Modern implants have wireless in them, this include pacemakers and cardiac defibrillators, Neurostimulators, or even upcoming cochlear device that help with hearing problems.
Having wireless in these devices has multiple benefits.

First, it makes it easier to communicate with the implant itself.

More importantly, it enables remote monitoring of the patient’s status.

The patient can be in her home; she would have an implant reader that periodically queries the implant for patient’s vital signals. The reader then forwards this information to the medical professionals over the internet.
Benefits of Wireless

- Easier communication with implant
- Remote monitoring
  - Reduces hospital visits by 40% and cost per visit by $1800
    
    *Journal of the American College of Cardiology, 2011*

What about security?

Studies show that such remote monitoring reduces the number of hospital visits by 40% and also reduces the cost of each clinical visit by about 1800 dollars.

So having wireless in medical implants has many benefits. But, it also brings along new security and privacy issues.
In particular there are two attacks that are important.

First a passive attack. In this case, the attacker listens on the medium. Whenever the implant transmits, the attacker snoops on these transmission to obtain the patient’s private data. This could be the patient’s diagnosis or vital signal like EKG. Such a snooping is a significant violation of the patient’s privacy.

Second an active attack. In this case the attacker sends unauthorized commands to the implant. For example, the attacker here can send wireless commands which turn off therapies on the implant.

These passive and active attacks are not just fantasies. They have been demonstrated in practice using off-the-shelf software radios. For example, the researchers have showed that an attacker can make a cardiac defibrillators deliver an electric shock to the patient’s heart.
How Do We Protect Against Such Attacks?

Cryptography?

So how can we protect medical implants against these attacks?

The first thing that comes to mind is to add cryptography to medical implants.
It turns out, there are two main problems with adding cryptography to the implants themselves.

The first problem, say that the patient has an emergency. The patient may be taken to a foreign hospital where the doctor don’t have the secret key. So the doctor won’t be able to access the implant and help the patient which could be fatal.

Another reason why simply adding cryptography to implants doesn’t solve the problem is that there are already millions of patients who have unsecured implants. In fact in the US alone there are three millions such people. It would be impractical for them to go through surgery to replace their implants with ones that have crypto.
Ideally,
Ideally, we want a solution that can secure implants without modifying them. So the implant continues to operate as it does today, however there is a device different from the implants that guarantees its security. That is we want to delegate implant security to an external device.

If we can achieve such a delegation then in case of emergencies if the patient is taken to a foreign hospital, the doctor can simply turn off the external device and get direct access to the implant.

Also, since the solution doesn’t require modifying implants, it would help patients who already have these implants.

But, how can we delegate implant security to an external device.
Here is our solution idea.

We are going to use an external device we call the shield to secure medical implants. The shield is a small wireless device that can be worn like a necklace or a chain.
The first thing that the shield does is that it protects from active attacks.

Say the adversary sends an unauthorized command to turn off the therapy on the implant, the shield would simply jam the adversary’s message.

In particular, the shield checks if the implant ID in the header matches that of its protected implant. If they match, the shield jams the message on the wireless medium.

As a result, the implant can no longer decode the adversaries message and hence does not react to it.
The first thing that the shield does is that it protects from active attacks.

For example, here we have an implant and an active attacker.

The shield always listens on the wireless medium. Whenever it sees an unauthorized message whose destination is the implant id like this one, it jams that message.

As a result of jamming, the implant can no longer decode the attacker's message and hence it does not react to it.

Thus, with this simple jamming, we can protect from active attacks.
But, how do we protect from passive attackers which snoop on the medium to obtain the patient private data.

Naively, it might seem that we can do what we did for active attacks, use jamming. So in this case, the shield listens on the medium, when ever the implant transmits, the shield jams these transmission preventing the attacker from decoding.

This naïve solution, however doesn’t work.

Simply jamming not only prevents the attacker from obtaining the patient’s data, but will also prevent everyone, including the doctor from getting the data.

So the question is how can we prevent an eavesdropper from getting the data while still deliver the data to the doctor?

Our solution is called analog one-time pad.
Before I explain to you our approach, I need to remind you of the classic one-time pad which works as follows.

Say a sender wants to encrypt the following message. He is going to pick a random key and encrypts the message by xoring the message with the key.

