Security Assessment Plan (SAP)

Team #2 - Large Spearfish

Members: Jaeden Carpenter, Zijian Liu, Zari Malbacias

SIE 471/571

Table of Contents

ACRONYMS

ATM	Automated Teller Machine
CFAA	Computer Fraud and Abuse Act
CPU	Central Processing Unit
FCC	Federal Communications Commision
IEC	International Electrotechnical Commision
IP	Internet Protocol
ISO	International Standards Organization
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
PEN	Penetration (Testing)
PIN	Personal Identification Number
RFID	Radio-Frequency Identification
SAP	Security Assessment Plan
SAR	Security Assessment Report
UID	Unique Identification

1.0 INTRODUCTION

1.1 Applicable Laws and Regulations

This section includes the applicable cyber and privacy laws and regulations that are included and considered for this Security Assessment Plan (SAP). While the United States government does not have general federal law regulating cybersecurity and privacy, there are cases for specific sectors private and public or even state legislated laws and regulations. The laws and regulations in this SAP are component specific and also general in terms of cybersecurity assessments. Our team has researched and studied how these relate to our system. Table 1 below shows a comprehensive list.

Laws and Regulations	Title
Computer Fraud and Abuse Act (CFAA)	Prohibits accessing a computer without authorization
FCC Part 15	Radio Frequency Devices

Table 1. Applicable Laws and Regulations

1.2 Applicable Standards and Guidance

This section includes the applicable standards and guidance that are included and considered for this SAP. The following standards and guidance come from organizations such as International Standards Organization (ISO), International Electrotechnical Commision (IEC), and National Institute of Standards and Technology (NIST). These standards and guidance cover areas such as Radio-Frequency Identification (RFID) and general cyber security assessment topics. Table 2 below shows a comprehensive list.

Standard/Guidance	Title and Brief Description
ISO/IEC 14443	Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol
ISO/IEC 18000	Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C
ISO/IEC 18000-2	Information technology — Radio frequency identification for item management — Part 2:

	Parameters for air interface communications below 135 kHz
NIST Special Publications	Technical Guide to Information Security Testing and Assessment
NIST SP 800-39	Managing Information Security Risk

Table 2. Applicable Standards and Guidance

1.3 Scope

The scope of this SAP is focused on the door access control system used for the Red Team/Blue team simulation project. These parts will be used for the Red Team/Blue team simulation project. We will not be focused on components not identified in this SAP nor other system devices. Due to the experience of the team and the short class schedule this semester, our team will not be doing any actual penetration (pen) testing. We will clearly outline our plans and assessments needed as if we were to carry out actual penetration testing. We will not have clear, quantifiable results, but we will seek to assess every aspect of the system. Our team will be using NIST's *Technical Guide to Information Security Testing and Assessment* as a guideline for the system assessment.

1.4 Assumptions and Limitations

We are carrying on with the assumption that our team has done a complete, extensive research on the door access control with the best of our team's current abilities and time constraints. We are also making the assumption that this plan is comprehensive enough to proceed with the creation of a Security Assessment Report (SAR) that details eventual pen testing procedures. A big limitation in our analysis would be our team's knowledge and capabilities for properly carrying out the tests for a proper and full assessment. Our team's two graduate students only have backgrounds in Civil and Industrial Engineering. Only our team's lone undergraduate member has a Computer Engineering background. An additional constraint is the time to do this project and do our system assessment is limited to the semester. If we had more time, our team could proceed with our assessment plans and even do a full pen testing of the door access control system.

2.0 SYSTEM OVERVIEW

2.1 System Description

The RFID Proximity access controller by AGPTEK is an access control system designed for door security. AGPTEK's door access control system kit allows users to open the door using proximity cards, passwords, or a combination of the two. The access controller also provides users with various options by connecting to terminals, including the button for opening the door, doorbell, and electric lock that is normally

open or closed. The system can be and designed to be connected to power through a connection protected by the CPU and integrated circuit within the kit's power supply control unit. This door entry system is qualified as an ideal equipment for businesses, offices, factories, and communities (*Amazon*). Figure 1 below shows a picture of the system. Figure 2 also shows a picture of a use case diagram that shows the various scenarios of how the user, developer, and attacker can use the system.

