Bluetooth (Low Energy) and Security

or sensors, privacy and security in general

We have an increasing amount if sensors in our environments. We can monitor our house and adjust the heating, control the lighting or have a look with a camera. All from a distance using our smartphone. Sensors play an important role in all of this. But when others can access that data as well it poses a threat to privacy and security.

secureapps

Author	Matthijs de Vries
Date	Februari 24, 2015
Created for	secureapps.eu

Context

This document is based on a combination of hands-on experience with Bluetooth Low Energy (BLE) and literature review. Many of the issues are however applicable to all wireless connected sensors or devices that do not have an internet connection at their disposal.

Bluetooth Low Energy, also called Bluetooth Smart, is a relatively new but it is increasingly finding its way into sensor technology and home appliances. Together with traditional Bluetooth, NFC (near field communication) and Wi-Fi solutions are filling up our living and working environments with connective devices and sensors. The internet of things is becoming a reality and seems to be gaining momentum. This also sparks new interest in the privacy and security of those devises. A lot of those devices are made for easy, unobstructed use and not with security in mind. This can have some unexpected side effects.

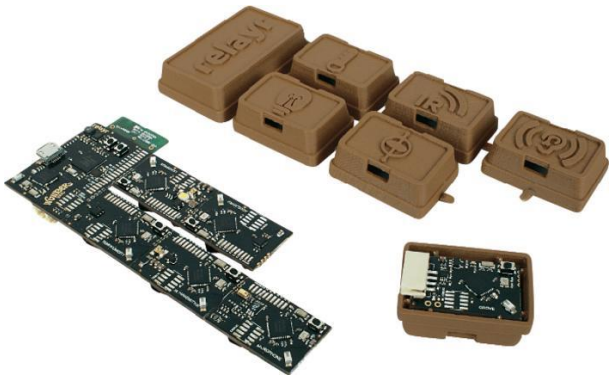
This document is meant to generate awareness not to trigger a sense of alarm. Every technology comes with weaknesses, that's just how it is. Knowing the issues will allow you to make better decisions. Security is about the exception, about the few who want to do harm.

Current Developments

In our currents world some examples are already a normal part of life. Security systems are in a lot of cases already controlled by our smartphone. We can control the heaters in our house. Many basic functionality is already offered with home automation systems like Home Wizard.

Lately multiple new initiatives have seen the light. These test beds and starter kits will likelly trigger new ideas and developments. Products like the Wunderbar by Relayr, the SensorTag by Texas Instruments, or the new Airboard are examples of products like that. They're not ready to use products as such but meant for developers and creative people to create their own products.

- http://www.theairboard.cc/
- https://relayr.io/
- http://www.ti.com/tool/cc2541dk-sensor



Some of these products are also accompanied with SDK's and example code for the mobile platforms Android and iOS. Without too much additional expertise a mobile developer can develop application that will use data from the sensors.

General Technical Issues

The Bluetooth Low Energy stack was introduced with version 4.0 in 2010. This relatively short period also means that not all platforms have the same maturity level. Apple has been ahead of the competition a bit because it has been pushing iBeacon technology, Android has been lagging behind a bit, only adding support in recent versions.

This has the effect that Android support is still not as wide spread as you might have liked. In versions 4.3 and 4.4 there have been bugs like freezing the device when getting near an iBeacon. Adaption is however picking up and the latest versions have better support.

Power Consumption

One of the biggest issues with the widespread usage of sensors and Bluetooth in general was the power needed. Wiring up a dozen standalone sensors, even in your own home, was not acceptable. Using batteries was either too bulky, too expensive or battery life was much too short. With the new BLE standard this issue was addressed.

BLE was a big paradigm shift for the Bluetooth standards. Instead of aiming for higher bitrates, as in the previous versions, the focus was moved to energy consumption. When it comes to placing those standalone sensors this is of course a huge step forward. Batteries would have to be changed every couple of days and this was a problem. BLE sensors, depending on hardware and configuration, can go on for months. This makes using this kind of technology far more attractive.

