IT Security

Security of Smart Sex Toys

A State of the Art Analysis of Smart Sex Toys

Bachelor thesis

For attainment of the academic degree of

Bachelor of Science in Engineering (BSc)

submitted by

Doris Hauser

01104726

in the
University Course IT Security at St. Pölten University of Applied Sciences

The interior of this work has been composed in LaTeX.

Supervision
Advisor: Dipl.-Ing. Daniel Haslinger, BSc
Assistance: -

St. Pölten, April 24, 2020 ____________________ ____________________

(Signature author) (Signature advisor)

St. Pölten University of Applied Sciences, Matthias Corvinus-Straße 15, A-3100 St. Pölten,T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E:office@fhstp.ac.at, I:www.fhstp.ac.at

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

In der heutigen Zeit werden immer mehr IoT Geräte verwendet, darunter unter anderem auch smarte Sex Toys. Aktuell gibt es bei vielen solcher Geräte Sicherheitslücken. Diese Arbeit untersucht im wesentlichen 4 smarte Sex Toys auf ihre angewendeten Protokolle und Sicherheitsfeatures mit besonderem Augenmerk auf die Schnittstelle zwischen der App und den Herstellerservern. Es wurden einige bedenkliche Praktiken in den Geräten entdeckt. Laut aktuellem Stand müssen die Sicherheitspraktiken dieser Geräte noch verschärft werden.

Abstract

Nowadays more and more IoT devices are used, among them smart sex toys. Currently lots of such devices have vulnerabilities. In this research 4 such devices have been analyzed in terms of the protocols used and their security features with a focus on the communication between the app and the company servers. A few vulnerabilities have been found in the reviewed sex toys. The status quo is that the security practice for such devices still have to be improved.

Contents

1 Introduction

The Internet of Things is a term that presumably first came up in 1999 in a presentation by Kevin Ashton[1]. There are different definitions of IoT: Haller et al. defined it as "A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business process."[2]. Sarma et al. have further specified in defining which "things" are considered part of the Internet of Things as "physical objects to virtual objects which represents as the identities with Internet connectivity."[3]. The IEEE defines the term as follows: "a wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement."[4].

In 2018 IoT Analytics reported 7 billion IoT devices to have been connected and estimates a rise to around 10 billion by 2020[5]. Many of those devices either collect data via sensors or have means to control certain appliances in case an event occurs that triggers a mechanism or they are commanded via remote control. The more sensitive the data they collect or the appliance they control is, the more important it is to implement a higher level of security.

"Teledildonics were first imagined in 1991 by author Howard Rheingold who was speculating on how people in the future would interact with each other and how human interactions would be expressed through robots"[6]. Some of the apps of current smart sex toys include mechanisms to befriend other app users, start a text or video chat, send pictures to each other or requests to control their partner's device. All data and communication revolving around those smart sex toys are considered sensitive data, especially since sex toys are banned in several countries in Africa, the Middle East and Asia[7].

At DEFCON 2016[8][9] two experts have presented an analysis of a We-Vibe device, how they were able to take over control of a nearby device and found out that sensitive usage data like the intensity and temperature of the toys were sent via the smartphone app to the servers of the producers. The manufacturer's irresponsible acquisition of user data has resulted in a lawsuit against them[10].

In cases of long-distance relationships or partners going on business trips for longer periods of time it can be hard for couples to cope with being away from each other for a while. Devices in the category of Teledildonics or smart sex toys can help overcome such phases by promoting a feeling of keeping in touch with your significant other and being able to share intimate moments with each other despite the distance. Aside from these reasons, people are also able to introduce new ways of excitement into their sex life by giving their partner the ability to surprise them or the owner being able to control their own device via app instead of possibly hardly reachable buttons on the device itself. On the other hand due to weak authentication it might also bear risks to use those devices[7]. Attackers could manage to intercept messages from the devices and could gain access to sensitive data or might even be able to control the device. Depending on regional legal definitions the latter might even be considered rape or sexual assault in some countries. According to Peter Treffer[11] in Belgium the legal definition of rape contains the phrase "by whatever means without consent". In Ireland the legal definition of sexual assault includes "vaginal intercourse manipulated by any object by another person".

A security researcher going by the nickname Renderman has started a project called the "Internet of Dongs", in which he tests devices and gets in touch with the manufacturers to help them fix any detected issues[12]. On the website he has, among other things, listed some general information for vendors about best practices or things to take into consideration security-wise when designing a new product.

Another project by the name Buttplug provides a library, which allows you to send and request messages to or from any device which is already supported. From a client, messages are exchanged with a Buttplug server instance, together with information which device from which manufacturer you want to communicate with and then translates the traffic between devices. This way you can set up a direct path of communication to your devices instead of sending all messages via the manufacturer server, therefore ensuring more privacy. Furthermore you have more fine-tuning possibilities in controlling the intensity and vibration patterns of your devices.[13]

The researcher Sarah Jamie Lewis had the idea to secure communications from a smart vibrator by sending the messages via Ricochet, a messenger software which sends data through the Tor network[14]. Ricochet doesn’t use usernames but instead creates a hidden-service with a unique address with randomized characters[15]. Lewis has managed to set up her test devices to send and receive messages via Ricochet, which leads to the data being encrypted and the manufacturers not being able to see (meta-)data about the usage of those devices, thereby protecting the privacy of the users[16]. The term she uses for this technology is Oniondildonics, a mixture of Onion Services (Tor) and Teledildonics.

As the amount of smart devices including smart sex toys is rising it becomes more and more important to ensure that those devices are manufactured in a secure way, especially since the first experiments on not only hacking toys to gain access to them, but also planting malware onto compromised smart sex toys have been performed [17].

1.1 Thesis Outline

This document is organized in several parts. chapter 1 introduces the topic, problems, challenges and motivation. chapter 2 describes some prerequisites and fundamental knowledge. chapter 3 lists the related work.
chapter 4 describes the work done and the results. chapter 5 concludes.

2 Prerequisites

Most of the devices use Bluetooth Low Energy (BLE), a variant of Bluetooth made for IoT devices with adaptations such as for lower battery drainage and low-rate communications. "BLE offers new privacy and security features to protect IoT users. Some of these include the ability to hide the name or address of the devices (so devices are not discoverable by others, only by previously paired devices), randomization of the addresses of the device, so users cannot be tracked as they move to different places, and encrypted communications."[7]. Furthermore all devices are usually communicating with the smartphone app via BLE or (common) Bluetooth and the app communicates with the manufacturer via the Internet.

The Bluetooth connection is usually established via an app by the company of the product, which is also the gateway of communication between the user and the company servers. This is, among other things, to make a remote connection between two partners possible via the Internet as the server establishes connections between two people trying to connect to each other via the app or via a generated URI that connects the recipient via a web browser to the user's app and therefore giving them control over the device.

3 Related Work

3.1 Matthew Allen Wynn[7]

Wynn et al. have written a paper about the security of smart sex toys[18], closely analyzing three devices: Vibease, OhMiBod blueMotion and We-Vibe 4 Plus. Wynn has later expanded this paper[7] by four more devices: Kiiroo's Pearl2 and Fleshlight Launch and Lovense's Nora and Max.

First Wynn et al. describe the Vibease, its app contains possibilities to exchange chat and voice messages, pictures and vibration requests and even offers audiobooks with custom vibration patterns available for download. Users may register either via their Facebook account or via email and password. Then the user can choose a nickname, by which they will show up on the app, and can optionally choose a verification code to ensure that they can only be found by people who have been given the code or received a URL. Once two users are connected, they may communicate. The first sent vibration request has to be accepted or rejected by the receiver.

The Bluetooth pairing is done by holding the power button on the device for 5 seconds during startup to get into the pairing mode, otherwise it will automatically try to connect to the last paired smartphone. Unfortunately, even when not in pairing mode, the device will send its device name to any object scanning for Bluetooth devices, which restricts the privacy of its users. The Vibease also doesn't make use of a BLE function which randomizes MAC-addresses in order to obfuscate its real address. The communication between the device and the phone is encrypted via BLE encryption protocols and couldn't be cracked by using Crackle[19], a tool to crack keys during the BLE pairing process.

Communication from the app to the cloud showed usage of unencrypted XMPP (Extensible Messaging and Presence Protocol) messages, since the server supports OAUTH2 authentication, but the client uses PLAIN mode which sends authentication data encoded in base64 and is therefore easy to decode. The sent password in this case is a token which is a derivative from the user's password and will not change unless the user changes their password. With this account data it is possible to log in to any XMPP messenger and communicate with the users associated with this account and even send them vibration requests. From the unencrypted packets sent between two users an attacker is also able to eavesdrop on messages and see their usernames. Additionally the app does not offer permission settings as of Android Version 6.0 and higher, which would allow the owner to allow or deny every single permission of apps, resulting in a "take it or leave it" situation with either all permissions allowed or denied. It also shows indiscreet notifications whenever an event occurs which poses a further risk to the user's privacy.

The OhMiBod offers predefined vibration patterns and styles, touch input and voice recording. It uses Bluetooth 2.0 to communicate with the app instead of BLE. Users can add other users as contacts by searching for an account username and either request control over the receiver's device or offer control over their own device. Accounts can at any time be switched between public or private: private accounts can only be found by the complete exact account name, public profiles can be found by partial matching strings.

In Bluetooth discovery mode the OhMiBod also broadcasts its name and non-randomized address to scanning devices. Furthermore, if the previously paired device is not available, the vibrator automatically goes into discovery mode and will pair with any requesting device (manual 0000 pairing passcode). The device can also be addressed like a speaker and will translate the amplitude of the audio file as the vibration intensity.

By installing the CA certificate and installing a proxy, Wynn et al. were able to intercept the encrypted SSL communication between the app and the server. On further inspection, a user request packet reveals their userID, username and a token, all of which allows one to impersonate any user. This can be done as easily as by manipulating the app configuration file by exchanging the user data with the acquired user's data in a rooted phone and restarting the app.

The We-Vibe allows users to control the pattern and intensity of the device via the app and doesn't need a registration, only a pairing of the device and the app via BLE. It is possible to give partners control over the device by sending them a URL. By default the app doesn't allow capturing screenshots, however Wynn et al. were able to modify flags on their rooted phone to override this setting.

The Bluetooth pairing of this device is managed via the app directly, but the device also propagates its name to scanning devices and doesn't randomize its MAC-address.

Since the findings of the DEFCON 2016[8][9] about the insecurities of the We-Vibe device and a following lawsuit[10] regarding those it seems like the manufacturers have implemented or enhanced a lot of the security mechanisms they use. Communications between the app and the server are securely encrypted and hashed via the XMPP protocol. The app has a hard-coded hashed CA certificate implemented, which makes it hard to decrypt traffic unnoticed via proxy and remote functionality is disabled until an initial session has been established. Trusted partners are stored in the form of an encoded and obfuscated username and used as XMPP credentials to send vibration control commands. Voice and text chat appears to be sent via the external service Twilio[20], which uses session tokens to connect two users. A token request checks whether the used agent of the querying device is correct and requires account credentials for the app. Additionally the app blocks screenshots and by default disables notifications. Communication with the server is addressed to its IP address, and no deduction about the nature of the destination can be made from DNS PTR records.

The Kiiroo devices can be synchronized with each other and allow remote control. Furthermore, via the app it is possible to connect to the FeelMe website, which offers videos with predefined vibration intensity metadata. A user can register on the website with their laptop and scan a given QR code with their app so that the devices build a secure connection via a PubNub[21] stream over which the haptic data is transferred.

The app appears to only use encrypted communication via TLS or QUIC save for the firmware downloads, which connects to a HTTP website, containing a JSON file with HTTPS links of all available firmware files. In specific situations, the server uses JSON Web Tokens (JWT) to communicate with the client, including a hash-value to prohibit manipulation of the data. In terms of privacy, DNS queries to the servers were addressed to feel-technologies.com, from which you might draw conclusions as to which type of device is used.

The Lovense devices are also designed for local as well as remote usage and a possibility of synchronization with each other. The app offers vibration control via sliders, music files, recorded sound, preset patterns and creation of patterns. It offers similar chat and vibration requests than the other device apps, but additionally provides means to set up a 4 digit pin code to be able to open the app and send photos.

All communication of the app appears to be encrypted via TLS according to the research team. Communication between partners is sent via encrypted XMPP traffic through a TLS tunnel. However, it is possible to decompile the APK file and even though the code is obfuscated, the general functions of the program are clear. Furthermore, the encryption data for the XMPP messages are written in plain text in the code and thus open to the public. Since the messages are transferred via TLS, it should still not be possible for an attacker to decrypt the data. The usernames used for XMPP are the given e-mail addresses of the user, which might pose a risk in terms of privacy.

