securityinformed.com
Making The World A Safer Place

Advantages And Pitfalls Of Electronic Locking Solutions

Published on 14 Jun 2018

The concept of door locks means something totally different in our current age of smarter buildings that house data-driven businesses. Hardware locks and keys are still around, but they co-exist with a brave new world of electronic locks, wireless locks, networked systems, and smarter access control. Locks can also increasingly be a part of a smart building's flow of data. The opportunities of these new technologies and approaches are significant, but there are also pitfalls. I heard an interesting discussion about these topics presented by several business leaders from lock company Allegion at a press event at ISC West earlier this year. Here are some highlights from that discussion.

Q: What new developments in emerging technologies do you see in the coming years?

> There’s opportunity for implementation of the technology to solve real problems"

Mark Jenner, Market Development Director: Connected locks, other types of sensors and all the data being aggregated inside buildings provide opportunity for data analytics. The buzzwords around technologies can cause confusion for integrators and end users, such as artificial intelligence, deep learning and machine learning, and what’s the difference among all of them? My opinion is that they are important, but the big theme across them all is opportunities for new business models for the integrator, and opportunities to solve problems for end users. And it’s not just technology for technology’s sake. There’s opportunity for implementation of the technology to solve real problems.

Devin Love, Market Development Manager: You can’t just have a solution looking for a problem. You see a lot of people who understand technology in their own lives, and they want to translate that into their businesses. That’s where I think it’s exciting. You now have all this technology, and people understand it to the extent that it improves their daily life. They go through their day with less friction, with more ease, and technology fades to the background. There are two levels of value. One is the longer, bigger, broader scope of what the technology can bring to a company using it, but on an immediate basis, there is the value of tracking how a business is running. These sensors are collecting data. For example, if you are a multi-tenant property, you can look at how amenities are being used. What do my residents really care about? That informs future decisions.

Robert Gaulden, Project Based Business Leader, Electronic Access Control: I have been studying the multi-family space for the last couple of months. The customer experience is really driving a lot of that technology adoption. What you're seeing today, whether it's a mobile device or some other device, is the ability to move throughout the property, and gain access to the perimeter and to your tenant space. All of this adoption is around that experience. There's multiple players coming into the space, from Amazon wanting to deliver packages into the tenant space to residents who don't want the inconvenience of using a key. Technology adoption to solve problems, and also to drive experiences, is where a lot of the balance will play out.

> It's important that we look at how integrators can use the technology to do business more effectively and efficiently"

Brad Aikin, Channel Led Business Leader, Integrator Channel: From an integrator perspective, there are two things. One is how they can approach end users, and the scope of what integrators consult with them about is wider. I think we as an industry are getting beyond those high-traffic, high-security applications. Those are still critical, but the value we bring around security and convenience is opening a new incremental opportunity. Also, the experience of the integrator and how they conduct their business is important, from generating quotes to communications to proactive servicing. It's important that we look at how integrators can use the technology to do business more effectively and efficiently.

Gaulden: We as an industry, and we as manufacturers, need to understand what data we are generating so we can run our businesses more efficiently from every aspect, whether you're the property manager, the building owner, the integrator, or whether you're the manufacturer. These devices and technology are being pushed out everywhere and will generate the data. How we learn from that – especially when you apply security to it to be more proactive – provides huge opportunities.

Jenner: What data is important and what's not? Folks get overwhelmed with too much data at some point. What's important for an application at the end user level? What do they really need to

solve the problem?

Love: Privacy gets involved as well, especially with consumer products. The attitude is *"stay out of my private business."* But if you're an employee now, all bets are off. Now you have a professional relationship with the people you work with, so there is a different lens that you look through when tracking data. You use the data to everyone's benefit, and it's a different paradigm than in your private life.

Aikin: Also, where does that data create a better experience for the person? That's what drives the money and value: What level of information sharing makes my experience better? The technology is also getting smarter in terms of "*how do we sort through the valuable information*?"

Q: As facilities connect more devices and sensors, the cybersecurity threats increase. We have already seen Internet of Things (IoT) devices being used as the attack point of cyber breaches. What are the vulnerabilities that make those attacks possible, and how can integrators protect their customers?

Love: Certainly, this is an extremely – maybe the most important – piece of our industry. What is the point of everything we do if we can't instill that trust? But what we need to solve here also comes with opportunity. There's certainly hope. You're not seeing a frontal attack on the technology. It's usually some loophole, or some older device that hasn't been updated, or wasn't installed correctly, or it was social-engineered. The opportunity is, not that it can't be solved, but that it absolutely needs to be solved – and it can.

Gaulden: Integrators need the ability to understand that cyber layer and what it means. Nowadays, everything runs on the network, and you won't even get past the IT department to get on the network if you don't have the right staff, the right credentials. From an integrator standpoint, you need the ability to add to your staff, to understand everything from the product level to the firmware and the software level, all the way to the deployment of the holistic system. You can't just say, "*That's not part of our responsibility.*" All these devices are now riding on the network. They can be protected from a cyber perspective, or you will have vulnerabilities.

