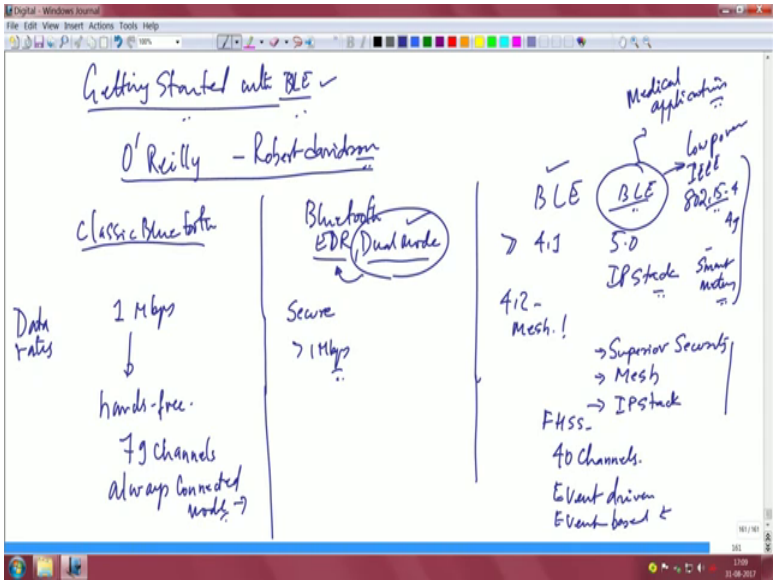
Design for Internet of Things
Prof. T V Prabhakar
Department of Electronic Systems Engineering
Indian Institute of Science, Bangalore

Lecture - 27
BLE Security

Bluetooth: it is always useful to look up a text book.

(Refer Slide Time: 00:17)



There is a book by O' Reilly publications getting started with BLE, please do look up this book and you will get a wealth of information related to BLE. I just give you my understanding of several things with respect to Bluetooth itself. Go back you look at classic Bluetooth then you have enhanced data rate then came Bluetooth low energy you wanted backward compatibility to old Bluetooth.

Therefore, you needed dual mode systems then by and large everything was ignored and you only started getting BLE modules which are currently now 4.1 and 4.1 and above very important. And 5.0 is already coming 5.0 BLE is already there, it supports full I p stack and 4.2 and above can also support mesh part. So, 4.2 mesh is possible right. So, if you go if you look at what has actually happening in this world and come back, you will see that BLE had to stand out compared to previous versions because it provides you it provides superior security.

It does mesh, it does good amount of I p stack availability it gives you the I p stack directly right it gives you (Refer Time: 02:14) stack directly. So, if you look at the security of Bluetooth enhanced data rate or dual mode there is security, but it is you can simply say it is security it is secure, but not really the superior in terms of security and data rates well. This was if you look at one important distinction data rates right people were talking about 1 megabit per second and quite a bit of current consumption because it was meant for many hands-free application and so, it was really power was not really the issue here with either one MBPS with either classic Bluetooth or enhanced data rate systems.

But as you went on to you know EDR data rates, EDR data rates were greater than one MBPS there are claims that it is even 2 and maybe when 3 M BPS. So, enhanced data rate I will say is greater than one MBPS I will simply say one MBPS and greater I would not quantify that number because there is you can look it up then of course, you wanted backward compatibility. So, you must bring in dual stack into picture and then of course, BLE which is does not need to do any fallback apart from this in terms of channels the classic Bluetooth had 79 channels ok.

