# Initial Adoption of a Distributed Access-Control System

Kami Vaniea
Carnegie Mellon University
kami@cmu.edu

Lujo Bauer
Carnegie Mellon University
lbauer@cmu.edu

Lorrie Cranor
Carnegie Mellon University
lorrie@cmu.edu

Michael K. Reiter
Carnegie Mellon University
reiter@cmu.edu

## 1. Grey: A Distributed Access-Control System

We are investigating usability issues related to distributed access control systems by studying users of a deployed distributed access control system known as Grey[1]. Grey is described in detail elsewhere; here we provide a short overview of the system.

Grey is a set of software extensions that converts an off-the-shelf smart phone into a device that allows the user to exercise, create, and request access-control permissions. Using her smart phone a user can interact with any Grey-enabled resource around her. If she has the appropriate credentials she can access the resource and grant access to other users. If she does not have access to a resource then she can send a request for help to the owner.

A user accesses a resource by first sending it a hello message. The resource responds with a statement that the smart phone must prove. The phone proves the statement locally or makes a remote connection and asks for certificates it doesn't possess. It then sends the completed proof to the resource, which checks it and performs the desired action (e.g., opening, logging in).

For example, if Alice wants to get into Bob's office her phone sends his door a hello message. Bob's door responds with: prove "Bob authorizes his office to be opened" Alice's phone must now create a set of certificates that proves that Bob says that the door should open. In this case, Alice is one of Bob's students and Bob has granted to all his students the authority to access his office. Alice's phone sends the door a set of certificates ("Bob says students can open my office","Bob says Alice is in group students", and "Alice says open"), along with a proof that this set is sufficient to grant Alice access. The door checks this proof and, finding no errors, unlocks the door.

Of course, this only works if Alice's phone has all the certificates it needs. If a needed certificate is missing or expired, the phone will fail to find a proof and will instead prompt Alice to send a help request to someone who can provide or create the missing certificate. In this case, Alice might choose to send a help request to Bob, since it is his office that she is trying to access. Bob's phone would then ask him if he wanted to help Alice get in the door, and, if so, the phone would provide Bob with a set of options such as let "Alice in once" or "add Alice to group students". Once Bob has created a certificate it is returned to Alice's phone, which in turn uses it to construct a proof to get into Bob's office.

[1] Bauer, L., Garriss, S., McCune, J. M., Reiter, M. K., Rouse J., and Rutenbar, P., Device-enabled authorization in the Grey System. *Information Security: 8th International Conference, ISC, pages 431–445, 2005.*

Resources in the Grey system can be both physical (e.g., doors) and virtual (e.g., computer logins). For the moment, we are concentrating on physical doors. The Grey infrastructure is in the process of being deployed in over 65 doors in two floors of office space comprising nearly 30,000 square feet of space. The space has a potential population of roughly 150 people. In the future we plan on introducing Windows and Linux login interfaces that allow people to log into their computers using Grey phones.

## 2. Study Design

The aim of this study is to examine the initial adoption of Grey. We are particularly interested in seeing whether users change their security policies as a result of using Grey and if the resulting policies are more or less secure.

### 2.1 The Users

We currently have 13 users; seven have their own offices, while the rest have cubicles. As the study progresses we plan on adding more users.

### 2.2 Environment

The environment is a standard office setting at a University. There is a large common area with cubicles and locked offices. During working hours this area is left unlocked. At night and on weekends the perimeter doors are locked and a physical key or Grey-enabled phone is required to enter. The offices are all individually locked and can be left locked or unlocked at the desire of the owner.

### 2.3 Procedure

The study consists of monthly interviews with the users over a period of six months. First, the user participates in an initial interview where she is asked about her current security practices. After the interview, the user is given a smart phone with Grey installed and instructed how to use it. A month later, the user is interviewed again, with the goal of understanding how she is making use of the abilities of the system. Finally, the user participates in monthly interviews to see how her use of the system changes over time.

## 3. Preliminary Results

This is an ongoing study; the results we present here are preliminary and encompass only the first two interviews with the initial set of users. We plan to present more complete results in future papers.

### 3.1 Initial Interviews

The initial interview consisted primarily of determining how the user dealt with access control before using Grey. Because the users would primarily be using Grey to unlock physical doors the majority of our questions pertained to physical access control. A few interesting themes emerged.

### *3.1.1 Obtaining Physical Keys Is Difficult*

In the building where our study takes place, obtaining a new or duplicate key is difficult. Several users mentioned waiting months to get duplicate keys to give to new students or employees. This result was not unique to the building. Users mentioned having similar difficulties at other places they had worked.