Figure 1. Door Access Control System

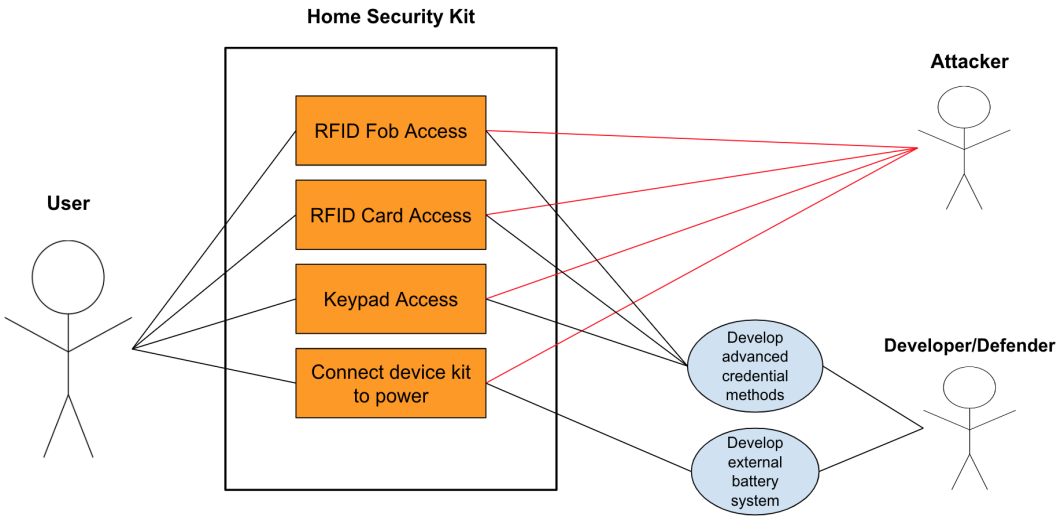

Figure 2. Use Case Diagram

The main components of the system include the RFID Proximity Door Entry Pad, Power Supply, Electric Magnetic Lock, and Push Release Button. These components are

connected together and attached to the door of a house or building. Figure 3 shows the System Architecture Diagram while Figure 4 shows a real-life picture of the system after it has been assembled together and connected. Figure 5 shows the wiring diagram for the system.