3.2 Werner Schober[22][23]

This researcher performed a thorough vulnerability analysis of three different devices in the Teledildonic category. His findings however are mostly about a device called "Vibratissimo Panty Buster" as it showed so many vulnerabilities during the first inspection phase, that he focused on this sex toy. This device is intended for external stimulation by putting it in underwear.

First, he used a tool called Dirbuster to find stored filenames and directories and has found a .DS_STORE file. This is a file created by Apple devices and contains filenames that were opened by the Finder application. Among those was a directory called "config", which was accessible via browser and listed all files in this directory. There was a file named "config.php.inc" which contained credentials for the local database in plaintext.

Next he was able to get access to the PHPMyAdmin service, which has had many vulnerabilities over the past years. Together with credentials found online, an access to the database with all customer information and credentials in plaintext, among other data, was possible.

The Vibratissimo app provides a feature to upload and send pictures to other users. Schober found that all pictures were saved to the same folder online with a short ID as the filename and were accessible without restrictions. With a script he managed to check all IDs and download the images, most of which were explicit pictures from users who most likely were unaware of the pictures being publicly accessible.

As an authentication method, the app sent username and password in clear text with each request. This is both a risk because an attacker is easily able to read the credentials from packets sent over the network and able to use the credentials to forge packets with requests.

Furthermore the researcher found that one form of Cross-site-scripting was possible on the website of the manufacturer. This allows a potential attacker to execute javascript code, which opens many possibilities to access or manipulate data.

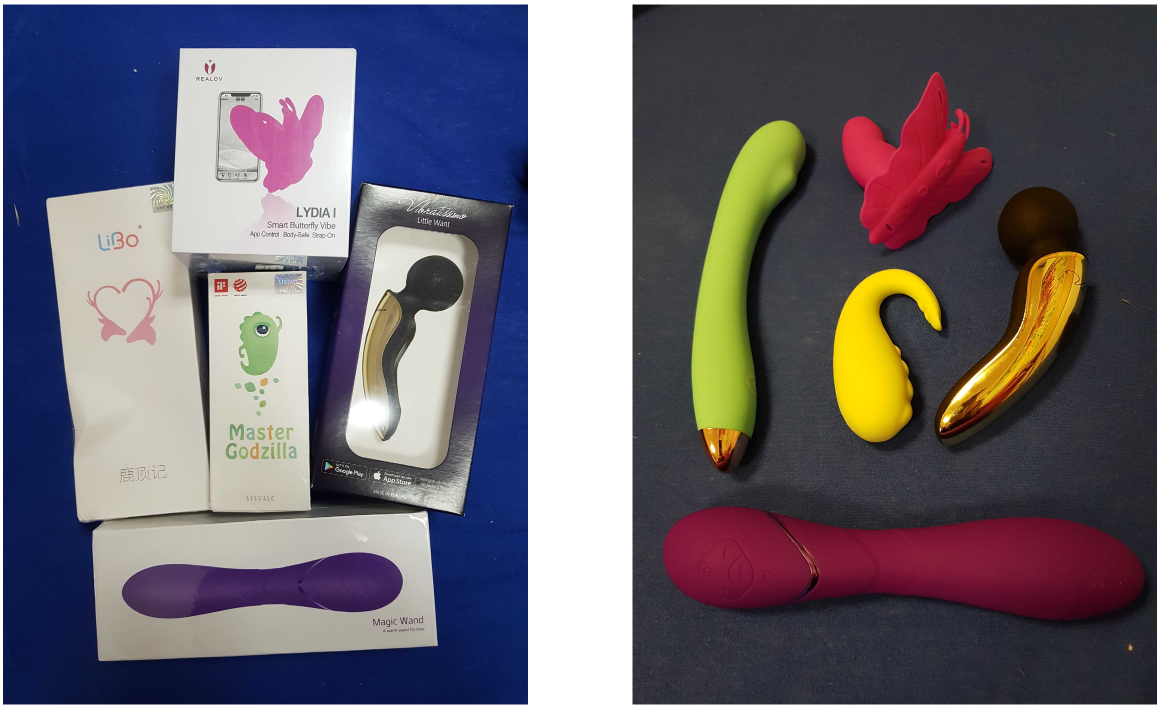
Last but not least, users have the possibility to send a link to other users to give them control over their devices. This link, similarly to the images link, is a static link which only includes an ID as variable information. This ID can simply be exchanged with another ID to control someone else's device and the receiver often doesn't even have a possibility to accept or deny those requests as this option is disabled by default.

Additionally, the paper includes a detailed analysis of Bluetooth and BLE vulnerabilities and possible solutions as well as a TLS security analysis before further examining the hardware. Upon inspection of the FCC number written on the device the researcher searched online and found design plans about the hardware. The first thing he noticed was a debug interface that was implemented in all productive devices instead of just in the prototype for testing. This facilitates access to the bootloader, flash memory and the firmware on the chip. The manufacturer also didn't include means to update the firmware of the device. Therefore it is not possible to fix the threats mentioned above in devices of this generation.

4 Approach

Before diving into the research a little disclaimer for fellow researchers: The Internet of Dongs has developed a code of conduct for researchers in the field of Teledildonics. This has the purpose to coordinate discovered vulnerabilities, possibly have some other researchers verify the findings and have a central point of contact to gather vulnerabilities from vendors and responsibly disclose them to the respective vendors[24]. It is highly recommended to follow this code of conduct in case of performing individual research on smart sex toys.

4.1 Choice of Devices



(a) Packaged Devices

(b) Unboxed Devices

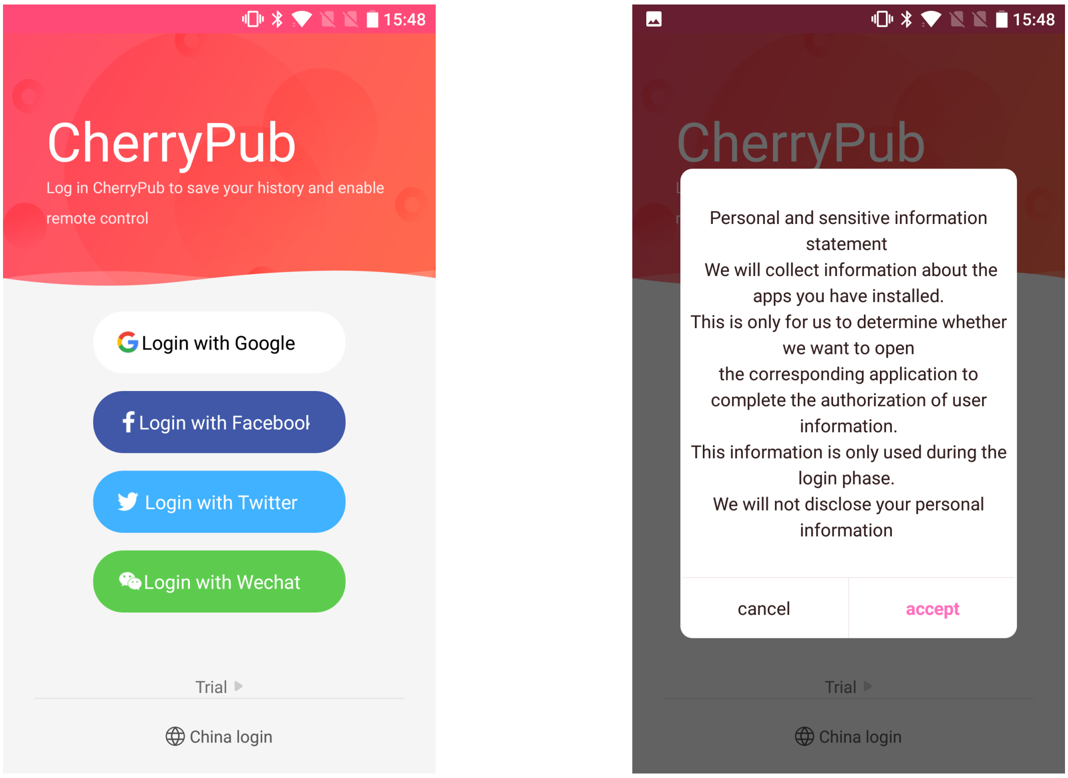
Figure 4.1: Chosen Devices

In order to perform a meaningful "state of the art" analysis, I have tried to choose devices that will cover multiple attributes that are likely to affect the intensity of security implemented and the methods used. The Criteria I have therefore chosen are the following:

- Price of the Product
- Known brands and no-name
- Brands that have and have not yet been investigated security-wise
- Remote-Controlling feature via the Internet as a must-criterion

As a result I have decided to analyze 5 devices that I will shortly introduce in the following subsections.

4.1.1 Libotoy Lolita



CherryPub

Log in CherryPub to save your history and enable remote control

(a) CherryPub Login

Personal and sensitive information statement
We will collect information about the apps you have installed.
This is only for us to determine whether we want to open
the corresponding application to complete the authorization of user information.
This information is only used during the login phase.
We will not disclose your personal information

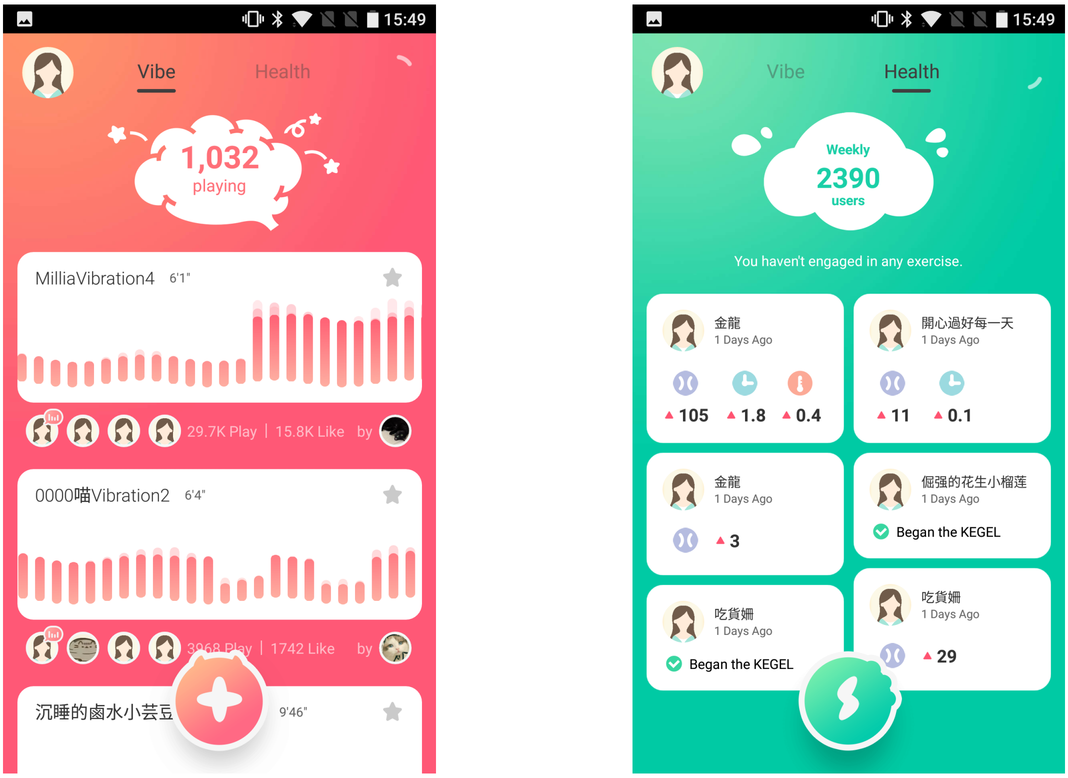
(b) CherryPub Agreement

Figure 4.2: CherryPub App

Price: 24,93€

This is a no-name product from China which has not been investigated yet. The device has one button and can be used manually or remotely, by first turning it on (long press) which brings it automatically into Bluetooth advertising mode, and then pressing the button again to get into manual mode. In manual mode you can cycle through the vibration styles by pressing the button again. The app is called CherryPub. When you first open it, you can either log in via one of four social media platform accounts, or start into "trial" mode. Then you have to connect to a device to to get to the next menu

4.1.2 Sistalk Monster Pub s1



You haven't engaged in any exercise.

