CONNECTED DRUG DELIVERY DEVICES: BENEFITS AND CYBERSECURITY

In this article, João Budzinski, R&D Director at Debiotech, discusses the benefits of connected drug delivery devices and the importance of cybersecurity when developing them, including the threats, key considerations and potential solutions.

> "There is more to consider than just the potential advantages; connecting a drug delivery device also requires careful consideration of several issues, including regulatory requirements, data protection and cybersecurity."

There are many reasons to connect drug delivery devices. Firstly, there are benefits for the patients. However, healthcare providers and medical device manufacturers can also benefit greatly from connecting devices and opening communication channels to send or receive information. Obviously, there is more to consider than just the potential advantages; connecting a drug delivery device also requires careful consideration of several issues, including regulatory requirements, data protection and cybersecurity.

ADVANTAGES FOR PATIENTS, HEALTHCARE PROVIDERS AND DEVICE MANUFACTURERS

Home-based devices bring obvious benefits to patients; enabling patients to perform their therapy at home instead of having to go to a clinic or hospital improves their quality of life. In some cases, the liberty of being able to perform the treatment at home can actually improve the therapy's results due to more frequent dosing and better adherence to treatment. Connected home-use devices allow these benefits to go one step further.

Physician Advice, Based on Data

Connected home-use devices can provide physicians with a wealth of valuable data to improve a patient's therapy. Connected drug delivery devices can inform them of the exact doses that were administered and when, meaning a physician can see when doses were skipped and try to understand why – there is no more need for guesswork. With access to this data, physicians are no longer left wondering, "Did my patient forget a dose? Did they really take it regularly? Am I getting the whole story?"

Connected drug delivery devices also enable physicians to act on the data before the patient's next consultation. Indeed, devices that can receive prescription updates over the cloud can enable physicians to improve a patient's therapy quicker and more effectively than by traditional methods.

Device Diagnostics

A connected device can easily transmit logs and information about its usage. Sensor data can provide early warnings about device failures. This data is extremely valuable for device manufacturers to understand their device's behaviour in the field, providing priceless insights in how to build better devices or improve current ones.

Coaching for Better Therapy

Many use cases for a connected drug delivery device involve passing on information so that other stakeholders can analyse it. However, advances in machine learning and artificial intelligence are proving their effectiveness in adapting therapies to patients' unique physiological responses. Although this is a new field, there are efforts to create regulatory pathways for this type of technology.

If it is indeed deployed, this type of technology can coach each patient individually to improve their therapeutic results, such as by proposing doses precisely tailored to a patient's physiological response. This is particularly notable in the case of insulin, where there are general rules to calculate insulin doses but each person responds differently to therapy. In this case, connected drug delivery devices could allow

João Budzinski
R&D Director
T: +41 21 623 6000
E: j.budzinski@debiotech.com

Debiotech SA
Av. de Sévelin 28
1004 – Lausanne
Switzerland

www.debiotech.com

> "Ransomware has boosted the motivation for hacking medical devices to a whole new level, making it vital to consider every aspect of cybersecurity on connected medical devices – patient safety is very much at stake."

access to advanced and powerful algorithms that can analyse substantial amounts of patient data and propose improvements to a patient's individual therapies at a much higher frequency than clinicians could.

CYBERSECURITY

Motivation

Not so long ago, cybersecurity was not a great concern for medical device manufacturers. Hacking was perceived as a threat for activities like banking and other high-profit apps, where the motivation for hacking was considered high. There was the misconception that the only reason a hacker would want to attack a medical device would be to harm a patient. There is an argument that, if you want to kill someone there are much easier and more effective methods than hacking their medical device. As such, motivation for hacking drug delivery devices was considered low.