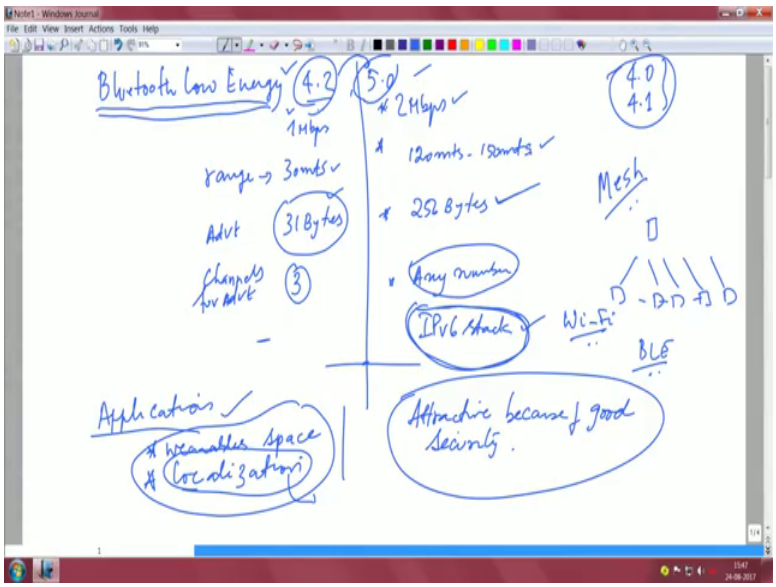
And whereas, the BLE actually has only 40 channels, there are differences of how many you can always you can use in for advertisement purposes, there were only 3 in the earlier case and currently all channel there is no restriction on the number of channels that can be used for advertisement. So, that is a very important thing. BLE very very importantly in terms of paradigm this is really event driven event driven, you can say it is event based and so on.

Whereas, which is for the other classic Bluetooth and so on you can say that this was like an always connected mode which will you know indicate the which indicates that power was really not the key point there therefore, you can say this was much more power consuming as compared to this event based which is really looking at power as a very important thing. Applications have changed BLE people talk about medical applications, many many new things happening in the world of BLE medical applications whereas, classic Bluetooth as I mentioned for several hands-free applications and other audio. So, there were different types of profiles. So, really the structure of the systems where different of course, there is lot of (Refer Time: 05:54) to noise because it uses frequency hop spectrum.

So, frequency hopping FHSS as it is called is something gives you superiority in terms of it is immunity from interference from other 2.4 giga hertz devices. So, the adaptive the data the adaptive data ability of the BLE system seem to be also something very interesting from for the choice of BLE. So, in broad view it is an exciting technology that you should look out for, perhaps it is time that BLE might replace other low power technologies particularly I triple E 802.15.4 15.4 has a lot more technologies like a is for something 4 a, 4 b, 4 c, 4 g essentially is for I think for smart metering applications.

So, lot of interesting things happening with the different variants of the basic 15.4 protocol, but at the same time I think BLE will ultimately be one of the pioneer leading technology for low power sensor network application. So, all of this put together makes it a very exciting protocol and what seems to be very exciting is this 4.2 and 5.0 because they are very very close to each other let us see what it what really the differences are.

(Refer Slide Time: 07:55)



In the case of BLE 4.2 you get one MBPS and 5.0 claims to be two MBPS. Range is about 30 meters in this case and they say 4 fold so, I expect anywhere between 120 metres and 150 metres. Advertisement packet although could be encrypted in both cases was only restricted to 31 bytes, and in the case of 5.0 you could go as high as to 56 bytes. The advantage is you just advertise whichever node is trying to pick the data can pick it and decode it de encrypt un encrypt the data and then simply use it. Which is a nice thing and the problem was in the earlier case was just restricted to 31 bites, and now you get

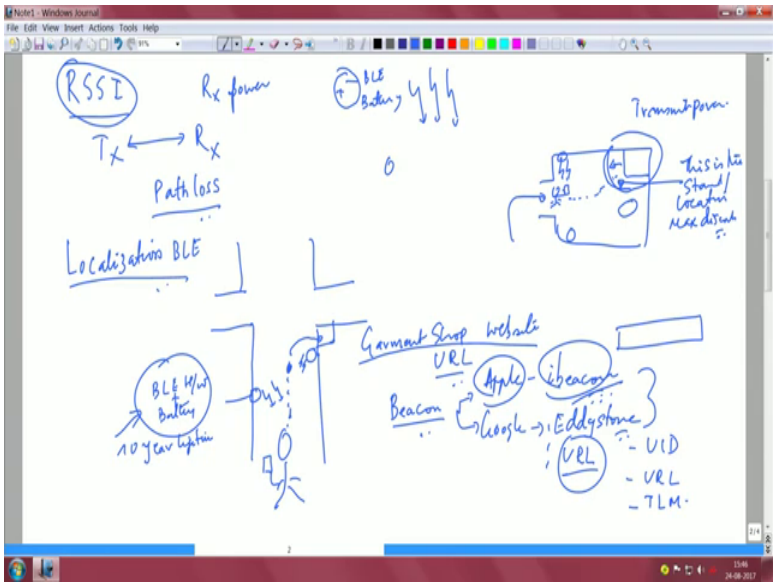
super 256 bytes of payload which is possible and even the advertising channels were just restricted to 3 in 4.2 it is now any number of channels can actually be you know assigned for the purposes of advertisement.