(a) MonsterPub Start

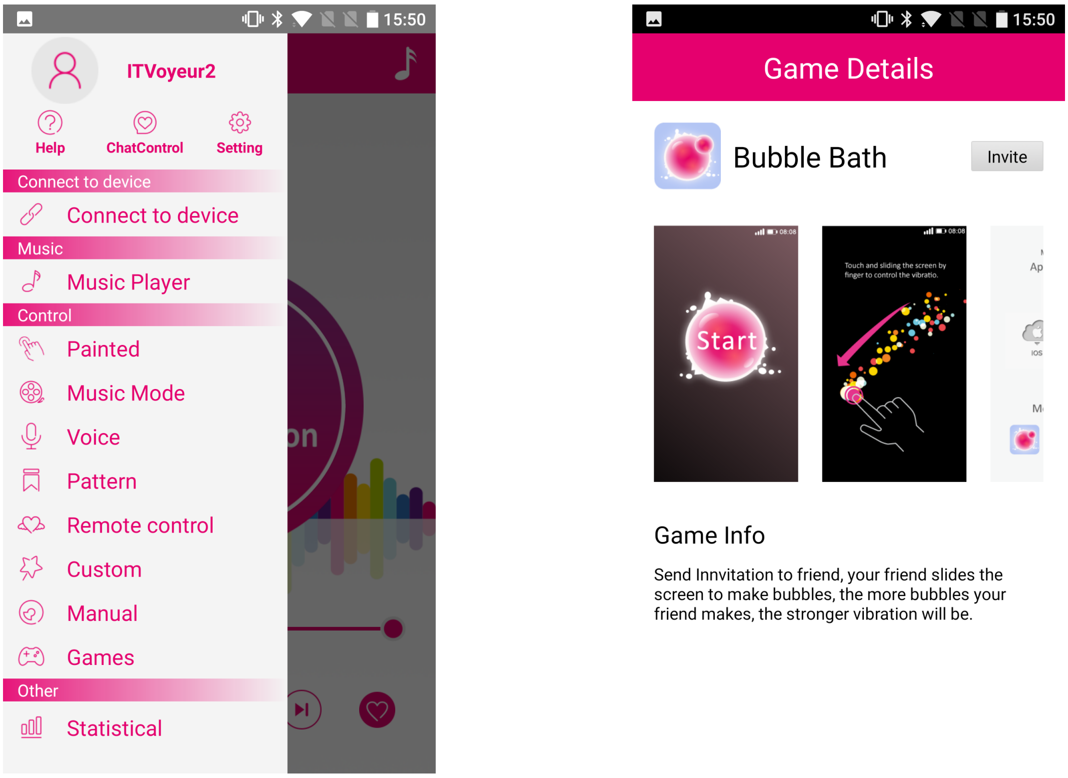
(b) MonsterPub Kegel

Figure 4.3: MonsterPub App

Price: 21,44€

This device is also from a no-name chinese brand. As I found out after the devices arrived, Sistalk seems to either be the same company as Libotoy or cooperate with them, as both advertise and sell each other's toys on their online shop. The vibrator has one button to power on and just as the Libotoy device first goes into Bluetooth advertisement mode and with another click can be controlled manually. The app is called MonsterPub and requires you to log in or register first off. One can either create an independent account or use a Facebook, KakaoTalk or WeChat account to log in. When logged in, there is the choice to either control your device manually or remotely, perform a guided kegel training, log their Ovulation Period and chat with other people. Furthermore there is a Tab in which you can check the battery status of your connected device, its product name and firmware version.

4.1.3 Magic Motion Magic Heating Wand



Send Innvitation to friend, your friend slides the screen to make bubbles, the more bubbles your friend makes, the stronger vibration will be.

(a) MagicMotion Menu

(b) MagicMotion Agreement

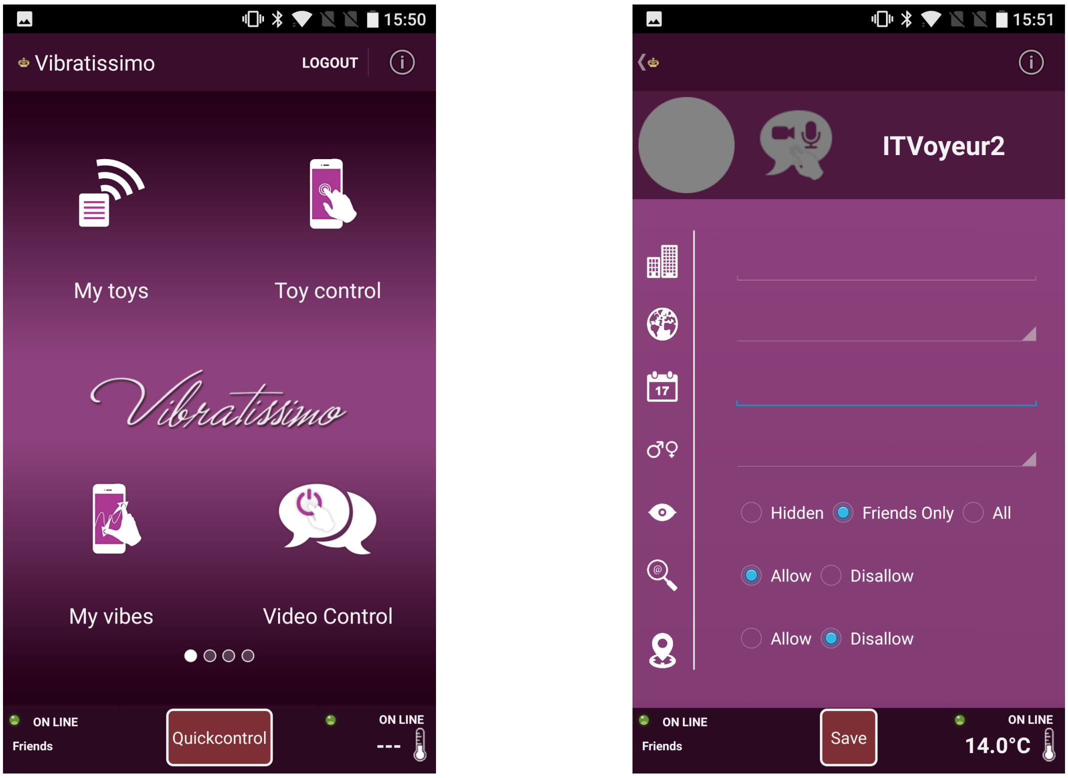
Figure 4.4: MagicMotion App

Price: 72,90€

Magic Motion is also a chinese company, but a bit better known and pricier. So far there have not been any security assessments for this brand, although they were first planned to get assessed in the paper of Werner Schober [22] but ended up not getting analyzed. This is the only one of the 5 devices to have more than one button: It has an on/off button, a plus and a minus to adjust the intensity and a "smart" button. The "smart" button is actually a button with two possible functions, which you can choose by tapping on the temperature bubble in the app. The first option is called "continuous vibrating" and the second "rapid heating". The first didn’t seem to change anything noticeable, the second lets you choose between 38 to 42 degrees of temperature by steps of 1 degree and when pressing the button it heats the device to the set temperature and keeps it on that level until you press the "smart" button again.

On startup, the MagicMotion app requires you to register or log in. From there you get a broad spectrum of things to do compared to the other devices. Among those are multiple ways to manually control the device ("painted" mode, preprogrammed vibration patterns, voice controlled, music player controlled, customized patterns by adjusting 8 intensity regulators or adjusting the intensity by tilting the phone) and three ways for remote control (one web link to a "guitar", one web link to a "bubble" game and a chat with remote control feature).

4.1.4 Vibratissimo Little Want



○ Hidden ● Friends Only ○ All

● Allow ○ Disallow

○ Allow ● Disallow

(a) Vibratissimo Start

(b) Vibratissimo Settings

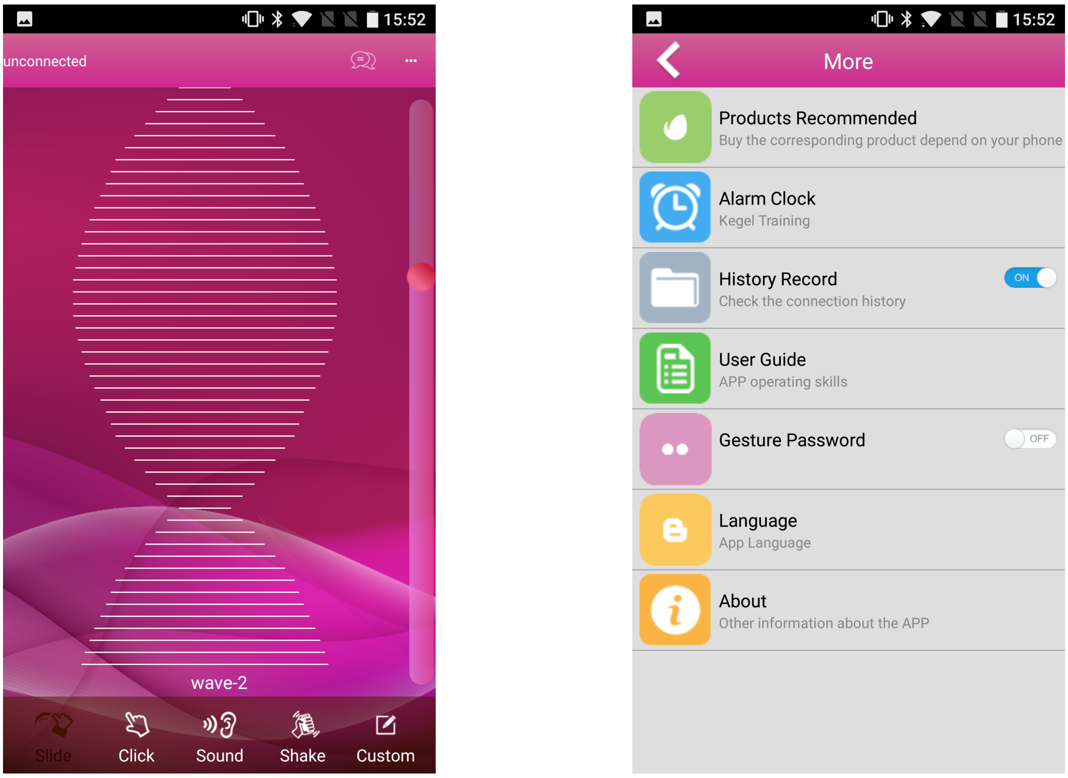
Figure 4.5: Vibratissimo App

Price: 38,95€

Vibratissimo is a german brand, it is the brand that was analyzed in the paper of Werner Schober [22] and is being included in this paper to have a comparison to a brand whose security has already been assessed and the issues reported to the manufacturers. One of the first things noticeable about this device is that it doesn't seem to have a means to be turned off completely. This shows by the device advertising itself via Bluetooth non-stop. Otherwise, it also has one button, a manual mode and an app to control it.

The app is called Vibratissimo and requires one to register or login first. It allows one to control a toy, download vibration patterns by other users, add friends, send them messages in a similar format as e-mails, chat with them if they're online, invite them to control your device or request to control theirs, video chat with device control or send a remote control link to an e-mail address. There is also a panel to show device information like battery status, temperature, whether it is plugged in, its MAC address and versions of the software. Furthermore, some functions are greyed out that you can activate via monthly or longer subscriptions. These functions include a search for nearby located users, a multi control feature that allows to control up to three devices and a music player vibration mode.

4.1.5 Realov Lydia



(a) Realov Start

(b) Realov Settings

Figure 4.6: Realov App

Price: 49,90€

This brand also seems to be one of the better-known ones and is a chinese company. The device was also first planned to be assessed in Mr. Schober's paper [22] but not carried out. It has one button with a manual mode and an app.

One first pleasant discovery was, that unlike the other apps this one only requires one to register and login when trying to access the remote functionality, all manual modes are available offline. Manual modes include preprogrammed or custom vibration patterns with an intensity regulator, touch controlled, shake controlled and sound controlled. To give someone remote control over your device, you first have to add them as friends. Once the friend has accepted, there is a chat with possibility for remote control.

4.2 Analysis

4.2.1 Methodology

The chosen devices have been analyzed in terms of privacy and security. This has been examined by first doing a general assessment of the functions of the device and the app and traffic to and from the app while using app features both using a simple traffic sniffer to analyze whether some data is sent in plain text and using an SSL proxy to decrypt the traffic.

