NFC Authorized Outlet

Ryan Fahsel
Georgia Institute of Technology
ryan.fahsel@gatech.edu

Colin Gray
Georgia Institute of Technology
colin.gray@gatech.edu

Ramya Ramakrishnan
Georgia Institute of Technology
rramakrishnan3@gatech.edu

ABSTRACT
In this project, an authorization system was implemented using the NFC technology on mobile devices. The motivation behind this research was to make authorization of tools in a lab easier and more effective. This way, users would be allowed to enter labs, but certain tools would have restricted access. Previous studies have looked into RFID and NFC technologies for many applications, such as for hospitals and virtual ticketing systems. In our work, we have implemented a system that controls a 120 volt outlet, which will provide or restrict access to the user based on their credentials. We use the mobile device as an NFC reader and attach NFC stickers to each tool that act as tags. We implemented the hardware and software sides and a site that allows us to manage the user permissions. From this project, we learned that the NFC technology embedded in our phones is an effective way to transmit the credentials of users. In future work, we hope to add a tracking feature.

Author Keywords
NFC; RFID; Authorization.

ACM Classification Keywords
K.6.5.

General Terms
Human Factors; Security.

INTRODUCTION

Project Description
The goal of this project was to create an access controlled, household 120v outlet. The system is composed of an Android application, web server backend, and Arduino controlled circuit. The best way to describe how the system works is through the following example: Alice wants to use the prototyping lab. She attends the mandatory training session and is given access to the lab. This is great for tools like the screwdrivers, hammers, and other small tools; however, how can the lab owners control access to potentially dangerous tools (i.e. saws, waterjets, etc)? This is how. A user comes up to a saw, opens an Android application, and taps his or her phone against an NFC tag on the desired tool. The phone sends a request to a webserver with the users credentials. The web server checks a database to see if the requestor is authorized to use the desired tool; if he or she is, the outlet the tool is connected to is powered; if he or she is not, the outlet to the tool remains powered off. While all of this sounds complicated, it happens in less than five seconds. The outlet is powered or not powered by a relay, which is controlled by an Arduino board. Additionally, the housing for the outlets is locked, so no one can tamper with the plugs to the tools or the authorized outlet.

Motivation
The idea of access control to locked areas via RFID is not a new idea; however, using NFC to control access to outlets is. When Scott Gilliland came to give a presentation on project ideas, he expressed the desire to be able to grant access to the lab to a large set of people, while only allowing a subset of trained users to use some of the more dangerous tools; however, Scott did not want to go purchase all new tools that had authentication built into them. Even if Scott was starting a new lab from scratch, he would not want to go and limit himself to only tools that have authentication built into them (which as far we know, do not even exist). There has to be a way to access control tools that already exist in the lab; the only way to do that is to control the power given to the tools. This creates a cheap and universal way (via a standard 120v plug) to grant a large group of people access to a space, while only allowing a subset of those people to use certain devices within a space.

NFC is the technology of choice for this control because it is more robust than RFID. NFC tags can store much more data than RFID tags. NFC readers are becoming commonplace in phones, which is an object a majority of people carry around with them daily.

This research is based on figuring out if this is doable. Once this is discovered, this technology can be scaled to much larger uses. For example, airports could build this technology into all their outlets; thus, people have to be authorized (essentially pay) to use the outlets, which is much more convenient than charging stations that require a user to awkwardly stand in the middle of a terminal for long periods of time.

PREVIOUS/RELATED WORK
Several past studies have analyzed the benefits of NFC and RFID technologies for authentication and have implemented

Submitted for review.

systems using these for applications such as healthcare monitoring, ticketing systems, etc. One study looked at NFC capabilities for mobile interactions and concluded that NFC in mobile phones can be used for ticketing, mobile payment, and authentication. This was determined through field trials and through analysis of current use of NFC. Some of the current systems using NFC include accessing public transportation in the Paris Metro System and managing stock in the Finnish company JCDecaux Finland Oy (Falke et al. 8). In this research, we hope to explore the idea of using NFC for controlling access to lab equipment, and since more phones are starting to be equipped with NFC, there can be more potential for work in this area. We hope to use the useful NFC technology embedded in phones to make access control as simple as possible.