Last, but not the least very attractive you get the IP stack available on 5.0, it is pretty hot at the moment people have not seen devices which have started using IP v 6 stack already, but this is what is being big standard now and I think this will really sort of become the closest cousin to Wi-Fi because it will offer you full I p connectivity and so on. What will happen to the zig bi kind of devices is hard to say at the moment, also because now with the BLE 4.2 and above fantastic ability to do mesh has come up which was not the case you had a master and slave devices and all data used to go between master and slave which was indeed how BLE actually started right you had 7 slaves and a master and so on.

This concept of master slave is now out when you talk about 4.2 and above you can actually do many to many one to many many to many point to point point to multi point multi point to multi point which means they are fully connected mesh network is actually possible to both 4.2 and 5.0 making it very attractive, perhaps what s the one big advantage that (Refer Time: 10:31) actually had was the fact that we could do mesh with it and that also is now something that BLE can do. So, contending protocols rich wireless protocols for the internet of things, well definitely involve the BLE has a big big contender for all small range low energy applications and Wi-Fi perhaps even low energy Wi-Fi which might actually turn out to be a big advantage for slightly longer ranges.

So, do look out for BLE and do look out for the way BLE 4.2 and above are actually shaping up for many of your applications, and what kind of applications are we talking about? We are talking about variables; variables is a big big big area for internet or for the design for internet of things applications and that is one thing. Second thing interestingly BLE has sort of gone into localization requirements for localization. Recall many things that wireless networks can actually provide, one of the things that they can provide is RSSI right receive signal strength indication.

(Refer Slide Time: 11:45)



Essentially we are talking off at a transmitter and a receiver and this distance between the transmitter and receiver if it is line of site, it can be governed by the path laws expression which we all know very well I expect you to look it up as a (Refer Time: 12:07) law essentially with the received power you should be able to with the received power and if you know the transmit power you actually know what is the range between the transmitter and the receiver. And this is essentially being exploited in many of the RSSI based localization applications using in BLE.

For example I can motivate you like going to a mall or a supermarket where as you are entering the mall or a supermarket already the first beacon which is installed up there beacon essentially means that it is a small device BLE hardware device with a battery, and this essentially is sending out advertisement packets periodically. And with a given transmission power and looking at the transmission power and let us say there is a user who is walking with the phone in his hand with a phone in his hand the mobile phone smart phone in his hand. So, let me draw it big; so that we will maintain certain proportions. So, this is the corridor space and somewhere in this corridor space there is a small beacon which is installed this beacon essentially has BLE hardware plus a battery and when I say BLE hardware and battery I obviously, mean 10 year lifetime right we are talking of 10 year lifetime and essentially issuing periodically beacons.

And there is a human with a mobile phone in his hand, whose walking by this corridor to reach the nearest let us say some junction point and then wants to move on and then there is a shop here. Now as he moves on here and goes closer to this there is another beacon right and he now as he comes here to this part already the phone in his hand will tell him that s very close to let us say a garment shop right. And some pop up kind of a message can come which will allow him to look up something about this garment shop and how is that possible.

That is possible because the garment shop let us say has a website has a beautiful website garment shop oops let me draw write this well this garment shop has a website. Now as he goes closer a beacon which carries the URL instead of advertising any location information can actually advertise for a URL, and this URL is caught by the smart phone and immediately the browser kicks up and connects directly to the garment shop s website. There on the garment shop website there are attractive offers you know you know which are enticing the user to go and buy this or buy that and so on right which essentially will allow the vendors the retailers also to attract customers, there is good amount of sales the customers also can get a good deal depending on what they are looking for buying and all that. So, it really is a nice ecosystem building up.

