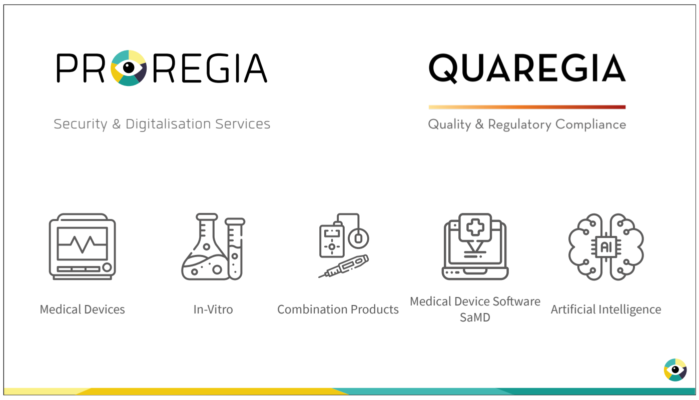
# Cybersecurity

ASPECTS IN THE DEVELOPMENT OF A MEDICAL DEVICE

Mathias Eng
Dr. Larissa Naber

Good Morning Ladies and Gentlemen and welcome to our presentation about CYBERSECURITY ASPECTS IN THE DEVELOPMENT OF A MEDICAL DEVICE

My name is Mathias Eng, I am the Founder and CEO of QUAREGIA and PROREGIA.



PROREGIA

Security & Digitalisation Services

QUAREGIA

Quality & Regulatory Compliance

Medical Devices

In-Vitro

Combination Products

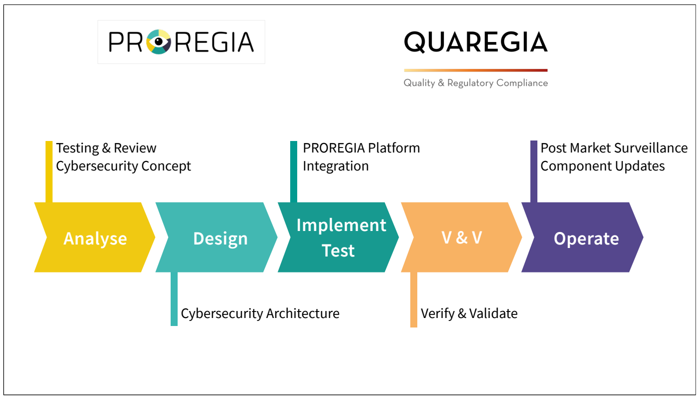
Medical Device Software
SaMD

Artificial Intelligence

It is all about Digital Health.

QUAREGIA provides Qualitymanagement and Regulatory Affairs Services for Medical Devices, IVDs, Combination Products, Medical Device Software, Cybersecurity and Artificial  Intelligence.

The QUAREGIA management team consists of Dr. Sabine Nieba, acting as COO and me acting as CEO.



PROREGIA is a team of top notch, full stack Hardware and Software developers, providing Digitalization Services for the Lifescience Industries. We provide you Software and Hardware as a Service for Secure Operation and Maintenance of IoT Applications and Data.

Leaving you to concentrate on your core competencies while we securely connect your products into the Internet of Medical Things.

In a Nutshell, what you need to reach is end to end Cybersecurity and it all starts with a firm Cybersecurity Strategy.

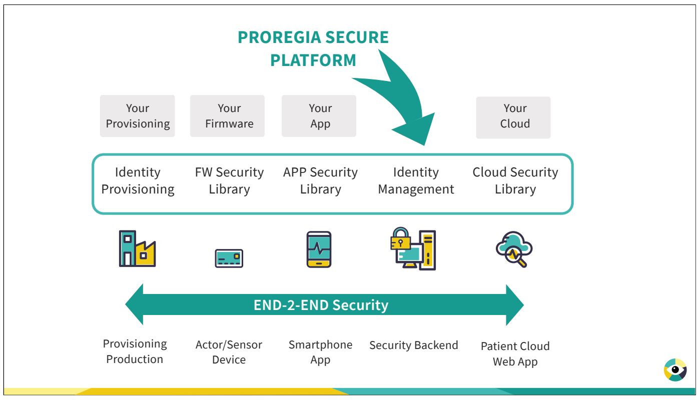
For a Cybersecurity Concept you need to identify:
- Your system's scope
- The threat actors
- Attack vectors and specific attacks on these vectors
- Appropriate countermeasures