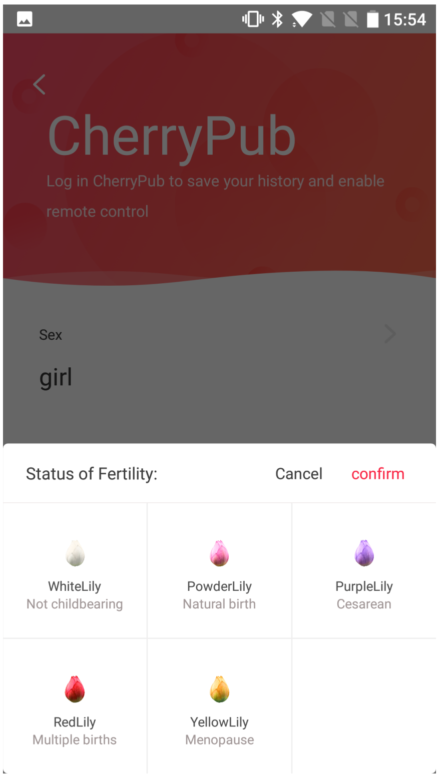
The inspected traffic was in specific sniffing the communication during a login to the app, connecting to the device, using the manual control mode, using the remote control mode and using the chat function.

The Plain text analysis has been performed with an app called tPacketCapture, this app was installed on an Android phone to capture all traffic from said phone. The app uses the VPN service of Android OS to route all traffic through the app and saves the captured packets as pcap files which can then be opened and analyzed with WireShark[25].

In BurpSuite a proxy was configured which acted as an invisible proxy and signed per-host certificates with its integrated CA certificate. Using the proxy was done by changing the advanced settings of the WiFi connection on the Android phone to use the PC running BurpSuite as a proxy, which ensures that all connections through the Internet are first sent to it. Then a browser was used to access "http://burp", which will connect you to your proxy and allow you to download the certificate. This CA certificate was installed on the Android phone so that all intercepted traffic via BurpSuite is still shown as trustworthy.

This research focuses on collecting data about the protocols used, if and which kind of encryption is used to secure the communication and what personal data is being sent to the company servers. Furthermore the app functionality is tested for vulnerabilities that are exploitable by people with no or little IT background, such as user enumeration, direct object reference and password brute force.

The section "Collected Data" is a summary of the personal data each device is sending towards the server. Data that is needed for registration will be excluded from the list (e-mail address, nickname, profile picture, age and gender).



15:54

CherryPub

Log in CherryPub to save your history and enable remote control

Sex

girl

Status of Fertility: Cancel confirm

WhiteLily Not childbearing	PowderLily Natural birth	PurpleLily Cesarean
RedLily Multiple births	YellowLily Menopause	

Figure 4.7: CherryPub Profile

4.2.2 Libotoy Lolita

General Features

During the tests and analysis of this device, soon one big problem arose: The connection to the device via the app was only successful around every 50th to 100th try. The behavior was such, that most of the times, when powering on the vibrator and opening the app, the toy switched from connecting (blinking light) to connected (continuous light) and the app showed "Connected Lottie", but it wasn't possible to control the device via the app. Only sometimes, mostly when it said "Connected Lu Ding Ji", was it possible to control the vibrator via the app. Due to this very time consuming bug, I have decided to exclude this device from my research.

Until then, one curiosity I have found out about this device, is that when the Sistalk Monster Pub vibrator was turned on, it was possible to connect to this device via the Libotoy app and control the device. Therefore I assume that Sistalk and Libotoy's partnership might be close enough for them to share parts of their software.

Furthermore, registration and login to this app was only possible via a Google, Facebook, Twitter or WeChat account. Unlike the other apps it wasn't possible to register an account to an e-mail address or otherwise unrelated to another social media. Also when logging in for the first time, the user is prompted to fill in some basic data like sex, age (in 5 year spans), but also one's fertility status.

The remote control feature generates a URI that looks as follows: `http://api.bianquejia.cn:8080/remotecontrol/index.html?roomid=8Uuis_6Wl9dY4vAkAAK3`. Apparently the roomid consists of a 20 random alphanumeric characters.

4.2.3 Sistalk Monster Pub s1

General Features

This device which advertises itself as "Monster Pub" via Bluetooth soon showed a first privacy issue: To add friends, there is a search function that matches your input followed by a wildcard. This way it is very easily possible to find out all existing users by using each letter of the alphabet as input.

The URL to access the remote control feature looks as follows: `https://oversea.sistalk.cn/play/remote/536550?area=INTER`. The number used is the user ID, which is shown on each person's profile, but it is only possible to control a device, while the remote feature is activated.

Gaining access to another person's account via the "password forgotten" feature seems hard at first, as they ask for an e-mail address and send you an e-mail with a 6 digit code that is only valid for 24 hours. The current (presumably forgotten) password stays and additionally, when clicking the "password reset" button, a new form shows up asking to enter the 6 digit code that was sent and set a new password:

Listing 4.1: Monster Pub Password Reset

```
POST /api/user/password/email_reset HTTP/1.1


code=blabla&password=blabla&uuid=05f13f5c-2bfc-483a-b114-0f3a74e77bf4
```

Entering invalid codes though is allowed without any limitations, the same is true for passwords. This means that an attacker could use the password reset feature to brute force into an account and set a new password without the user noticing except for getting a password reset e-mail, as it is still possible to log in with the current password.

Furthermore it is easy to find out if an account exists or not as the login is also done via e-mail address and password and the error messages tell you whether an e-mail address doesn't exist or the password is wrong. The password length is capped to a maximum of 15 digits again making it easier for attackers to brute force into accounts.

tPacketCapture Sniffing

The first part of the analysis, sniffing the app traffic without a proxy, showed that most traffic from the app is sent via HTTPS, except for some data about the phone including WiFi SSID and the chat. Some excerpts look as follows:

Listing 4.2: Monster Pub Phone Info

```
{"deviceid":"95899193-56ec-36f1-a009-8729143e98e4","android-id":"4
   e0e753fe6c013d5","app-id":"cn.sistalk.mp.lite","hid":"mp_en_536550
   ","os":"android","os-version":"9","manufacturer":"samsung","model
   ":"[redacted]","width":1080,"height":2076,"dpi":480,"wifi-mac-
   address":"[redacted]","lon":16.[redacted],"lat":48.[redacted],"
   wifissid":"\"[redacted]\""}
```

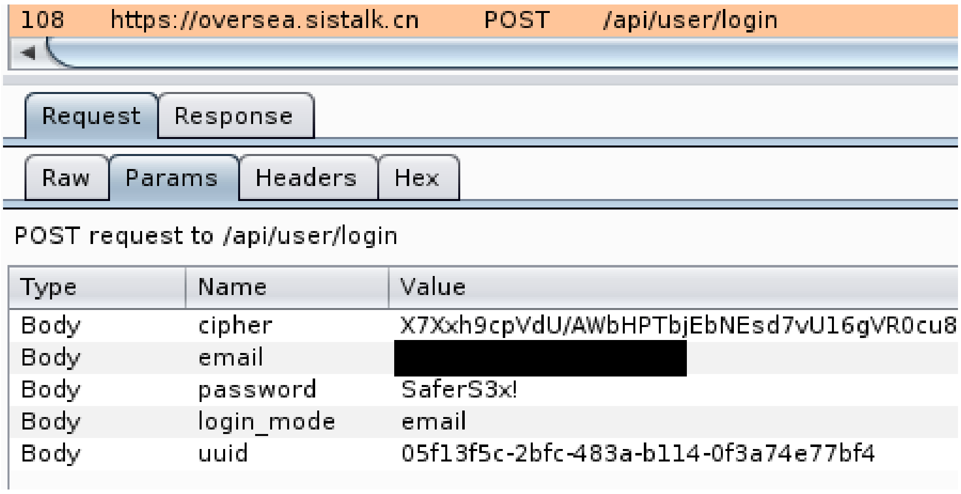
Listing 4.3: Monster Pub Chat

```
chat message from ITVoyeu2 to ITVoyeur:

<..mp_en_536550",android_95899193-56ec-36f1-a009-8729143e98e4....
   mp_en_566103(.2........mp_en_536550....mp_en_566103".....guten Abend
   *^
.em_apns_ext..2M{"extern":"im_message_notification","em_push_content":"
   ITVoyeur New message"}*.
.em_ignore_notification....*.
.user_id..... X....$..@.J.
```

```
.................... @.....-...D..@.J>

...

Reply:

mp-release..mp_en_566103..easemob.com",android_4adc92aa-ff9d-3212-bd7d
   -9404292c991f.2
.09696815-4#mp-release..mp_en_536550..easemob.com .....-(.2........
   mp_en_566103....mp_en_536550".....danke dir auch!*^
.em_apns_ext..2M{"extern":"im_message_notification","em_push_content":"
   ITVoyeu2 New message"}*.
.em_ignore_notification....*
```

Burpsuite Proxy decryption

Most of the traffic was HTTPS traffic communicating with oversea.sistalk.cn, IP address 47.75.26.49.



108 https://oversea.sistalk.cn POST /api/user/login

POST request to /api/user/login

Type	Name	Value
Body	cipher	X7Xxh9cpVdU/AWbHPTbjEbNEsd7vU16gVR0cu8
Body	email	[redacted]
Body	password	SaferS3x!
Body	login_mode	email
Body	uuid	05f13f5c-2bfc-483a-b114-0f3a74e77bf4

Figure 4.8: MonsterPub Login SSL traffic

As seen in the figure above, first the e-mail address and password are sent to the server. The server then responds with a token, that is further used to reference the authenticated session:

Listing 4.4: Monster Pub Login Token

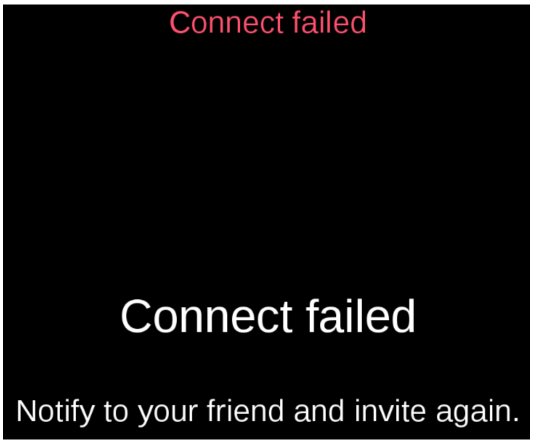
```
{"data":{"token":"UKvs8beFsz6PFXqCM5rdb8AofSUBiHf9rNwFglJa","expired
   ":2592000,"id":566103},"status":200}
```

Next all user profile information and settings are requested from the server. Then came an in-app popup with a new version. As the following packet from the server shows, the links to the app versions and firmware are sent and can be downloaded from there.

Listing 4.5: Monster Pub New Version

```
{"data":{"app":{"url":"http:\/\/static-hk.sistalk.cn\/downloads\/
   MonsterPub_v4.2.3_702_Official_release.apk","version":"4.2.3","build
   ":"702","require":false,"message":"The New Action-Reaction 2.0
   ------ more sensitive & more pleasure. Download and shake your phone
    to start it.","message_json":["The New Action-Reaction 2.0 ------
   more sensitive & more pleasure. Download and shake your phone to
   start it."],"version_minimum":"1.0.0"},"firmware":[{"product":"MP_JK
   ","version":"1.0.7","url":"http:\/\/static.sistalk.cn\/firmware\/
   MP_JK_1.0.7.zip","message":"\u00b7 \u4f18\u5316\u5f02\u5e38\u65ad\
   u5f00\u7684\u9707\u52a8\u4f53\u9a8c\u4e0d\u4f73\u7684\u95ee\u9898\
   u3002"},{"product":"MP_JKS","version":"2.1.0","url":"http:\/\/static
   .sistalk.cn\/firmware\/MP_JKS_2.1.0.zip","message":"\u00b7 \u4f18\
   u5316\u5f02\u5e38\u65ad\u5f00\u7684\u9707\u52a8\u4f53\u9a8c\u4e0d\
   u4f73\u7684\u95ee\u9898\u3002"}],"nordic":{"version":"1.0.7","url":"
   http:\/\/www.sistalk.cn\/downloads\/MP_App_1.0.7.zip"},"health":{"
   version":"3","url":"http:\/\/static.sistalk.cn\/common\/health.js
   "}},"status":200}
```

Furthermore, there are requests about "current play list" and "active list" which send back a big amount of data including usernames, IDs, location information and more. So far there doesn't seem to be a possibility to use this for an attack, as the remote control feature is only available if the users are actively using it and only one client can connect to this remote session, once connected every other request gets an error message as a response:



Connect failed

Connect failed

Notify to your friend and invite again.