I said something very interesting right as you walk there is a URL that is coming up from this little beacon the little BLE d hardware plus battery device and already the website opens. There was no application, there is no android app, there is no I o s app which got installed on the phone just as you walk by all these happened and why is all this possible how is all this possible. Because beaconing beacon is a big technology, and I will deviate into beacon technology before we move on to BLE other features of BLE.

Here beacons were first started way back use of beacons for purposes of localization first started by started by apple, and they called it I beacon. There is nothing special about I beacon let me tell you this there is nothing new hardware, it is a same hardware that you can buy from any vendor only the frame format the BLE frame format follows a particular order structure, and that structure is understood by many applications which are which you can download from apple store and essentially which will tell you few things about where you are what you are doing so on and so forth; that was the I beacon technology. This was by apple and if apple does something Google is not going to keep quiet right. So, Google came out with it is own technology and made it open source and

called it eddystone, and it did something more than just saying eddystone which is also a beacon technology and said look guys there are ways by which you do not need to install any app unlike what you can what you should be doing with I beacons.

We will give you a way of using eddystone technology whereby I we can push an URL as well. So, that is something that eddystone technology provides. So, you could be having an android phone in your pocket and you could be walking across, and you could be receiving an eddystone URL type of beacon message, and that eddystone type of URL message essentially will make you open up the garment shop website.

Let us continue further. Now the user enters the garment shop there he finds. So, let me expand this garment shop into a bigger window as he enters. So, let me put an entrance for the garment shop otherwise there is not going to be any business for the user. So, now, the user enters the garment shop and out in this corner, there is a let us say a sale indicator; a sale indicated here which is let us say 30 percent or 40 percent of some garment. Now as he enters beacons inside are already telling the user on the phone about where the best discount sale is available inside the shop please note this is inside the shop. It is not interfering in the corridor which means you control the transmit power and you make the range of the beacon small enough so that you entice the user to tell him to move in a particular direction which will give him the maximum discount at garment in that shop.

Now, as he moves along and comes closer to the stand where the sale is situated located, there it will tell this is the place this is the stall no this is the stand, this is the location within the shop which has the maximum discount. All of this is done beautifully quite seamlessly by just controlling the transmission power and creating bigger and medium sized range around the user by using these beacons. So, this is a very interesting technology I must say many things about I beacon. It is not true that I beacon works only on apple phones that is incorrect. I beacon technology it is a technology right which you which is a frame structure on top of BLE, this frame structure also works on android phones. So, do not restrict yourself and get locked up that I beacon is only meant for apple phones it was invented by apple. So, that is a nice thing.

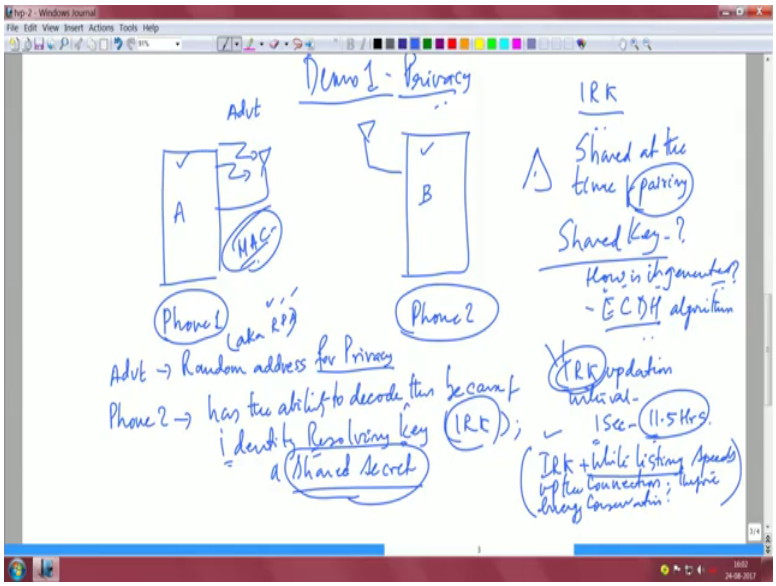
There are other types of beacon types in eddystone as well. I just took the one that seems to be very close to this example. Just look up I beacon and eddystone together to

understand exciting applications which are possible with BLE. So, this is in the sense the most important thing other things about eddystone are there is something called an eddystone UID, there is an eddystone which I just talked to you about URL and there is another thing called eddystone TLM. Well I do not want to get into the detail, but you could definitely look them up and see and everything is an open source you can go to get hub and you can download these solutions very good that s very important thing about BLE.