Another study looked at using NFC for health care systems to facilitate more efficient patient treatment. Because staff members often have to treat a large number of patients, there is a chance that the wrong medication will be given to a patient. In order to avoid this type of error, NFC technologies can be used to ensure that the correct medication is given to each patient (Lahtela 242). NFC has been further studied for other applications such as virtual ticketing. An application called NFCTicketing was created to allow users to buy public transportation tickets using their phone (Ghiron 46).

Haselsteiner also described the capability of NFC technologies to be used in ticketing and micropayment. In his explanation, he details how contactless Smart Cards or phones with embedded NFC technology can be used to communicate with a reader, which can accept or reject the ticket (3). Similarly, we want to create a simple system that allows a reader to receive information from a phone and accept or reject access to the piece of lab equipment, based on the users credentials.

Overall, many of these past studies have studied the use of NFC in hospitals and virtual ticketing systems and have outlined the potential of using NFC technologies. We would like to extend this use of NFC by implementing a system to control access to lab equipment by enabling and disabling a 120 volt outlet with phones as our NFC reader and NFC stickers as our tags.

OUR WORK

Resources

There are three main components to this project: an NFC enabled Android device, a webserver, and an Ardurino controlled circuit. Additionally, we need an aesthetically pleasing and easy to use housing for the circuit.

- NFC enabled Android device: A Nexus 7 was used, which is NFC enabled.
- Webserver: Georgia Tech offers free hosting to all students. A Fedora server running PHP/MySQL was used for authentication decisions.
- Arduino powered circuit: Arduinos and basic relays are relatively cheap. The supplies were purchased from JameCo and Radio Shack.
- Housing: The housing was constructed from basic wood, acrylic, hinges, and a simple MasterLock lock. This was all purchased from Home Depot.

Implementation

First, an Android application was created. The application had to be able to get credentials from the user and store them. The application also had to be able to read NFC tags. Lastly, it had to be able to send both sets of information to a webserver for processing. Based on the authorization response from the server, the application had to inform the user whether or not he or she has been authenticated or not, and if he or she had been authenticated, give the user a way to stop the tool when done. The Android application was coded in Java, while the webserver was written in PHP. The database on the webserver uses MySQL.

Secondly, the webserver takes requests for authorization via HTTP posts, checks the webserver database to see if the authorization request is allowed, and sets a enable bit for the requested tool based on the authentication request result.

Thirdly, a circuit had to be created that would be able to control the power to the outlets based on a value stored in a database on the webserver. Two relays intercept the power to each socket on the outlet. These relays are SPST relays and each relay has its own control line coming from a pin on an Arduino. An Arduino polls the webserver continuously checking if each socket should be on or not. Based on this, the two Arduino IO pins to the relays go high or low based on whether the webserver says each socket is on or off.

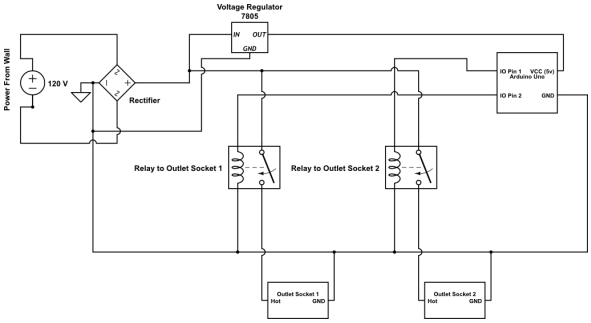

Figure 1. Circuit design.

Functionality

The deliverable of this project was a system that allowed outlets to be turned on by authorized users by tapping their Android phone against an NFC tag associated with an outlet. The following enumerates the basic functionality of this system:

- The application can read NFC tags and send them to the web server.
- The system can distinguish between authorized and unauthorized users trying to power outlets and make decisions accordingly.
- The controllable outlets should be protected in such a way that users (with the exception of authorized administrators)

cannot remove the plugs of devices from the controlled outlet to plug into another outlet.

