Blog of Adam Warski

Java, Scala, programming, ...

How do iBeacons work?

By Adam Warski 13 January, 2014 71 Comments

iBeacons are certainly a trending topic recently. They allow indoor positioning, letting your phone know that you are in range of a beacon. This can have many applications: from helping you to find your car in a parking garage, through coupons and location-aware special offers in retail, to a whole lot of apps that we can't imagine right now.

There are many posts about what iBeacons are and what can be done with them, but from a technical perspective, how do they work? The underlying technology is Bluetooth LE, so …

What is Bluetooth LE?

Bluetooth Low Energy (BLE, official page, wikipedia) is a part of the Bluetooth 4.0 specification, which was released back in 2010. It originated in 2006 in Nokia as Wibree, but has since been merged into Bluetooth. It is a different set of protocols than “classic” Bluetooth, and devices are not backwards-compatible. Hence you can now encounter three type of devices:

- **Bluetooth**: supporting only the “classic” mode
- **Bluetooth Smart Ready**: supporting both “classic” and LE modes
- **Bluetooth Smart**: supporting only the LE mode

Newer smartphones (iPhone 4S+, SG3+), laptops, tablets, are all equipped with full Bluetooth 4.0 and hence “Smart Ready”. Beacons, on the other hand, only support the low energy protocols (which allows them to work on a single battery for a really long time) and hence they implement “Bluetooth Smart”. Older devices, like peripherals, car systems, older phones usually support only the classic Bluetooth protocol.

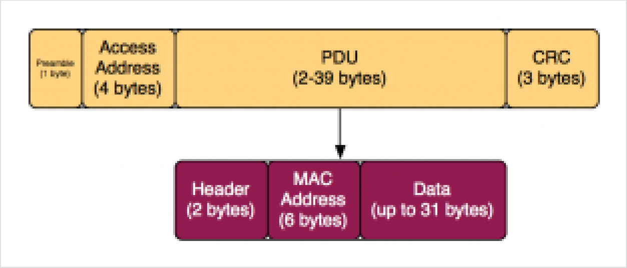
The main focus in BLE is of course low energy consumption. For example, some beacons can transmit a signal for 2 years on a single cell battery (the batteries are usually not replaceable, you’ll probably just replace the beacon when they stop working). Both “classic” and LE Bluetooth use the same spectrum range (2.4 GHz – 2.4835 GHz). The BLE protocol has lower transfer rates, however it’s not meant to stream a lot of data, but rather for discovery and simple communication. In terms on range, both LE and “classic” Bluetooth signal can reach up to 100 meters.

How does BLE communication work?

BLE communication consists of two main parts: **advertising** and **connecting**.

Advertising is a one-way discovery mechanism. Devices which want to be discovered can transmit packets of data in intervals from 20 ms to 10 seconds. The shorter the interval, the shorter the battery life, but the faster the device can be discovered. The packets can be up to 47 bytes in length and consist of:

- 1 byte preamble
- 4 byte access address
- 2-39 bytes advertising channel PDU
- 3 bytes CRC



For advertisement communication channels, the access address is always `0x8E89BED6`. For data channels, it is different for each connection.

The PDU in turn has its own header (2 bytes: size of the payload and its type – whether the device supports connections, etc.) and the actual payload (up to 37 bytes).

Finally, the first 6 bytes of the payload are the MAC address of the device, and the actual information can have up to 31 bytes.

BLE devices can operate in a non-connectable advertisement-only mode (where all the information is contained in the advertisement), but they can also allow connections (and usually do).

After a device is discovered, a connection can be established. It is then possible to read the services that a BLE device offers, and for each service its characteristics (this is also known as an implementation of a GATT profile). Each characteristic provides some value, which can be read, written, or both. For example a smart thermostat can expose one service for getting the current temperature/humidity readings (as characteristics of that service) and another service and characteristic to set the desired temperature. However, as beacons don't use connections, I'll skip the details. If you want to read more about connecting to BLE devices, Apple's Core Bluetooth guide provides a good overview, even if you are not an iOS developer. For articles which are even more technical, take a look at EE times (Introduction to BLE, Making the most out of BLE advertising mode).

How do beacons use BLE?

Beacons use only the advertisement channel. As the “beacon” name suggests, they transmit packets of data in regular intervals, and this data can be then picked up by devices like smartphones. Hence iBeacons are simply a specific usage of BLE advertisements, with some additional support on the iOS side.