Figure 4.9: MonsterPub Connection Failed

The next interesting thing were login data to Easemob. "EaseMob is a PaaS-based platform that allows developers to integrate instant messaging, voice, and data services to their apps" according to crunchbase [26]. The communication was to the IP address 39.97.9.52 and looked as follows:

Listing 4.6: Monster Pub Easemob Login

```
request:

{"grant_type":"password","password":"U9ArcGVUJM2XnuMp","username":"
   mp_en_566103"}

response:

{"access_token":"YWMt0T5jBhdMEeqaYI-
   _HGhKpvsCFrAmmRHoubkVBhyWFMTFNuhwC6kR6pfUsQA-
   JLh0AwMAAAFu1a0z8gBPGgABieoq8oZYWe6JQUnSp2JMFoCxt88ky1VAV5GiCKgSnA
   ","expires_in":5184000,"user":{"uuid":"c536e870-0ba9-11ea-97d4-
   b1003e24b874","type":"user","created":1574263437438,"modified
   ":1574263437438,"username":"mp_en_566103","activated":true}}
```

According to the user id in the Easemob username, presumably every user has its own Easemob account. This login started, when the remote control session started, which which points to the remote data being transferred via Easemob.

The remote play values and chat messages seem to not be communicated via HTTPS, as the packets didn't show up in BurpSuite. Only at the end of the remote play there was a packet sent to the server including information about the duration of the remote play session in milliseconds and some "get user info" packets were exchanged for the messaging. Sending and presumably storing data about the duration of user's play sessions is a very sensitive information to save, as is has already lead to the company Standard Innovations being sued for their We-Vibe 4 Plus vibrator for doing exactly that[27].

Listing 4.7: Monster Pub Played Time

```
request: /api/play/remote_log

token=UKvs8beFsz6PFXqCM5rdb8AofSUBiHf9rNwFglJa&pid=MP_YD&played_time
   =184465

response:

{"message":"upload ok","status":200}

get user info:

{"message":"get user info success","status":200,"data":{"id":536550,"
   address":"","avatar":"","birthday":"[redacted]","sexuality":"female
   ","city":"","favorite_topics":0,"followers":1,"following_users":1,"
   launch_topics":0,"nickname":"ITVoyeur","participate_topics":0,"
   zodiac":"\u767d\u7f8a","signature":"","cover":"","address_code":"
   AT_Vienna","record_count":0,"is_following":1,"is_follower":1,"
   contact_type":"","contact_id":"","type":"common","is_unfollow":1,"
   mark":"common","monster_list":[{"monster":"godzilla_1s","product_id
   ":"MP_YD","monster_id":"dffb1912f3c4","user":{"id":51,"nickname":"\
   u54e5\u65af\u62c9\u5927\u5e08","avatar":"http:\/\/static.sistalk.cn
   \/uploads\/avatar\/2017\/1207\/sistalk_5a28b1553e9e3cnXCB.png@!
   q80webp"},"created_at":1570637410}],"signature_sound":"","
signature_sound_duration":0,"is_banned":false,"albums":[],"im_remind
":1,"greet_remind":1,"is_greeted":true,"is_black":false,"
is_blackened":false,"hxid":"mp_en_536550","gift":[],"send_gift":[],"
is_finish_survey":1,"is_open_play":0,"is_open_kegel":0}}
```

Collected Data

Sistalk collects the following data:

- Information about the phone used
- Which sex toy model is used
- Location data (coordinates)
- WiFi BSSID
- Time played

This information combined could be used to identify a user completely. Especially the location data and WiFi BSSID narrow down the area of use to a specific location. This together with the phone model, sex toy model and time played already reveals a fairly detailed profile of a user and therefore create a big attack vector.

4.2.4 Magic Motion Magic Heating Wand

General Features

This device is advertised as "Magic Wand" via Bluetooth. On the first glance everything looks like standard procedure: You register an account with a nickname and can then use features. When looking more closely though, there doesn't seem to be an account storage at all: There is no logoff button in the app, one has to delete the app data to log off. Once Logged off, the only choice is to register an account by entering a nickname and accepting the agreement, there is no password input field. When submitting a previously used nickname, it seems to create a new "account" as the profile settings are back to default. In fact, the only feature that uses the nickname is the remote chat control. This shows your chosen nickname and picture to the person connecting to the link via the app and vice versa.

The remote URL links for chat control contains a 5 digit ID to enter in the app. This ID is generated randomly, but as it only consists of 5 digits it might be easy to randomly get to chat controls that are currently open.

`http://game.magicmotion.cn/invite/en/invite.html?token=79508`

Game room URIs look a bit different and more secure, as they include a long random alphanumeric room ID. Games can be played in a browser and go on even after the initiating person has disconnected. This way it seems impossible to find active game rooms to hijack.

Bubble Bath: `http://game.magicmotion.cn/static/en/1/index.html?room=ad23b537-6215-49d9-88e9-34dc91db4ef41573729500067`

Remote Guitar: `http://game.magicmotion.cn/static/en/2/index.html?room=f7375b1e-2782-4001-b5d4-06b4aa8112ca1573729903599`

tPacketCapture Sniffing

This device yielded a little more information in the first traffic analysis than the others:

IP: 47.96.117.28

Listing 4.8: Magic Motion Get User Info

```

POST /user/get_user_info HTTP/1.1
Content-Length: 0
Host: mmaccount.vtio.cn
Connection: Keep-Alive
Accept-Encoding: gzip
Cookie: connect.sid=s%3AEywJl0H61JpKMSIUY1EUAo6RL2ocXa2l.dp3yce%2
   BGm9TIbuYIcKF%2BV0K4q69tAR0ZdsidXA4D3fk
User-Agent: okhttp/3.3.0

HTTP/1.1 200 OK
Server: nginx/1.14.0
Date: Mon, 25 Nov 2019 18:37:21 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 354
Connection: keep-alive
X-Powered-By: Express
Vary: X-HTTP-Method-Override
Access-Control-Allow-Origin: *
```

```
Access-Control-Allow-Headers: Content-Type, X-Requested-With
Access-Control-Allow-Methods: GET, POST, OPTIONS

{
  "success": "true",
  "result": {
    "meta": {
      "createAt": "2019-11-25T18:37:20.862Z",
      "updateAt": "2019-11-25T18:37:21.730Z"
    },
    "username": "2aca2c00441de9fd92272a1e0cdf95bc",
    "company": "MagicMotion",
    "product": "MagicMotion",
    "tags": [],
    "uuuid": "2aca2c00441de9fd92272a1e0cdf95bc",
    "nick": "ITVoyeur"
  }
}
```

IP: 121.41.74.212

Listing 4.9: Magic Motion Remote Session

```

n=97118
{"result":"success"}
{"room":"someone joined"}
{"reqId":"2a34d459a8affee809f0ef8b2108bbd5","nick":"ITVoyeur2"}
{"userId":"2aca2c00441de9fd92272a1e0cdf95bc","nick":"ITVoyeur"}
{"x":"0","y":"0"}
{"x":"139","y":"129"}
{"x":"139","y":"126"}
{"x":"139","y":"123"}
{"x":"139","y":"120"}
```

```
{"x":"139","y":"117"}
{"x":"139","y":"114"}
{"x":"139","y":"111"}
...
```

The above shows that at least some of the data is being transferred in plain text. The second code snippet shows the room id as n, the user IDs, nicknames and the values sent to control a device.

Burpsuite Proxy decryption

Since there is only a sign up at Magic Motion, the "Login" process is actually the registry. The sign up went to the URL mmaccount.vtio.cn/user/signup. This domain seems to provide a VTrump server, which offers middleware services int the IoT sector [28]. The traffic looks as follows:

Listing 4.10: Magic Motion Login

```
request:

uid=6647985bd62c615e03b38cb4058504a7&username=6647985
   bd62c615e03b38cb4058504a7&password=0c864e18fa4e50cac304ec59f433b761&
   company=MagicMotion&product=MagicMotion

response:

set-cookie: connect.sid=s%3AF5uEesb85XWzsnXvSMDXYUSjQelPcjzH.lDV9ggvHe2
   %2FpiuwOObstec5nNgPxTQREOA9X%2F3duiTk; Domain=.vtio.cn; Path=/;
   Expires=Fri, 31 Jan 3000 16:00:00 GMT; HttpOnly

{
  "success": "true",
  "result": {
   "meta": {
     "createAt": "2019-12-07T09:54:09.191Z",
     "updateAt": "2019-12-07T09:54:09.191Z"
```

```
    },
    "username": "6647985bd62c615e03b38cb4058504a7",
    "company": "MagicMotion",
    "product": "MagicMotion",
    "tags": [],
    "uuuid": "6647985bd62c615e03b38cb4058504a7"
  }
}

request (mmapi.vtio.cn/app/device_put_data):

data=%7B%22Version%22%3A0%2C%22SyncData%22%3A%7B%22userinfo%22%3A%5B%7B
    %22content%22%3A%22%7B%5C%22uuuId%5C%22%3A%5C%226647985
    bd62c615e03b38cb4058504a7%5C%22%2C%5C%22nick%5C%22%3A%5C%22Anonymous
    %5C%22%2C%5C%22birth%5C%22%3A%5C%22-1%5C%22%2C%5C%22gender%5C%22%3A
    %5C%221%5C%22%2C%5C%22height%5C%22%3A%5C%220%5C%22%2C%5C%22hasDevice
    %5C%22%3Afalse%2C%5C%22dateTime%5C%22%3A%5C%222019-12-07%2010%3A54%3
    A09%5C%22%7D%22%2C%22createTime%22%3A%222019-12-07%2010%3A54%3A09
    %22%2C%22opType%22%3A%22C%22%7D%2C%7B%22content%22%3A%22%7B%5C%22
    uuuId%5C%22%3A%5C%226647985bd62c615e03b38cb4058504a7%5C%22%2C%5C%22
    nick%5C%22%3A%5C%22ITVoyeur2%5C%22%2C%5C%22birth%5C%22%3A%5C%22-1%5C
    %22%2C%5C%22gender%5C%22%3A%5C%221%5C%22%2C%5C%22height%5C%22%3A%5C
    %220%5C%22%2C%5C%22hasDevice%5C%22%3Afalse%2C%5C%22dateTime%5C%22%3A
    %5C%222019-12-07%2010%3A54%3A09%5C%22%7D%22%2C%22createTime%22%3A
    %222019-12-07%2010%3A54%3A09%22%2C%22opType%22%3A%22U%22%7D%5D%7D%7D

message above decoded:

{"Version":0,"SyncData":{"userinfo":[{"content":"{\"uuuId\":\"6647985
    bd62c615e03b38cb4058504a7\",\"nick\":\"Anonymous\",\"birth
    \":\"-1\",\"gender\":\"1\",\"height\":\"0\",\"hasDevice\":false,\"
    dateTime\":\"2019-12-07 10:54:09\"}","createTime":"2019-12-07
```

```
   10:54:09","opType":"C"},{"content":"{\"uuuId\":\"6647985
   bd62c615e03b38cb4058504a7\",\"nick\":\"ITVoyeur2\",\"birth
   \":\"-1\",\"gender\":\"1\",\"height\":\"0\",\"hasDevice\":false,\"
   dateTime\":\"2019-12-07 10:54:09\"}","createTime":"2019-12-07
   10:54:09","opType":"U"}]}}

request (mmaccount.vtio.cn/user/set_user_info_ex):

cookie: connect.sid=s%3AF5uEesb85XWzsnXvSMDXYUSjQelPcjzH.lDV9ggvHe2%2
   FpiuwOObstec5nNgPxTQREOA9X%2F3duiTk
User-Agent: okhttp/3.3.0

nick=ITVoyeur2

response:
{
  "success": "true",
  "result": {
    "meta": {
      "createAt": "2019-12-07T09:54:09.191Z",
      "updateAt": "2019-12-07T09:54:10.140Z"
    },
    "username": "6647985bd62c615e03b38cb4058504a7",
    "company": "MagicMotion",
    "product": "MagicMotion",
    "tags": [],
    "uuuid": "6647985bd62c615e03b38cb4058504a7",
    "nick": "ITVoyeur2"
  }
}
```

This interaction has already partly been seen in the non-encrypted traffic analysis, as this is sent in plain

HTTP.

Upon connecting to the vibrator, a short information packet about the phone is sent to the servers:

Listing 4.11: Magic Motion Phone Info

```
request:

{"notifier":{"name":"Android Bugsnag Notifier","version":"4.18.0","url
   ":"https://bugsnag.com"},"app":{"versionCode":62003,"releaseStage":"
   production","type":"android","version":"6.2.3"},"device":{"osVersion
   ":"6.0.1","manufacturer":"OnePlus","jailbroken":false,"cpuAbi":["
   arm64-v8a","armeabi-v7a","armeabi"],"osName":"android","
   runtimeVersions":{"osBuild":"ONE A2003_24_171024","androidApiLevel
   ":23},"model":"ONE A2003"},"sessions":[{"id":"1b4dc426-8558-4c08-9
   be2-cc77652fc1b1","startedAt":"2019-12-07T10:05:35Z","user":{"id
   ":"8595cb33-751b-4b67-a910-c956ad4ab930"}}]}
```

The manual control of the Bluetooth device doesn't seem to be communicated to the Magic Motion servers at all.