Enter ransomware. Now, hackers can hold entire hospitals hostage, waiting for payment to release the hacked computer systems from their grasp. If a model of connected drug delivery device is vulnerable, a hacker could prevent an entire group of patients from getting their therapy until their demand for payment is met. The requested ransoms for these attacks can be astronomical. Ransomware has boosted the motivation for hacking medical devices to a whole new level, making is vital to consider every aspect of cybersecurity on connected medical devices – patient safety is very much at stake.

Sources of Cybersecurity Risks

An attacker has several potential points of entry into a system, so it is important to protect a device against as many types of attack as possible. The best way to ensure this is by a systematic analysis of potential threats and making sure none of these can be exploited by a malicious entity.

Interfaces

Obviously, connected devices will have internet access, via some kind of physical interface, such as wi-fi or an ethernet cable. It is vital to restrict the attack surface on these interfaces. However, there are other interfaces that must also be considered. For example, a connected drug delivery device could connect to a smartphone over Bluetooth. Bluetooth interfaces are notably a weak point for cybersecurity; therefore, a device manufacturer must take extra steps to ensure this interface cannot be exploited by an attacker.

Even lower-level interfaces, such as JTAG connectors used to install software on a processor during the manufacturing process, must be considered. Such interfaces might be neglected; the argument for doing so is that an attacker needs physical access to a device to exploit such an interface. While it is true that this interface is difficult to exploit once the device is on the patient's body, it is important to consider the risk that an attacker could gain access to the device at other moments of a device's lifecycle – after manufacturing, during transport or in a warehouse. There are ample opportunities for attackers to insert malicious software.

Services

Beyond the physical interfaces, at a higher level, software services provided with a device may introduce new security weaknesses. For instance, the ability to remotely update, enabling the quick deployment of new software versions, is a necessity for cybersecurity patches. Ironically, such remote update services are a favourite target among hackers – if exploited, they allow a hacker to deploy virtually any software they wish onto a device.

Software Supply Chain

There are potentially vulnerable steps on the software supply chain. During these steps, an attacker could alter the software to include malicious code:

- **Build:** Even with perfectly secure software on a drug delivery device, an attacker could render all that security worthless if they attack its build environment. This is a particularly insidious type of attack, as the hacker can use the developer's own infrastructure to generate a valid certificate for their malicious software.
- **Delivery:** How a developer sends its software to the manufacturing site is also critical. An attacker could intercept this delivery and alter the software at this stage.
- **Manufacturing:** If a hacker successfully attacks the manufacturing plant, they could use the plant's manufacturing capabilities to deploy devices with their malicious code installed on them directly from the factory.
- **Maintenance:** Maintenance usually requires elevated privileges on the device for a technician to perform the necessary work in the field, including software updates. It is important to consider the possible consequences of these privileges carefully; otherwise, an attacker could exploit this privileged access to a device.

WHAT TO DO

Unfortunately, there is no easy one-size-fits-all solution for cybersecurity. As with any medical device development, it starts with risk analysis. From a regulatory perspective, the US FDA has more detailed guidance and stricter requirements than the EU when it comes to cybersecurity. However, when considering data protection laws, the EU has stricter regulations than the FDA.

Consider the following example of a connected device being developed for the American market. Knowing the strict cybersecurity requirements from the FDA, the developer secured the device – the threat model was done, all interfaces were analysed, sensitive data at rest was encrypted, all communication with the cloud services was encrypted, public key infrastructure was deployed and secure, and all applicable vulnerabilities were analysed and treated.

This was all fine for the FDA, but the first feedback required the developer to go one step further – they also needed to implement secure boot mechanisms to ensure that every step of the boot process is verified and secure. Implementing such mechanisms naturally slows down development. With this requirement, the developers became unable to simply install new software on the device for necessary development tests – for the devices to boot at all, the software must be signed correctly. This required significant effort, but it paid off – the device in question received 510(k) clearance this year.

