 93/42/EEC of 14 June 1993 concerning medical devices

ERNW RESEARCH
pursuing knowledge.

The Environment – Medical Devices

- Not stationary
- Expensive → Lifetime++
- Use Proprietary data exchange formats
- Various audiences with individual backgrounds, expectations and needs
- Disrupt IT management processes
- Operations is key: Essential for a patient's life

Photo by Jair Lázaro on Unsplash

The State of IT Security in Germany 2019

- The increasing degree of networking and distribution, coupled with society's rising acceptance of mobile applications, is now associated with an elevated level of risk of cyber attacks
  - More smart products in the health sector
  - Range of medical applications covered by mobile solutions is rising
  - Many applications are already classified as medical devices
  - Cybersecurity is often not given any particular priority
- New legislation, Medical Device Regulation (MDR): Medical devices will be required to have certain cyber security properties
- Operation is key: Medical functionality vs. security

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7, July 28, 2020]

ERNW RESEARCH
pursuing knowledge.

Federal Office for Information Security

Project ManiMed - Manipulation of Medical Devices

- Initiated by the German Federal Institute for Information Security (BSI)
- The project aims to:
  - Carry out a security analysis of selected products by security assessments
  - Assess the current state: No finger-pointing
  - Increase awareness, communicate transparently, facilitate a trustful communication and cooperation between manufacturers, security researchers, and authorities
  - Illustrate questions medical device vendors are facing by making devices smart

ManiMed: Finalization

- A final report for the German population will be prepared and published in German and English
- Purpose:
  - Establish active cooperation and collaboration between all stakeholders
  - Increase awareness, communicate transparently, enhance/built/keep trust, get a “feeling” for vulnerabilities
- Contents:
  - Abstract description of the different device categories and vulnerabilities
  - Lessons learned and current state of disclosure processes
  - Manufactures can decide on naming their product
    - Show their cooperation and lessons learned
    - No finger-pointing

ERNW RESEARCH pursuing knowledge.

ManiMed: Product Categories

Federal Office for Information Security

- Implantable Pacemakers, Programmers, Home Monitoring Units
- Insulin Pumps
- Ventilators and Anesthesia Devices
- Infusion and Syringe Pumps
- Patient monitors

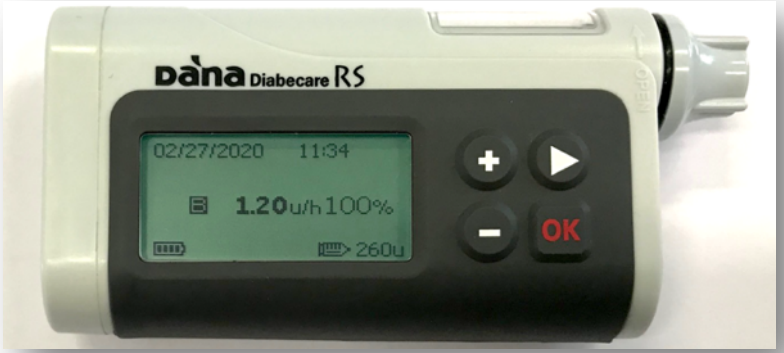
ERNW
providing security.

Part II: Testing Setup

- The Medical Device: Intended Use
- Where do I get Medical Devices?
- Security Assessment Methodology

The Medical Device

- Intended use by the manufacturer:
  - The insulin pump is the central component of the therapy system
  - Can be controlled with Android and iOS apps via BLE
- Other uses:
  - Artificial Pancreas System (APS)
  - #WeAreNotWaiting
  - There are mobile applications compatible with this pump on GitHub
  - Patients need to build the system for themselves



SOOIL DANA Diabecare RS insulin pump

Where do I get medical devices?

- Insulin pumps and their accessories are listed as application aids in the aid register of the German Statutory Health Insurance (GKV)
  - Regarded as prescriptible at the expense of the GKV
  - Insulin pumps are not publicly sold in Germany
  - The manufacturer provided us with two insulin pumps ☺

- Other common procurement problems:
  - Direct sales:
    - Vendors do not provide private persons with medical devices
    - Public tenders → Heterogeneous environmental requirements
  - Lab setup requires complex medical information systems
  - Do not perform device assessments in production!