Starting a remote game session via either the "bubble game" or the "guitar game" resulted in few communication between the app and the Magic Motion servers, which didn't look vulnerable in any way.

The "chat control" function seems to use a different method though: Once the button "chat control" is clicked, a web socket is built.

Listing 4.12: Magic Motion Web Socket

```
request:

GET /socket.io/?EIO=3&transport=polling HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; ONE A2003 Build/
   MMB29M)
```

```
Host: remote.magicmotion.cn
Connection: close
Accept-Encoding: gzip, deflate

response:

set-cookie: io=An5qA4iUH-eke2KfAWQa
date: Sat, 07 Dec 2019 10:16:52 GMT
connection: close

request:

GET /socket.io/?EIO=3&sid=An5qA4iUH-eke2KfAWQa&transport=websocket HTTP
   /1.1

request:

POST /user/imbind HTTP/1.1
Content-Length: 0
Host: mmaccount.vtio.cn
Connection: close
Accept-Encoding: gzip, deflate
Cookie: connect.sid=s%3AF5uEesb85XWzsnXvSMDXYUSjQelPcjzH.lDV9ggvHe2%2
   FpiuwOObstec5nNgPxTQREOA9X%2F3duiTk
User-Agent: okhttp/3.3.0

response:

{
  "success": "true",
  "result": {
    "imToken": "YCQhDAECYM8kJgy15uKSnBG6bM+0Yd0q7xrnnqG+
      huG4ywo4KXxDWrTFMMzOJCUNCxAz32GzYrh/
      CwqHvS1kCv0LoqjbfAkHf67otBLCckRBWvfzkIHdMAgVKQ3gE6Z8MI5DsPtBQ1U="
  }
}

request:

POST /navi.xml HTTP/1.1
Connection: close
User-Agent: RongCloud
Host: nav.cn.ronghub.com
Content-Length: 173
Content-type: application/x-www-form-urlencoded
appId: uwd1c0sxdykd1
Accept-Encoding: gzip, deflate

token=YCQhDAECYM8kJgy15uKSnBG6bM%2B0Yd0q7xrnnqG%2
   BhuG4ywo4KXxDWrTFMMzOJCUNCxAz32GzYrh%2
   FCwqHvS1kCv0LoqjbfAkHf67otBLCckRBWvfzkIHdMAgVKQ3gE6Z8MI5DsPtBQ1U%3D&
   v=2.9.13&p=Android

response:

<navi><code>200</code><userId>6647985bd62c615e03b38cb4058504a7</userId
   ><server>120.92.117.15:443</server><voipServer></voipServer><
   uploadServer>upload.qiniup.com</uploadServer><qnAddr>upload.qiniup.
   com</qnAddr><historyMsg>false</historyMsg><chatroomMsg>false</
   chatroomMsg><bs>120.92.117.15:8015,t-tcpproxy-cn.ronghub.com:443,t-
   tcpproxy-cn.ronghub.com:8100</bs><monitor>1610611711</monitor><
   isFormatted>0</isFormatted><joinMChrm>true</joinMChrm><openMp>1</
   openMp><openUS>0</openUS><compDays>0</compDays><connPolicy>1</
   connPolicy><grpMsgLimit>0</grpMsgLimit><extkitSwitch>1</extkitSwitch
   ><gifSize>2048</gifSize><openHttpDNS>0</openHttpDNS><kvStorage>0</
   kvStorage><videoTimes>120</videoTimes><offlinelogserver>http://
   feedback.cn.ronghub.com</offlinelogserver><onlinelogserver></
   onlinelogserver></navi>
```

Creating the actual chatroom is a fairly short request, which directly sends the 5-digit room id back as an answer:

Listing 4.13: Magic Motion Chat Room

```
request:

GET /app/random?max=99999&min=10000 HTTP/1.1
Host: mmapi.vtio.cn
Connection: close
Accept-Encoding: gzip, deflate
Cookie: connect.sid=s%3AF5uEesb85XWzsnXvSMDXYUSjQelPcjzH.lDV9ggvHe2%2
   FpiuwOObstec5nNgPxTQREOA9X%2F3duiTk
User-Agent: okhttp/3.3.0

response:

{
  "success": "true",
  "result": "36962"
}
```

Collected Data

Magic Motion seems to only collect information about the phone the app is run on additionally to the registration data. Given that they also don't seem to save account information this company seems to be fairly safe in terms of data privacy.

4.2.5 Vibratissimo Little Want

General Features

As mentioned in the introduction of this device, while not connected it constantly advertises itself via Bluetooth, by default via the name "Vibratissimo". Although there is a way to change the name of the device and hence the way it advertises itself, it is unfortunately not possible to stop the advertisements unless connected to the device. This means, that one can mask what kind of device it is by changing the name, but if an attacker found out or guessed correctly, they could simply connect to the device.

The "Password forgotten" feature sends an e-mail with a temporary 6-character password that can be used to log in. It doesn't prompt one to change it afterwards, which means if someone's password was reset and they don't proactively change it, it would be easy to brute force the password since there are no limitations to login attempts. However an attacker would first need to find out which e-mail address belongs to which account, as the login is via nickname and the password reset via e-mail address. Furthermore the app is returning the same error message "invalid data" when either nickname or password are wrong, which makes it impossible to find out whether an account exists or not. The password is capped to a maximum of 16 characters which makes brute forcing a user password a bit easier.

To use the remote control feature your partner needs the app, whether you connect via "Quick Control" or the app doesn't matter. In the first case, an e-mail is sent to the supplied address with a URI that looks as follows:

`https://vibratissimo.com/quickControl.php?id=684232744887`

The ID at the end is chosen randomly at every retry and only valid as long as the user doesn't close the "Waiting for RemoteControl" popup. This website has another link that refers you to another URI, that is only understood by the app:

`Vibratissimo://684232744887`

The other possibility to connect remotely is to become friends in the app. To do this, there is a similar search feature as that of the MonsterPub app, which means you can find out all existing users. Once connected, there are two options: to request control over someone's device or to give someone control over your device. For the first option, the remote partner can only accept the offer, if they also have a device connected on their side, otherwise the request is declined. In the latter, the remote partner can simply request control, decide whether they would like to share their device too and if the user is logged in and connected to the device, the remote session automatically starts. There is no setting for a user to turn off being remote controlled or add a prompt to be able too choose whether to accept or decline. Furthermore, it doesn't matter if the user appears as offline to the partner due to hiding their status, as long as the device is connected and the user is logged in, the remote control starts.

tPacketCapture Sniffing

The first analysis again didn't bring much insight, as most packets are transferred via TLSv1.2. Nonetheless, the remote session and chat stream was sent unencrypted via port 5001:

Listing 4.14: Vibratissimo Chat 1

```

R helo:::ffff:80.110.247.156:59808
gm
n ITVoyeur3
c 206888206020
m GChat:accept:1
m Status0:battery:82
m Status0:temperature:16.5
M system:GChat:name set to ITVoyeur3
M system:GChat:joined:206888206020
M system:GChat:rooms count:488
M ITVoyeur2:GChat:toyIDs:
m GChat:toyIDs:0
m Status0:battery:82
m Status0:battery:82
m Status0:temperature:16.5
m Status0:temperature:16.5
M ITVoyeur2:c0:0:75:
M ITVoyeur2:c0:1:75:
M ITVoyeur2:c0:2:75:
M ITVoyeur2:c0:0:78:
```

```
...
```

Listing 4.15: Vibratissimo Chat 2

```
R helo:::ffff:80.110.247.156:59824
gm
n ITVoyeur3
c
no ITVoyeur2 native_chat
M system:GChat:name set to ITVoyeur3
M system:GChat:joined:772524775560
M system:GChat:rooms count:487
M ITVoyeur2:GChat:join:
M ITVoyeur2:GChat:accept:
M ITVoyeur2:Icelink:OFFERANSWER:{"peer_id":"772524775560:ITVoyeur3:
   ITVoyeur2","offeranswer":"{\"sdpMessage\":\"v=0\\r\\no=-
   4186007307445186560 1794700480 IN IP4 127.0.0.1\\r\\ns=IceLink\\r\\
   nt=0 0\\r\\nm=application 1 DTLS\\\/SCTP 5000\\r\\nc=IN IP4
   0.0.0.0\\r\\na=ice-ufrag:ac3cd288\\r\\na=ice-pwd:415
   f4c98a5bbb67cb7563123b006dc8e\\r\\na=fingerprint:sha-256 23:32:93:2A
   :F7:AA:B9:E4:8B:F6:52:39:C9:0F:AC:06:3F:A1:33:63:48:A0:41:D2:C6:66:
   B4:C4:CE:30:E5:51\\r\\na=setup:actpass\\r\\na=sctpmap:5000 webrtc-
   datachannel 1024\\r\",\"tieBreaker\":\"d7134aa1-a25a-45a2-9056-
   aea6eea58815\",\"isOffer\":true}"}
m Icelink:OFFERANSWER:{"peer_id":"772524775560:ITVoyeur3:ITVoyeur2","
   offeranswer":"{\"isOffer\":false,\"sdpMessage\":\"v=0\\r\\no=-
   2155321747260539904 1353992418 IN IP4 127.0.0.1\\r\\ns=IceLink\\r\\
   nt=0 0\\r\\nm=application 1 DTLS\\\/SCTP 5000\\r\\nc=IN IP4
   0.0.0.0\\r\\na=ice-ufrag:939f1318\\r\\na=ice-pwd:
   e1738664431f185b5f8286de080edf07\\r\\na=fingerprint:sha-256 A8:B1:B1
   :78:B0:F1:87:84:F2:2D:D2:86:29:5E:5C:09:7B:6A:D1:58:52:2B:5F:C1:68:
   F5:95:00:D1:8B:C1:2D\\r\\na=setup:active\\r\\na=sctpmap:5000 webrtc-
   datachannel 1024\\r\",\"tieBreaker\":\"bfc4e588-77a3-4890-b1a6-0
   fbdc40fbed3\"}"}
M ITVoyeur2:Icelink:CANDIDATE:{"peer_id":"772524775560:ITVoyeur3:
   ITVoyeur2","candidate":"{\"sdpCandidateAttribute\":\"a=candidate:442
   c8c53b92159a264d58c351de4177e 1 udp 2130706431 192.168.178.20 49164
   typ host\",\"sdpMediaIndex\":0}"}
m Icelink:CANDIDATE:{"peer_id":"772524775560:ITVoyeur3:ITVoyeur2","
   candidate":"{\"sdpCandidateAttribute\":\"a=candidate:3
   d6bb90f1de1f03b925b7589c1f9d528 1 udp 2130706431 192.168.178.28
   29894 typ host\",\"sdpMediaIndex\":0}"}
m Icelink:CANDIDATE:{"peer_id":"772524775560:ITVoyeur3:ITVoyeur2","
   candidate":"{\"sdpCandidateAttribute\":\"a=candidate:063056
   b16db59ca78a7fa854cfbe08f6 1 udp 2130706175 10.8.0.1 7246 typ host
   \",\"sdpMediaIndex\":0}"}
49164\",\"sdpMediaIndex\":0}"}
```

Burpsuite Proxy decryption

One thing that is eye-catching about the Vibratissimo traffic from start to end is that there is no session token used. With each request, the username and password are sent to the server over and over again and in plain text (once SSL is decrypted). This makes it easy for an attacker performing a man-in-the-middle attack to gain the username and password, which he could then use to log into the app to possibly see some private messages or pictures or try the credentials on other platforms in hope to get access to other sensitive information. The Login request looks as follows:

Listing 4.16: Vibratissimo Login

```

request:


GET /userManager.php?action=loginUser&user_login=ITVoyeur2&password=
   SaferS3x%21&reg_id=fPXRMoiJCcQ%3
   AAPA91bG_KqcFGdTaSFCZ8qIYBgTdUWwaYdIUoQJ1zn48t8nnvUmF9gO17aV3bnvSQq
   JhaNVYDG7-Xs-4Ku2-HFWP-
   L679whxjQHpH1CkoON5EePeMPlmztyLRT5Jaa74O4oTCSMi5I0Y&app_version=142&
   device_type=android HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; ONE A2003 Build/
   MMB29M)
Host: vibratissimo.com
Connection: close
Accept-Encoding: gzip, deflate

response:

{"code":202,"message":"User logged in"}

request:

GET /userManager.php?action=getUser&user_login=ITVoyeur2&password=
   SaferS3x%21

response:

{"user_id":"102985","username":"ITVoyeur2","name":"ITVoyeur2","email
   ":"[redacted]","userPicture":"","lastPictureUpdate":"0000-00-00
   00:00:00"}

request:

GET /userManager.php?action=getProfile&user_login=ITVoyeur2&password=
   SaferS3x%21

response:

{"profile_id":"102985","visibility":"1","gender":"0","birth_date":"[
   redacted] 00:00:00","town":"","country":"","introduction":null,"
   allow_email_search":"1","allow_radius_search":"0"}

request:

GET /userManager.php?action=setUnlocked&user_login=ITVoyeur2&password=
   SaferS3x%21&type=multicontrol&enabled=0

response:

{"code":202,"message":"Unlocked status updated."}

request:

GET /userManager.php?action=changeStatus&user_login=ITVoyeur2&password=
   SaferS3x%21&user_status=1

response:

{"code":202,"message":"User data updated"}
```

So after sending the credentials to the server, the latter responds with "logged in" and sends all the profile data associated with the user. The last two exchanges are used to track, whether the app/phone is currently locked or not, the "changeStatus" request sets it to "locked" and the "setUnlocked" sets is to "unlocked".