Now, only nodes that have the random key can decrypt this message. So if you have the key, all you have to do to decrypt the message is xor again with the random key, which effectively subtracts the impact of the key to gives us the original message.

Clearly, since the implant doesn’t have keys, we can’t use this approach as is.

But, we are going to build on this classic approach to design our analog one time pad.
Our shield protects from passive attacks using analog one-time pad.

It works as follows.

Say this is the implant’s signal transmitted in the clear.

The shield transmits a random signal that jams the implant’s signal.

The wireless channel naturally combines the two signals together and as a result the adversary gets a random sum of the two signals.

Since the adversary doesn’t know the random jamming signal, it can’t decode the implant’s transmission.

The Shield, on the other hand, knows this jamming signal because it is the one who transmitted it. Hence it can subtract the jamming signal from this random sum to obtain the implant’s signal which it can then decode normally.

By have the shield both jam and subtract the jamming signal from what it received, we imitate one-time pad approach. Thus, we have an analogy for one-time pad in the analog domain where the jamming signal effectively acts like the random key.
Let me tell you how the whole system works together.

In the original system, the doctor directly obtains information from the implant.
In contrast in our system, the doctor configures the shield with a secure key. Note that this is very different from putting crypto on a implant because the shield is an external device; hence it is okay to add crypto to it.

Later whenever the implant transmits data, the shield simultaneously jams and subtracts the jamming signal to obtain the implant data.

Once the shield has the implant data, it forwards it to the doctor over an encrypted channel.

Hence the shield acts as a proxy for the implant.

I gave you a high level description of our system works. But the devil is in the details. In particular, we assumed that the shield can subtract out the jamming signal it transmitted. In practice, however, this is really hard to do.

The rest of the talk is how we get these details right. Before we go into these details, let me give you our contributions.
Here are our contributions.

We present the first system that secures wireless implants without modifying them.

To do this, we design a wireless system that can simultaneously jam and decode the transmissions from a medical implant and hence can achieve our concept of analog one-time pad.

Finally, we implement the shield using software radios and evaluate it using commercial cardiac defibrillators. Our results show that the shield is effective at protecting the implant from both active and passive adversaries.
Okay, let’s go into more details about how our system works.

To achieve analog one-time pad, the shield should simultaneously jam the implant’s signal and also decode it.

So we need a radio that can transmit and receive simultaneously, i.e., a full-duplex radio.

Traditional wireless radios are however half-duplex in nature, i.e., they cannot receive when they transmit. So the first thing we ask is how do we design full duplex radios for medical implants?
Last year MOBICOM had this nice paper which showed a practical realization of a full duplex radio. The idea underlying their design is as follows:

We have two transmit antennas and one receive antenna. You put the receive antenna half a wavelength further from one transmit antenna than the other.

It so happens that by the laws of physics that if we send the same signal from the two transmit antenna, they arrive out of phase at the receive antenna and hence cancel each other out. Thus, we can receive other signals on the receive antenna and operate as a full duplex radio.

While this design is elegant for WiFi which operates at 2.4GHz, medical devices operate at much lower frequency at 400MHz. At these low frequencies half a wavelength is about 40cm. So if we build a prototype for our shield, the antennas have to be placed more than 50cms apart and hence would be too large for portable medical devices.
So we need a full-duplex design that does not require any antenna separation.

To achieve this, we bring the transmit and receive antennas close to each other and merge them into a single antenna.

Thus, our shield has two antennas, a jamming antenna and a receive antenna.

Whenever, the jamming antennas transmit a jamming signal, the receive antenna transmits an antidote signal. The antidote signal is crafted such that it cancels out the jamming signal exactly at the front end of the receive antenna.

To do this, we want the jamming signal, $S_{\text{jamming}}$, that traverses the cross channel between the two antennas and the antidote signal that traverses the self-looping channel to sum up to zero.

Thus, we want the antidote signal to satisfy this equation.

Since the shield knows the jamming signal and can estimate these channel parameters, the shield can always generate the appropriate antidote signal.

Thus, the shield can simultaneously jam and receive at the same time.

Further, since the antennas can be placed next to each other, we can design the shield to be a small and portable device.
There is one additional concern.

Anyone who has heard of full duplex before, would have also heard that to achieve full-duplex radio one need to cancel the transmit signal with very high accuracy. That is the full duplex radio needs to cancel about 60-80 dB of the transmit signal.

