Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 319–327
https://doi.org/10.54941/ahfe1008265

Design Innovation of a Remotely-Controllable Portable Door Lock for Physical Security

John McIntire, Matt Srnoyachki, Jason Sopko, and Adam Adducchio

Air Force Research Laboratory, Wright-Patterson AFB, OH 45433, USA

ABSTRACT

Portable door locks are personal security mechanisms designed to secure a door independently of its installed hardware. These devices are commonly advertised to be used in commercial applications such as hotel stays, short-term rentals, and shared residential environments where users seek to supplement existing lock systems. In addition to general travel and privacy use cases, portable locks have grown to be employed in emergency scenarios, including active threat incidents and domestic safety situations. Most existing designs require the user to be located inside the secured space to deploy the portable door lock, which limits functionality in scenarios requiring external locking or unattended room security. An infrastructure-agnostic, remotely-actuated portable locking device was developed to address this operational gap. The system interfaces directly with standard residential and commercial strike plates without modification to the door or frame, and functions independently of any pre-installed lockset. All mechanical and electronic components reside entirely on the interior side of the door, with actuation enabled via remote wireless communication. No exterior-facing elements are present, minimizing detectability and physical vulnerability. Utilizing the Design Innovation methodology, we incorporated methods such as user-centered requirements gathering, scenario analyses, and iterative prototyping. Primary operational scenarios included personal use in hotels, tenant-controlled room security in shared housing, and temporary field deployment for government or military personnel. The device architecture includes physical anti-tamper features, concealed input mechanisms, wired power option with battery back-up, tamper detection, and other design features to resist manipulation, unauthorized access, and signal spoofing. This system expands the design space of portable door locks by enabling unattended, remote-controlled physical security in non-permissive or infrastructure-limited environments.

Keywords: Portable door lock, Physical security, Remote control, Design innovation, User-centered design, Anti-tamper measures

INTRODUCTION

The Design Innovation process starts with a general problem or "opportunity," followed by an exploration of the opportunity space—this helps the designers learn about the users and stakeholders, develop deep fundamental insights about their problem, and determine if the team is attempting to solve the "right" problem, or if the project goals need to be rescoped, reframed, or otherwise reconsidered (Lauff et al., 2003). The problem our original

Received August 31, 2026; Revised October 8, 2026; Accepted October 13, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

innovation team started with was: How do we protect bystanders during active threat emergencies (McIntire et al., 2017)? Our research in this general problem space led us to the realization that there were many fruitful sub-problems and related opportunities specifically involving giving people new and unique tools to quickly, safely, and effectively barricade a room.

For instance, for active threat emergencies in public or commercial spaces, law enforcement guidance suggests it is often safest for bystanders to immediately shelter-in-place or barricade oneself into a locked room (e.g., U.S. Department of Homeland Security's guide on "Active Shooter: How to Respond," 2008). Unfortunately, many doors in public spaces simply do not have locks; or if they do, the locks are intended for privacy but not physical strength/security; or even if strong, the locks can easily be unlocked by persons with multiple approved shared keys (staff or security guards). Personal portable locking devices can be useful for these types of emergency scenarios.

In other general or non-emergency situations, like in hotel rental spaces or apartments, door locking hardware is already installed and available for use by the guests or lessees. But in such instances, the owner of the property is the owner of the security hardware. The primary user of the hardware, the hotel guest or apartment tenant, has no control over the type and quality of the security hardware provided, and may desire additional layers of security or protection. For the above scenarios, there exist a variety of commercially available portable door locks that might be utilized to help fill this gap. Members of this authorship team at the Air Force Research Laboratory have previously developed, tested, and even patented new portable door lock designs to overcome some of what we identified as weaknesses or usability problems in the commercially available portable door locking solutions at the time (McIntire et al., 2017; McIntire et al., 2019; McIntire & Srnoyachki, 2024a; McIntire & Srnoyachki, 2024b).