Neither connecting to a toy nor using the manual control seemed to send any information towards the Vibratissimo servers.

To use the remote control feature, one first has to open the friends list which then gets loaded and then select a friend's profile which in turn gets loaded. Because of the phenomenon mentioned above, that both users need to have a device connected for a remote session unless the initiator chooses not to share their device, the remote client was used to send the remote request to the phone that was being intercepted. This resulted in the following packets:

Listing 4.17: Vibratissimo Remote Session

```
request:

GET /userManager.php?action=friendsList&user_login=ITVoyeur2&password=
   SaferS3x%21&length=100&detail=40&from=0

response:

[{"user_id":"101885","username":"ITVoyeur","userPicture":"","
   lastPictureUpdate":"0000-00-00 00:00:00","status":"0","isSuper
   ":"0","isSub":"0"},{"user_id":"103253","username":"ITVoyeur3","
   userPicture":"","lastPictureUpdate":"0000-00-00 00:00:00","status
   ":"0","isSuper":"0","isSub":"1"}]

request:

GET /userManager.php?action=getProfile&user_login=ITVoyeur3&password=
   dummy

response:

{"profile_id":"103253","visibility":"0","gender":"0","birth_date
   ":"1924-11-22 00:00:00","town":"","country":"","introduction":null,"
   allow_email_search":"1","allow_radius_search":"0"}

receive remote request:
request:

GET /userManager.php?action=isSuper&user_login=ITVoyeur2&password=
   SaferS3x%21&friend_name=ITVoyeur3

response:

{"code":400,"message":"User is not Super"}
```

The chat function must also use another protocol than HTTPS, as no packets were intercepted when using it. This was different for the "message" function, which looks e-mail like in terms of having a subject and a body.

Listing 4.18: Vibratissimo Messaging

```

request:

GET /userManager.php?action=getMessages&user_login=ITVoyeur2&password=
   SaferS3x%21

response:

[{"messages_id":"111496","from_user":"101885","from_user_name":"
   ITVoyeur","to_user":"102985","to_user_name":"ITVoyeur2","subject":"
   test","content":"huhu!"},{"messages_id":"112589","from_user
   ":"103253","from_user_name":"ITVoyeur3","to_user":"102985","
   to_user_name":"ITVoyeur2","subject":"hey","content":"sexy"}]

request:

GET /userManager.php?action=getFriendNames&user_login=ITVoyeur2&
   password=SaferS3x%21

response:

```

```
["ITVoyeur","ITVoyeur3"]

request:

GET /userManager.php?action=getFriend&user_login=ITVoyeur2&password=
   SaferS3x%21&name=ITVoyeur3

response:

{"user_id":"103253","username":"ITVoyeur3","userPicture":"","
   lastPictureUpdate":"0000-00-00 00:00:00"}

request:

GET /userManager.php?action=sendMessage&user_login=ITVoyeur2&password=
   SaferS3x%21&to_user=103253&subject=Re%3A+hey&content=%0Dfind+ich+
   auch%21%0A%0D%0A%3E+sexy%0D%0A

response:

{"code":202,"message":"Message sent"}
```

Last but not least, the "quick control" function via e-mail looks as follows:

Listing 4.19: Vibratissimo Quick Control

```

request:

GET /userManager.php?action=sendQuickControlEmail&user_login=ITVoyeur2&
   email=[redacted]&id=57926592183

response:
```

```
{"code":202,"message":"Quick Control email sent."}
```

Collected Data

Data collected by Vibratissimo is the following:

- Information about the phone used
- Whether the phone is locked or not
- Sex toy battery level and temperature

The periodically updated battery level and temperature of the device might not offer a direct attack vector but could be used by attackers as a control feature if their attack has succeeded or not. By monitoring the battery level and temperature of a device, it can be deduced whether the sex toy is currently inside of or close to a human body and if it is currently active.

Information about the phone used furthermore facilitates an attacker to find potential vulnerabilities of said phone offering another attack vector on a user.

4.2.6 Realov Lydia

General Features

This vibrator is advertised on Bluetooth as "REALOV_VIBE". After starting the app one is directly able to use the manual functions without logging in. This theoretically prevents the company from correlating manual control to an account, which means more privacy.

The app doesn't seem to provide a "password forgotten" feature, so if a password is forgotten a new account needs to be created. There are again no login attempt limitations and at first the error messages seem secure as it only says "invalid username or password". However when trying to log into an account that doesn't exist (e.g. random characters) apparently the account is simply created with the provided password and the user is logged in. So despite the generic error message for an invalid password it can still be determined whether an account exists or not. The maximum password length is 20 characters, which at least makes it a bit harder for attackers to brute force passwords.

The remote control feature can only be used with friends via the app. There is a search function to look for someone, it is not possible to determine if the account exists though, as every input shows up with an "invite" button. This makes it impossible to find out all existing users via the app.

tPacketCapture Sniffing

Of all the findings from analysis part 1, this device offered the most alarming: To generate the token for communication, the username and password are sent in plain text via HTTP. Then a list of joined chatgroups is requested, which is also delivered unencrypted. :

Listing 4.20: Realov Joined Chatgroups

```
POST /realov-lch/realov/token HTTP/1.1
Content-Length: 70
Content-Type: text/plain; charset=UTF-8
Host: 39.97.9.52:80
Connection: Keep-Alive
User-Agent: Easemob-SDK(Android) 2.2.4

{"grant_type":"password","username":"itvoyeur","password":"SaferS3x!"}
   HTTP/1.1 200
Date: Mon, 25 Nov 2019 19:16:49 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

{"access_token":"YWMtISqRLg-4
   EeqptnlS2wBWWnrmK5CpLxHltx0JEWDSwv1QLjKQ9BsR6bD_fzki4G2cAwMAAAFuo_6
   2GQBPGgBeCxTyI4mtZgourA59VLMuUIZTWKY963bTYW3eu105IQ","expires_in
   ":5184000,"user":{"uuid":"502e3290-f41b-11e9-b0ff-7f3922e06d9c","
   type":"user","created":1571673375807,"modified":1571673375807,"
   username":"itvoyeur","activated":true}}
```

```
GET /realov-lch/realov/users/itvoyeur2/joined_chatgroups?detail=true
   HTTP/1.1
Authorization: Bearer
   YWMtcHx2ghj8EeqKA2V9uSSprHrmK5CpLxHltx0JEWDSwv1GhimgBuAR6pMQ_8FkOm_F
    AwMAAAFu4LnhkQBPGgCF3RxzdsUIDfpgrdB1Byz6x_qtVmzw39kkR9Jo3WWs3w
Host: 39.97.9.52:80
Connection: close
User-Agent: Easemob-SDK(Android) 2.2.4

response:

set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Fri, 06-Dec
   -2019 14:18:36 GMT
Content-Length: 374

{
  "action" : "get",
  "application" : "7ae62b90-a92f-11e5-b71d-091160d2c2fd",
  "params" : {
    "detail" : [ "true" ]
  },
  "uri" : "http://39.97.9.52/realov-lch/realov/users/itvoyeur2/
     joined_chatgroups",
  "entities" : [ ],
  "data" : [ ],
  "timestamp" : 1575728316330,
  "duration" : 0,
  "organization" : "realov-lch",
  "applicationName" : "realov",
  "count" : 0
}
```

The rest of the communication was handled in TLSv1.2.

Burpsuite Proxy decryption

Apart from the unencrypted login traffic, there are only many packets sent that look as follows:

Listing 4.21: Realov Parse

```
request api.parse.com/1/classes/hxuser:

{"where":"{\"username\":\"itvoyeur2\"}","limit":"1","_method":"GET"}

response:

HTTP/1.1 410 Parse.com has shutdown - https://parseplatform.github.io/
```

Collected Data

Neither in the traffic analysis nor according to the GDPR answer of Realov is there any indication that any personal data other than account information is sent or stored.

4.3 GDPR Data Inquiry

To find out a bit more about how the chosen brands operate in terms of collecting and storing data, an inquiry about the collected data according to GDPR has been requested.

The E-Mail that was sent looked as follows:

Listing 4.22: GDPR Request

```

Hello!

I have recently bought a <device> and have been a bit worried about
   what data is collected from me.
Could you please send me all data collected about me according to GDPR?
My Username is "ITVoyeur" and I registered with the e-mail I’m writing
   from.

Thank You!
Doris
```

There have been some misunderstandings which are probably results of language barriers and the GDPR being a relatively new regulation.

4.3.1 Sistalk

Sistalk was the first brand to answer my request, unfortunately not the way it was expected:

Listing 4.23: Monster Pub GDPR Reply 1

```
Where did you buy the product from please? and the order number?
```

After replying which webshop the product was bought at and with which order number, there was soon a second reply:

Listing 4.24: Monster Pub GDPR Reply 2

```
Hi, thanks for the confirmation. Libotoy is our official distributor
    and patnter. Can confirm your got a genuine & authentic product with
    our full warranty :) If you got your product from our official
 store / authorized distributor, your personal data and privacy is full
     protected according to GDPR. No worries :) However, there are some
     sellers from Amazon/ebay and other marketplaces selling fake
    copies/ counterfeits, with hacking tech can temporarily connect
 their product with our app, but we are doing our best to block those
    products. If the products are not form our official store/
    authorized partners, there is NO warranty on the product itself as
    well as App access and service. Please rest in ease and enjoy
 our product. Please feel free to contact us if any inquires :) Have a
    good day!
```

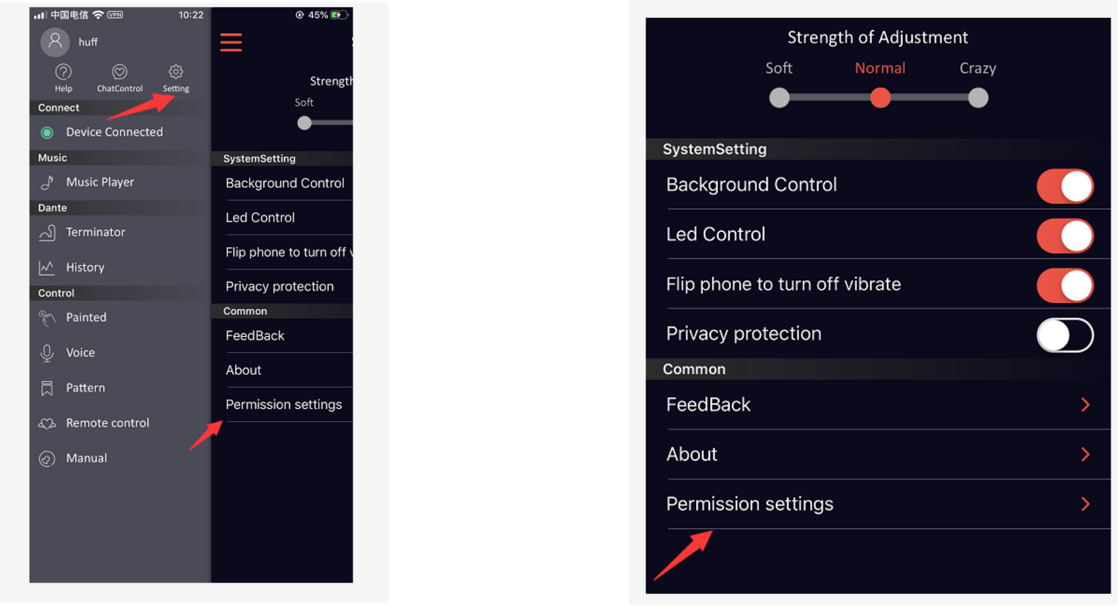
As this didn't exactly answer the original question another reply was sent to clarify the request and inquire about it again. Unfortunately there was no further response even after multiple mails sent.