For the Cybersecurity Architecture you need to define
- Define Cybersecurity Requirements
- Perform Cybersecurity Risk Management

- Define detailed  security design

Cybersecurity Verification and Validation
- Implement and Perform Cybersecurity Verification and Validation
- Document your security measures in a concise and easy to follow way

At last, you need to perform Cybersecurity Post-Market Surveillance to make sure your system stays secure.



PROREGIA SECURE PLATFORM

Your Provisioning | Your Firmware | Your App | Your Cloud

Identity Provisioning | FW Security Library | APP Security Library | Identity Management | Cloud Security Library

END-2-END Security

Provisioning Production | Actor/Sensor Device | Smartphone App | Security Backend | Patient Cloud Web App

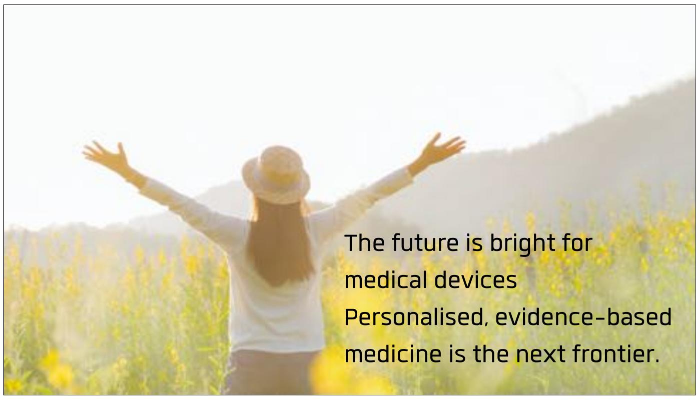
et me introduce the importance of end 2 end Cybersecurity with a few words about the Proregia Secure Platform, which combines all these activities in one Product and out of the box. More technical details about end 2 end Cybersecurity will be provided to you later on in this presentation.

The PROREGIA Secure Platform is the secure bridge for your applications to enter the Internet of Medical Things.

- it is Ready to go and therefore guarantees fastest time to market
- it provides very simple integration
- it provides End to end encryption and End to end authentication
- you have 100% control over every actor and sensor and 100% control over system- and personal data
- you have acces to and can visualize Telemetry data through customizable dashboards

The PROREGIA Secure platform is bulletproof and based on established technologies and security architectures from online money transaction systems, contactless payment systems and national security agencies applications.

Integrating your medical devices into the Internet of Medical Things, with the PROREGIA SECURE PLATFORM it will be simple, fast and according to highest security standards and data protection regulations



The future is bright for medical devices

Personalised, evidence-based medicine is the next frontier.

Hello & Welcome to our talk about cybersecurity for medical devices. My name is Larissa Naber, and I will guide you through cybersecurity root causes and mitigation strategies.

Personalised, evidence-based therapy is the next big thing in medicine. The combination of personal medical data with automated drug delivery systems will ensure patient compliance, eliminate over and underdosing and help minimise side effects. Automated gathering of detailed medical data in the field will speed up the drug development process.

Unsecured connected devices
can seriously harm patients,
device manufacturers and
drug development

The future looks bright; however, there are clouds on the horizon:

Connected devices pose a significant threat to patient safety and security.

Connected devices do not only endanger patients but are also a threat to their manufacturers. Manipulated data can seriously jeopardise drug development, depending on that data.

While patient safety is foremost on the mind of medical device manufacturers, cybersecurity is not, as evidenced by glaring security gaffes by major players in the field.

Are connected medical devices a bad idea after all?

So, are connected medical devices a bad idea after all? No, but they do require a stringent cybersecurity strategy.

I will be focussing on devices for patient use, as they tend to pose more cybersecurity risks. Still, most of the root causes and countermeasure equally apply to devices for institutional use.

Root Causes

Root causes of cybersecurity risk vastly differ from the reasons for electromechanical failure.

