The Solution to Medical Device Security Also Could Save Tens of Thousands of Lives and Millions of Dollars

February 24, 2017

Evolver, Inc.

The Solution to Medical Device Security Could Save Tens of Thousands of Lives and Millions of Dollars

The cybersecurity of medical devices has become a major topic in recent news in the last year as stories about the vulnerabilities of the Hospira Infusion System[1] and the St. Jude implantable devices[2] hit the front pages. The threat to patient safety through the cyber-attack of devices has even risen to the level of Congressional hearings[3]. Numerous stories have been written on the subject and multiple conferences have been held, including FDA public workshops[4]. Consequently, the FDA has published pre- and post-market guidance documents[5] for device manufacturers. Understandably, many of the discussions are focused on how to design protection into future devices, which may require design changes that will take several years before they are available for deployment in hospitals. One answer to the medical device security problem, however, may actually save thousands of lives per year and save hospitals millions of dollars.

Most of the discussion around medical devices has focused on how the companies building the devices can either make their newest devices more secure or how to modify existing devices to improve their security posture. The reality is that many of the devices cost tens of thousands of dollars and have operating lives of five to fifteen years. A hospital is not going to replace these devices solely because of a cyber vulnerability …it is just not practical. So the devices that are in the hospitals are likely to be there for quite a long time. Therefore, the cybersecurity solution has to assume existing legacy devices have to be made more secure.

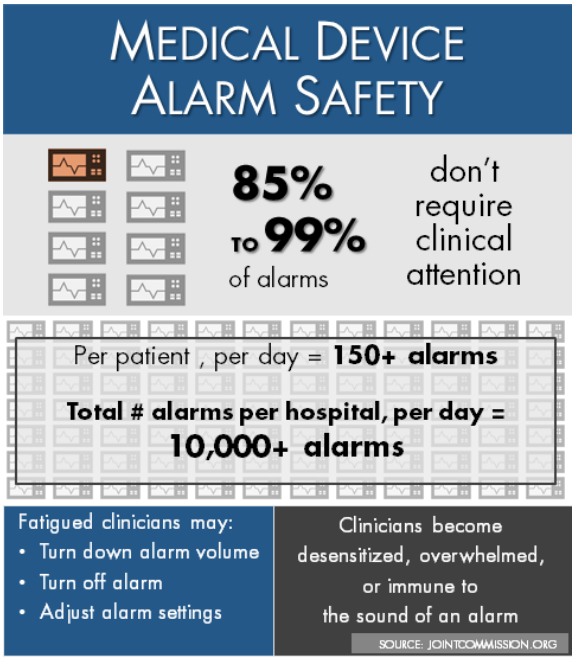

Figure 1

Many Devices, Many Alerts, Many Deaths

Hospitals require a myriad of medical devices to deliver modern healthcare, and many of these devices generate alarms or alerts when patient or device parameters are out of an acceptable range. Most medical device alarms are "nuisance" (or non-actionable) alarms that don't require intervention by a doctor or nurse – they resolve by themselves. Medical staff are bombarded by alarms that eventually desensitizes staff to their criticality. Additionally, the alarms alone are not sufficient do not put the problem in context of the overall patient status, complicating decisions and actions. As shown in Figure 1, excessive alarms are a well-recognized problem since 85-99% of alarm signals do not require clinical intervention.

This type of alarm fatigue is just one part of an alarming safety problem. According to the 2013 *Journal of Patient Safety,* between 210,000 and 440,000 patients each year who go to the hospital for care suffer

some type of preventable harm that contributes to their death[6]. In May 2016, Johns Hopkins released a study indicating that death from medical errors account for the third highest cause of death in the U.S. behind cancer and heart disease [7]. The rapid growth of technology has provided opportunities for new clinical information systems and capabilities that *should* be decreasing preventable harms. Despite the promise implicit in these new technologies, there is increased information overload and alarm fatigue.