If you try to intercept an iBeacon advertisement packet, for example coming from an Estimote beacon, you’ll see the following data:

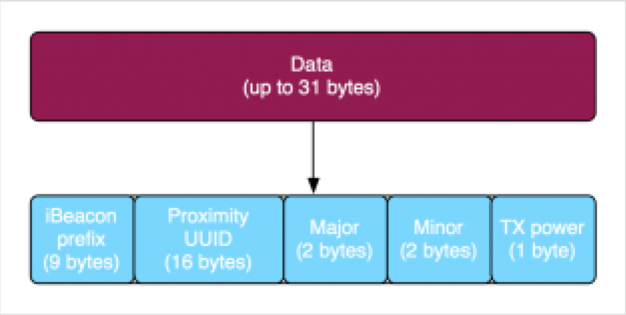
```
02 01 06 1A FF 4C 00 02 15 B9 40 7F 30 F5 F8 46 6E AF F9 25 55 6B 57 FE 6D 00 49 00 0A C5
```

(to capture such data, if you have OSX, an additional XCode download contains a Bluetooth scanner and a packet logger. For Windows, see for example here)

The data above already has the preamble, fixed access address, advertisement PDU header and MAC address removed; it is only the advertisement data – 30 bytes, so it fits nicely in the 31 byte limit.

What makes a BLE advertisement an iBeacon one? The format is fixed by Apple. To break it down (see also SO):

```
02 01 06 1A FF 4C 00 02 15: iBeacon prefix (fixed except for 3rd byte - flags)
B9 40 7F 30 F5 F8 46 6E AF F9 25 55 6B 57 FE 6D: proximity UUID (here: Estimote’s fixed UUID)
00 49: major
00 0A: minor
C5: 2’s complement of measured TX power
```



What follows is that if you want to experiment with beacons, you don’t really need any special devices. If you have a newer phone (e.g. iPhone 4S+, SG3+) or a Bluetooth 4 laptop (e.g. Retina MacBook), you can turn any of these devices into an iBeacon transmitter and receiver. For iPhones, see for example the “Locate iB” app in AppStore. For MacOS, see here. And of course, you can use Raspberry Pi as a beacon as well.

Breaking down the iBeacon format

Apart from the mostly fixed iBeacon prefix (`02 01 ... 15`), what is the meaning of the other components?

The **proximity UUID** (`B9 ... 6D` in our example), is an identifier which should be used to distinguish your beacons from others. If, for example, beacons where used to present special offers to customers in a chain of stores, all beacons belonging to the chain would have the same proximity UUID. The dedicated iPhone application for that chain would scan in the background for beacons with the given UUID.

The **major number** (2 bytes, here: 0x0049, so 73) is used to group a related set of beacons. For example, all beacons in a store will have the same major number. That way the application will know in which specific store the customer is.

The **minor number** (again 2 bytes, here: 0x000A, so 10) is used to identify individual beacons. Each beacon in a store will have a different minor number, so that you know where the customer is exactly.

Measuring distance

The final field, **TX power**, is used to determine how close you are to a beacon. This can be presented either as rough information (immediate/far/out of range) or as a more precise measurement in meters (you can convert to feet of course ;)). How is it done?

The TX power (here: 0xC5 = 197, 2's complement = 256-197 = -59 dBm) is the strength of the signal measured at 1 meter from the device (RSSI – Received Signal Strength Indication). As the strength of the signal decreases predictably as we get further, knowing the RSSI at 1 meter, and the current RSSI (we get that information together with the received signal), it is possible to calculate the difference. iOS has this built-in, for other platforms, it needs to be hand-coded, see this SO answer for a specific algorithm.

Obstacles such as furniture, people or communication congestion can weaken the signal. Hence the distance is only an estimate.

iOS integration

iOS comes with some additional integration with iBeacons. Your app can receive notifications when a beacon comes into range – but not only when the app is in the foreground, also when it is in the background! An app can subscribe to region enter/exit events, so that it is partially woken up even if it isn't running. In response to such events, the app can send e.g. a local push notification, prompting the user to open the app and see the in-store promotion (which can be for example fetched from the internet), or other relevant content.

