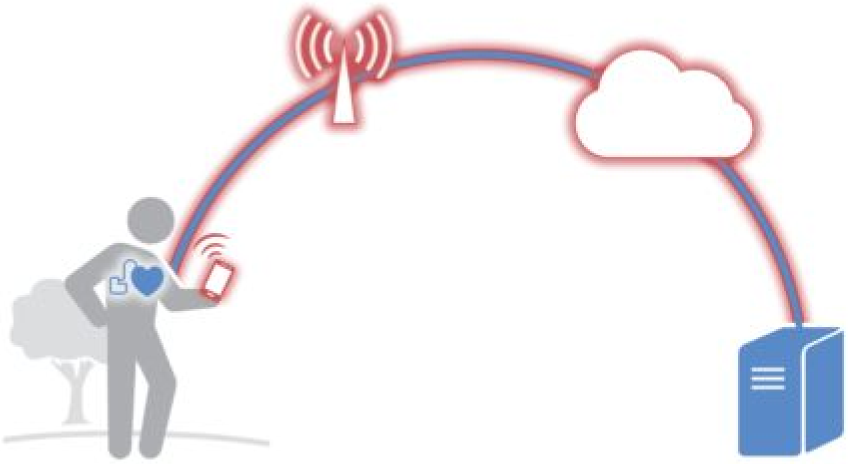
Security for Mobile Medical Devices

27 October 2017 | **Healthcare, Internet of Things** | Andreas Beck, Reto Eichholzer
Reading time: 3 minutes

Cloud based data analytics provides an efficient approach to Personalized Medicine – experience of huge patient collectives can be aggregated, analyzed and immediately used to derive optimized treatment plans. However, it has considerable security implications: Nobody wants his location profile or blood sugar levels disclosed, or his pacemaker settings or the dosage of his insulin pump changed by the latest computer virus.

Security for mobile medical devices is a challenging task, as the security of the overall system is determined by its weakest link. A common weak link in IoT type devices is the use of the end customer's mobile phone. While it allows for a smooth user experience at low cost, it is inherently unknown whether they are secure: Mobile phones often run old, unpatched software, jailbreaks and other apps of questionable origin.

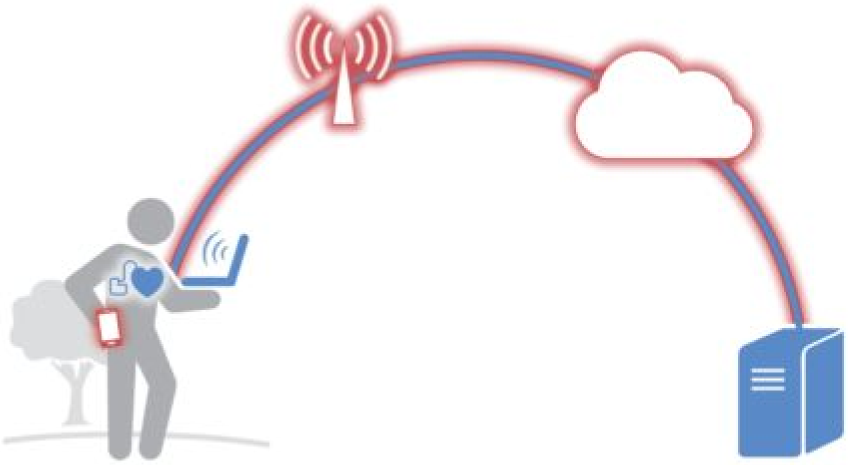


Safely connecting to your company servers by using an encrypted VPN channel (blue) that is routed through unsecure networks (red).

This is a challenge that has been elegantly solved in the Enterprise IT world for a while now using VPN technology.
By using an encrypted communication "tunnel", it has become possible to connect to your company network from anywhere in the world and access highly sensitive data, regardless of the security of the network you are using.

This principle of securing the communications channel by an encryption layer can be applied to Medical Devices, making the mobile phone just another piece of untrusted network infrastructure, relaying the communications between the device and the cloud service with no chance of eavesdropping or tampering with it. With modern microcontroller technology, this has become feasible with no significant impact on device size, energy consumption and component cost, enabling the use of the concept even for embedded devices.

Even if the mobile is used to display values or change settings, this approach allows for logging and validating such data by the cloud infrastructure before transmitting them to the IoT device. This minimizes exposure to threats on the mobile device, leaves a clear audit trail, and allows triggering emergency procedures on suspicious activity .



Safely connecting a medical IoT device to the cloud: The device communicates with its backends servers on an encrypted, secure channel (blue) that is routed through unsecure devices and networks (red).

Obviously, the challenge of making medical IoT devices secure is more complex than that. There are numerous details from securely storing encryption keys and authentication tokes, over authenticating data from devices that may have been tampered with, isolating devices against interference, right down to ensuring availability and upgrade paths that need to be done right, if you want to have a secure product.

Zühlke has developed a comprehensive set of methods and solutions to address these issues. We provide security in depth by combining technical measures like strong cryptography and code hardening with an organizational framework that ensures data is only stored and disclosed on a need-to-know basis, allows for keeping data within a regulatory domain and the owner of the data in control of it.

Please feel free to contact me, if you would like to discuss your IoT security concept.