Updating Devices or Firmware

One of the general issues with many Bluetooth devices is the lack of updating possibilities. House hold appliances, automotive applications or sensor technology rarely get updates after having been sold. Either because it isn't possible or because people just don't take the time or know it is possible. This means a growing amount of devices will be running old software or firmware.

Smart phones receive regular updates as they are often connected with the internet and tend to grow out of fashion within a few years anyway. Many other products like headphones, toothbrushes or speaker systems will grow out of fashion far slower and be around for much longer. Although updates are needed far less often when, for some reason, they are needed, possibilities are limited. Although it is possible, it is far harder to get people to check and actually perform the updates.

Dealing with callback situations can be expansive and not very effective. For a lot of devices this might never be needed, but when it comes to devices that might yield privacy sensitive information this could proof to be a problem. A health monitoring device with broken security is a problem. Now what?

You could invest in mechanisms to update firmware and educate the user to do so regularly. You could also make an educated guess and sell the product with an expiration date (the sensors might degrade as well, making this a good approach). A health monitoring device should be used for no longer than two years, after that quality or privacy are not guaranteed anymore. Or come up with another approach altogether.

Lacking Security

Confidentiality

Confidentiality can actually be provided with Bluetooth communications. It is possible to encrypt the data exchange between devices. There are however known weaknesses and many device use the none encrypted mode. There are known attacks that would possibly allow for sniffing BLE traffic, have a look at the following article.

Bluetooth: With Low Energy comes Low Security

Many BLE devices are not connected to the internet, exchanging keys thus requires a non-encrypted or pre-programmed first step and two-factor mechanisms are not possible. This means that sniffing or man-in-the-middle are possible attacks. For most situations the security offered will be good enough for BLE devices but when used in combination with, for example, medical applications there might be issues.

Authentication

This is hard when it comes to devices that have no internet connectivity. With most products you don't know who is going to buy it, and whoever buys the device should be able to use without much trouble. Most devices will allow to be connected with every smartphone. Sometimes a PIN is required, which can ensure confidentiality but provides no authentication. Especially when data is used beyond the two paired devices and is send over the internet or to a cloud solution.

Authentication requires predetermined public and private key pairs that are either exchanged in advanced or using a third party. The first has the disadvantage of having the private key on the device from the moment it leaves the production plant, maybe someone will be able to get it from the device. The second has the disadvantage of needing a way to communicate with the third party, most likely needing an internet connection.

Adding a second factor can increase the level of authentication. In addition to the hardware ID there could be an identifying number printed on the device or the packaging. When using a mobile app the user will be asked to enter this code. The server can now check wether the combination of hardware and printed ID are valid. Although not the most secure method it does add a level of authentication.

In some cases a button on the device needs to be pressed before the device will advertise itself. This way the devices needs to be close and a human action is needed additionally. This will provide some assurance the right devices are paired.

Authenticity and Integrity

Is the data you are getting from a Bluetooth or mobile device valid data from the right party? Technology like the iBeacon uses UUIDs that allow identification. It is technically fairly easy to impersonate a Bluetooth device, especially when they are standalone devices. This makes it hard to know for sure that your getting data from the right device. This is called spoofing.

When pairing with a device using your smart phone you can be fairly sure you are connecting to the device you are seeing (although not 100%). But you might not know who placed it there, was it Coca-Cola or Philips as advertised or someone impersonating their beacons? Maybe a cheap rip-off brand of soda will announce itself as a Coca-Cola fending machine.

Spoofing

It is certainly possible to impersonate an iBeacon, this had been done already and without too much effort. This is an inherent problem because many BLE devices actively advertise themselves to potential interested parties.