All of these portable door lock concepts we've discussed so far function on a central premise: the person needs to be physically inside the space in order to lock themselves within the space, and the device cannot or should not be unlockable from outside the door. In many cases, like active shootings, or sleeping overnight in a hotel, this makes perfect sense. However, there are many other imaginable scenarios in which it would be useful to lock a space from its exterior and be able to leave it protected, like a padlock but usable on virtually any door, without permanent modifications to the door or frame, and hidden within the room itself with no visible signs of the mechanism on the outside of the door. When traveling, many people other than the traveler may have access to one's hotel room without their knowledge or permission. Electronic key card access causes many doors to be locked against general use, but these doors are still unlockable with an electronic card possessed by employees, staff, or others. Unfortunately, this may also include thieves, organized crime, or even foreign government operatives. In shared space living environments, like apartments configured with private rooms but shared general areas, a resident may wish to lock their private rented space without permanently installing new door hardware.

For both travelers and residents in particular, there is a need for the ability to lock a private room, for instance, and to be able to leave for the day and know that the room is inaccessible from the cleaning staff, from prying roommates, or from illegal or surreptitious entry. In this work, we describe the User-Centered design and invention of a portable, remotely-controllable inswing door lock that can accomplish this functionality (as patented in McIntire et al., 2024). The lock includes various anti-tamper features, to protect against nefarious, surreptitious methods of defeat. The types of innovation methods we used, and insights gained from those processes, will be shared while referencing the features of the product design.

DEVELOPMENT METHOD: CO-CREATION, USABILITY TESTING, AND USER FEEDBACK

Getting feedback on innovation design ideas is a crucial step in the design process. That there would even be a need or desire for a remotely-controllable portable door lock was not immediately obvious to us, even though we had been working on portable door lock design concepts for more than a year at that point. The genesis actually came from discussions with military Subject Matter Experts (SMEs) in the US Special Forces, when our team was showcasing our original non-remote-control lock design prototypes (for inswing and outswing locks).

These prototypes were shown to end user SMEs, such that they could "play with" and test them, and imagine using them in various scenarios of interest to them, to involve actively emplacing the devices in different door frames and to practice engaging the locks. Feedback from one user led to the question: "Can you make this remote controlled, so I can leave it behind to secure a space? It would be great for traveling, to add extra protection for some of our gear." This simple question was the initial seed that led to the present design innovation effort. Our team then set about thinking on how we might design such a product; and what other problems or scenarios it might be useful for.

DISCOVER & DEFINE METHODS: SCENARIO ANALYSES AND SCOPING

We pursued further initial discovery research and held discussions with other potential users and stakeholders, to include military members with experience traveling CONUS stateside, US Secret Service special agents that specialize in asset protection, and security agents from the AF Office of Special Investigations. We identified three key scenarios that we wanted to develop our new product for; these were:

1. Private space locking, like for an apartment or dorm;
2. Traveler hotel room locking (general public); and
3. Traveler hotel room locking (government/military).

This helped our team scope and clarify who we wanted to design for, what type of scenarios we were addressing, and what the device should accomplish, thus leading into our next steps of identifying how we might accomplish those design ideas.

DISCOVER, DEFINE & DELIVER METHODS: CONTEXTUAL NEEDS ANALYSES, EXTREME USER SCENARIOS, AND PROTOTYPING

To use a remotely-controlled portable door lock, assuming an inward-swinging door, a generic activity diagram was constructed (see Figure 1). Starting from inside a room or space that one wishes to lock, a user starts by opening the door, placing the locking device into the strike-plate hole, removing their hands and then stepping through the open doorway into a hall or other open space. Then the user should shut the door behind them, and use the remote control to activate the locking mechanism which electromechanically moves a blocking barrier into the way of the door so that it is held shut in a closed position. The user is then able to leave the secured space. Upon their return, the user can unlock the device via remote, and once the physical blocker portion of the device swings out of the way of the door, then the door can be opened and the lock manually removed from the door frame.