More precisely, when the phone isn't active, iOS goes into a low-power **monitoring** mode: only iBeacon region enter/exit events are detected. When the phone and app are active, you can enter **ranging** mode, which enables you to detect the signal strength and estimate the distance more precisely.

Note that it can take some time for your phone to detect a beacon. Firstly, the beacons transmit the advertisements from time to time. Secondly, if your phone isn't active, it monitors for bluetooth signals only sometimes as well. For a beacon to be detected, these two intervals must overlap. In practice, it can take up to 15 minutes to detect a beacon.

For a step-by-step guide to writing an iOS iBeacon application, see here. Beacon manufacturers also often provide dedicated SDKs which help in writing beacon-enabled applications. See for example Estimote's iOS SDK and Android one.

How can I get some beacons?

Beacons are currently a scarce resource; you often have to wait a couple of weeks to get some; but certainly availability will become better and better.

Hence the fastest option is to build a "softbeacon": turn your iPhone/Android/MacBook/other laptop/RaspberryPi into one (as described above).

Your second option is to try and order some beacons:

- pre-order Estimote beacons; 3 for $99
- Kontakt beacons come in a couple of packages; 4 for $99, 10 for $279
- RaspberryPi kits from RadiusNetworks: 1 for $99
- RedBearLab offers BLE shields for Arduino for $30
- Bleu sells USB-iBeacon dongles. 1 for $40, 5 for $150

Alternatives

iBeacons isn't the only proximity BLE-based technology. Qualcomm is developing its own beacons, Gimbal, together with iOS and Android SDKs. They will offer a similar feature set, however the format of the BLE advertisement may be different. My developer kit is on its way, so I haven't tested them yet, but the beacons certainly look interesting – especially because of the pricing – **$5/basic beacon**.

What's next?

Now the only thing left to do is to develop some beacon-enabled applications! For this purpose, keep SoftwareMill in mind: we are always on the lookout for interesting projects just waiting to be developed :).

SOFTWAREMILL

SHARE THIS:

Twitter LinkedIn Google Facebook 87 Reddit Email Pocket

Categories: **Blogroll**, **Bluetooth**, **different**, **iBeacon**, **Uncategorized**

71 Comments **Blog of Adam Warski** 1 **Login**

♡ **Recommend** 1 Tweet Share **Sort by Best**

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

saipavan rapolu • 5 years ago

hi, iam new to the ibeacon concept, can you please give any sample code for working with roximity ibeacon for android...pls

2 ^ | ˅ • Reply • Share ›

John Bachman ➦ saipavan rapolu • 3 years ago

Here you go saipavan: https://github.com/xamoom/x...

^ | ˅ • Reply • Share ›

^ v • Reply • Share ›

Neil Young • 5 years ago

Nice blog.

You wrote:

"This happens if the app goes in to the background if you don’t tell iOS to keep the BT service running."

From my experiences it is not possible to keep the iBeacon advertisement alive, if the app goes into the background. Do I miss something?

2 ^ v • Reply • Share ›

Adam Warski Mod ➦ Neil Young • 5 years ago

Which fragment do you mean exactly?

If it's the one I think it is, then I meant the other way round - when the phone is the receiver, not the transmitter. iPhone listens to BT advertisements all the time (when BT is on), and even if the app is in the background, it is woken up for a short period of time if an advertisement is received.

2 ^ v • Reply • Share ›

captaink99 ➦ Neil Young • 5 years ago

I would assume that once the app assumes initial connection with the Beacon -- then the beacon can talk to the device even if the app goes into background mode.

^ v • Reply • Share ›

Adam Warski Mod ➦ captaink99 • 5 years ago

There's no "connection" really, beacons simply transmit (like a lighthouse). Although iOS can treat beacon signals seen previously differently from new ones.

^ v • Reply • Share ›

Tickto • 2 years ago

Nicely written detailed blog post.

^ v • Reply • Share ›

ashish • 2 years ago

I want to scan and connect with a beacon through java program (as my machine is bluetooth enabled so I think there wont be an issue) but don't have an idea from where to start. though for android and IOS there are plenty of tutorial and libraries.