Methods: Security Assessment

- Highly specialized and individual in the device's medical use case, interfaces, technologies, and assumptions to its environment
- Scope:
  - Proprietary Communication Protocol on top of Bluetooth Low Energy (BLE)
  - Assessment Modules: Cryptography, Authentication & Pairing Process
- Methodology:
  - Black-box approach without source code insight
  - Reverse Engineering of the communication protocol using the manufacturer's Android and iOS applications as well as communication captures

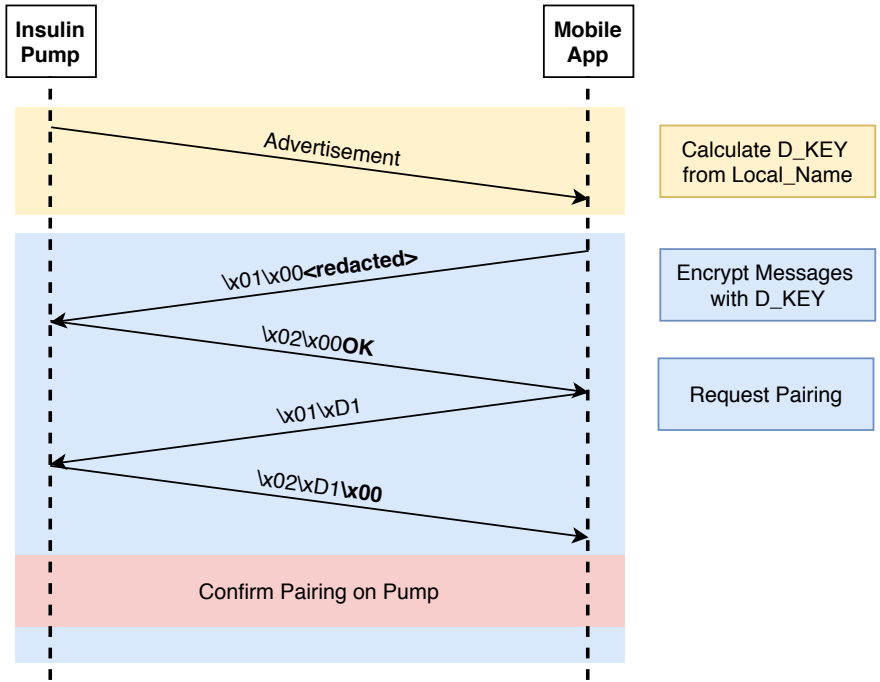
ERNW
providing security.

Part III: Technical Analysis

- Communication Protocol
  - Pairing Process
  - Authentication Process

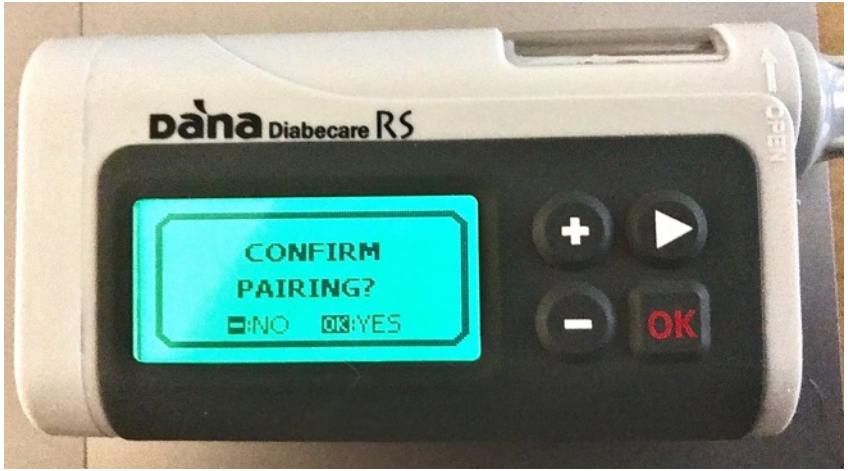
Application-Layer Pairing

- Every communication starts with the signaling bytes `\x01\x00` followed by the insulin pump's serial number
- 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