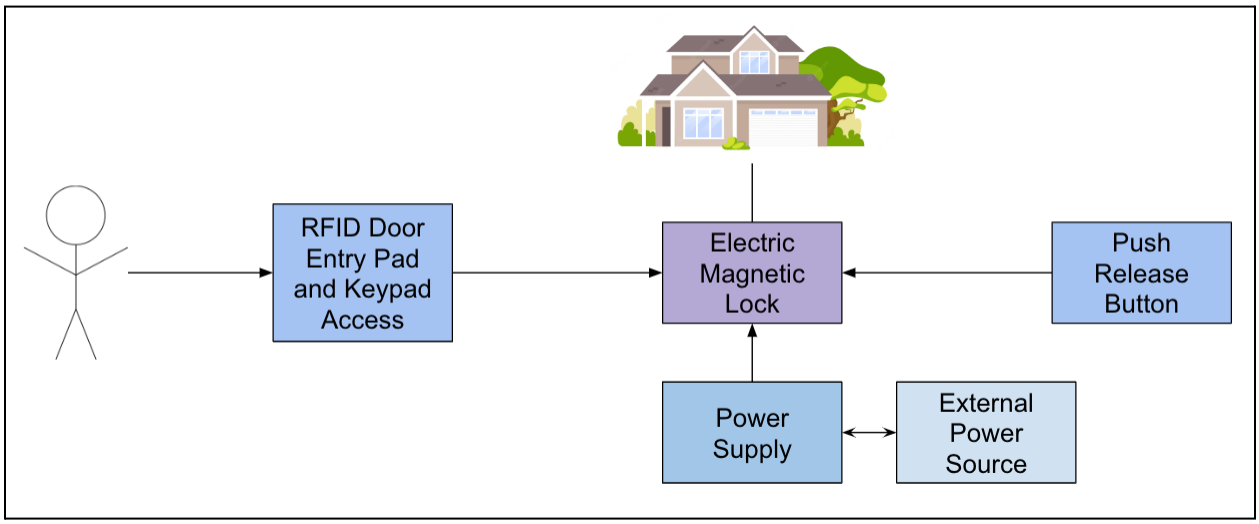

Figure 3. System Architecture Diagram

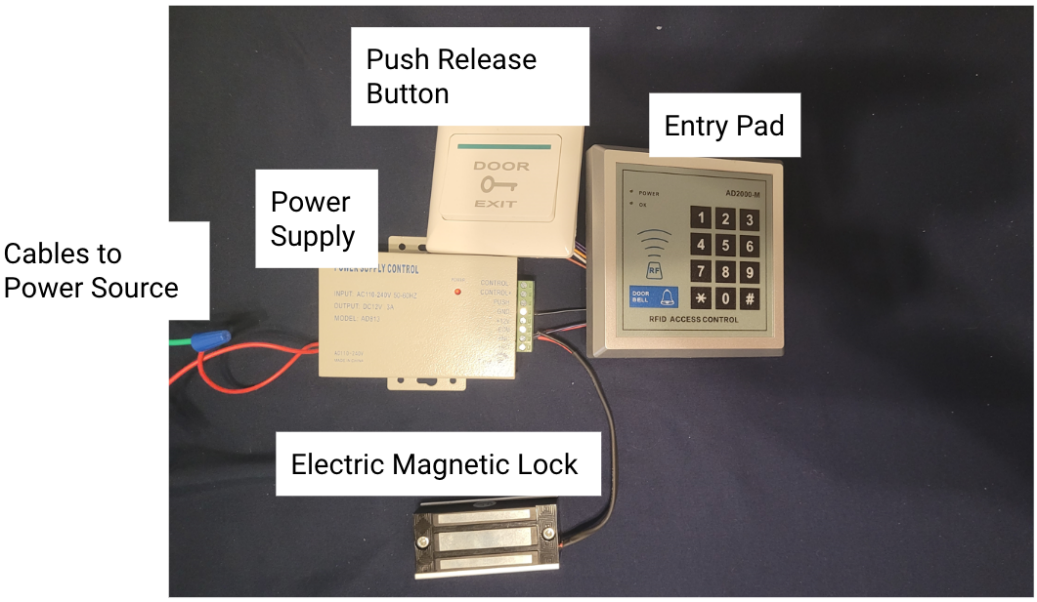

Figure 4. Picture of Assembled Door Access Control System

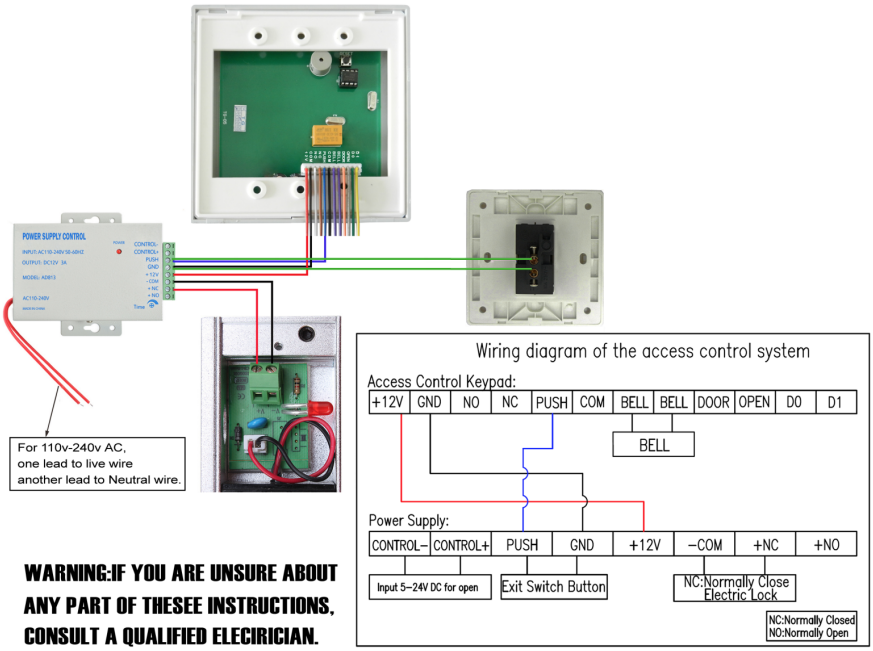

Figure 5. Wiring Diagram

Table 3 below includes the major product specifications for the door access control system. Information in the table is taken from the manufacturer's user manual guide.