> As manufacturers and business consultants to integrators, we should facilitate the conversation, that it is one ecosystem"

Aikin: Everything is a communication device. With the concern and need comes an opportunity for the integrator. But it's also in making sure integrators are having that conversation with end users and setting the expectations up front. What I'm providing you on day one is the best in the industry at this time, but tomorrow it may not be. My accountability and service are to maintain that environment and keep it running. I may not physically change the device you see, but the service I'm bringing to you is that security, and that comprehensive dialogue. The IT stakeholders already have that expectation, but there is a chasm in some organisations between the physical security and the IT stakeholders, and the integrator is facilitating that conversation. As manufacturers and business consultants to integrators, we should facilitate that conversation. It is one ecosystem.

Q: Aside from cybersecurity, what are some of the other threats that integrators should be aware of as they work with customers to implement the new trends and technologies we have mentioned?

Aikin: It is diversifying, all the options and the capabilities. With that comes confusion and misapplication. If I look at the trends around just wireless; I go back 10 years ago, there were even questions of whether wireless was a secure technology. That has progressed and continues to be part of the cyber conversation, just like any hardwired product. It's something you have to maintain

and be aware of. Wireless has really diversified. There is still a need for education within the channel, and most importantly, to the end user. There are still end users that assume a WiFi widget is the same thing as a Bluetooth widget is the same thing as a low-frequency widget. But they are all different. There are reasons there are different technologies. Nothing stifles the adoption of technology more than misapplication.

> We have different architectures within our lock base and among our software partners to allow a mix of technology"

Gaulden: Integrators understand the differences in how various doors are used and how those applications will work. In the K-12 school environment, you want the ability for an instant lockdown, and a WiFi deployment probably isn't your best option. You need a real-time deployment. However, my office door at headquarters doesn't necessarily need real-time communication. I can pull audits off it once or twice a day. You have to mix and match technologies. For a high security door, you would proactively monitor it. But for a door where convenience is the goal, we can put electronic security on it but we don't need to know what's going on at any moment in time. We have different architectures within our lock base and among our software partners to allow that mix of technology.

Jenner: End users want the latest technology, but it may not be for their applications. Those things drive more costs into it, when end users need to be putting money into cybersecurity and some other things. That's part of the misapplication. Another risk is interoperability. That's a big piece of the technology and as things change. How do we do a better job of supporting open architecture? It may not be a standards-based protocol, although we use a lot of standards, but we just need to make sure whatever protocols we use are open and easily accessible so we can continue to work with them in the future. We know that when our devices go in, they will support other parts of the ecosystem from an interoperability perspective. That's important for integrators to know: How is this going to be applied and integrate with something in three, four or five years from now? It's an expensive investment, and I want to make sure it will work in the future.

Main photo: Business leaders from Allegion discussed new trends in electronic and wireless locks at a recent press event: (L-R) Robert Gaulden, Devin Love, Brad Aikin and Mark Jenner.

Author Profile

Larry Anderson

Editor, SecurityInformed.com & SourceSecurity.com

An experienced journalist and long-time presence in the US security industry, Larry is SecurityInformed.com's eyes and ears in the fast-changing security marketplace, attending industry and corporate events, interviewing security leaders and contributing original editorial content to the site. He leads SecurityInformed's team of dedicated editorial and content professionals, guiding the "editorial roadmap" to ensure the site provides the most relevant content for security professionals.

You may also be interested in...

How Access Controlled Revolving Doors Can Protect Businesses From Crim...

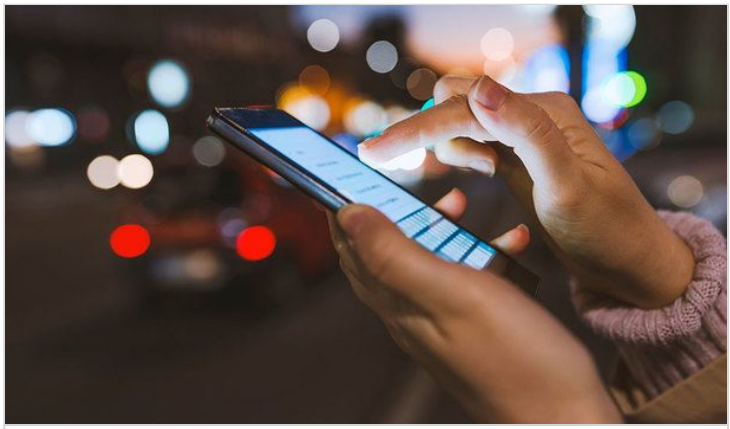
Today's security professionals are tasked with protecting the entirety of a facility or campus from every possible threat. It's...

Smart Access Control Is Essential To The Future Of Smart Cities

Throughout the UK there are many examples of smart city transformation, with key industries including transport, energy, water and waste bec...

How Smart Access Control Will Improve Rental And Landlord Security

Until recently, the convenience and security of "smart" electronic locks have been exclusively enjoyed by owners of homes, with...



Social Media Data Provides Security Professionals With Real-time Situa...

Twitter has around 350 million active users a month, all eagerly posting 280-character "tweets" about the world around them. It&...