Application-Layer Pairing

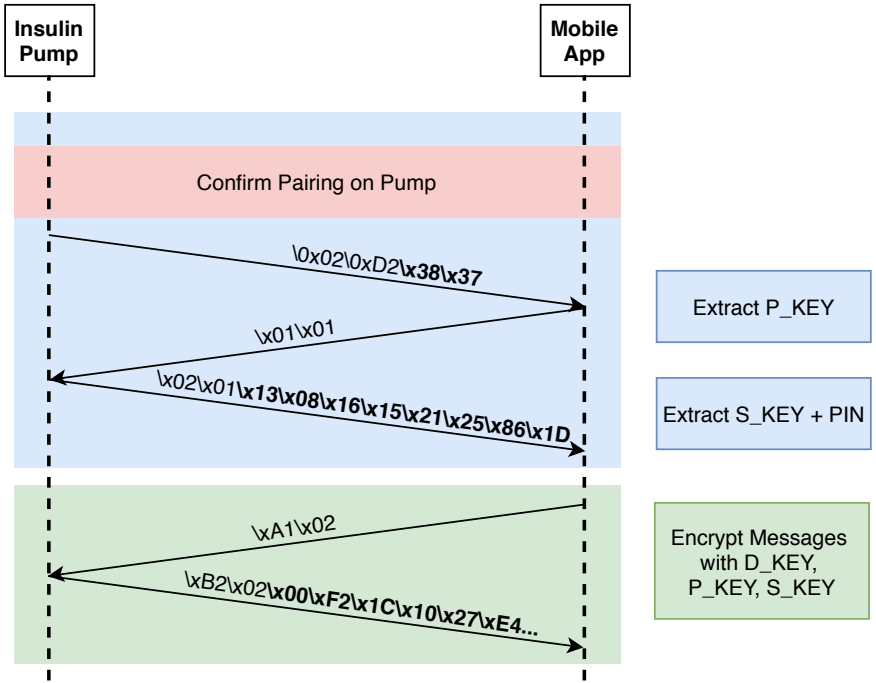
- Every communication starts with the signaling bytes `\x01\x00` followed by the insulin pump's serial number
- The pump's response indicates that the serial number is matching
- The second message initiated by the mobile application (`\x01\xD1`) requests the pairing
- This is confirmed by the insulin pump with the response `\x02\xD1\x00`
- After this, the user needs to manually confirm the pairing request shown on the pump's display



Pairing Prompt

Application-Layer Pairing

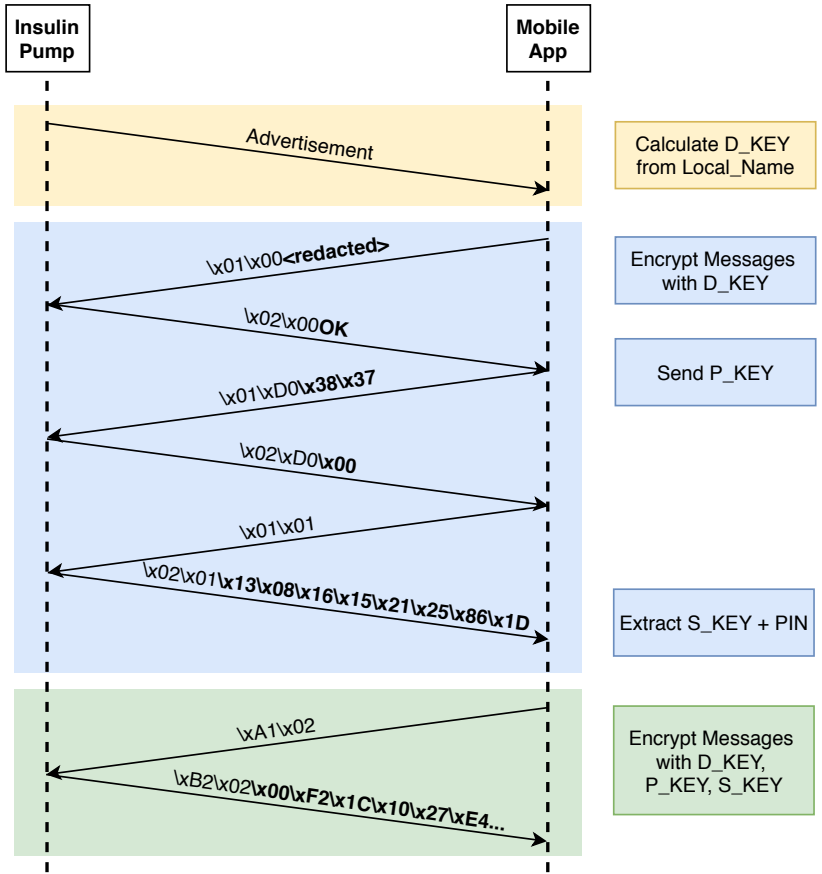
- With the manual confirmation, a `\x02\xD2`**`\x38\x37`** message is sent to the mobile application
- The two bytes after the signaling bytes represent the pairing key (`P_KEY`)
- `\x01\x01` requests a session key (`S_KEY`)
- With all three keys:
  → Initiate higher-privileged requests