So what did users do while they waited a month for a new key? Most of them had been through the key-requesting process before and had kept extra keys around to be loaned out in just such an emergency. Other users bypassed the key requesting process all together by simply getting a single spare key and putting it in a secret shared location. Anyone who needed to access the resource was told the secret location and asked to return the key when done. The result was a security policy that depended not only on locks and keys but on the presumed responsibility and goodwill of the other users who shared the secret.

### *3.1.2 Key Ring Setup Is Important*

The majority of users had multiple sets of physical keys which tended to consist of work keys in a single set and keys for personal use in another set. Additionally, a single set of keys would often be organized using separate rings. Sometimes the separation was arbitrary but often it was so that a single ring could be easily removed and given to another person.

Speed of access was very important to some users. Approximately half the users organized their key rings in such a way that commonly used keys could be found quickly. A subset of this group had organized their keys so that the desired key could be identified without looking at it. The most common method was to arrange all the keys such that the ridges pointed in the same direction and then order the keys based on frequency of access so that the first key encountered was the most frequently needed.

### *3.1.3 Not Everyone Likes Carrying Things*

Not everyone carries their phone or their keys. During the day several users would leave keys in their offices because they didn't want to deal with the weight of their keys. Other users habitually took their keys or their cell phones out of their pockets whenever they sat down at their desks because the extra bulk in their pockets was annoying. Some users don't have pockets and carry their keys and phone in their hands. Because many users divide their keys into smaller subsets they were able to carry a minimum amount of objects with them. These users liked the idea of only having to carry their cell phone.

## 3.2 Second Interview

In the second interview we looked at the adoption of Grey and the effect it had on the security practices of our users.

### *3.2.1 Certificates Are Confusing*

The majority of users ran into some sort of confusion involving how certificates are handled in Grey. Most often this confusion was brought about by a single certificate expiring. In order to gain access to a resource the phone must present a set of certificates proving that the owner of the resource says it should open. If any certificate in the proof expires the proof is no longer valid. Users often thought that the expiration time of the last certificate created was the expiration time of the entire set and were therefore very confused when they mysteriously lost access when they knew they should still have it. This result suggests that when a request is denied users need more information on why.

### *3.2.2 Pre-arranged Requests Are Good*

During the first month only a couple users remotely requested help while accessing a resource. In all cases access was granted only if the resource's owner was previously expecting the request. In one case the owner was not expecting a request but the requester called first, then sent the request through Grey. In another case a request came in with no prior reason given and the owner denied the request because they didn't understand why the requester wanted in. Grey allows a text or voice message to be sent along with a request but users rarely made use of these features. By calling the other person the requester made certain the other person had their phone and was able to explain why they needed in.

### *3.2.3 Why Do I Need People in My Address Book?*

One of the advantages of PKI is that it gives the user some way to verify that a request came from whom they think it did. Grey implements this using an address book that contains entries for each person whose public key is known and verified. Public keys are entered via the camera: one phone displays the key as a barcode, and another phone takes a picture of the barcode and extracts the key. If a request comes in from a person in the user's address book it is simple for Grey to verify that user's identity. However, many users did not understand this and could not understand why they would need to populate their address book with people they know. One user was certain that the identity of a requester was automatically verified by some server and is therefore guaranteed to be correct. The problem is that when a help request comes in Grey does not clearly convey whether the requester is trusted or not. As a result the user fails to understand that adding other people to their address book is beneficial.

### *3.2.4 Speed Is Important*

The majority of the users considered speed to be a very important factor in their adoption of Grey. Those that considered Grey to be significantly slower than physical keys primarily complained about the number of button pushes and having to wait for a door to open. Additionally, several of these users lock the keypad on their phone, adding to the number of button pushes required to access a resource. To get a better comparison between Grey and physical keys we ran a small experiment where we observed users accessing a door using both methods. The result was that Grey comparable in speed to keys. Another observation from the study was that key users spend more time manipulating keys while Grey users spend time waiting for the door to open. We hypothesize that users perceive this waiting time as being longer than it is.

# 4. Conclusions

Distributed access-control systems are a potentially valuable technology but they run into the same problem as other new access control systems; users are accustomed to the previous technology and measure the convenience of other systems against it. Physical locks and keys may be an imperfect system but users have spent most of their lives adjusting to those imperfections. In this study we looked at some of the adjustments users have made to accommodate the inconveniences and deficiencies of using keys. As our study progresses we hope to see users make similar adjustments in the Grey system, and we hope to learn how to design this type of system so that the transition to it is as seamless and convenient as possible.