Cybersecurity Risk Analysis

It is useful to make a clear distinction between security and safety. For cybersecurity issues, one of the most useful methods for identifying threats is threat modelling. In threat modelling, the goal is to identify all external interfaces and perform a systematic analysis of the common threats for each interface. A useful model for this analysis is the STRIDE model – for each interface, the goal is to identify the consequences of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege.

Given the wealth of information available, it can be challenging to identify the correct methods and resources for each device. Furthermore, once everything is identified, there is a lot more work to be done – analyse all the results, make the necessary modifications to the software, go through usually hundreds (if not thousands) of applicable vulnerabilities and document the results. However, being able to provide a secure device for the patients is worth the effort. The following are useful sources of information to help build cybersecure devices:

OWASP

The Open Web Application Security Project (OWASP) provides a wealth of resources, including security-testing guidance, dependency tracking, a list of source code analysis tools, threat modelling tools and lists of software composition analysis tools, among others.

FDA Guidance

The FDA provides detailed guidance on cybersecurity and is a useful support for cybersecurity activities. However, while FDA guidance tends to be practical and detailed, the challenge is how to interpret the guidance most appropriately for the particularities of a given device.

UL 2900 Series

The UL 2900 series particularly can be useful in the development of cybersecure devices. Obviously, not all the clauses apply to all drug delivery devices, but it is a useful exercise to analyse all the clauses and decide explicitly if each clause is applicable to a given device – a systematic analysis of all clauses helps protect a device against the most common threats. It is key to document what is applicable, what is not applicable and the rationale behind each decision.

> "When it comes to cybersecurity, it is best to use standard, state-of-the-art components with proven efficacy."

Cybersecurity Risk Control Measures

Safety and security risks are not mitigated by the same type of risk control measures. For example, while a drug delivery device may have proprietary safety measures, some of the security measures could be based on open-source solutions. This may be the case because cybersecurity risk control measures often require algorithms for encryption, certificate generation and signatures, which may be outside the scope of a digital drug delivery device's development process. When it comes to cybersecurity, it is best to use standard, state-of-the-art components with proven efficacy.

Secure the Software Supply Chain

This is a remarkably interesting area when looking to take security one step further. There are three frameworks to note regarding software build and update processes. Indeed, as mentioned before, software-update mechanisms can be a significant security breach if exploited by a hacker.

- **in-toto:** Full supply chain framework from initiation to end-user installation
- **The Update Framework (TUF):** A software framework designed to protect mechanisms that automatically identify and download updates to software
- **Uptane:** Similar to TUF, but tailored for the automotive industry and therefore particularly well-suited for embedded applications such as drug delivery systems.

CONCLUSION

Connected drug delivery devices offer remarkable benefits to patients, physicians and manufacturers. However, these benefits come at the cost of security risks. A thorough process for cybersecurity throughout the software development and deployment chains is necessary to ensure that all stakeholders enjoy the benefits of connection, without worrying about attacks by malicious players.

ABOUT THE COMPANY

Debiotech has a long history in the design and development of highly innovative medical devices. The company started with complex mechanical systems and incrementally developed its team and expertise to develop compliant and fully connected medical devices, allowing patient monitoring and remote patient treatment definition. Debiotech's expertise is available to the community; it provides design and development services for medical devices, components or other solutions with similar cybersecurity and data-management constraints. The company's know-how has been recently highlighted by the 510(k) clearance of the home-use peritoneal dialysis system developed by Debiotech for Fresenius Medical Care.

ABOUT THE AUTHOR

João Budzinski completed his academic training at the Federal University in Brazil and started his career in safety-critical devices at Dräger Safety in 2002, developing both hardware and software for toxic gas detection devices. Later, he joined SICPA in 2004, where he was responsible for the development of security solutions against counterfeiting and tax evasion. There, he started as a hardware and embedded software engineer for security solutions, later becoming Project Leader for the development and deployment of these solutions for international customers, and finally becoming Engineering Manager and Principal Engineer. Mr Budzinski joined Debiotech in March 2015 and was appointed R&D Director in 2022.