ERNW RESEARCH
pursuing knowledge.

Paired Communication

- After the pairing and exchange of the pairing key:
- The `P_KEY` is appended to `\x01\xD0` signaling bytes → `\x01\xD0`**`\x38\x37`**
- The session key (`S_KEY`) is requested to finish the handshake



ERNW
providing security.

Part IV: Technical Analysis

- Vulnerabilities

ERNW RESEARCH pursuing knowledge.

Weak PINs

- Default Device Keypad Lock PIN: `1234`
- Recommending Weak Device Keypad Lock PINs:
- Use device PINs near `0000` such as `1000` to easily disable the device lock
- „The PIN `0000` can be used to unlock the device easily“
- Default Physician Menu PIN: `3022`
- Manufacturer: The PINs’ Purpose is to prevent erroneous operation of the keypad
- An attacker needs physical access

ERNW RESEARCH
pursuing knowledge.

Client-Side Controls

- Mobile applications ask users for the keypad lock PIN
  - The pump does not require this PIN to establish a connection
  - The client-side check implies the disclosure of the PIN
  - An attacker can omit the check when communicating with the pump
- The AnyDANA application denies the connection to the insulin pump when the pump is configured with the PIN `1234`

Keypad Lock PIN Disclosure

- The PIN is transmitted without establishing a privileged connection via BLE
- The request is intended to be sent after successful pairing or after the pairing key has been provided
- An attacker can calculate the device keypad lock PIN with a magic number

→ Extract the keypad lock PIN

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

Weak Generation of Encryption Keys

- Device Key (`D_KEY`)
  - Derived from the pump‘s serial number
  - Calculation does not contain any randomizing element
  - The device serial number can be obtained from the BLE advertisements
  - → Key will never change
- Session Key (`S_KEY`)
  - Derived from the device keypad lock PIN and the pump’s time
  - → Attackers can extract information needed to calculate the S_KEY from captures

ERNW RESEARCH
pursuing knowledge.

Weak Generation of Encryption Keys

- Pairing Key (`P_KEY`)
  - Derived from the insulin pump's time
  - Calculation does not contain any randomizing element
  - → Attackers can extract the key and hijack the pump

```
[*] Device [Name=<red> BD=<red>]
[+] 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 15:50:56.741305
```

ERNW RESEARCH pursuing knowledge.

Further Vulnerabilities

- Spoofing the Pump's Identity
  - No active verification of the pump's identity

  → An attacker sending BLE advertisement messages may spoof the pump and perform Man-in-the-Middle (MitM) attacks on the communication system
- Missing Replay Protection
  - The protocol has no replay protection measures