Ignoring Dynamics

The difference originates in the device’s environment.

An unconnected device lives inside a **static environment**, whereas a connected device lives inside a highly **dynamic environment**.

An unconnected device faces a **static set of threats**, whereas a connected device faces **dynamic threats**, which can arrive without even a minute’s notice.

Discounting Intentional Harm

Intentional harm is a misuse case that is absent from unconnected devices.
If you need physical access to the device’s user, there are more efficient ways to harm the user than tampering with his medical device.

If a hacker compromises a connected device via the Internet, the number of potential victims rises to the thousands.

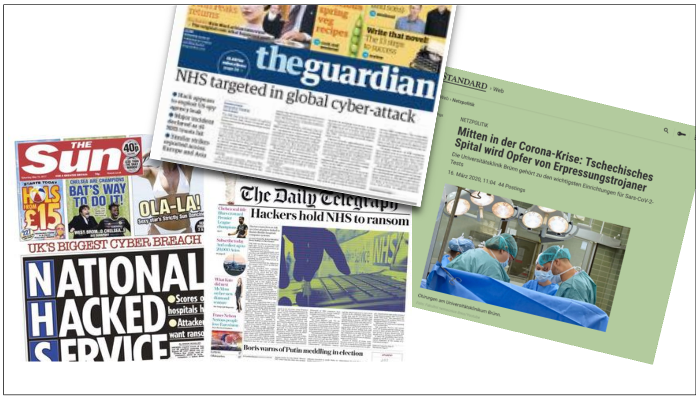
Of course, only psychopaths would attack thousands of innocent people.

Still, ordinary criminals have no qualms to hold them hostage for ransom.

Medical device manufacturers and pharmaceutical companies make for enticing targets.

—

Image credit: Hannibal Lecter, as he appears portrayed by Anthony Hopkins in The Silence of the Lambs. (c) MGM Pictures



theguardian

NHS targeted in global cyber-attack

The Sun

UK'S BIGGEST CYBER BREACH

NATIONAL HACKED SERVICE

The Daily Telegraph

Hackers hold NHS to ransom

Boris warns of Putin meddling in election

STANDARD › Web

Web › Netzpolitik

NETZPOLITIK

Mitten in der Corona-Krise: Tschechisches Spital wird Opfer von Erpressungstrojaner

Die Universitätsklinik Brünn gehört zu den wichtigsten Einrichtungen für Sars-CoV-2-Tests

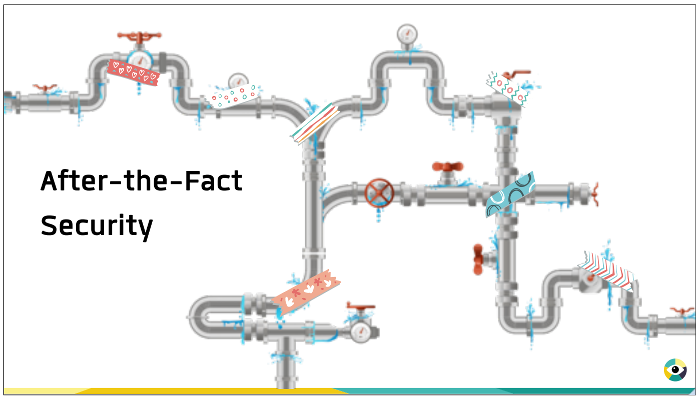
16. März 2020, 11:04 44 Postings

Chirurgen am Universitätsklinikum Brünn.

If you think this is rather far fetched, please note that in 2017 a ransomware attack shut down the British National Health Service (NHS) for **all of England and Wales.**

Within hours NHS was running hospitals in emergency mode, having to forego electronic patient records and advanced machinery such as MRI.

They are not alone: Currently, health care providers suffer ransomware attacks on a weekly basis.
The vast majority of these attacks are not targeted.
Health care providers fall victim to widespread, undirected ransomware attacks.



After-the-Fact Security

Adding connectivity to a legacy device is a surefire way to add cybersecurity vulnerabilities and associated risks.
Applying cybersecurity after effect, is like putting bandaids on burst pipes. You'll drown before you are done.
Therefore, cybersecurity must be an integral part of the design process.