One way of countering spoofing is combining data. For example an additional code on the device of packaging might need to be required when registering a device. This adds a second channel. Thought it is not the most secure channel it does require additional information to get all data. Simply eavesdropping is not enough. You need to have the device to show you actually have it. The weakness of course is that having had it at some moment in the past is enough as well. All data also needs to be available for conformation on a server. Your app has to verify with the vendor's server that the Bluetooth ID and the additional code are an expected match.

It is also possible to temper with the sensors themselves. When this data is used for billing, indoor climate control or health monitoring this might be an issue. When using sensors to determine energy usage it might be very lucrative to tweak the thermometer a bit, saving you 10% on the energy bill. You create your own sensor, spoofing the original id's, and start using your own sensor to gather energy usage data.

Non-repudiation

This is about accountability. It is about supplying proof that something did actually happen. When billing someone you want to know if a product has been delivered or if a service actually has been provided. Especially when later on someone denies having used your service and refuses to pay. When you don't have any proof you will lose that discussion.

Bluetooth, or wireless connectivity in general, can play an important role in service delivery. Sensors can be very useful in determining who used it, for how long or how many times. Car sharing services might rig their cars with iBeacons and use a rental app to determine usage and bill accordingly.

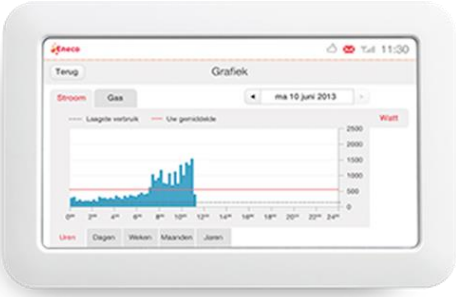
With standalone, non-internet connected devices non-repudiation will be a problem. Devices with internet connection could offer mechanisms to ensure non-repudiation.

It is possible to add mechanisms where, for example, additional interaction is needed. The same car sharing service might require the user to explicitly confirm her presence in the car before a code will be presented to start the car.

Privacy Issues

Sensor Data Issues

Sensor data can sometimes tell you a lot about the ones using the sensors. For example: controlling in-house climate to safe energy depends on temperature measurements. Knowing that the temperature drops off between 8:30 and 18:30 will tell you when someone's at work and not at home. This might obviously be useful information for a burglar.



Healthcare devices are also increasingly using BLE connectivity. Eavesdropping on this might yield more privacy sensitive data. It could only be about your exercising habits but also might be about a heart condition. This can be very privacy sensitive and might need additional protection.

Using Bluetooth in home or office security might work nicely, but monitoring the presence of Bluetooth devices will also give you points that are not equipped with sensors. There will be a heartbeat mechanism to ensure all sensors are up and running. That will give away the exact positions of all the sensors and, maybe even more useful, the locations where no sensors are placed.

Similarly the known usage of headphones, sound systems, shaving devices or toothbrushes will tell you a lot about a household. Especially when all this data is combined. Knowing what devices you are using might be very useful for targeted advertisement.