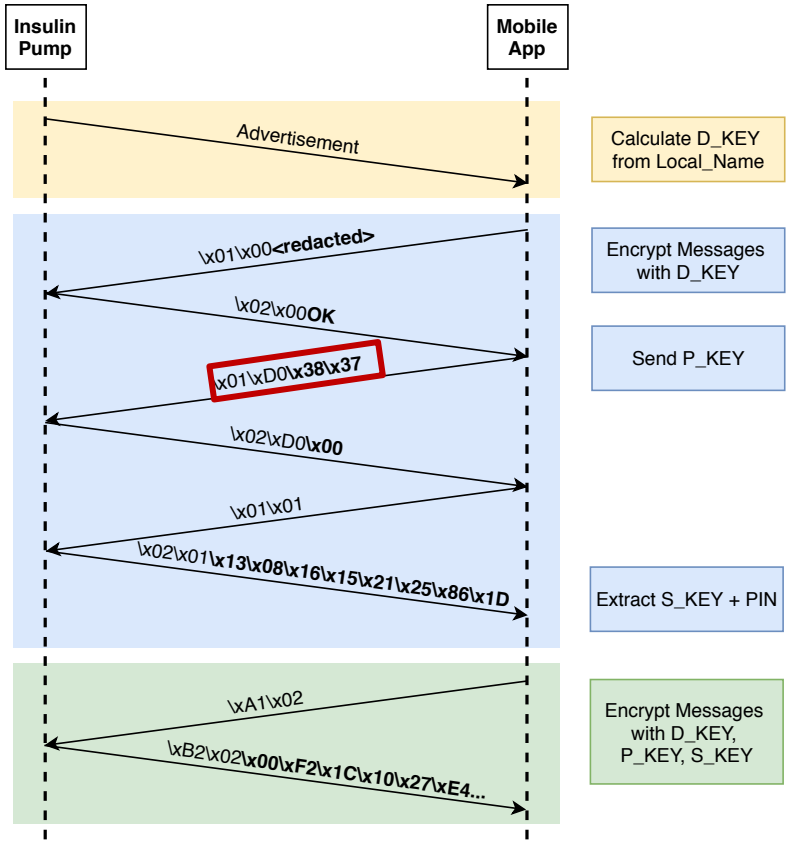
  → An attacker hijacking a BLE session between an application and the pump or in a MitM position may be able to replay messages
- Insecure Transmission of Cryptographic Keys
  - All key material and the cryptographic keys are transmitted in clear text

  → An attacker can eavesdrop the BLE communication and extract all keys

ERNW RESEARCH pursuing knowledge.

Weak Authentication Mechanism

- The authentication mechanism relies on the possession of the `P_KEY`
- The `P_KEY` key can be extracted from captured BLE messages
- An attacker sniffing a single communication between a pump and a paired mobile application can extract the `P_KEY` and hijack the pump
- → May lead to patient harm



ERNW
providing security.

Part V: Impact & Temporary Measures

- Impact
- Demo: Hijacking the Pump
- Remediation & Temporary Measures

ERNW RESEARCH pursuing knowledge.