And. So, let me just go back to where we started with the two applications for the localization applications, here you talk about beacon technology and the variable space which is an interesting thing. Now look at what I wrote here I said this is also very exciting because it has a very attractive security feature. Remember what I have been saying all along security without security the internet of things is going to fail, you cannot be talking about billions and billions of devices which are insecure therefore, communication security is indeed critical.

What we will do now is we will spend some time setting up small little experiments, to understand the security features of BLE 4.2. If we know 4.2 well we can already make an assumption that we know the security features of 5.0, because the differences are very minimal. So, let me start with the demo one Madhuri and Anuja are here, and idea is there is a phone 1 here and then there is phone 2.

(Refer Slide Time: 23:13)



Phone 1 is advertising and I have to show an antenna so that BLE antenna and then there is a receiver antenna, just for completeness let us put the two antennas. These are two phones they can be android they can be anything idea is that of this demo one is all about privacy; is about the privacy of this phone one ok.

Then here one of the nice features in BLE 4.2 and above is the fact that address resolution part also known as RPA resolvable private address, essentially means that this phone one continuously changes it is what is equivalent of MAC address in ethernet that you know continuously it keeps changing, and randomly it generates a MAC address, but yet it is successfully able to be decoded by phone 2 that is the nice thing about it. That is this phone continuously generates random MAC addresses link layer addresses although the link layer address is random, the phone two is able to catch that because it has what is known as a identity resolving key also called the IRK.

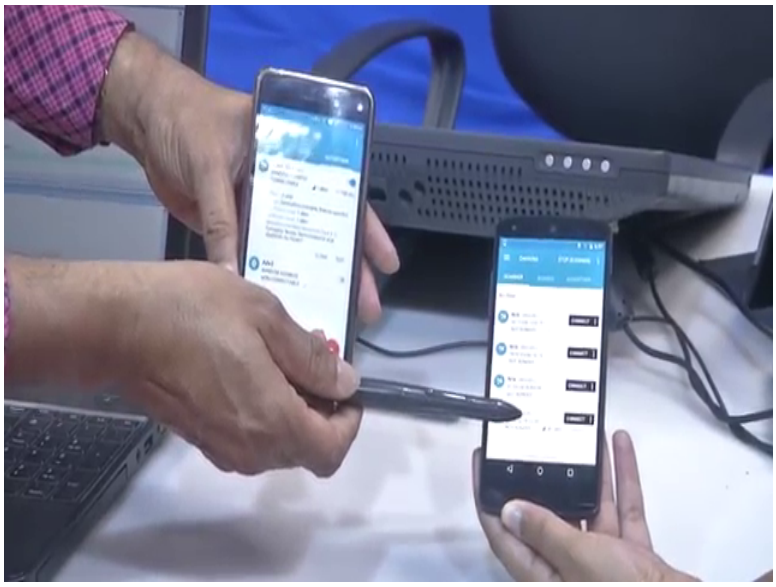
And what is IRK? IRK is a shared secret and how do you generate a shared key? A shared key is generated using eclectic curve (Refer Time: 25:13) algorithm. We will not get into the shared key generation part, but this shared key is available at the time of pairing it appears right and this IRK updation that is you keep changing the shared secret itself, to keep it very very hard for any person to penetrate into this privacy of these devices, you keep changing the shade key itself oh from a anytime between one second to 11.5 hours. For instance if you are in a public place you perhaps want to keep changing the IRK very very often with many devices you do not know what kind of devices are around you who are hackers who are listening to you.