⌃ | ⌄ • Reply • Share ›

Doni Winata • 3 years ago

Hi adam, nice post :) ,can you help me to answer this question.. do you know if apple watch is able or not to become beacon (broadcaster) and then after some circumstance it will establish BLE connection and then stop broadcasting data ? i mean it is like change status from broadcaster and then do pairing mode, thank you adam

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Doni Winata • 3 years ago

Sorry, but I don't know

⌃ | ⌄ • Reply • Share ›

Doni Winata ➦ Adam Warski • 3 years ago

No problem, Thanks for replying adam, much appreciated :)

⌃ | ⌄ • Reply • Share ›

Alsey Coleman Miller ➦ Doni Winata • a year ago

It wasn’t, but with the new WatchOS version all CoreBluetooth APIs are supported.

⌃ | ⌄ • Reply • Share ›

Kevin O'S • 3 years ago

Hi Adam, I've just come across your blog and this post is really interesting! I'm hoping you'll be able to help me with a question I have related to iBeacons. A client of mine is very persistent in using iBeacons for advertising purposes. At the moment their app doesn't have push notifications enabled, I can see this through looking at the settings on the app. For the technology to work, does the app need to have notificatoins enabled and also the user to have accepted these notifications? Thanks for your help. Kevin

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Kevin O'S • 3 years ago

You don't need notifications (in iOS I assume) to be enabled for the app to be woken up by a nearby ibeacon. However you probably do need notification (local, not push) to be enabled ot be able to communicate with the user somehow probably do need notification (local, not push) to be enabled or be able to communicate with the user somehow

⌃ | ⌄ • Reply • Share ›

Kevin O'S ➦ Adam Warski • 3 years ago

Thanks for coming back on this Adam! Much appreciated! Kevin

⌃ | ⌄ • Reply • Share ›

Jianan • 3 years ago

Hi！About a year ago, I found this blog post when I developed iBeacon.It help me most to understand How iBeacon working.It's amazing that I never found in China.So I translated it to Chinese and posted it to here:http://blog.csdn.net/qinxia... .Of course, I keep your name and your website link at the translation's head. I hope this translation can help more Chinese Developer, and in fact, it's true.
But I am aware of that I translated your post without telling you first maybe violate your right.I'm sorry to tell you this late, but I still hope you can allow me to keep this translation for most Chinese which need.If you feel that's bad, I'll delete it.I'm sorry to make this trouble for you:(

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Jianan • 3 years ago

No problem, thanks for letting me know and posting the link!

⌃ | ⌄ • Reply • Share ›

Jianan ➦ Adam Warski • 3 years ago

So kind of you.Thanks for your support! :)

⌃ | ⌄ • Reply • Share ›

Mike Tallent • 4 years ago

I found these for $6.00 http://www.aliexpress.com/s...

⌃ | ⌄ • Reply • Share ›

Güliz Seray Tuncay • 4 years ago

Hi. Thanks for this very good article. However, I think there is a mistake in here. According to this post http://stackoverflow.com/qu... (and also from what I observed), it isn't true that the iBeacon prefix is fixed. Only the last two bytes are fixed and can be used to identify an iBeacon.

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Güliz Seray Tuncay • 4 years ago

Thanks! Everything is fixed except for the 3rd byte - flags. I changed the text to reflect that.

⌃ | ⌄ • Reply • Share ›

Kate • 4 years ago

Hi Adam,
Great post - this has helped me a lot with my dissertation at uni. I was wondering if you could help me a bit more by explaining to me in really simple terms how transmitting personal offers (i.e. when retailers use beacons) works? I understand that customers' personal data can be accessed in order to provide them with offers based on their shopping habits, but I don't understand how the beacons access this information and transmit it to the phone. I hope that makes sense?
Thanks for your help,
Kate

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Kate • 4 years ago

The beacons only transmit a very simple signal, they don't transmit any offer data. When the phone picks up the signal (e.g. a "region enter" event on an iPhone), the application is woken app and fetches the data from internal storage or the Internet.

⌃ | ⌄ • Reply • Share ›

Bob Bensetler • 4 years ago

Adam - I am researching for an asset tracking app where I might be tracking several thousand items. I presume I would use the same uuid for all tracked items and that this would give me 256 major ids and 256 minor ids, or 65536 total items. Sounds OK for starters, but as we know, applications tend to grow over time. I've read elsewhere that the uuid can also be modified on a given beacon but you seem to believe otherwise. Is that a fair statement?
And thanks for this blog, it's the best iBeacon source of info I've found so far. But how do you get any paying work done?