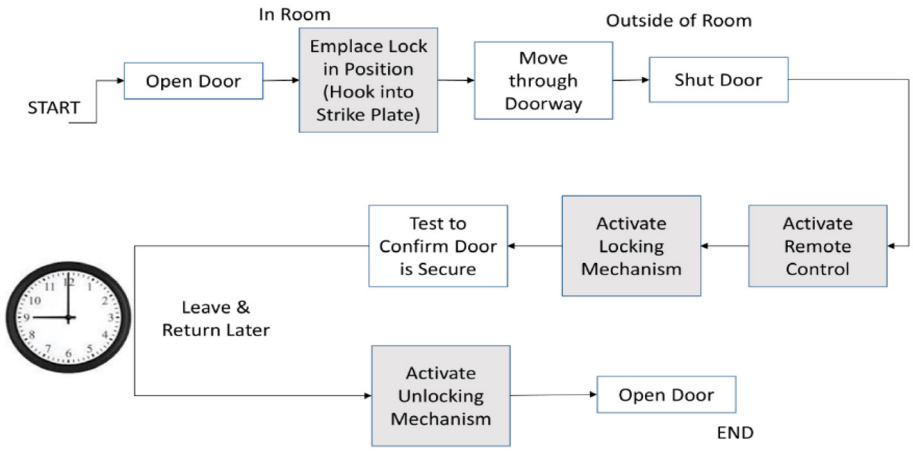


Figure 1: Activity diagram for an electronic remotely-controlled inswing portable door lock; greyed activity boxes indicate user interactions with our system.

Designing for the general public traveler (Scenario 1) was somewhat "easier," as the desired feature set was considerably smaller. In this case, the users just needed a way to easily emplace and then lock the device into an inward-swinging door space. We recognized through early testing of our original in-swing lock device that leaving a lock anchored in position via the strike-plate latch hole—without it falling to the ground when the user's hands are removed—needed to be solved.

The team performed several design iterations with concepts like expanding shapes that would fill the strike plate hole; non-sticky adhesives (like "gecko" or "nano" tape) that would help grab to appropriate surfaces and hold in

place; and with tab hooks that could hold in place against and within the strike plate hole itself. Prototype testing suggested that a tab that used "hooks" or "barbs" would work best, and could be designed for easy manufacturability with minimal metal cutting/bending needed to create the necessary shapes (see Figures 2 and 3).



Figure 2: Remote control portable door lock prototype drawing (left) and zoomed-in photo of the hooking barbs (right) that help keep the device in-place in the strike plate hole during the lock emplacement action by a user.



Figure 3: The portable door lock emplaced/positioned in a hotel's strike plate hole, with door open (left) versus door closed (right).

Designing for Scenarios 2 and 3 was more challenging. For instance, the US Secret Service specializes in asset protection, and US Special Forces as well as other military groups often travel but may stay in commercial lodging, while still wishing to keep their supplies and equipment in a secured space, even if left unattended. These scenarios could include threats like nefarious intelligence groups attempting to gain access to the space, or thieves hoping to steal the gear stored there. To overcome these threats, our design could benefit from other additional features. We needed to consider designs that were anti-tamper, and resistant to hacking, spoofing, or manual manipulation with tools.

DELIVER METHODS: PHYSICAL MODEL, PROTOTYPE ITERATION, AND USABILITY TESTING

The team went through a multitude of design iterations. Different remote controller button schemes were tested; different emplacement hooking mechanisms; and different power schemes for longevity and reliability. Particularly for the latter half of the effort, there was additional focus on making the device easy to manufacture to facilitate future transition efforts. The final advanced prototype designs are shown in Figures 4 and 5.