So, depending on where you are you may want to change the I r key as often as possible. If it is inside your house, it is a onetime thing and you do not want to worry so much about security, because it is confined to a small private area then you may want to set it to something like 11 hours or 12 hours or whatever the standard permits. So, office environments public places and all that you may want to keep modifying the IRK as often as possible.

Now, the real good thing about 4.2 and above that is the reason I did not want to talk about anything prior to 4.2 is because 4.2 has this and above has this advantage that you can use this identity resolving key along with white spacing white listing we have black listing white listing. White listing are the those whom you want to trust right. So, IRK

plus white listing is possible and because of this combination, the connection between this phone a and phone b phone a and phone b really is speeded completely gets speeded up and as a result energy is also saved to a large extent. So, let us see a demonstration of this.

(Refer Slide Time: 27:33)

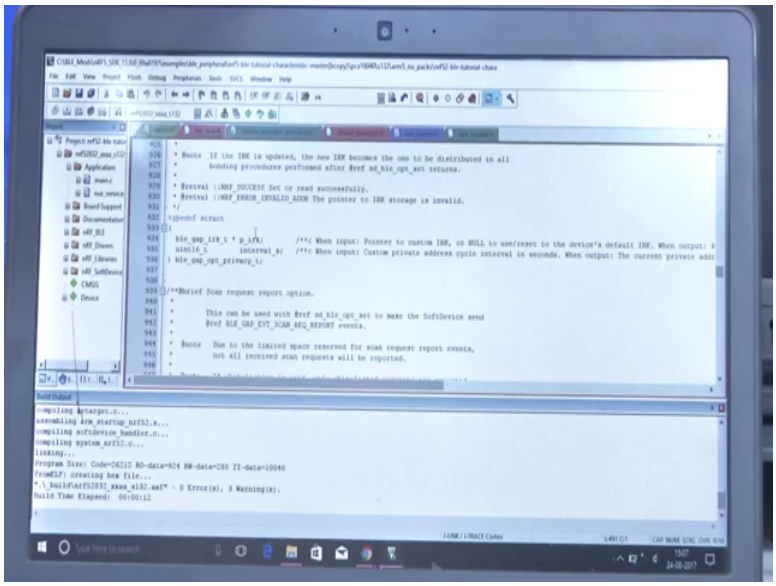


This is the phone that is advertising and we are talking about privacy of these two devices and what I will show you now is that this device as you can see has flashed this MAC address. So, the MAC address flashed is 61 colon 553406 b 454, and this is the RSSI received signal strength of.

This received on the receiver (Refer Time: 28:06). So, now, what we will do is we will stop we will stop this I have stopped it and again you will see that it has stopped transmitting and now we will start it all over again and Madhuri starts this and you will see this time it is a different random MAC address 6 b 203 f 7822 and then 0 0 and of course, the received signal strength is minus 40, now it is minus 52 and if I keep take it far off it is minus 65. If I bring it closer it is minus 49, you can see ranging is possible localization is possible assume that this is the phone in the pocket and this is the beacon you will see that ranging is actually possible.

So, while we demonstrate the privacy you can also see that ranging is being ranging the beacon technology which I mentioned is also easily exploitable because the RSSI can be exploited very effectively.

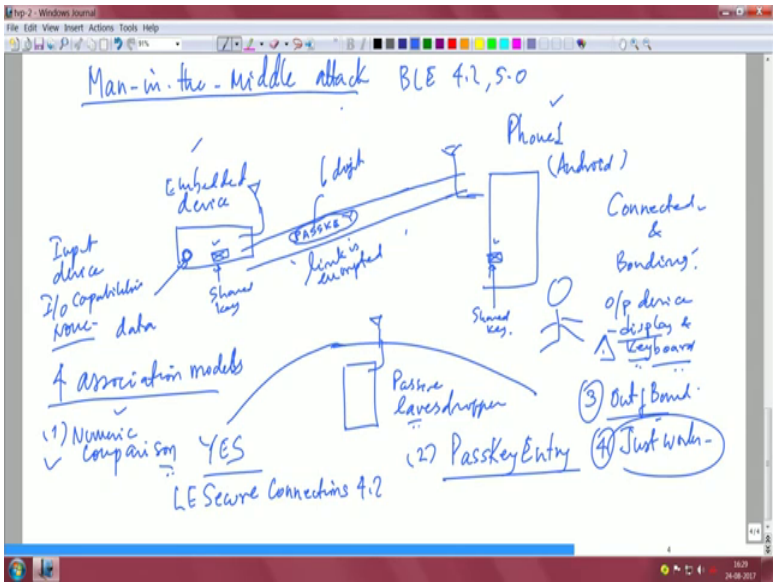
(Refer Slide Time: 29:18)