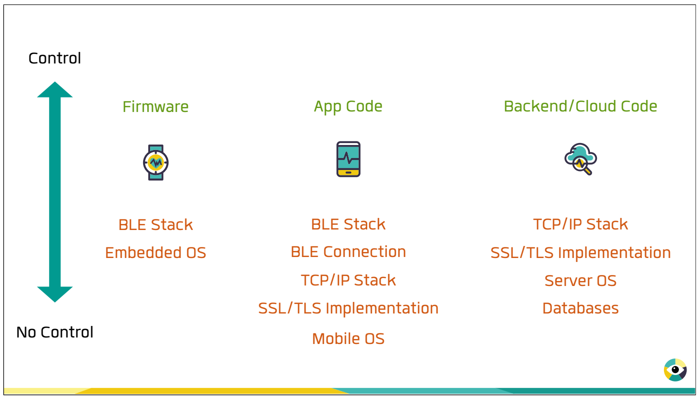
Inferior Components

Using inferior components

Most software does not concern life-or-death situations. Consequently, most software components are not developed to medical device software standards. After all, nobody dies if the bakery’s customer loyalty program gets hacked.

Before you include components, make sure that they satisfy your security and safety requirements.

Not all 3rd party components are equal:        Generally accepted cryptographic protocols, and software components developed for automotive, aerospace or banking use cases are usually more trustworthy.



Control

No Control

| Firmware | App Code | Backend/Cloud Code |
|---|---|---|
| BLE Stack | BLE Stack | TCP/IP Stack |
| Embedded OS | BLE Connection | SSL/TLS Implementation |
| | TCP/IP Stack | Server OS |
| | SSL/TLS Implementation | Databases |
| | Mobile OS | |

But for many dependencies, no trustworthy implementations are available.
You will need to leverage components entirely outside of your control:
mobile operating system, server operating system, wireless technology, TLS, server platforms, databases.

None of these components were designed for live or death scenarios.
These components have been exploited in the past, and likely they will be exploited in the future.

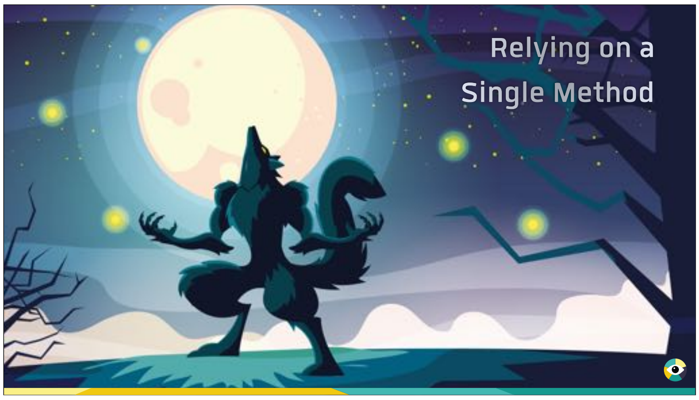
Fixing errors in transport protocols, communication stacks, or other standard libraries requires software owners, product manufacturers and users to act in unison. Unless the fix is deployed, the system remains vulnerable.

Stuff Outside Your Control

These uncontrolled components must never be your sole line of defence.

If you rely on standard operating systems or communication stacks for cybersecurity, you will reap what their creators sowed.

And you won’t like it.



Relying on a Single Method

Silver bullets are for werewolves. The idea, that a single measure will get rid you of all cybersecurity problems, is straight out of a fairy tale.

In real life, there is no silver bullet and no magic wand. There is no single measure that can magically secure your medical device. You will have to work for its security. You will have to continue working for its security; for as long as the device is in the field.

If you depend on 3rd party components, as we just discussed, each of these components must be safeguarded by some other mechanisms.

Risk Aversion

Let’s move on to a surprise entry: Risk aversion

I’m kidding you not. Too much risk aversion can compromise cybersecurity in three ways:
It can lead you
- To choose an unsuitable software development methodology or
- To choose an inappropriate risk assessment framework or
- To take the wrong risks entirely

Risk aversion? Really? Are you kidding me? How can risk aversion ever be a bad thing?
Risk aversion can seriously harm your product if it leads you to take the wrong risks, choose the wrong risk estimation method or the wrong development

methodology.