A Flawed Connectivity Architecture for Medical Care and Cybersecurity

The rapid growth of technology over the past twenty years has resulted in a lot of new clinical information being available. Unfortunately, there was never a patient-centric device integration architecture for these devices, and many have been integrated through a series of one-off, one-to-one, and proprietary systems.

As shown in Figure 2, a common patient environment has numerous devices all providing independent data though individual displays and unique interfaces to medical staff. As devices proliferate, so does the complexity of both device management and information correlation. Caregivers must become information integrators at the same time as they are dealing with the heavy demands of caring for patients. The introduction of new devices to improve patient care is hampered by the concern of further complicating device management and information correlation.

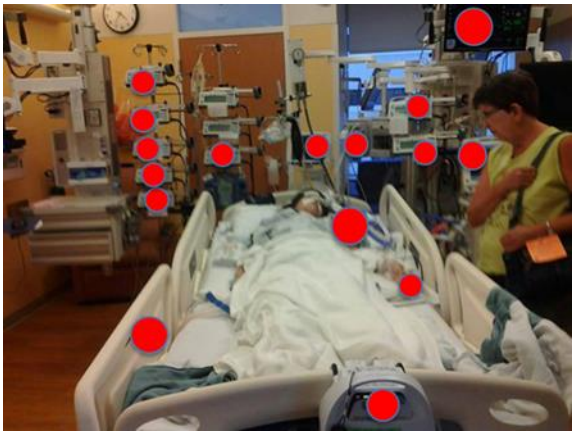

Figure 2, courtesy of [http://1.bp.blogspot.com/-S-nPZ1G0-3Y/UfRe7R339yI/AAAAAAAAAc8/s2w59_5QCU8/s1600/CHW4.jpg edited by JM Goldman, MD]

The ad-hoc connectivity typical of medical devices shown in Figure 3 also is a challenge to cybersecurity. In cyber terms, each of those red dots is an attack surface that can be exploited as part of a cyber-attack. Increasingly, devices use wireless data connectivity, making the attack surface even broader.

Furthermore, since many of the devices were made wireless with little cyber protection in the design, the attack surface may be broad and immature…a very bad situation from a cybersecurity perspective. As mentioned earlier, these devices cost tens of thousands of dollars and will likely be in use for years before prior to replacement.

Saving Lives and Protecting Hospital Infrastructures

Interestingly, an approach to enable safer care while improving cybersecurity is the same: a change in architecture. The recommended change is the result of research performed by Dr. Julian Goldman and his team at Massachusetts General Hospital (MGH), funded by the National Institutes of Health, National Science Foundation, and U.S. Army over the past twelve years. Dr. Goldman is the Medical Director of Biomedical Engineering for Partners HealthCare System and an anesthesiologist at MGH. He founded the Medical Device "Plug and Play" (MD PnP) Interoperability program in 2004 to promote patient safety and clinical care by leading the development of patient-centric integrated clinical environments (ICE) 8. Years

of collaborative work resulted in an international standard for a platform-based ICE architecture – ASTM F2769. 9

DocBox

An important outcome of Dr. Goldman and the MD PnP program's research collaborations has been the development of the first commercial ICE platform by DocBox, Inc. DocBox, Inc. is headquartered is Newton, MA, developed a point of care ICE platform for use at the bedside. The DocBox implementation changes the overall architecture of the clinical environment from a series of independent devices into an interoperable platform. Figure 3 shows the current architecture, both networking and data, that is employed in clinical environments today.