This nice screen for us which will this is for the this is using (Refer Time: 29:24) platform it is meant for Nordic n r f series of s o c s, I want you to look up this particular part in the c code where you are talking about the IRK right and the interval. Now I mentioned to you during the demonstration during the explanation that the shared key has to be changed after a certain interval which depends on the scenario right.

So, that interval change actually is affected by this particular in this particular structure that is defined in the BLE source code. So, that is it says when input custom private address cycle interval is in this is mentioned in seconds, you can actually change it up to whatever maximum interval that we said is 11.5 hours. So, this is the updation interval of the IRK. And once this updation happens of course, the shared key has to be primed back on these two devices so that the new shared key is now available on both these devices and again they can go on you know exchanging they can maintain their privacy whenever there is an exchange of data between the two devices.

(Refer Slide Time: 30:53)



The ability of BLE to thwart man in the middle attack, BLE again I am restricting myself to BLE 4.2 and greater which means 4.2 and 5.0 only 4.2, 5.0 kind of situations take this picture in mind alright. So, here is a passive eavesdropper who is listening to two devices look at this look at these devices one is an embedded device the other is a phone and idea of this experiment let us say is you want to get hold of this data this user wants this data if he wants this data he has to basically access this data over a secure link, and how is this link encrypted? Remember we mentioned about the shared key the shared key is available on both the end devices.

And therefore, this side of the link starts the encryption let us say this side gets decrypted and vice versa for secure exchange of the data over this link which is encrypted. Now the pass key is something nice that unless the pass key is specified access to this data is not possible although the link maybe encrypted the pass key is should be typed by the user and only if the user types the pass key this data access is possible, otherwise simply nothing is given you may just be able to connect between the devices and be done right. So, this is mostly in the connected and bonding mode we call this device, the output device we call this device the input device again go back and look at the capabilities.

This output device because this is a phone has a display and keyboard and therefore, has the ability by this user to type the pass key. This device is the one that has the data it is an it is a it has I o capabilities which are none no display no keyboard and so on and so forth

and this is also as I mentioned is also the input device. From a very broad perspective the thwart m I m attack there are 4 association models I will write one by one and then we will take a understanding from this pictures perspective only one association model is called numeric comparison.

What it simply means? It simply means that by the way this pass key is 6 digit this 6 digit password and the use. So, in numeric comparison both devices display the 6 digit number; that means, you cannot be talking of an I o capability none anymore, you will also need a display and keyboard on this side. So, this is one thing. So, if you are having really an embedded device and you do not want to have any display and keyboard that is one type of association, which we will what we will demonstrate, but you can have both sides phones right which means display and keyboard maybe available then if you have both sides phones, phone like capability then you can do numeric comparison where by the devices have display a 6 digit number and the user authenticates by selecting yes ok.

And if both devices are displaying the same number you say yes, the association model is actually introduced in L E secure low energy secure connections of which version 4.2 and above DLE that is very important. We will not worry so much about the capabilities of earlier versions. The second method is you have only one side capability the output device has the ability to do the it enter the pass key using keyboard and display and the other side is what I showed here there is no display and keyboard the exchange of pass key one bit at a time in BLE is an important enhancement, over the legacy models we will not worry so much about all of that.

The user either inputs an identical pass key into both devices or one display one device displays the pass key and user enters the pass key into the other devices that is what we are going to do here and. So, you have different capabilities for the on both sides of the device. So, essentially this is one way, the other way is I do not want to either use numeric comparison or I do not want to use the pass key method pass key entry, I do not want one two I do not want to do pass key entry which I mentioned is essentially this where user either inputs an identical pass key into both devices or one device displays the pass key, and the user enters the pass key into the other devices like what is here you do not want to do this.