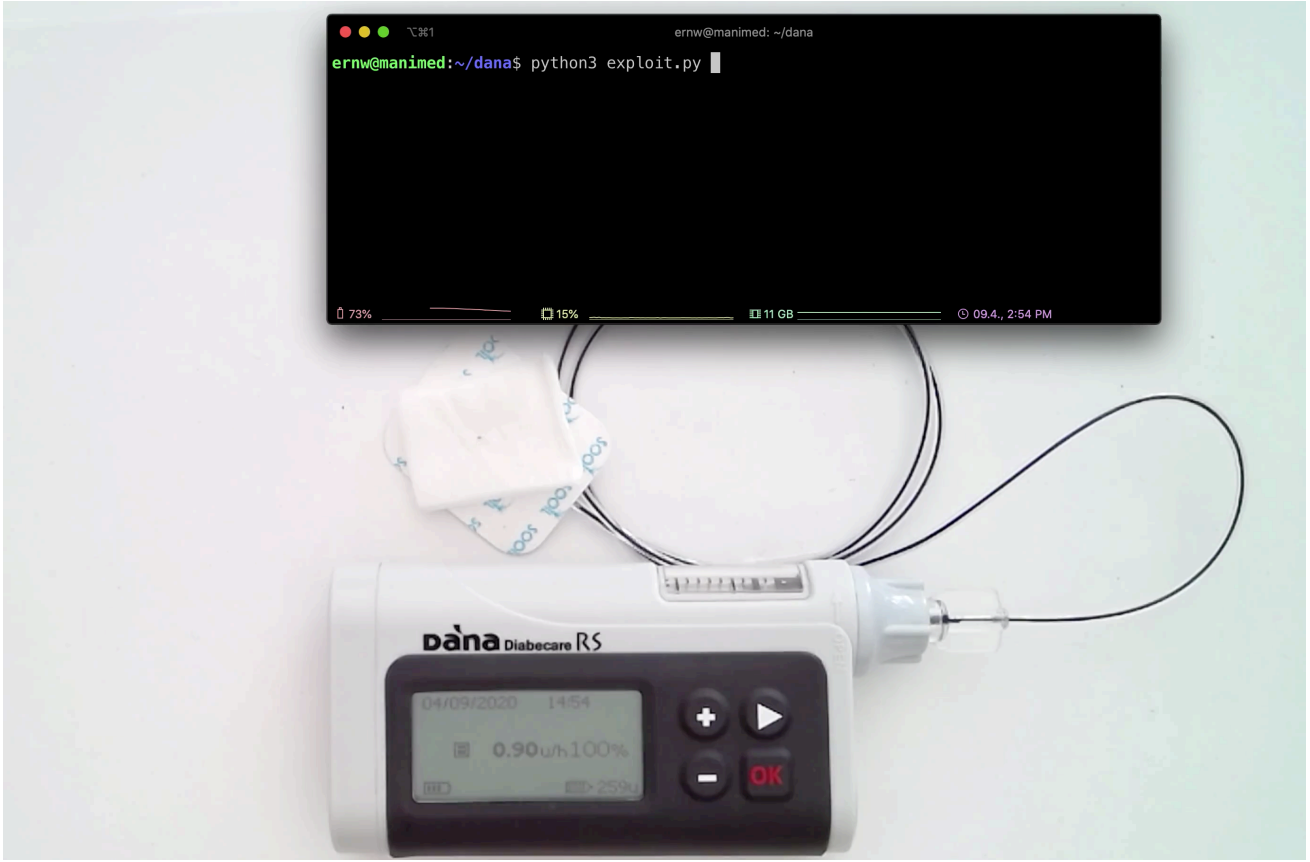
Impact

- Physical attacks (weak PINs) are not as critical as adjacent attacks (BLE)
- The combination of the identified vulnerabilities empowers an attacker to hijack the insulin pump (all functionalities that are utilizable via BLE)
- An attacker needs to be in proximity of the insulin pump sniffing a single communication between a DANA Diabecare RS insulin pump and a paired mobile application
- The attack is practical and can be performed automatically in productive environments
- The manufacturer released an updated device firmware

Results: Demo – Hijacking the Pump

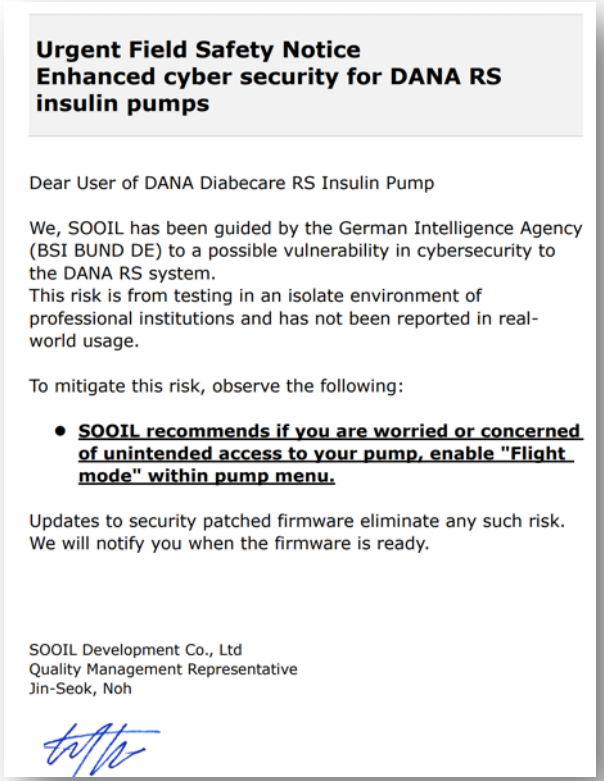
- In the following video:
  - An attacker captures messages between an insulin pump and a mobile app,
  - extracts the `P_KEY` from this communication,
  - hijacks and terminates the session between the pump and its paired app,
  - creates a new session impersonating the app using the `P_KEY`,
  - and administers multiple insulin boluses.
- The patient notices the administration and cancels it on the pump, but more boluses are following..