DISCUSSION

This project had several important findings. One was that using the NFC technology built into the Android device was an effective way to transmit information about the user. This was easily used to determine whether the user was authorized to use the tool. The NFC stickers were simple to use and worked well with the NFC embedded in our mobile device. We had no issues with the transmission of information between the sticker and our phone. Thus, this system could be implemented in a larger scale because phones with embedded NFC are much more common and NFC stickers can be easily incorporated.

Another challenge we faced was creating a small, effective form factor. It was difficult to build the system in a small control unit because of the complexity of the circuit. Although the current size was sufficient to accomplish the task, we know that the form factor of the physical device will be important for making the system work on a larger scale. We hope to improve the form factor in future work on this project.

We also found that the time taken for the tool to turn on after tapping the device next to the NFC tag was slightly longer than we expected. We don't, however, see much potential for improvement here because of the time taken to transmit information to the server.

Although this technology worked well for the tools that we tested, we realize that in order for our system to work effectively, we would have to associate an NFC tag with every tool that we want to incorporate. Thus, there are difficulties in implementing this in the real world. However, we feel that the benefit of this system is higher than the cost of setting up NFC tags for each tool.

FUTURE WORK

Looking to the future, this project presents several opportunities for improvements, updates, and additions, specifically the form factor of the physical device and the addition of a tracking feature.

The current prototype is not a practical form factor for actual use. Practicality is the driving force behind improving upon the existing form factor. Additional outlets will be added along with a more compact form factor and added wireless technology instead of Ethernet. Additional outlets would make the project more practical for most of the use cases including labs, manufacturing plants, and airports. The current prototype is built using individual components fastened to a plank of wood. Transferring these components to a circuitboard would allow for a much more compact and smaller form factor.

A tracking feature would add a whole new facet to the project. This feature would allow for machine, outlet, or tool use to be tracked. With this data, several useful metrics can be recorded and translated back to the application or the admins. For instance, in a lab, machine use could be recorded to see if specific machines are used more than others or which users use which machines the most. With this information handy, training sessions can be better tailored to better explain the most important machines. Also users could identify an expert of a specific machine if they have questions.

CONCLUSION

Through the NFCOutlet prototype, the ability to regulate access to power through NFC has been demonstrated, especially in a laboratory setting. NFCOutlet was able to allow and disallow access to a bandsaw and drillpress in our experiment based on a persons training status. Because of the modularity of the concept, there was no need to buy special bandsaws or drillpresses to create the system. Additionally, the key to the authentication is an object that most people have, a smartphone. Even if NFC does not catch on among all major phones, it would be trivial to switch the method of authentication to QR, RFID, or whatever future interfaces the smartphone world comes up with.

REFERENCES

1. Falke, Oliver, et al. "Mobile services for near field communication." University of Munich, Department of Computer Science, Media Informatics Group, Tech. Rep., LMU-MI-2007-1 (2007).

2. Ghiron, S.L.; Sposato, S.; Medaglia, C.M.; Moroni, A.; "NFC Ticketing: A Prototype and Usability Test of an NFC-Based Virtual Ticketing Application," Near Field Communication, 2009. NFC '09. First International Workshop on , vol., no., pp.45-50, 24-24 Feb. 2009.

3. Haselsteiner, Ernst, and Klemens Breitfu. "Security in near field communication (NFC)." Workshop on RFID Security RFIDSec. 2006.

4. Lahtela, A.; Hassinen, M.; Jylha, V.; , "RFID and NFC in healthcare: Safety of hospitals medication care," Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on , vol., no., pp.241-244, Jan. 30 2008-Feb. 1 2008.

ACKNOWLEDGMENTS

We thank Dr. Gregory D. Abowd, Dr. Thad Starner, Clint Zeagler, and Caleb Southern for leading the class Mobile and Ubiquitous Computing, which was the inspiration for this project.