If we think about this, this means that one needs to reduce the transmit signal power by a 100 million times. As you would imagine, this is extremely difficult.

In fact, if you ask any circuit guy, they cannot achieve such high cancellation unless you have extremely linear hardware components. Which means that the hardware is going to be extremely expensive.

So the question we ask is can we build our shield with way lower cancellation, say 30-40dB?

As it turns out 30-40dB cancellation is sufficient, and here is the reason.
Unlike a general full-duplex radio which has to decode any kind of a signal, our shield has two specific requirements.

First, it should decode the implant’s signal. Second, it should jam the eavesdropper.

The implant transmits a FSK signal which requires a 10dB SNR to decode correctly. So to decode successfully the shield needs to receive the implant signal at an SNR of 10 dB or higher.

On the other hand, the shield should jam the eavesdropper to ensure that it cannot get any information from the implant’s transmission. That is the shield wants to ensure the eavesdropper is no better off than making a random guess about the implant data. This is equivalent to ensuring that the eavesdropper sees a bit error rate of 50%.

Clearly if the shield increases its jamming power, the bit error rate at the eavesdropper increases. So let’s plot the bit error rate as a function of the ratio between the jamming power and the implant power. Here are the results.

As we can see, if the jamming power is 20 dB above the implant’s power, the eavesdropper has a bit error rate of 50%, that is, he is no better than making random guess.
Shield Requirements

Decode Implant’s signal
- FSK signal
- Implant signal has a 10 dB SNR

Jam eavesdropper
- 50% bit error rate
- Jamming power 20 dB higher than implant’s power

![Graph showing Bit Error Rate vs. Jamming power/Implant power (in dB)]
So we have the above two constraints on the shield operation.

Now say this the implant’s signal. We want the jamming signal to be 20 dB higher than the implant’s signal. So here is the jamming signal that is 20dB higher than the implant signal.

We also want for proper decoding that after cancellation the implant signal to have 10 dB SNR. That is the power of the implant signal has to be 10 dB above the noise. Since the noise in our case is mostly coming from the jamming signal, we want to cancel the jamming signal such that after cancelation it is 10dB below the implant signal.

Since it is already 20 dB above the implant signal, we want a cancellation of 30 dB.

Thus, with just 30 dB cancellation the shield can both decode the implant’s signal and also jam the eavesdropper effectively.
Empirical Results

So now lets see at how the shield perform in practice
We evaluate our design using the medtronic cardiac implants. We also acquire a programmer for this implant from ebay and reverse engineer its communication.

Now that we know the communication protocol, we implement our attacker and shield on USRP2s.

Finally, as in prior work, to simulate implantation in a human being we place the implant within layers of bacon and beef.
We evaluate our design on a testbed with 20 locations. We pick two locations in the test bed and assign them as the locations for the implant and the shield. We then place an node at every other location to act as an adversary.

The closest location is about 20 cm away and the farthest location is more than 30 meters away.
First let's look at the performance with a passive adversary which eavesdrops on the private data of the patients.

To do this, we place eavesdropper at different locations in the testbed, and have each of them decode the implant’s transmissions.

Our implementation of the eavesdropper uses the optimal FSK decoder in order to decode these transmissions.
The first question we ask is can the eavesdropper do any better than randomly guessing the bits?

If you have some data, and I randomly guess it then the bit error rate will be 50%.

So we want to check that regardless of his location, the adversary will get a bit error rate of 50%.

So on the x axis we plot the attacker bit error rate and on the y axis we have the CDF taken over all attacker locations in the testbed.

Before showing you our results, as a baseline, let me plot you the bit error rate for an adversary that is randomly guessing the bits in the packet. As expected, the bit error rate for such random guesses are close to 50%.

Now let's see the actual bit error rate at the eavesdropper in the presence of jamming.
Can Eavesdropper do Better Than Random Guess?

CDF over attacker locations

Attacker Bit Error Rate

Random Guess

0 0.2 0.4 0.6 0.8 1

0 0.2 0.4 0.6 0.8 1

Random Guess
As we can see the curves are pretty close to each other.

Thus, we conclude that independent of its location, an eavesdropper can do no better than randomly guess the bits in the implant’s transmissions.

In fact in the paper we show that even in theory this holds independent of the eavesdropper’s location.
Can Shield Decode Implant’s Messages?