”Do or do not,
there is no try “

*Puppet character Yoda, as depicted in The Empire Strikes Back. © Lucasfilm Ltd.*

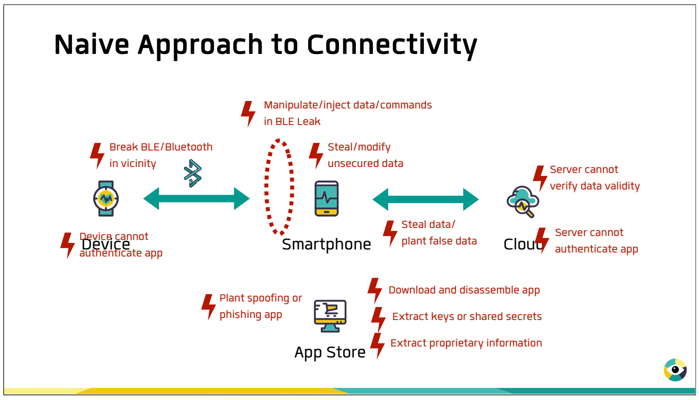
Just as Yoda says: “do or do not, there is no try”

At least not when talking about connected medical devices.

We often encounter the naive strategy: “Let’s use only a little bit of connectivity, just to be on the safe side.”

Unfortunately, a little bit of connectivity is not associated with a little bit of risk.

Rather, a little bit of connectivity might be just enough connectivity to get your customers killed.



## Naive Approach to Connectivity

Manipulate/inject data/commands in BLE Leak

Break BLE/Bluetooth in vicinity

Steal/modify unsecured data

Server cannot verify data validity

Device

Device cannot authenticate app

Smartphone

Steal data/ plant false data

Cloud

Server cannot authenticate app

Plant spoofing or phishing app

Download and disassemble app

Extract keys or shared secrets

Extract proprietary information

App Store

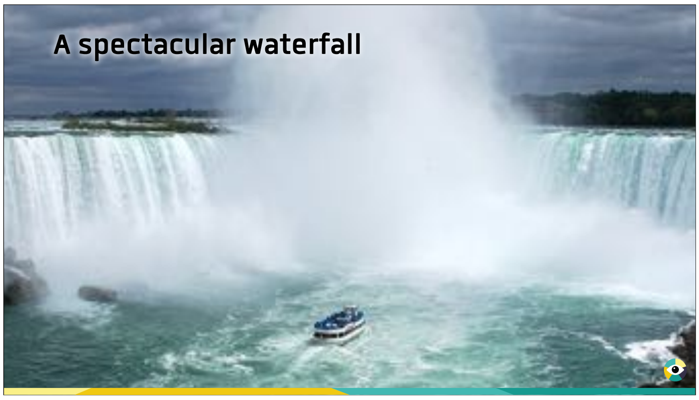
The naive strategy looks like this: you have the device, the user’s smartphone and an app downloaded from the app store. Maybe a web app, too.

Simple and Safe?

<click>

I’m afraid not.
Smartphones are toxic swamps entirely outside of your control, and you should treat them as **enemy territory**.

I won’t go into the details on these fallacies.



A spectacular waterfall

You wouldn’t ride a barrel down Niagara falls, so why are you using the waterfall model for a connected device?

There is a reason why the waterfall model fell out of favour in the mid to late 90ies: it is ill-suited for the connected world!

In a world, where strangers can dictate your security requirements via the Internet, you need to be able to react within hours, not months.

Since Lukas Ackerman has already extolled the virtues of agile development, I'll skip the details.

**Suffice to say: Speed matters**

Traditional risk estimation works very well for electromechanical devices, and might even work for your own software.
But, it will not work for tons of 3rd party software components.

You just included half the Internet as a dependency, and now you are speculating on the **probability of error occurrence** of other people's code.

Worse, you are speculating about **code that hasn't even been written**, yet. Some of the people you are speculating about, are are still in in kindergarten right now.