Results: Demo – Hijacking the Pump



Remediation & Temporary Measures

- Remediations are complex as most vulnerabilities are design defects.
- The manufacturer rolled out a firmware update for the insulin pump in 04/2020.
- Operations is key:
  - Disable the insulin pump's BLE functionality by putting it in airplane mode
  - → Preserve the pump's therapeutic purpose
  - The device implements safety features such as a maximum daily dose or bolus block



Urgent Field Safety Notice
Enhanced cyber security for DANA RS insulin pumps

Dear User of DANA Diabecare RS Insulin Pump

We, SOOIL has been guided by the German Intelligence Agency (BSI BUND DE) to a possible vulnerability in cybersecurity to the DANA RS system.
This risk is from testing in an isolate environment of professional institutions and has not been reported in real-world usage.

To mitigate this risk, observe the following:

- **SOOIL recommends if you are worried or concerned of unintended access to your pump, enable "Flight mode" within pump menu.**

Updates to security patched firmware eliminate any such risk.
We will notify you when the firmware is ready.

SOOIL Development Co., Ltd
Quality Management Representative
Jin-Seok, Noh

[https://advancedtherapeutics.org.uk/wp-content/uploads/2020/03/User-FSN-DANA-RS-Cybersecurity-002-6-March-2020.pdf, accessed July 28,2020]

ERNW
providing security.

Part VI: Disclosure

- Disclosure Timeline
- Publications

Disclosure Timeline

- The disclosure was managed by the ManiMed project team (BSI and involved ERNW staff in a consultative capacity)
- The ManiMed project strives to identify vulnerabilities in medical devices for sustainable strengthening cybersecurity, consumer protection, and patient safety
  → Trustful communication with the manufacturer
- A publication of the vulnerabilities does not pose serious risks or harm to patients as short-term measures or workarounds exist that preserve the pump‘s therapeutic purpose

ERNW RESEARCH pursuing knowledge.

Disclosure Timeline

Date	Event
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	Field Safety Notice (FSN) 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

In Press: ERNW White Paper

- Julian Suleder. ERNW Whitepaper 69: Safety Impact of Vulnerabilities in Insulin Pumps. September 11, 2020. Online: https://ernw-research.de/en/whitepapers/issue-69.html.

- CISA ICSMA will be released soon!

ERNW RESEARCH
pursuing knowledge.

Conclusions

- **Security updates** affecting **safety** should be handled with **high priority**.
- **Security updates are inevitable** to protect against vulnerabilities.
- **Mature processes** for handling cybersecurity vulnerabilities with safety impact on active medical devices are not yet common among all medical device manufacturers, even though recognized procedures based on pervasive community knowledge are in place.
- **Coordinated Vulnerability Disclosures** are a trustful basis for mutual exchange.
- Inspire authorities and manufacturers in terms of best IT-security practice.

ERNW RESEARCH
pursuing knowledge.

Outlook

- Besides cybersecurity professionals many different stakeholders are also interested in the results:
  - Physicians such as diabetologists
  - Standards-developing organizations
  - Academia
  - Health Delivery Organizations
- Therefore, dedicated publications such as blog posts, white papers, academic papers in medical informatics journals, and talks are planned

ERNW RESEARCH
pursuing knowledge.

Federal Office for Information Security

Thank you for your Attention!

- The vulnerabilities shall be acknowledged to Julian Suleder, Birk Kauer, Nils Emmerich and Raphael Pavlidis from ERNW Research GmbH.

Julian Suleder
E-Mail: jsuleder@ernw.de
Twitter: @jsuleder
ERNW Research GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
Germany

Dr. Dina C. Truxius
E-Mail: dina.truxius@bsi.bund.de
Referat DI 24
Federal Office for Information Security (BSI)
Godesberger Allee 185-189
53175 Bonn
Germany