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Bob Bensetler • 4 years ago

Both the major and the minor are 2 bytes so that's 65536 * 65536 combinations - you should be good :)

You can set the UUID of the iBeacon to any value you want (at least in the most popular beacons), but you can only tell the iPhone to scan for a limited number of UUIDs (can't remember the exact number, sth like 10).

If you are using another scanner (e.g. through a RaspberryPi), then you receive notifications for all the UUIDs that come into range.

So far I luckily manage to get some paid work done but if you have some interesting projects - let me know - SoftwareMill would be happy to help :)

⌃ | ⌄ • Reply • Share ›

Bob Bensetler ➦ Adam Warski • 4 years ago

Oops. Sorry about the math. Using your example, 0049 is different from 49. I'll let you know if this project goes anywhere and I am able to involve SoftwareMill. I take it you folks are in Warszawa.

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Bob Bensetler • 4 years ago

0x0049 is hexadecimal, so 4*16+9=73 (different number base). 49 in hex would be 0x31 (or 0x0031, same thing).

We are from around Poland, mainly from Warszawa, that's correct :)

⌃ | ⌄ • Reply • Share ›

trath • 4 years ago

hi, is it possible to reverse the functionality of the beacons so that you get a notification if you get a certain distance away from the beacon rather than getting closer to it?

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ trath • 4 years ago

Yes, you can get an iBeacon exit event. It's up to the app really what it does in reaction to these events. Nothing in the beacon itself.

⌃ | ⌄ • Reply • Share ›

trath ➦ Adam Warski • 4 years ago

Brilliant! Seems to be exactly what i have been looking for. I am new to your blog so I don't know if you accept jobs here? I would like to propose a protect.

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ trath • 4 years ago

If you could e-mail us at hello (at) softwaremill.com, that would be great - looking forward, thanks!

⌃ | ⌄ • Reply • Share ›

trath ➦ Adam Warski • 4 years ago

Emailed earlier. Looking forward to hearing from you.

⌃ | ⌄ • Reply • Share ›

Ezra Weinstein • 4 years ago

Hi Adam, great article. I was wondering if you had any idea how many beacons a single device can connect to at once. We are developing an app to track inventory in a vehicle and there might be 100 items that we want to track individually. Is there a limitation? Any idea on how performance would be? Also wondering if you have come across any beacons that have a light that can be activated programmatically when I want to locate an item. Thanks in advance!

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Ezra Weinstein • 4 years ago

Beacon's don't really connect anywhere, their signal is being picked up be receivers. So that's entirely up to the receiver. I don't see why 100 wouldn't work, though at some point you might get interference between the individual signals, but I don't know physics enough to answer that confidently.

Haven't heard about beacons with lights - yet :)

⌃ | ⌄ • Reply • Share ›

Alex Mann • 4 years ago

Great blog post Adam. excellent overview and some good in depth stuff too. I didnt know it was so easy to clone/spoof iBeacons.

⌃ | ⌄ • Reply • Share ›

Case Anderson • 4 years ago

I'm the lead firmware engineer at BlueCats and we sell great iBeacons as well. I'm guessing the reason we are not on the radar as much is because we target the larger commercial audiences. Nonetheless, we sell to everyone. Great article btw, informative and simple. BLE can be quite complex for the first-timer as you know.

⌃ | ⌄ • Reply • Share ›

Ankit Purohit • 4 years ago

Thanks

˄ | ˅ • Reply • Share ›

mikeeugine • 4 years ago

BLEduino, BLE bee, BLE adapter: http://www.elecfreaks.com/s...

˄ | ˅ • Reply • Share ›

Andres • 4 years ago

Hey Adam appreciate the write up.

Excuse my ignorance but if bluetooth is turned off (aka the bluetooth icon isn't present in the top right of my iphone) I assume that renders the beacon useless, is that correct? Is this the case even if you have an app installed that belongs to the beacon owner and they have agreed to receive push notifications?

˄ | ˅ • Reply • Share ›

Adam Warski Mod ➦ Andres • 4 years ago

Yes, if BT is turned off, nothing will happen.

1 ˄ | ˅ • Reply • Share ›

Akshay • 4 years ago

Hi,

Can I know that How can I communicate between BLE to BLE ?
If one BLE has temperature sensor built, then How could I request from another BLE to read the temperature ?