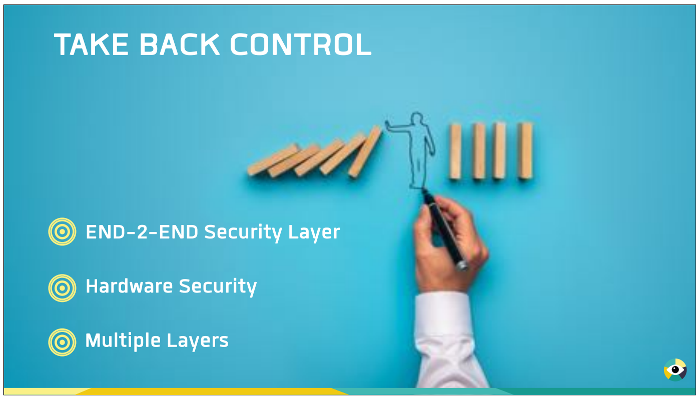
Better polish your crystal ball and call the local diviner. Or ask us about our **comprehensive cybersecurity risk assessment framework** - which would be a talk entirely on its own.

## Implementing Security

Enough of the problems, let’s move on to the solution.

How do I defend against the unknown?

So, how do you defend against the unknown?
How do you estimate the risk of the unknown?
How will you live with uncertainty?

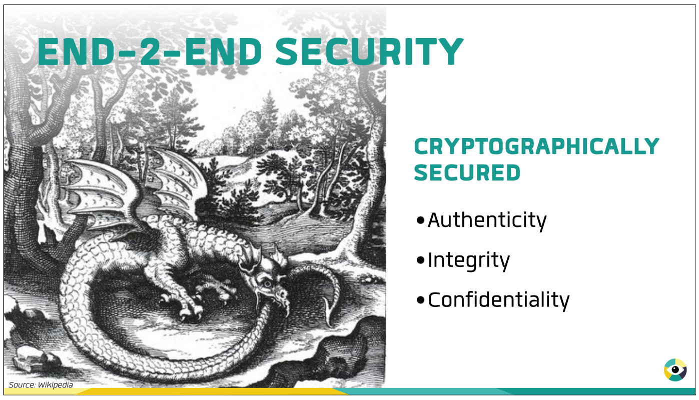


## TAKE BACK CONTROL

- END-2-END Security Layer
- Hardware Security
- Multiple Layers

To defend your connected device, you first need to take back control.

You obtain control
- by implementing an end-2-end security layer
- by using hardware backed security
- and by applying multiple security layers



## END-2-END SECURITY

### CRYPTOGRAPHICALLY SECURED

- Authenticity
- Integrity
- Confidentiality

Source: Wikipedia

The first thing you need, is a cryptographically secured end2end layer entirely under your control. You must be able to replace all parts of this layer as needed.

You need to secure

- Authenticity: by applying Digital Signatures or Authenticated Encryption
- Integrity: by applying a CMAC (Cypher-based Message Authentication Code)
- Confidentiality: by using encryption

Authenticate Everything

Who? Me?!

That wasn't me!

Speaking of encryption: people tend to focus on the wrong end of the cryptographic chain.

In medical device use cases **authentication usually is more important than confidentiality**, and way more difficult to provide.

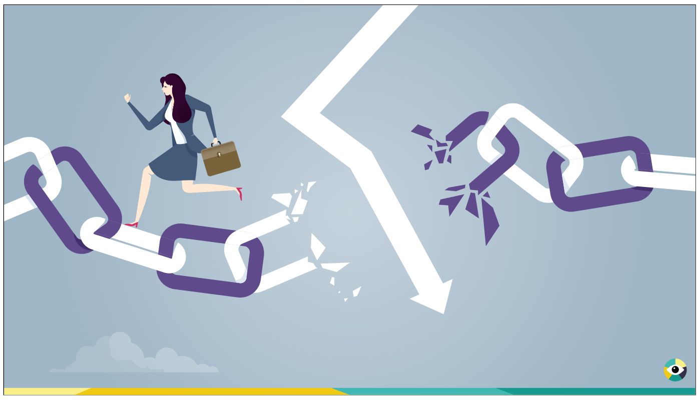
If you do not provide authenticity, your devices can execute fraudulent commands or a hacker could inject false data.