4.3.2 Magic Motion

Magic Motion was another brand with a case of misunderstanding, even though their answer was good on another level. They have included mostly images, which will be included after the text with "<images>" as a reference to where the images would be:

Listing 4.25: Magic Motion GDPR Reply 1

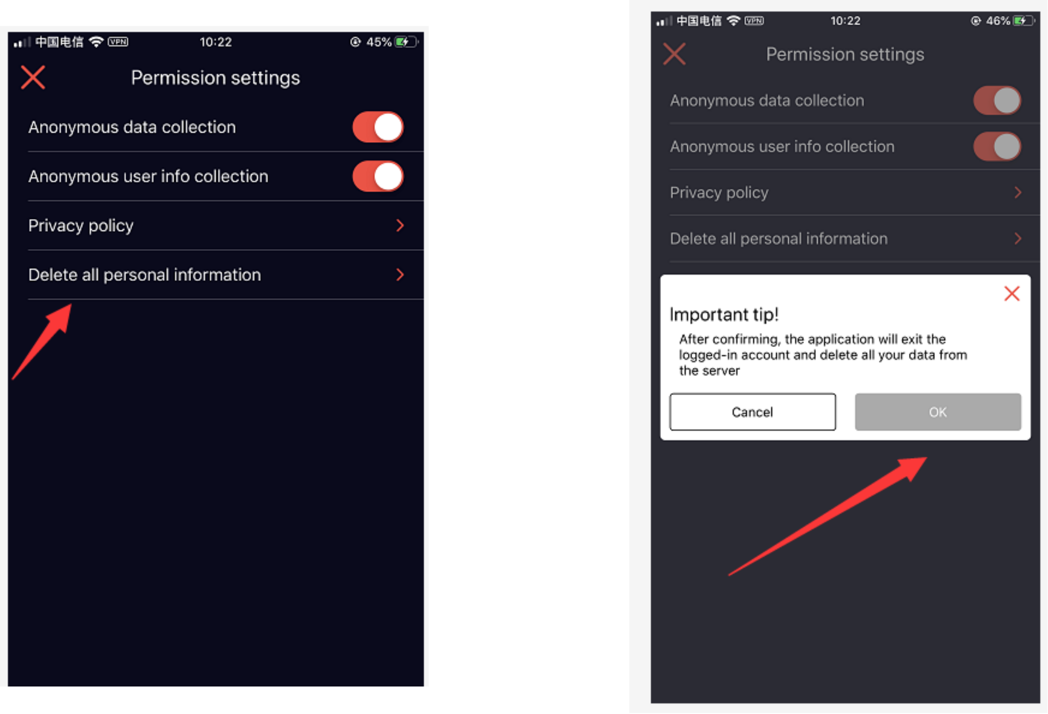
```
hi Doris,
 good day.
pls operate as following
<images>
any questions pls let me know
regards
```



(a) E-Mail image 1

(b) E-Mail image 2

Figure 4.10: Magic Motion GDPR Mail pt. 1


Permission settings
Anonymous data collection
Anonymous user info collection
Privacy policy
Delete all personal information
Cancel
OK

Important tip!

After confirming, the application will exit the logged-in account and delete all your data from the server

(a) E-Mail image 3

(b) E-Mail image 4

Figure 4.11: Magic Motion GDPR Mail pt. 2

As seen on the images they have provided a way to allegedly delete all personal information from the remote servers via the app. Unfortunately them too did not answer my initial inquiry even after multiple tries to clarify my request.

4.3.3 Vibratissimo

As Vibratissimo is a german brand belonging to the company "AMOR Gummiwaren GmbH" the request was in this case written in german so as to minimize misunderstandings due to language barriers. This company was the second one to answer my inquiry and replied within the same day. The response is in german and will be shortly translated after the citation:

Listing 4.26: Vibratissimo GDPR Reply 1

```
Guten Tag Doris,

vielen Dank für Ihre Nachricht. Da wir selber erst die gewünschten
   Daten anfordern müssen, bitten wir Sie um etwas Geduld. Sobald wir
   eine Rückinfo für Sie haben, melden wir uns wieder.

Wir wünschen Ihnen ein angenehmes Wochenende.

Für weitere Fragen, stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen / Kind regards
```

Basically it says that they have to inquire the data in question themselves and will get in touch once they received the information.

A few weeks later they sent another e-mail with the data attached:

Listing 4.27: Vibratissimo GDPR Reply 2

```
Guten Tag Doris,

im Anhang finden Sie die über Sie gespeicherten Daten. Es wird alles
   recht verschlüsselt dargestellt. Wir hoffen Sie können damit etwas
   anfangen.
Es waren keine Daten vorhanden zu folgenden Punkten:
- Blacklist
- Galerie
- mit Passwortschutz registrierte Toys

Für weitere Fragen, stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen / Kind regards

Juliane Stützer
```

This means that the respective data is attached and that there is no data existing regarding blacklist, gallery and password secured toys.

The user data included the nickname, e-mail address, hashed password, creation time, user ID, phone OS and app version. The profile data included the profile ID, gender, country, birthdate and all settings like visibility, allowed to be searched via e-mail or location and status. The messages are saved via a message ID and include the sender and recipient user ID and nickname and the subject and body of the message in plain text. Lastly, the friendship table looks a bit more cryptic, as apart from the user IDs and the key ID which identifies the friendship uniquely, there are a few fields whose meaning could not be accurately assessed. Those field are called "message", "accepted", "super", "chat_request" and "remote_control" and are all numeric fields, possibly for boolean values.

4.3.4 Realov

Realov took about 3 weeks to respond to the request but has so far given the clearest answer with the best outcome in terms of security:

Listing 4.28: Realov GDPR Reply 1

```
Hi Doris,

We only collect registration information, and don’t collect any other data.

Best Regards
```

5 Conclusion

In this thesis, the focus was on examining the state-of-the-art in terms of security of smart sex toys with a focus on the communication between the app and the company servers. There have been discovered quite a few practices that don't fit the standard of today's knowledge about security practices. Considering the topic of intimacy and therefore smart sex toys is personal and sensitive, there should be a higher focus on the security of such devices.

The following table shows an overview of the findings of the traffic analysis:

	MonsterPub	**MagicMotion**	**Vibratissimo**	**Realov**
Protocols	HTTPS	HTTP(S)/Websocket	HTTPS/Port 5001	HTTP(S)
Encryption	✓	Partly	Partly	Partly
Hashed Passwords	✗	N/A	✗	✗
Tokens	✓	✗	Partly	✓
Random IDs	✗	✓	✓	N/A
User Enumeration Prevented	✗	N/A	✗	✓

Table 5.1: Results Overview

As seen in the table, apart from all devices using HTTPS as a protocol for at least parts of the communication, they all had their unique features. This shows that so far there is no "state of the art" in this field of devices yet and a lot of improvement is yet to be made on the security of such products.

Additionally, as Burp Suite was used as a proxy to intercept HTTPS traffic and sign the certificates with its own certificate authority it can be deduced that none of the reviewed products is using certificate pinning in order to avoid man in the middle attacks.

5.1 Future Work

As this research focused on the communication between the app and the company servers, further research has yet to be made on the Bluetooth traffic between the sex toys and smart phones, the hardware and detailed analysis of the web servers of the companies.

List of Figures

List of Tables

Listings

Glossary

BLE	Bluetooth Low Energy
IoD	Internet of Dongs
IoT	Internet of Things
IT	Information Technology
Malware	Malicious computer software
OS	Operating System
SSL	Secure Socket Layer
Teledildonics	Remote controlled sex toys
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

Bibliography

[1] Kevin Ashton, “That ’internet of things’ thing,” 2009, Accessed: 2019-01-23. [Online]. Available: https://www.rfidjournal.com/articles/view?4986.

[2] Stephan Haller, Stamatis Karnouskos, and Christoph Schroth, “The internet of things in an enterprise context,” in *Future Internet Symposium*, Springer, 2008, pp. 14–28.

[3] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh, “Iot security: Ongoing challenges and research opportunities,” in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Nov. 2014, pp. 230–234. DOI: 10.1109/SOCA.2014.58.

[4] George Corser, Glenn Fink, Mohammed Aledhari, Jared Bielby, Rajesh Nighot, Sukanya Mandal, Nagender Aneja, Chris Hrivnak, and Lucian Cristache, *Internet of things (iot) security best practices*, eng, https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf, Accessed: 2019-01-23, 2017.

[5] Knud Lasse Lueth, “State of the iot 2018: Number of iot devices now at 7b – market accelerating,” 2018, Accessed: 2019-01-23. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[6] Anna Lilja Steensig and Jacob Øhrgaard Westh, “Intimate sensory technology in long distance relationships,” 2016.

[7] Matthew Allen Wynn, “Categorizing the security and privacy of"internet of things"devices,” PhD thesis, 2018.

[8] Iain Thomson, “Your ’intimate personal massager’ – cough – is spying on you,” 2016, Accessed: 2019-01-25. [Online]. Available: https://www.theregister.co.uk/2016/08/07/your_sec_toy_is_spying_on_you_hackers_crack_our_plastic_pals/.

[9] Daniel Oberhaus, “The internet of dildos is watching you,” 2016, Accessed: 2019-01-25. [Online]. Available: https://motherboard.vice.com/en_us/article/9a3zdy/dildo-data-hacking.

[10] Elizabeth Armstrong Moore, "Woman sues sex-toy maker for invading privacy," 2016, Accessed: 2019-01-25. [Online]. Available: https://eu.usatoday.com/story/news/2016/09/15/woman-sues-sex-toy-maker-invading-privacy/90400592/.

[11] Peter Treffer, "Sex toys and smart robots: Who's liable?," 2017, Accessed: 2019-01-23. [Online]. Available: https://euobserver.com/science/137456.

[12] Internet of Dongs, eng, https://internetofdon.gs/about/, Accessed: 2019-01-25.

[13] Kyle Machulis, eng, https://buttplug.io/, Accessed: 2019-01-23.

[14] Joseph Cox, "We anonymously controlled a dildo through the tor network," 2017, Accessed: 2019-01-25. [Online]. Available: https://motherboard.vice.com/en_us/article/wjnwgb/we-anonymously-controlled-a-dildo-through-the-tor-network.

[15] Ricochet, eng, https://ricochet.im/, Accessed: 2019-01-24.

[16] Sarah Jamie Lewis, "Oniondildonics: Securing sex toys using privacy-preserving protocols," 2017, Accessed: 2019-01-23. [Online]. Available: https://mascherari.press/oniondildonics/.

[17] Jordan Rabet, eng, https://www.youtube.com/watch?v=CsQ2VWEfduM, Accessed: 2019-12-08.

[18] Matthew Wynn, Kyle Tillotson, Ryan Kao, Andrea Calderon, Andres Murillo, Javier Camargo, Rafael Mantilla, Brahian Rangel, Alvaro A Cardenas, and Sandra Rueda, "Sexual intimacy in the age of smart devices: Are we practicing safe iot?" In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, ACM, 2017, pp. 25–30.

[19] Mike Ryan, eng, https://github.com/mikeryan/crackle, Accessed: 2019-01-24.

[20] Twilio, eng, https://www.twilio.com/, Accessed: 2019-01-24.

[21] PubNub, eng, https://www.pubnub.com/, Accessed: 2019-01-24.

[22] Werner Schober, *Iod - internet of dongs - a long way to a vibrant future*, 2018.

[23] ——, "Internet of dildos: A long way to a vibrant future – from iot to iod," 2018, Accessed: 2019-01-25. [Online]. Available: https://sec-consult.com/en/blog/2018/02/internet-of-dildos-a-long-way-to-a-vibrant-future-from-iot-to-iod/.

[24] Internet of Dongs, eng, https://internetofdon.gs/code-of-conduct/, Accessed: 2019-12-08.

[25] Taosoftware, eng, `http://www.taosoftware.co.jp/en/android/packetcapture/`, Accessed: 2019-12-05.

[26] Crunchbase, eng, `https://www.crunchbase.com/organization/easemob`, Accessed: 2019-12-05.

[27] Rose Minutaglio, "Is your sex toy spying on you?," 2019, Accessed: 2019-12-08. [Online]. Available: `https://www.elle.com/culture/tech/a28846210/smart-sex-toy-dildo-butt-plug-hacking/`.

[28] Vtrump, eng, `http://www.vtrump.com/`, Accessed: 2019-12-07.