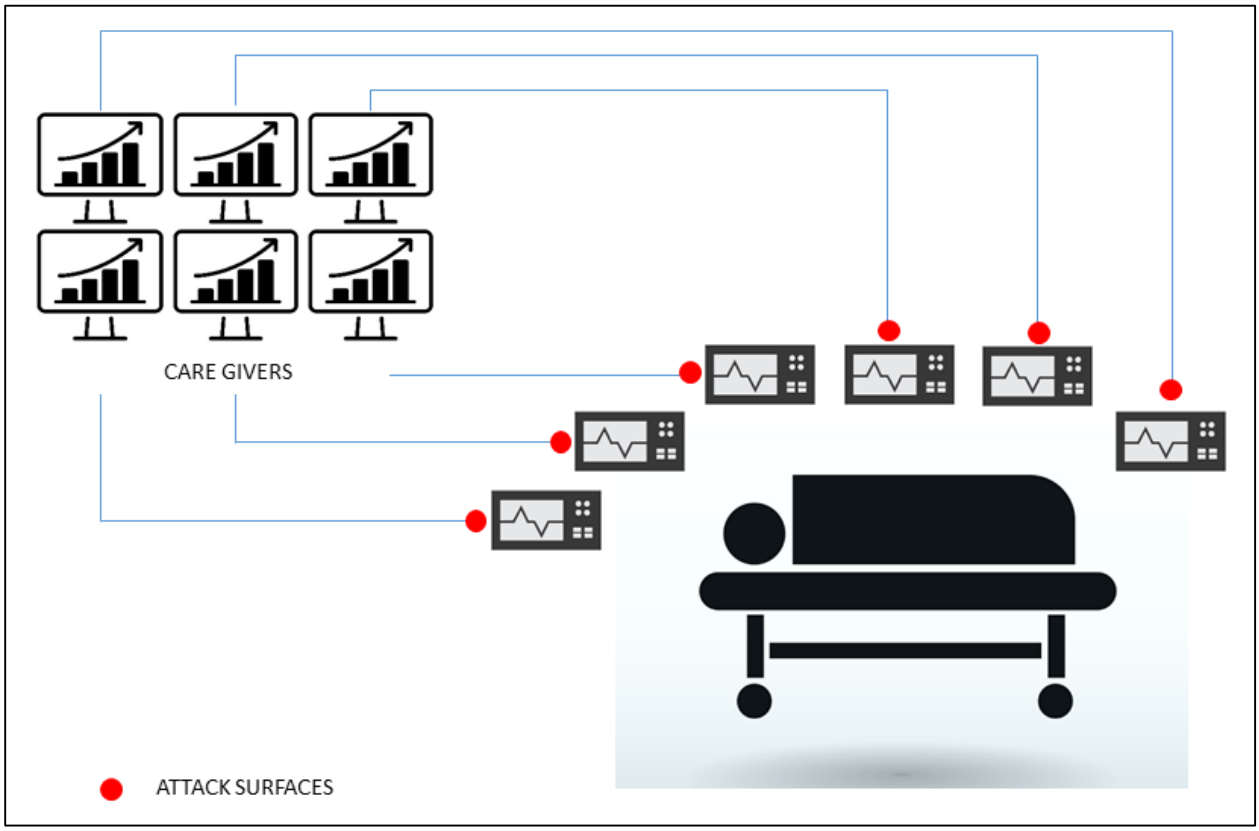

Figure 3

Under the ICE approach, the architecture changes dramatically. The devices communicate with a DocBox unit at each bed that then normalizes the data and provides a correlated view to the caregiver at the bedside. Instead of presenting caregivers with numerous potentially partial and differing views of information from individual devices, the caregiver sees a contextually aware, integrated view of the patient through apps which run on the platform. The platform enables the development and deployment of apps which can reduce alarm fatigue.

Reducing Attack Points

The change in architecture also has another positive outcome, it reduces the cybersecurity attack surface of the clinical environment. As described before, the current environment has numerous attack points using devices that were not built with strong cyber protections. The implementation of the ICE architecture with DocBox reduces the attack surface to one unit at each patient. Furthermore, increased capabilities can be built into the interface layer of the DocBox that communicate with the devices, providing a greater level of security. Figure 4 shows the reduced attack surface and improved cyber protection from the current environment to a DocBox driven clinical environment.