For all your creature comforts regarding cryptography, you should invest in a root of trust.
No, we are not talking about a holiday in the Caribbean, but of a computer-chip called Secure Element (SE). The server equivalent is called an HSM (Hardware-Security-Module).

Hardware is completely impervious to social engineering, which still makes up the bulk of cyberattacks.

You probably never heard of secure elements, but you use them every day. They are inside your debit and credit cards, your smartphone and your passports.

Why should you trust it? Because FIPS-140-2 Level 3 is way worse than all medical device norms together.



Any risk mitigation strategy for the connected world has to accept that there will be compromisation; it's inevitable.

Therefore, a single vulnerability must never bring down the whole system.

But, how do you design such a system?

Impenetrable cybersecurity architecture requires many ingredients.
-- Think about a burger.
— You have your meat patty - very tasty,
-- but the skimpy bun won’t do you much good -
-- you definitely need more flavour.
-- Veggies are good for you - five a day, keep the doctor away.
So let’s add some

- salad,
- Savoury tomatoes
- and maybe some onions.

-- Still not good enough? Hmm, how about some secret sauce?
-- Very tasty, but how does that translate to cybersecurity?
-- Well, you need to protect your data and commands - the meat.
-- Transport security won't help you much, but **end2end**

- authentication,
- integrity
- and confidentiality

make it much better.
And as a nasty surprise for the hacker, let's include a secure element.

<click>
Tada!

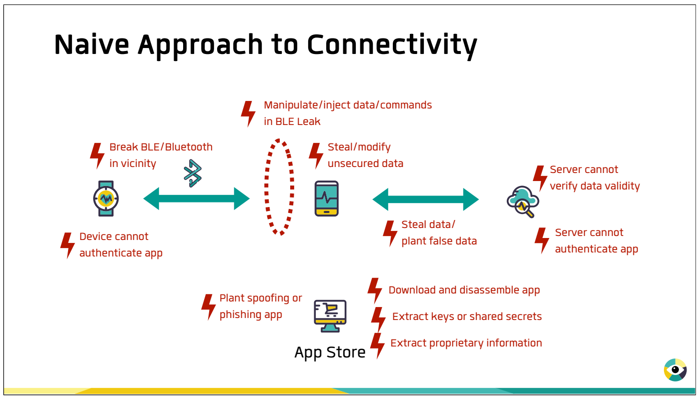
Cybersecurity managed!

Oh! Sooooo many layers of security

Since we are an equal opportunity security provider, there is also a veggie option.

We have a huge catalogue of technical and organisational countermeasures that are applicable to a wide range of attack vectors.
But I ran out of burger analogies.

The take away: Any attack vector should be safeguarded by numerous, independent countermeasures at all times. **The more layers, the better**.



## Naive Approach to Connectivity

Manipulate/inject data/commands in BLE Leak

Break BLE/Bluetooth in vicinity

Steal/modify unsecured data

Server cannot verify data validity

Device cannot authenticate app

Steal data/ plant false data

Server cannot authenticate app

Plant spoofing or phishing app

Download and disassemble app

Extract keys or shared secrets

Extract proprietary information

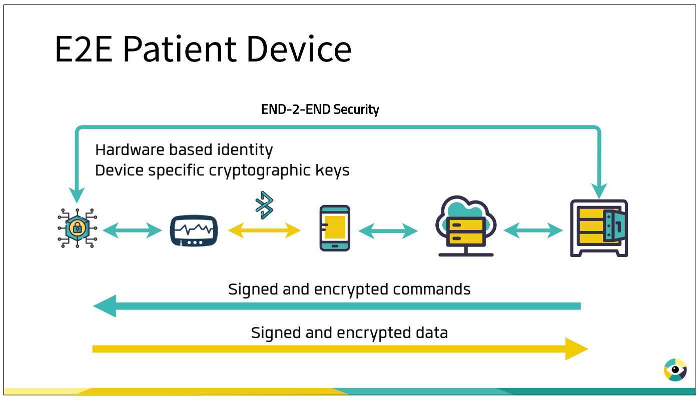
App Store

Do you remember this slide?