No.	Item	Specifications
1	Working power	AC: 110-240V
2	Unlocking relay	DC12V/2A
3	Ambient temperature	Working: 0℃~45℃ Storage: -10℃~55℃
4	Relative humidity	Working: 40%~90%RH Storage: 20%~90%RH
5	Number of cards allowed	1000
6	Proximity card recognition frequency	ID type: 125KHz
7	Proximity card recognition	ID type: EM or EM compatible cards
8	Car reading distance	ID type: 5~15 cm
9	Electric lock interface	Output from the relay or the level (optional)

10	External card reader interface	A Wiegand26 interface
11	Ways of opening the door	Door card or the unlocking password
12	Unlocking duration	3 seconds
13	Tamper alarm	Activated

Table 3. Major Product Specifications

2.2 Overview of the System Evolution

(1) Since the beginning of modern civilization, humans have needed to protect their valuables. The first known locking device was made in Egypt about 6,000 years ago, and it consisted of a rope with multiple intricate knots. The next major advancement in locking technology occurred in the Roman Empire when metal locks were first invented. This was the first real iteration of the lock and key we know of today. Since then, the design has improved, making it more resilient to picks and smaller and lighter, but the basic concept remains the same. It was not until 1967 when the first personal identification number (PIN) access control device was created. PIN controlled locks were considered the first major technological advancement in locking mechanisms. This type of device includes a keypad and a pin number, similar to a modern automated teller machine (ATM). It is a great invention for preventing unwanted access, but it is not without its disadvantages.

(1) Two major inventions in the 1990's transformed access control into what we know today. First, the internet made it possible for the creation of server-based networks and databases. Then, RFID was created, in part, to spare primary users the problem of demagnetizing magstripe cards. RFID technology utilizes a unique identification (UID) data that is programmed into the card and shares that data when a connected reader approaches it via electromagnetic waves. The UID data is then run through the access control database, and if the card has access to the door, it can unlock it in less than a second. These technological advances have changed everything about access control. Card readers have evolved to the point where a high-tech card reader can be its own control panel rather than being connected to a master controller. These internet protocol (IP) door readers can utilize an internet connection to check card credentials against a list created on a webpage or app.

2.3 Relevant System Documentation

Table 4 below includes the relevant system documentation that will be used in the system assessment. Each corresponding reference also has the website link for the documents listed.

Document/Reference	Website Link
Door Access Control System, AGPTEK RFID Home Security Kit	https://www.amazon.com/Access-Control-Security-Electromagnetic-Proximity
Instructions for AD2000-M Door Access Machine	https://m.media-amazon.com/images/I/C1vDk+6u+zS.pdf

Table 4. Relevant System Documentation

3.0 ASSESSMENT METHODOLOGY

3.1 Authorizations

The door access control system comes with a connection kit used for installation. The user has various options for home or business installation to match user needs. There are also options for how the door can be accessed once installed. The design and installation will be thoroughly assessed in the overall evaluation on the system. According to manufacturing specifications, the access controller can be connected to terminals that include a button to open a door, a doorbell, and/or an electric lock. In addition to terminal connections, the kit comes with an RFID Proximity Door Entry keypad. The team members involved with the security assessment of the product will require authorization and access to the system. To comply with major federal laws and regulations like the CFAA, the team members must sign a confidentiality agreement that known access to the system is limited to the scope of this assessment only and practice ethical “hacking.” Overall access authorization is critical to understanding vulnerabilities of the system.

3.2 Team Compositions

This section details the names, background, experience, and role in the security assessment of each team member. Our team follows the guidance outlined in NIST SP 800-39 which states:

> “The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).”

In the list below, our three member team's roles are outlined for the SAP for the door access control system.