CDF

Packet Loss at Shield

0 0.005 0.01 0.015 0.02 0.025

0 0.2 0.4 0.6 0.8 1
Remember that the shield should both jam the eavesdropper and at the same time decode the implant's message.

The next question we ask is can the shield decode the implant's message even though it jams the eavesdropper?

To check this I am going to plot the packet loss rate observed at the shield on the x axis and the CDF on the y axis.

Here are the result.

As we can see the packet loss rate is very low. In fact, the average loss rate is 0.002 which is negligible for wireless environments.

Thus, we conclude that the shield can reliably decode the implant’s message, despite jamming.
Next let's focus on active adversaries where the adversary sends unauthorized commands to the implants.

In each run, we make the attacker send a command to change the therapy parameters, the shield jams the command. We read the implant to check if the attacks was successful.
We distinguish between two types of active adversaries.

The easiest way for any adversary to mount an active attack is use off-the-shelf implant programmers. 

→ Same power as our shield

• Customized hardware 

→ 100 times the power of our shield

We distinguish between two types of active adversaries.

The easiest way for any adversary to mount an active attack is use off-the-shelf implant programmers.

A more advanced adversary would reverse engineer the communication protocol of the implant and build customized hardware to mount the attack.

Since both the shield and the off-the-shelf programmer abide by FCC rules, they both have the same transmission power.

On the other hand, since customized hardware is illegal it doesn’t have to comply with FCC and have way higher power that the shield. We evaluate a scenario where it has 100 times the power of our shield.

Let’s evaluate both these kinds of attacks.
First, let's look at the result when there is no shield.

As we can see, the attacker would be successful as far as location 8.

Next, let's see the result in the presence of a shield. As we can see, even in location 1, the adversary was un成功fully in mounting the attack.

To get a sense of these locations, let me show you these same results on the testbed graph.
Can Shield Protect Against Unauthorized Programmers?

[Bar chart showing the fraction of successful attacks with and without a shield, with attacker location number on the x-axis and fraction of successful attacks on the y-axis.]

Without Shield
With Shield
Can Shield Protect Against Unauthorized Programmers?

- • - Any attack successful
- ○ - No attack successful

The black dots represent the locations of the active attackers.

I will change the color of the location to red if any of the attacks was successful from that location and to blue if none of the attacks every successful.
Here are the results without the shield. As we can see, the attacker is successful as far 14 meters away and in non-line-of-sight configuration. Thus, an attacker can be in a different room and still mount this attack on an unsuspecting target.
Next, here are the results in the presence of a shield.

As we can see, even at the closest attacker location which is about 20 cm away from the implant, the adversary is unsuccessfully in mount the attack.

Thus, we conclude that independent of the location, the shield protects from an adversary mounting active attacks using off-the-shield programmers.
Next, let's see if a shield can protect against an adversary who uses customized hardware which transmits at 100 times the power of the shield.

This time I am going to show the results directly on the testbed.

As before, I will change the color of the attacker location to red if any of the attacks from that location was successful and to blue if none of the attacks were successful.
First let's look at the result when there is no shield. Now the attack can be mounted from farther locations which are as far as 27 meters away. This is expected because the adversary uses much higher power and hence can reach longer distances.

Now let's look at the results in the presence of the shield.
Here are the result.

We can see that the attacker is successful only from nearby locations. Thus, although the shield cannot protect from all high power attacks, now the attacker has to get much closer to the patient to successfully mount its attack. Thus, it has significantly raised the bar on the attacker.

But, once the attacker gets close enough, it can overwhelm the jamming power and reach the implant.

This is an intrinsic limitation of jamming where the shield is constrained by the FCC limitations, while the attacker is not.
But can we do better?

It turns out the shield would always detect these high-power attacks. So it would raise an alarm informing the patient or the health care professional, thus providing an opportunity to reverse the damage.
To conclude, we present the first system to secure medical implants without modifying them.

Since our solution provides security without changing the device itself, it may be application in other scenarios like RFIDs, low power sensors or even legacy devices without crypto.

We believe that the convergence of wireless and medical devices open up a number of new research problems. This includes not only ensuring the reliability, security and availability of low power medical devices but also designing new MAC protocols appropriate for these devices.

Finally for those of you who are interested in working on this domain, we have an open medical device research library where you can borrow medical devices to do your research.

With this I will end my talk and take any questions.