Your Data is Only as Secure as Your Device

Alan Grau, CEO, Icon Labs

The inherent insecurity of many medical devices was highlighted in a recent FDA and Homeland Security alert. Over 300 devices have been identified that utilize a hard code password, creating a huge security loophole. With so many medical devices now collecting and storing patient data, this raises the question of how secure is the data stored on these devices? In the case of these 300 devices with hard coded passwords, not very secure at all.

There are two ways to gain access to the data stored on medical devices. The first is to intercept the data during communication. The second is to access the data from the device itself. Like any good chain, security is only as strong as its weakest link. To ensure the data is secure during communication, secure communication protocols such as IPSec, SSH, and SSL can be used. These protocols encrypt the data during communication, keeping it safe even if the traffic is intercepted.

To ensure that someone does not gain access to the device, and thereby gain access to the data stored on the device, requires that security measures be built into the device. The device should utilize a strong, configurable password or other secure authentication method. An endpoint firewall can also be utilized to control communication and block attacks. The bottom line is, your data is only as secure as your device.

Click here to see a feature article from Alan Grau on device security at mdtmag.com

[1].

Source URL (retrieved on *09/24/2014 - 12:45am*):
http://www.wirelessdesignmag.com/blogs/2013/09/your-data-only-secure-your-device?qt-photo_of_the_day=0

Links:
[1] http://www.mdtmag.com/articles/2013/07/medical-device-security%E2%80%94beyond-password