˄ | ˅ • Reply • Share ›

Adam Warski Mod ➦ Akshay • 4 years ago

That's not really the scope of this post, but it depends what your other BLE supports. There are e.g. C APIs which allow you to establish BLE connections. I suppose each platform will have their own set.

˄ | ˅ • Reply • Share ›

Avatar This comment was deleted.

Adam Warski Mod ➦ Guest • 4 years ago

The only thing you can program in a beacon are the major and minor ids. Apart from that, it's up to your application to use e.g. the major to differentiate between venues.

⌃ | ⌄ • Reply • Share ›

Avatar This comment was deleted.

Adam Warski Mod ➦ Guest • 4 years ago

Yes, all beacons come with some major/minor IDs, the exact values depend on the vendor. Usually the major is fixed, minor is random.

There's really no security to beacons. It's very easy to create a copy of beacon, transmitting the same data. There are some non-iBeacon, but BLE based solutions, with built-in security, such as Gimbals.

As for purchasing, I recommend Estimote and Kontakt.io.

⌃ | ⌄ • Reply • Share ›

Mohamed • 4 years ago

Nice blog ..thanks!
I have some trouble in locating iBeacon in the BLE protocol stack. is it an independent profile that interacts with the link layer to set the AdvData section of its packet? is it an app built on the GATT profile? i hope to find a technical documentation that can explains this.

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ➦ Mohamed • 4 years ago

iBeacons use a small portion of the BLE spec, specifically the advertisements. There are some links in the article which explain this. Also the BLE specification can be of help. It is not an app built on the GATT profile.

⌃ | ⌄ • Reply • Share ›

Neil Rader • 5 years ago

Hi there, we have an iBeacon app for a special project we are doing, but running into trouble with the slow "connect" time between the beacon and smartphone (10-15 seconds). Is this normal? Can anything be done about it? Otherwise, the only useful applications are ones that can ensure the user is near a beacon for 15 seconds. Thanks!

⌃ | ⌄ • Reply • Share ›

Adam Warski Mod ↪ Neil Rader • 5 years ago

If the app isn't active, iPhone scans for beacons only from time to time (to conserve energy), and you can't impact that. The newer the iOS version, the better the responsiveness (at least there was a difference in recent iOS 7 updates).

^ | ˅ • Reply • Share ›

Load more comments

ALSO ON **BLOG OF ADAM WARSKI**

In today’s post-OO world, is dependency injection still relevant?

8 comments • 4 years ago

Adam Warski — Who would have thought, implicit parameters in XSLT :)

Quicklens: traversing options and lists

21 comments • 4 years ago

Ben Hutchison — This lens library is awesome, creating lenses separately from using them (eg with monocle) was …

Inverse beacon positioning

20 comments • 5 years ago

Adam Warski — The code is here: https://github.com/adamw/ze..., maybe it will be of some help

Introducing Supler: a Functional Reactive Form Library

12 comments • 4 years ago

Adam Warski — You don't have to include every field of the case class in the form, you can just have a selection. …

✉ **Subscribe** **Add Disqus to your siteAdd DisqusAdd** 🔒 **Disqus' Privacy PolicyPrivacy PolicyPrivacy**

MOVED

I'm now blogging on SoftwareMill's blog. Please follow me there!

RECENT POSTS

- Kafka with selective acknowledgments performance & latency benchmark
- Why I started learning Emacs in 2016
- Add a “dependencies” badge & tree to your project using UpdateImpact
- Event sourcing + free monads = free sourcing?
- MacWire 2.0: composing modules & cleanup

LINKS

Follow me on twitter!

Follow @adamwarski

Looking for end-to-end software development, project management, Scala experts? SoftwareMill is here to help:

TOP POSTS & PAGES

- Starting with Scala Macros: a short tutorial
- How do iBeacons work?

- Event streaming with MongoDB
- Trying to understand CAP
- Benchmarking SQS
- Dependency Injection and replacing dependencies in CDI/Weld
- Why I started learning Emacs in 2016
- Evaluating persistent, replicated message queues (updated w/ Kafka)
- JSF2 navigation: post->redirect->get
- Using Scala traits as modules, or the "Thin Cake" Pattern

CATEGORIES

Select Category ▼

ARCHIVES

Select Month ▼