Bluetooth Discovery Issues

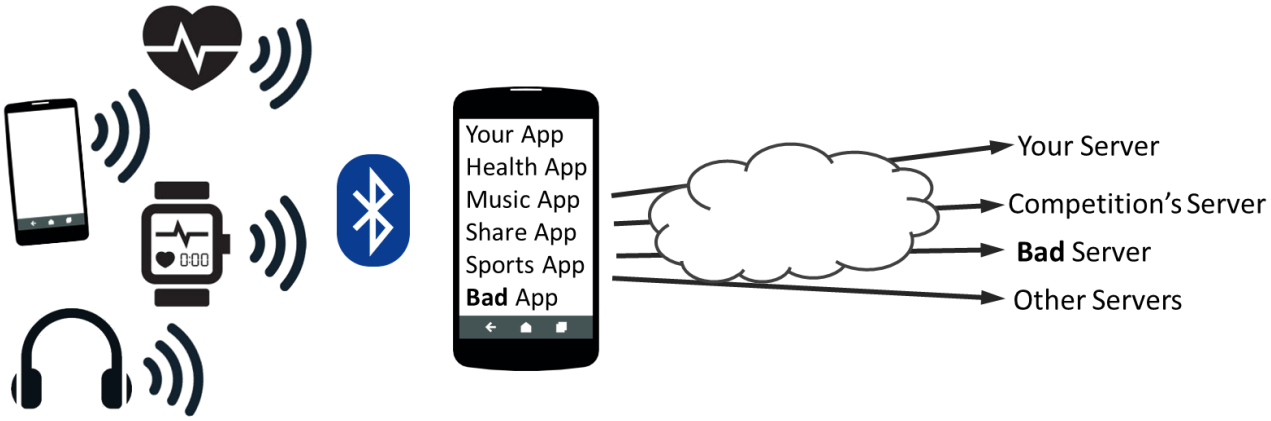
BLE devices present themselves to the world in order to be connected to. This is inherent to the way this technology works and therefore largely unavoidable. There already have been examples where thieves have been using smart phones to check cars for left devices. Knowing what devices are active and where those device are can be valuable information. With more and more household appliances getting BLE connectivity there are also new data harvesting options.

"*iOS doesn't allow to sense iBeacons around if you ignore their Proximity UUID; in other words, you need to know the Proximity UUID of the iBeacons beforehand in order to detect them; on the contrary, Android allow you to see any iBeacon regardless of its Proximity UUID.*" iBeacon Bible 2

A mobile device can scan for available B(LE) devices and send this information back to an interested party. The user of this device has a:

- Braun Shaving Device
- Philips Toothbrush
- Logitech Headset
- Home Automation equipment
- Samsung tablet

Having this kind of information opens up new possibilities in direct marketing. Knowing what you own and possibly knowing how much it is being used can be the trigger to offer you specific information. You have three Philips devices and a Logitech device, maybe this user should be presented a consumer test where Philips speakers outperform those made by Logitech. It can, and will, of course be used against you as well, other parties will harvest information as well. Prepare for it.



Wardriving

Listening devices passing near your house can possibly pick up on BLE devices and have look at what is available. This would allow for BLE wardriving, scanning for devices while in a moving vehicle. Examples and tools are available.

Google, for example, has been mapping WiFi data while capturing imagery for Street View. When updating their data they might also target Bluetooth devices as well. Of course other parties can do the same. Using the burglar as an example again: they could check houses for the equipment they would like to acquire and use this to select their next target. There are also some examples where drones where used. With the current dropping prices of drones this is not as farfetched as you might like to think.

Reverse Beacon

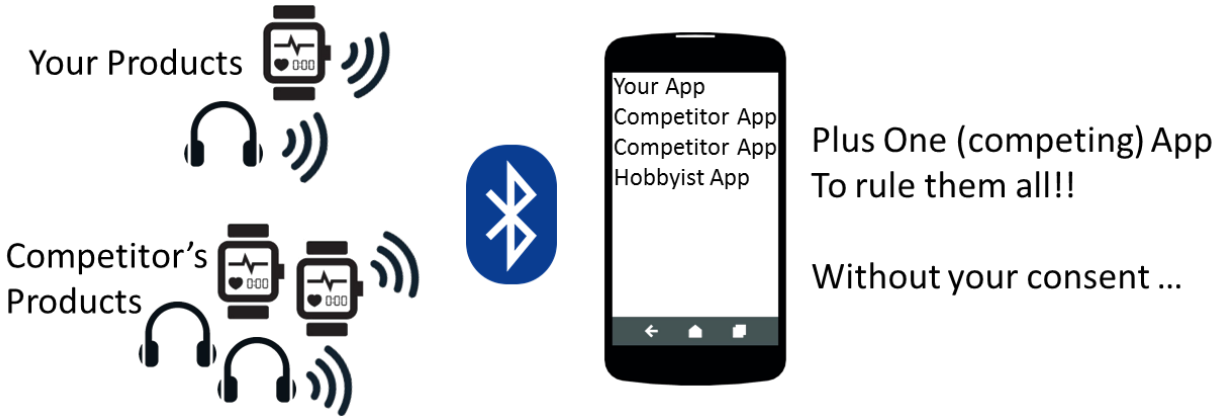
BLE Beacons can be used for determining your location in indoor situations where GPS is not available. The iBeacon by Apple is a popular example. The position of the beacon is known and your proximity to it can be calculated. Using the unique identifier, a device can look up this beacon and perform certain functions. In a museum you could, for example, get all information on the piece you are standing in front of at that moment.