What if I told, you all your troubles can disappear?

No,  not magically, but by applying the aforementioned countermeasures:

- End2end security layer
- Multiple layers of defences
- Hardware backed cryptography



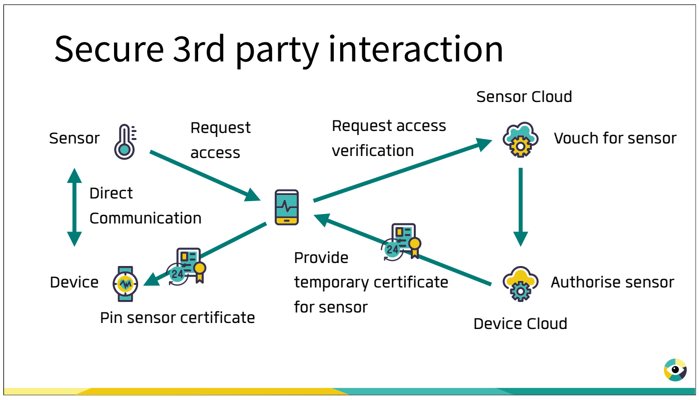
E2E Patient Device

END-2-END Security
Hardware based identity
Device specific cryptographic keys
Signed and encrypted commands
Signed and encrypted data

This diagram shows the previous naive use case, now hardened by end2end security and hardware-based cryptography.

Signed and encrypted commands move down to the device,
signed and encrypted data moves up to the cloud.

Even if a hardware change is out of question, most of the functionality can be realised as software and still garner a massive security boost.



Secure 3rd party interaction

Sensor Cloud

Sensor

Request access

Request access verification

Vouch for sensor

Direct Communication

Provide temporary certificate for sensor

Device

Authorise sensor

Pin sensor certificate

Device Cloud

Once you have secured your own device system, the concept can be easily extended to 3rd party device integration. For example, you could add a sensor to your dosing device.

The sensor needs to proof its identity in cryptographically strong way. The sensor will present his digital ID; the ID will be verified by the sensor manufacturer and forwarded to the device manufacturer. The manufacturer will then sign the the digital ID and forward it to the app and device.

Both app and device will pin the sensor certificate in the most secure manner available. The sensor certificate is device specific and will only work for the specified sensor and device pair. Sensor and device can now communicate directly in a highly secured manner with out the interaction of unreliable 3rd parties such as smartphones.

How much security is enough?

Photo by Jean Wimmerlin on Unsplash

Since there is no such thing as too much security, it is crucial to know when to stop. Let’s answer this with a story: ‚Two researchers happen upon a hungry lion in the savanna. The first researcher bends down to secure his shoelaces, and the second guy asks him: “Do you think this will help you to outrun the lion?”. The first one replies: “I don’t have to outrun the lion; I only have to outrun you!”

So, how much security is enough? If you implement all of the above suggestions and keep up with the security updates and latest product versions, you have a system that is secure enough to withstand cybercriminals. They start looking for lower hanging fruits. Hackers who hack for fun, not for profit do not move on: They enjoy the challenge. They are either users of your product or friends and family of a user and thus usually not a threat. Start a bug bounty programme or hire them to give them the recognition they deserve.

Too complicated?

Try our time and effort saving solutions:

- End-2-end security framework
- Design verification
- Post Market Surveillance

Our end-2-end security framework works out of the box. You can focus on your customer, we will focus on your security.

- Authentication, encryption, digital Signatures
- Asset management
- Multi Layer Security

Escape the regulation maze
with pre-market evaluation

Get independent pre-market evaluation now:

- Architecture & Design Review
- Penetration Testing
- Security Consulting

Post Market Surveillance

Cyber security threats

Don’t hire a private eye to surveil the market, we’ve got you covered:

- Customisable alerts
- Threat analysis
- Mitigation planning
- Preemptive maintenance planning

GAME OVER!

For the hacker ;-)

The future for medical devices is bright after all!

Game over, but this time for the hacker.
The future of securely connected medical devices is very bright, indeed!

Thank you for listening. I’ll hand you over to Mathias Steck.

The future for medical devices is bright after all!