3.2.1 Team Member 1

- Name: Jaeden Carpenter
- Current Occupation: Student
- Undergraduate Degree: Electrical and Computer Engineering
- Security Assessment Role: Team Lead, Security Controls and Countermeasures

3.2.2 Team Member 2

- Name: Zijian Liu
- Current Occupation: Associate QMD Manager
- Graduate Degree: Civil Engineering; Industrial Engineering (in progress)
- Undergraduate Degree: Civil Engineering
- Security Assessment Role: Risk Assessment

3.3.3 Team Member 3

- Name: Zari Malbacias
- Current Occupation: Logistics Engineer
- Graduate Degree: Engineering Management (in progress)
- Undergraduate Degree: Industrial Engineering
- Security Assessment Role: Vulnerabilities and Attacks

3.3 Assessment Tools and Resources

In order to perform the assessment, there are a number of tools and resources that are helpful. The main resource to use for understanding the vulnerabilities of the system as well as commonly used countermeasures is the NIST database.

The tools that are used to assess the system include an RFID jammer, a key fob copier, a radio frequency input/output device, an oscilloscope and a screwdriver. An RFID jammer is used to test if the radio frequencies are capable of being jammed in order to prevent user access to the system, a key fob copier is used to test if there are proper measures within the fob reader and the fobs themselves that prevent the duplication of a fob. A radio frequency receiver is used to test if a fob is capable of being emulated just by copying the RF signals that are passed between the fob and the keypad. An oscilloscope is used to measure the current and voltage that is delivered to the device in order to deactivate the lock. A screwdriver is used to take apart the system.

4.0 SECURITY ASSESSMENT PROCEDURE

4.1 Process Overview

The process for assessment of the security of the system is a procedure that requires five different steps. These steps are building an understanding of the use cases for the system in order to understand where threat actors could attack the system, reverse engineering the system, researching different vulnerabilities that are known about the system, testing the vulnerabilities to see if they work on the system, and then assessing possible countermeasures to the vulnerabilities that were found.

The first step of understanding the system infrastructure and use cases was done for this system and is displayed in the System Overview section of this report. There were four different use cases found that the user is able to interact with as shown in Figure 2. It was found that for each use case, a threat actor is also capable of attacking at that point.

For reverse engineering the system, Figure 5 shows a descriptive wiring diagram. The system shows that each part is capable of controlling the locking mechanism. If a threat actor has access to the power supply and is able to cause damage to the device, then the door will automatically open. If a threat actor has access to the RFID keypad, they will be able to attempt to hack into the system by either accessing the RF frequencies used and attempting to create a cloned fob, or they could attempt to create a device that can be linked to the PUSH signal where they can insert the proper signals that will deactivate the lock.

By researching the different vulnerabilities of the system, six different common vulnerabilities were found. These are the physical threat, the use of an RFID jammer, fob cloning or emulating, manipulation of the keypad access, password guessing, and attacks on the power supply.

In order to test these vulnerabilities, the tools and resources and how they can be used to attempt to hack into the system are listed in this report under Assessment Tools and Resources.

4.2 Modeling Techniques

The modeling techniques outlined in this section are used to represent the functionality of the system. Our team already modeled the system architecture in Figure 3 in Section 2.1 System Description. The system architecture diagram visualized how the components fit and function together in the system. Most of the figures and description in Section 2.1 capture and detail out the door access control system, the remaining models and diagrams will be for the full system assessment itself, which will be detailed

in the SAR. These models will visualize the threats, vulnerabilities, and risks like in Figure 6 below where it shows the attack tree diagram of the system. The same attack tree diagram information will be assessed for their specific risks and placed into a risk register and matrix. While our team has modeled the system itself, we will proceed with red team/blue team simulation also modeling all areas of a full system assessment.