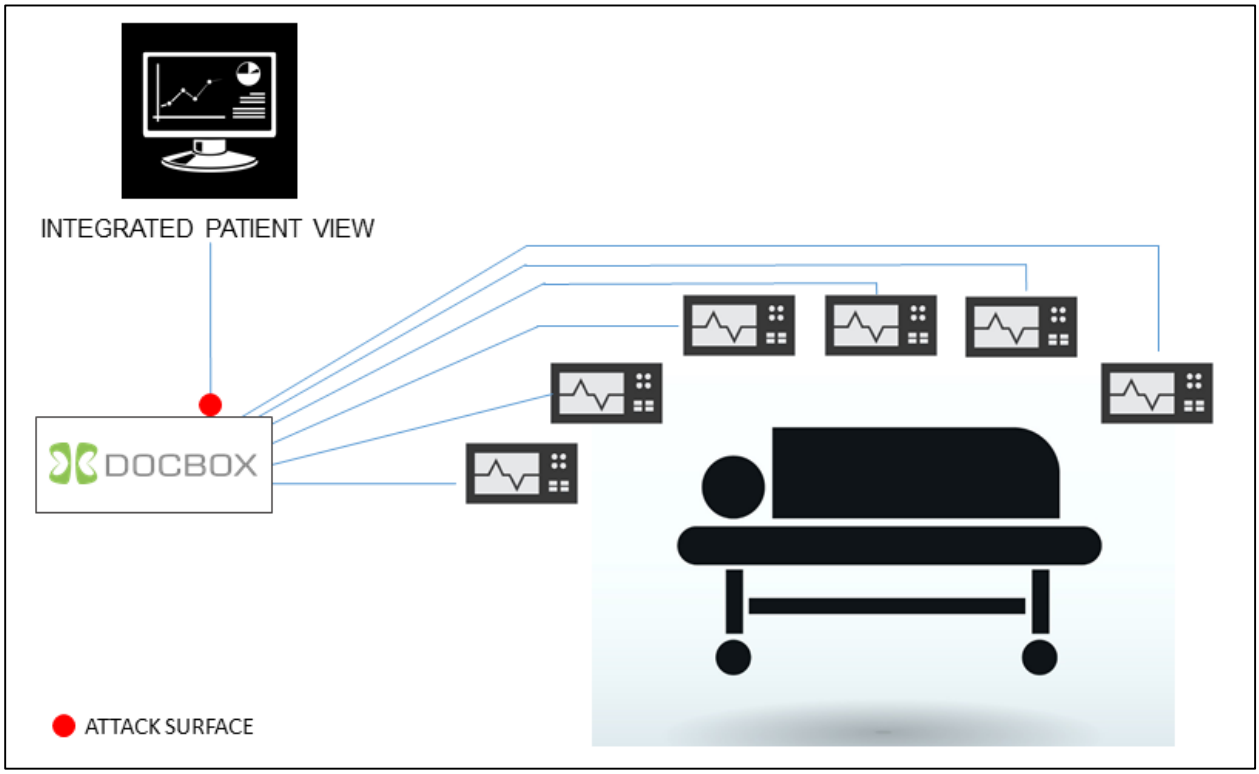

Figure 4

Another advantage to this architecture is that new technologies can be introduced into the environment without a major increase in cybersecurity risk to the facility network. Logical and business driven decisions can be made on devices as opposed restricting capability growth because of concern over introducing new technologies into the network.

Saving Patients, Protecting Devices

Three important capabilities of an ICE / DocBox implementation are

- the core mission of healthcare, saving the lives of patients, can be achieved
- there is a significant increase in patient care efficiency which reduces costs
- addressing one of the major issues facing clinical facilities today: cybersecurity

The DocBox platform is undergoing the first implementations today and is expected to be available in the US in late 2017. As hospitals and other facilities begin to tackle the cyber challenge, spending a lot of money on new devices and cyber tools would be better directed on changing the architecture of clinical care, which saves live, money and protects the cyber posture of the facility.