Beacon technology can be reversed as well. You can, for example, sell BLE devices with beacons and use the connecting device to determine the location of your beacon. When the device looks up the beacon it will send its last known location and possibly other information.

So simply adding reverse-beacon-like technology can potentially tell you a lot about where and when your devices are being used and by who. This offers a lot of possibilities but can of course pose privacy issues as well. An extreme example: What if your wife sees a message of a toothbrush running low on batteries when, at home, you have a completely different make and model? Or she is able to see that you shaving device is being used a couple of blocks away several times a month.

Functional Hijacking

Bluetooth devices or sensors could, in many cases, also be used by other parties as well. This might result in, for example, other mobile apps using your sensors or devices.



Philips offers a mobile app that will connect with a Philips Speaker to enable additional functionality. It is however fairly simple to decompile mobile applications, notably Android, and have a look at the inner workings of an app. This will enable other people to create a similar app as well. They might also take it a step further and offer a mobile app that will combine support for Philips devices but also for Logitech, Bose or any other brand with connective devices. An app like that might be more interesting for users than your own targeted app. This can of course be an opportunity as well and isn't necessarily a bad thing.

Unexpected Effects

New technologies can sometimes be utilised in unexpected ways. The easiest way to explain is by using a recent example. A couple of months ago a story was published where researchers showed that is possible to use a smartphone to eavesdrop one someone. Not by using the microphone but by using the its gyroscope. It turned out that this sensor was sensitive enough to pick up sound waves as well.

http://www.wired.com/2014/08/gyroscope-listening-hack/

While a device owner has to give permission to use certain sensors, this particular sensor wouldn't have been considered dangerous in any way and could be used without permission.

But what if sensors in a toothbrush or a shaving device become sensitive enough to become listening devices? What if a Philips or Bose device turns out to be used as a listening device by another app? Would Philips, or Bose for that matter, know how to react and do something about it?

Sensors or devices might be used in ways that were not anticipated. Preparing for the unknown is of course not possible. You can however anticipate the fact that you will need to react to something at some point. Quick update possibilities and clear communication channels are examples on how to anticipate and react swiftly when something does occur.

Dealing with the Issues

Bluetooth as a technology is not, on itself, the reason why we have seen the issues described in this document. When needing to communicate with sensors, household appliances or other mobile devices BLE is one of the most suitable techniques. The need for stand-alone, low power devices also reduces the possibilities to create a secure environment. Finding the right balance will be the challenge.

A Bluetooth Smart device can be a very capable, internet connected smartphone which will be capable of supporting complex security mechanisms and communicating with third parties. A Bluetooth Smart device can also be a temperature sensor with the basic capability of sending information to any interested receiver. Between the two a huge range of possibilities lay.

The not very satisfying answer is that, for now, each situation will have to be looked at separately. What are the devices capable of? What is the context in which the devices and sensors will be used? What developments do we expect in the near future? What level of security is required? What do the laws and regulations expect?

Developments will go fast and speed up in the coming period. The internet of things, interconnecting heaps of useful devices, sensors and actors seems to gain momentum. Along with many great applications, security and privacy will also become more important. Being aware of this is the first and most important step. Bring security into the development of a new product or service from the beginning.