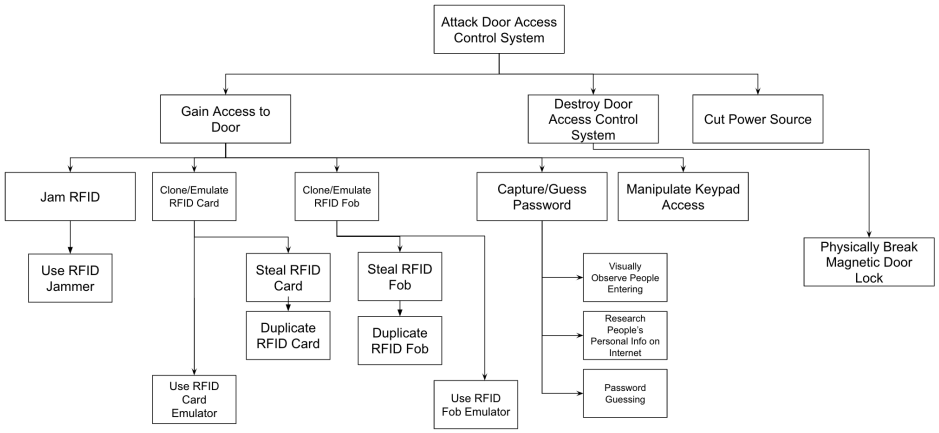

Figure 6. Attack Tree Diagram

4.3 Component Identification

Figure 7. RFID Keypad and Fobs

The RFID keypad and fobs shown in Figure 7 are the primary entry point of the system. A user can access the system by scanning their fob and inserting their four digit passcode. There is also a six digit administration passcode that can be used to activate new cards. Each card is assigned a three digit serial number upon activation in order to identify which card is being used. This also allows an admin to remove keys from the system by removing the serial number.

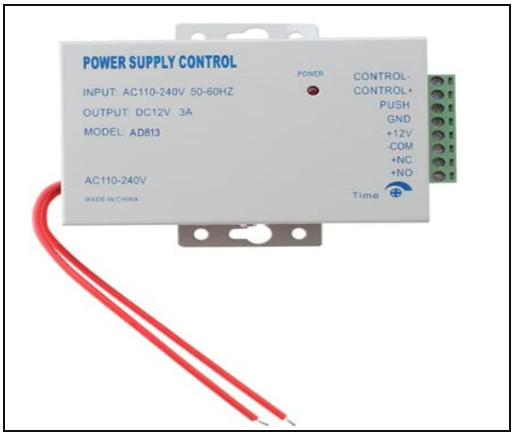

Figure 8. Power Supply Control

The Power Supply Control shown in Figure 8 takes in 110-240V AC and converts it to 12V DC in order to control the magnetic lock. The power supply also takes data from the Keypad and the Door Access Button in order to determine if the magnetic lock should be deactivated or not. If the Power Supply Control does not have power running through it, then the magnetic lock is turned off by default.

Figure 9. Magnetic Lock

The Magnetic Lock shown in Figure 9 is an electromagnetic lock that provides 120 lbs of holding force when activated. The activation of the lock is controlled by the Power Supply Control.

Figure 10. Door Access Button

The door access button shown in Figure 10 is a single button that when pressed, deactivates the Magnetic Lock.

4.4 Recommended Penetration Test Approach

For a penetration approach, there are five different recommended ways of attempting to penetrate the system. These are a physical attack, attempting to clone a fob, attempting to emulate a fob, attempting to manipulate the keypad, and attempting to jam the RF signal.

For the physical attack, the penetration tester will set up the system and attempt to open the door by overpowering the lock. Since the lock only has 120 lbs of locking force, this should not be a difficult task.

For attempting to clone a fob, the penetration tester will use a fob cloning device to attempt to duplicate one of the fobs that are used in the system. If the copied fob works, then the tester is successful.

For attempting to emulate a fob, the penetration tester will measure the RF waves that are sent between the fob and the keypad. They will then use the measured output of the fob to output a duplicate signal to the keypad.

For attempting to manipulate the keypad, the penetration tester will measure the voltage and current that is on the PUSH signal (Figure 5) when the system is activated. They will then attempt to send a similar signal to the device using a separate wire to see if the device accepts the signal.

For attempting to jam the RF signal, the penetration tester will use an RF jammer and then attempt to use a key fob to access the system with the jammer active.

References

Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007, April 6). *Guidelines for Securing Radio Frequency Identification (RFID) systems*. CSRC. Retrieved December 7, 2022, from https://csrc.nist.gov/publications/detail/sp/800-98/final

Lambrecht, B. (2021, December 1). *The evolution of access control*. Current Technologies. Retrieved December 7, 2022, from https://www.getcurrent.net/blog/the-evolution-of-access-control