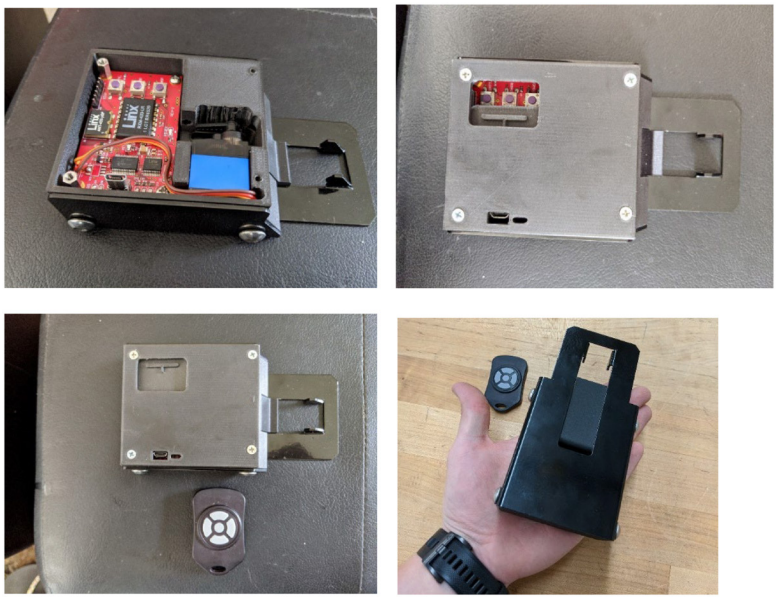


Figure 4: Final prototype designs. Top-left: lock with electronics and battery cavity exposed. Top-right: device with cover but manual control buttons exposed. Bottom-left: prototype with anti-tamper covers and remote control shown. Bottom-right: hand for scale.

The anti-tamper measures we developed for the device include:

1. **Sealed-in pin:** Mates the locking tab to the lock body, such that there is no way to remove the pin without disassembling the entire lock.
2. **Concealed control interface:** Power and control buttons are concealed on the lock body, protected by a closed casing/cover that cannot be accessed without intricate or two-handed manual manipulation.
3. **Cryptographic wireless control:** A lock/unlock multi-digit code must be entered by the wireless remote control device, to protect against signals interception and sniffing attacks.

We also considered incorporating tamper sensors on the device itself, potentially to alert a user that the device underwent physical manipulation (detection is post-hoc) or alerted in real-time if tampering is detected via a comms link to the outside world like Wi-Fi or cellular.

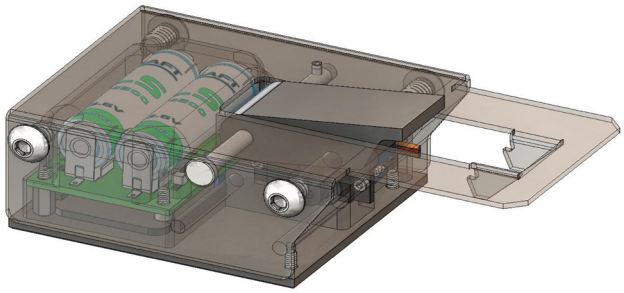


Figure 5: Final prototype see-through CAD drawing of the remote-controlled portable lock.

For a user's control of the device, several electronic communication protocols were considered. Bluetooth, Wi-Fi, and NFC are all technically feasible, but each has benefits and detriments. For a production version, a proprietary protocol may be employed to add additional security-by-obscurity. Regardless of the protocol, dual-factor authentication is recommended to be employed. Our prototype required a remote controller having a quasi-unique hard-coded address, in conjunction with a PIN entered by the user. The microcontroller can be configured to provide a timeout penalty for incorrect attempts, log invalid attempts, or allow for a master and subordinate PIN/transmitter structure, dependent on customer needs.

Battery life exceeds a week under normal operating conditions, and either USB rechargeable cells or lithium batteries may be used. If plugged into a wall outlet via the USB charging port, the device can operate indefinitely while in place. During power-up, a self-test is performed, and among other parameters that are checked, the device will not allow the locking mechanism to be put into service if the battery is at a critically low level. Battery status is conveyed to the user via LED colors and patterns. The device is configured in a fail-safe behavior (contrasted with fail-secure): if battery levels become critical while the device is in a locked configuration, this state is detected on the system and the locking tab will retract, preventing users from being accidentally locked out of the room.

Evaluation and user testing was not formal nor complicated. It primariy consisted of bringing potential users into the lab, introducing them to the device and training them on its use, then asking them to do some use testing. We observed their device usage, looking for pain points or issues; and also asked the testers to describe their likes, dislikes, and wishes for the tool. These notes were compiled and studied, and fed back into future design iterations of the device.