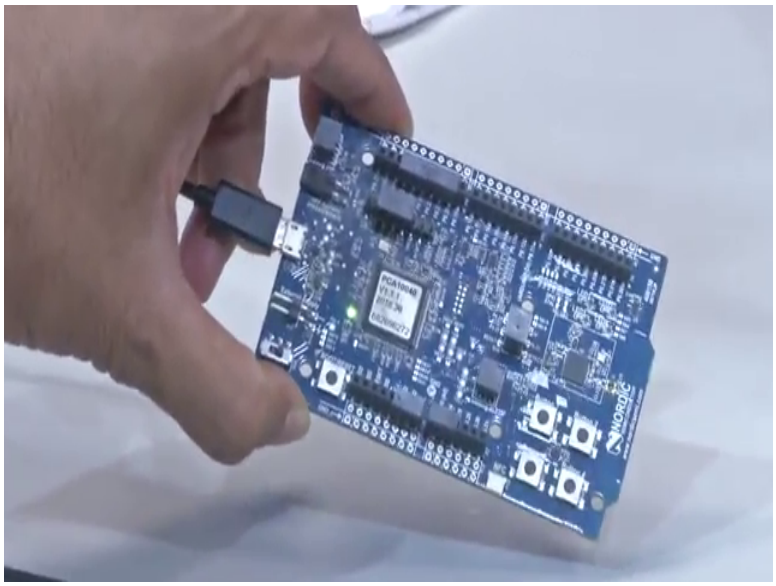
You could do it in a third way, the third way is you do out of band. In other words if you had two phones and you had an NFC channel NFC between the two phones now you could pass this particular pass key over out of band it is called out of band, that is you are not using BLE, but you are using some other channel in order to pass this pass key. The out of band association model is the model to use if at least one device with o o b capability, already has cryptographic information exchanged out of band here protection against MITM depends on the MITM resistance of the o o b protocol used for sharing the information. So, that is the third way, fourth way is called just works it is called just works.

Quite exciting this association model is used either when MITM protection is not needed or when devices have almost very limited I o capabilities. In other words there is no display and keyboard on either side and you need to use some other mechanism by which because they are really embedded very small embedded devices and just trying to you know use this association model without for this kind of very limited resource based devices. So, that is just works. So, there are 4 association models.

BLE 4.0 has 3 association models that protect against MITM and one for applications that do not need MITM protection and as I said just works is something that need not need MITM protection and. So, you could also use it you could use this. So, it is not that BLE 4.2 or 5.0 force you to do something, but they also give you this nice escape route by saying I do not think it is an overkill and you may not need this you know association model for to thwart MITM because there is no likelihood of an MITM at all. So, that is also possible. The numeric association models are all that were not available in previous version. So, again I do not want to get into those details.

So, let us see a demonstration of this pass key where input device has no capability, but on the other side the I o device has a display and keyboard. So, this is a demonstration of a certain data that you that we are interested in obtaining from this embedded device.

(Refer Slide Time: 40:03)



This is a 4.2 capable embedded device, you see this, this is from Nordic and this is this has some value some data that you want to read. And that is possible only if you follow a certain set of steps by which you should be able to give the pass key and only then the data comes. So, Madhuri will demonstrate this.

She does connect and then it says unknown service u u i d and something which is there. So, she clicks on that and then for that there is an unknown characteristic that is available and she wants to read that. So, she presses that and there is a pairing request and then she types in the Bluetooth pairing device that is the pass key that she is providing and she says and once this she presses then she gets the data value here you see value 2D F0 7 5 C 6 2 F 3 0, this is a clear indicator that unless the pass key is submitted the data access is not going to be possible. Where is the key here you may ask, either on this device or this embedded device or on this phone, we did not type any key because the shared key is already primed on either side. Only what we give now is the pass key.

So, that is important and you may have seen that we gave a pass key in plain text, because the link is encrypted using that key, that is already there on either end of the devices and this is a very important thing.