SECURITYIN30
LIVE WITH ALLEGION

Is your opening as secure as you think?

September 17, 2021

Question & Answer

## Q. What is the most concerning vulnerability of a mechanical opening?

A. Common door keying
B. Poor key management
C. Old hardware
D. No electronic access control

Even though any of the answers can be a vulnerability in a security system, poor key management is the most concerning. The practice of key management being one piece of Key Control as we discussed in the webinar.

## Q. What is the most concerning vulnerability of an EAC opening?

A. No cameras covering the opening
B. Lacking EAC in some areas
C. Lack of system understanding
D. Using unencrypted credentials

The popular vote was “C: Lack of system understanding.” It’s true, the larger a mechanical/electronic access control system gets, the more complex it undoubtedly becomes. The reason we believe that using unencrypted EAC credentials is the most concerning vulnerability on this list is because they cast the internal perception that the system is more secure than it is. If we turn a blind eye to the fact that unencrypted credentials like mag stripe or proximity are easy duplicated at a supermarket or using a cloner from Amazon, we’re now in a scary position where we’re underestimating our threats and / or overestimating our ability to deter them.

## Q. How about alerting someone when the door is not secure?

A. This is absolutely a capability of many enterprise access control software systems – alerting a “chain of command” either via SMS, email, or web/desktop client software. In my past work at a university, we had over 7,000 openings. About 1,000 of these openings were online, but we didn’t have the resources or personnel to respond to reports/alerts like these. We recommend prioritizing system features and automation that you have the resources to adequately support.

## Q. I find that cameras are mostly useful for after the fact.

A. Generally true. Cameras, if manned, are great for real time monitoring as well. Access control and video surveillance serve different purposes but are strongest when used together.

Q. Is the supplier statement that a credential is encrypted sufficient to assure that it's not vulnerable? Are there standards or 3rd party testing?

A. Not always (regarding, a supplier statement about sufficient encryption). Manufacturers still have a product to sell, and they will apply an appropriate level of creative marketing to serve that purpose without being dishonest. There are a few standards like ISO/IEC 14443 and 15693 around which contactless credentials are designed. Allegion does not create its own credential platform but instead uses the broadly accepted open-architecture credential technology created by NXP Semiconductors. This is the architecture of choice for most credential manufacturers.

Q. Is this presentation available to presentations to my customers? Can it be modified to include my company name and logo?

A. Customizing the presentation with your company name and logo is not currently an option, but we will be posting a recording of the webinar on our Security in 30 webpage. Please reach out to your local Allegion Sales Representative for support on creating a similar presentation, tailored to your needs. The presenters would be happy to share the original Powerpoint as a framework, but the content should be adapted to what you or your customer are looking for. Call Customer Service at 877-671-7011 for help identifying the representative in your area.

Q. Who determines what a "level of security"? What is a level?

A. In key systems Schlage offers 3 levels. Open, restricted and high Security. An easy way to think about it is; Open = good, restricted = better and high Security = best. The determination of what level to use on what door is situational. It's determining factor is what is the value of the assets you trying to protect behind that opening?

Q. The key is easy, where and when do you apply these levels?

A. The determination of what level to use on what door is situational. It's determining factor is, what is the value of the asset are you trying to protect behind that door? In conjunction with your organization's resources. A security consultant can help you make these determinations.

Q. With improving technology, do you see the need for a mechanical override key eventually going away?

A. This conversation has been in the industry for close to 20 years. Today, if the electronic security on the door fails, a mechanical key is the way into that opening. The determining factor is the speed to which the market adopts to change. As it stands the mechanical key override is still the industry standard. With that being said, a mechanical key override does not need to be present at every opening where another electrified access point also has a key override; one per space is often sufficient.

## Q. Please expand on mobile credentials.

A. Mobile credentials have been a hot topic for a while now. NFC (near field communication) has been an available technology for over 8 years on Android, but Apple has not allowed third-party use on its iOS platform until recently. Because of this, BLE has risen to be the widely accepted mobile credential technology of choice across all major mobile platforms. As previously stated, NFC has only recently been made available for access control use in the iOS wallet, specifically in the higher education and commercial spaces. There are several prerequisites to qualify for NFC mobile credentials on iOS, and requires a persona manager intermediary like CBORD, Atrium, Blackboard, or TouchNet to deploy the NFC credentials. Take a look at this Allegion case study to learn more: https://us.allegion.com/en/home/markets/higher-education/mobile-credentials-key-to-seamless-student-experience.html

## Q. How do access controlled key boxes play into key management?

A. It is a really good solution to help organize and control key management. It solves the problem of accidental vulnerability that we address in the webinar. It takes the two-individual tasks of securing the unissued keys and tracking those keys and combines them into one solution - The access controlled key box. An EAC key box allow brings quasi-EAC to a mechanical building by electrifying one point instead of many.