CONCLUSIONS, LIMITATIONS, AND FUTURE WORK

Commercially available portable door locks provide an essential layer of security but are fundamentally limited by the need for the user to be physically present inside the room to engage the lock. This work addressed that operational gap by developing a novel, remotely-controllable portable door lock. By implementing the Design Innovation methodology, including

user-centered discovery and iterative prototyping, we invented a device tailored to scenarios requiring unattended room security, such as for travelers, tenants in shared housing, and traveling government or military personnel.

The resulting system is infrastructure-agnostic, interfacing with standard door strike plates without any permanent modification or installations, and remains entirely concealed from the exterior, thus minimizing detectability and physical vulnerability. The final prototype successfully integrates a robust mechanical design with secure electronics, incorporating features specifically developed to counter sophisticated threats. These include physical anti-tamper elements, concealed device controls, and a multi-factor wireless communication protocol to resist unauthorized access and signal spoofing. Furthermore, the design incorporates practical considerations for real-world use, such as a fail-safe power system that prevents accidental lockouts and the option for continuous wired power.

Limitations of this research include the fact that while we performed bench-level testing and some lab usability testing with SME's, we were not able to do realistic-environment testing in real-world public spaces like hotels or apartments due to ethical, legal, time, and resource issues. We also were unable to perform formal strength-testing of this design, to assess how strongly it would resist a forceful attack from the outside of the door (e.g. an intruder trying to break down the door), again due to resource and time limitations of the effort. That information, while valuable, did not strike us as vital for continuing the research effort for our project's scope but could be a valuable design factor for some future customer groups.

Future work could focus on mass-manufacturing optimizations, the integration of network-based, real-time tamper alerting capabilities, and more sophisticated cyber or RF signal communications hardening. Future work should also focus on miniaturizing the size and footprint of the device, and minimizing weight both for travel ease and for improved initial placement (as it is less likely to rotate off out of the strikeplate positioning). This research and the resulting invention significantly expand the design space for personal security devices, demonstrating a viable solution for remote-controlled physical security in otherwise soft security environments. The utilization of the Design Innovation methodology proved extremely valuable during key stages of the research and development processes.

This paper has been approved for public release by the US Air Force: AFRL-2026-1466 as DISTRO A: "Approved for Public Release: Distribution is Unlimited." The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force or US Government.

REFERENCES

Lauff, C., Hui, W. Y., See, A., Raviselvan, S., Collopy, A., Jensen, D. J., Teo, K., Png, S., Swee, A., & Wood, K. L. (2003). *DESIGN INNOVATION METHODOLOGY HANDBOOK: Embedding Designs in Organisations* (2nd ed.). Published by the Design Innovation Team, DesignZ Centre, Singapore University of Technology and Design. DOI: https://doi.org/10.59977/VQPH8086.

McIntire, J. P., Boston, J., Smith, B., Swartz, P., Whitney-Rawls, A., Martinez Calderon, J., & Magin, J. (2017). "AFRL Commander's Challenge 2015: Stopping the active shooter." *Proceedings of the SPIE Defense + Security*, Anaheim, CA. DOI: https://doi.org/10.1117/12.2261418.

McIntire, J. P., Srnoyahcki, M., Sopko, J. D., & Adducchio, A. C. (2024). "Electronic remotely-controlled inswing portable door lock." *United States Utility Patent*: US 12,091,890.

McIntire, J. P., & Srnoyachki, M. (2024a). "Outward swinging door barricade." *United States Utility Patent*: US 11,834,875.

McIntire, J. P., & Srnoyachki, M. (2024b). "Outward swinging door barricade." *United States Utility Patent*: US 11,970,889.

McIntire, J. P., Boston, J. D., & Srnoyachki, M. (2019). "Inward swinging door barricade." *United States Utility Patent*: US 10,358,850.

United States Department of Homeland Security (October, 2008). "Active Shooter: How to Respond." [booklet]. Available: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf.