# CASA: A Framework for
# Context-Aware Scalable Authentication

**Eiji Hayashi**[1]    **Sauvik Das**[1]    **Shahriyar Amini**[1]    **Emmanuel Owusu**[1]    **Jun Han**[1]

**Jason Hong**[1]    **Ian Oakley**[2]    **Adrian Perrig**[1]    **Joy Zhang**[3]

[1]Carnegie Mellon University
5000 Forbes,
Pittsburgh PA, 15213, USA

[2]University of Madeira
Funchal,
9000-390, Portugal

[3]Carnegie Mellon University Silicon Valley
Moffett Field,
CA 94035-0001, USA

{ehayashi, jasonh, joy}@cs.cmu.edu, {sauvik, shahriyar, junhan}@cmu.edu,
eowusu@andrew.cmu.edu, ian@uma.pt, adrian@ece.cmu.edu

## ABSTRACT

We introduce context-aware scalable authentication (CASA) as a way of balancing security and usability for authentication. Our core idea is to combine a number of passive factors for authentication (e.g., a user's current location) with appropriate active factors. In this paper, we provide a probabilistic framework for dynamically selecting an active authentication scheme that satisfies a security requirement given passive factors about a user. We also present the results of two user studies evaluating the feasibility and users' receptiveness of our concept. Our results suggest that location data has good potential as a passive factor, and that users can reduce up to 68% of the number of user authentication when using the user authentication system designed with CASA compared to an authentication system that requires a fixed active authentication consistently. Furthermore, more than half of the participants who tested our prototype preferred to use our user authentication system on their phones.

## Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Authentication

## General Terms

Security, Human Factors

## Keywords

User Authentication, Context-Aware, Mobile

## 1. INTRODUCTION

Reliable authentication is an essential requirement for secure systems. Today, passwords are the most common form of authentication. However, passwords are also a major source of security vulnerabilities, as they are often easy to guess, re-used, forgotten, shared with others, and are susceptible to social engineering [5,6,16,22,23,25]. We argue that the commoditization of sensor technologies coupled with advances in modeling people and places offers us unique new opportunities for simplifying and strengthening authentication. This insight is the basis for what we call *context-aware scalable authentication*, or CASA.

CASA embodies two core ideas. First, these cheap digital sensors combined with models of people and places can offer us *passive and robust multi-factor authentication*. By passive authentication, we mean using background sensing and modeling to help verify or infer an individual's identity (such as location data, Wi-Fi MAC address, IP address, nearby devices detected, number of times having logged in at this place), as opposed to active authentication techniques that require explicit interaction from the end-user (such

as passwords and fingerprint biometrics). While behavioral biometric authentication also combines multiple features in authenticating users, these features tend to be constrained to a specific domain (e.g., key typing patterns) [29]. CASA differentiates itself by considering a wide array of features extending across multiple domains. Second, this passive multi-factor authentication can be used to *modulate the level of active authentication needed* based on the situation at hand. For example, with CASA, we want authentication to be quick and easy for situations perceived as low-risk (such as being located at work or home), and tough and reliable for high-risk situations (such as being located in an unfamiliar place). We believe that this approach can improve usability while still maintaining a reasonable level of security in the common case, while also improving security in unusual and risky cases.

In this paper, we take a step towards this vision of CASA, focusing on assessing the feasibility and usability of our ideas. This paper is comprised of three parts. The first part introduces our CASA framework that allows us to choose active factors that provide enough information given passive factors. The second part presents results of users' mobility pattern analyses, which indicates feasibility of using location data as a passive factor. The third part presents the results of a field study using a prototype that uses either weak or strong active authentication based on a person's current location.

## 2. RELATED WORK

Existing user authentication systems primarily depend on three types of mechanisms: *what you know*, *what you have* and *what you are*. Passwords are the most commonly used authentication system based on *what you know*. Password authentication has advantages in its simplicity and convenience [23]. However, many studies have found that passwords still put too much burden on users, resulting in users adopting insecure practices such as choosing weak passwords or reusing passwords [5, 25]. Our work in this paper does not seek to replace passwords, but rather complement it by taking into account passive factors and using those to modulate the level of authentication needed. More specifically, in our second analysis, we look at two cases: (a) no authentication when at home or work, and a PIN when at other places, and (b) a PIN when at home or work, and a password when at other places. We used these combinations as one instance of fast versus reliable authentication. Looking at other appropriate combinations is an area of future work for us.

Other authentication systems based on *what you have,* including eToken USB devices [1], RSA securID [2], and Google's two-step

verification [3]. Our work in this paper involves the user carrying a smartphone, but using the smartphone to gather data rather than being used as a token. We envision in the long-term that having one's smartphone nearby could be used as a passive factor, acting as a sort of token (though not in the traditional sense).

Finally, there are authentication systems leveraging *what you are*, or biometrics. A wide range of biometric techniques has been commercialized, including fingerprint scanners, iris recognition, and voice recognition, and face recognition. These kinds of biometrics tend to focus on *physical characteristics* of individuals. Researchers have also investigated a number of novel biometric techniques, e.g., walking gait [28], keyboard typing pattern [29], what applications and features on a mobile phone are being used [27], blinking pattern, and writing style. These kinds of biometrics tend to focus on *behaviors* of individuals.

Our work differs from traditional work on biometrics in two ways. First, we seek to use commodity devices as well as sensors that already exist on many computers today. In particular, in this paper, we examine the potential for using location a possible factor for authentication. Second, we seek to understand how to use these passive factors as a continuous and passive form of authentication, as well as how to use this information to influence the level of active authentication needed, as the situation warrants.

## 2.1 Modulating the Level of Authentication

It is worth noting that some online services already modulate the level of authentication based on the situation. For example, many bank web sites ask extra questions when logging in from a previously unseen network IP address. Facebook asks additional questions when using an unusual IP address, using a process called social authentication [4]. Users are asked to correctly identify several of their friends before being allowed to login, based on pictures that those friends have uploaded.

The main difference with our work on CASA is to vastly expand the number of factors used when adjusting the level of authentication needed. Our work will also focus on authenticating primarily with a device rather than an online service, as there are serious privacy issues with having behavioral data being stored on multiple online services. We do believe that CASA can be used to simplify authentication with remote online services. However, this is currently out of scope of the current paper.

## 2.2 Authentication Leveraging Context

There have been several systems using some form of contextual information to authenticate users. For example, proximity has been used to authenticate users [8, 11, 24] and pairing [18]. Seifert et al. proposed TreasurePhones that protected information on mobile phones based on a user's location as detected by near field communication technology [33].

The closest work to ours is the implicit authentication work by Jakobsson et al. [27]. Their core idea is to see whether user behavior patterns can be used to authenticate users. They considered two behavioral features from the mobile device: time lapse since the user last checked email and GPS location. The two feature scores are combined through a weighted linear function to calculate an overall "authentication score", which is then compared with a pre-defined threshold to authenticate the user.

We have similar goals, in terms of simplifying and strengthening authentication using sensor-based approaches. However, our work differs from these past works in several ways. First, we seek ways of selecting appropriate active authentication given passive factors rather than replacing active authentication with combinations of passive factors. Second, we offer a generalizable framework for combining multiple passive and active factors. Finally, we offer more empirical data of combining active and passive factors from both system perspectives and users' perspectives.

## 2.3 Human Mobility Analysis

There has also been prior work examining people's mobility patterns, showing that there are many predictable patterns [7, 17, 20, 30]. For example, past work by Gonzalez et al. [21] analyzed mobile phone cell tower data of 100,000 people over six months (based on call log and SMS log data). They found that people's trajectories had a great deal of temporal and spatial regularity, with people spending a great deal of time in just a few highly frequented locations. Hayashi et al. [22] present the results of a diary study investigating where people login to desktop and laptop computers. They found that 84.3% of logins were done at home (59.2%) and work (25.1%).

Combined, this past work suggests that location data may be quite promising in two ways. First, strong, predictable patterns in one's mobility patterns would make location data very useful as a passive factor for authentication. Second, if people often use their devices in just a few places with reasonable physical security (e.g., homes or workplaces), then modulating the level of authentication needed for those places could improve usability.

However, currently, there is little empirical data on where and how often people actually use their smartphones. This paper also contributes to this body of knowledge by providing analyses of where people actually use their smartphones, using GPS and Wi-Fi data for fine-grained information with ground truth.

## 3. CONTEXT-AWARE SCALABLE AUTHENTICATION

In this section, we introduce a probabilistic framework used in context-aware scalable authentication (CASA). One core aspect of CASA is to combine multiple factors to authenticate a user using a naïve Bayes classifier. This framework can also be used to calculate a "risk assessment" value to determine the appropriate level of active authentication required given other factors.

Most existing user authentication schemes can be considered binary classifiers, classifying a person as a legitimate user ($\hat{u} = 1$) or not ($\hat{u} = -1$). We can also model these schemes probabilistically as shown in Eq. (1) where $\hat{u}$ denotes the prediction (i.e., the result of the user authentication), $P(u = 1|s)$ denotes the probability the requester is the legitimate given the observation s, $P(u = -1|s)$ denotes the probability the person is not the legitimate user given the observation s, and $\alpha$ denotes a how conservative the user authentication is. The $\alpha$ parameter can be set based on one's comfort level with expected costs of false accepts and false rejects.

$$\hat{u} = \begin{cases} 1, & \alpha P(u = 1|s) > P(u = -1|s) \\ -1, & \alpha P(u = 1|s) \leq P(u = -1|s) \end{cases} \qquad (1)$$

For instance, for PIN-based authentication, if the system observes that a requester enters the correct PIN, the probability that the requester is legitimate is much higher than the probability he is not. Thus, the system predicts $\hat{u} = 1$ and authenticates the user. Conversely, the system predicts the opposite if the requester enters a wrong PIN.

Many current authentication schemes focus on a single factor that has large differences between the probability distributions of $P(u = -1|s)$ and $P(u = 1|s)$ across the range of values of *s*. In contrast, CASA combines multiple factors that may or may not

have as pronounced of a difference between the probability distributions of $P(u = -1|s)$ and $P(u = 1|s)$, but taken together offer strong advantage over a single factor approach. We define a factor as any data that provides information about a user's identity. Example factors include a user's location; voice obtained through a microphone; time since last login; and the observation that the user enters a correct (or incorrect) PIN; and other biometric information.

In Eq. (2), we show the underlying probabilistic model of multi-factor authenticators such as CASA. Again, $u$ denotes whether ($u$=1) or not ($u$=-1) a user is legitimate, and $s_i$ denotes the observation value for the $i$-th factor.

$$\hat{u} = \begin{cases} 1, & \alpha P(u = 1|s_1, \dots, s_n) > P(u = -1|s_1, \dots, s_n) \\ -1, & \alpha P(u = 1|s_1, \dots, s_n) \le P(u = -1|s_1, \dots, s_n) \end{cases} \quad (2)$$

We can reformulate Eq. (2) into Eq. (3) using the sign function, which extracts the sign (positive or negative) of a real number.

$$\hat{u} = \text{sign}\left(\log \frac{\alpha P(u = 1|s_1, \dots, s_n)}{P(u = -1|s_1, \dots, s_n)}\right) \quad (3)$$

Using Bayes' theorem, $P(u|s_1, s_2, \dots, s_n)$ can be simplified into Eq. (4). Then, by assuming conditional independence between each identifier, Eq. (4) can be written as Eq. (5), where $P(u)$ denotes a prior probability of how likely a person is a legitimate user (or not) in general. $P(u)$ will be canceled in the following reformulations.

$$P(u|s_1, s_2, \dots, s_n) = \frac{P(s_1, s_2, \dots, s_n|u)P(u)}{P(s_1, s_2, \dots, s_n)} \quad (4)$$

$$= \frac{\prod_{i=1}^{n} P(s_i|u) \, P(u)}{P(s_1, s_2, \dots, s_n)} \quad (5)$$

Finally, by substituting $P(u|s_1, s_2, \dots, s_n)$ in Eq. (3) with Eq. (5), we obtain a naïve Bayes classifier (Eq. (6)). Intuitively, the parameter in the sign function increases with the probability that a requester is legitimate and vice versa.

$$\hat{u} = \text{sign}\left[\log\left(\alpha \frac{P(u = 1)}{P(u = -1)}\right) + \sum_{i=1}^{n} \log \frac{P(s_i|u = 1)}{P(s_i|u = -1)}\right] \quad (6)$$

Note that because each factor might not be conditionally independent, Eq (6) may have approximation errors compared to Eq. (3). However, in Eq. (6), we can discuss each factor independently by estimating $P(s_i|u = 1)/P(s_i|u = -1)$. Further, in practice, we believe the approximation errors will be limited because we can choose largely independent factors (e.g. voice and PIN). Thus, we believe that the benefit of the independence assumption outweighs its drawbacks.

## 3.1 Selecting an Active Factor
CASA uses this probabilistic model to select an active factor that provides enough evidence to authenticate a user, given a set of passive factors. The model allows us to compare the strength of the evidence using the terms in the sign function in Eq. (6).

More specifically, let's assume we want to choose an active identifier $S$ that provides as much evidence when a user is at a café as compared to the situation where the user typed her correct PIN at her home. Assuming that location is the only passive factor, the condition that S should satisfy can be written as Eq. (7). The first term in Eq. (6) is canceled. $P_{S,1}(1)$ denotes the probability that the active factor $S$ indicates that a person is the legitimate user when a person is actually a legitimate user. $P_{S,-1}(1)$ denotes the same when a person is not the legitimate user. $P_{L,1}(l)$ (or $P_{L,-1}(l)$) denotes the probability the person is at the location $l$ when she is the legitimate user (or not). $H$ and $C$ denote *home* and *café* respectively.

$$\log \frac{P_{S,1}(1)}{P_{S,-1}(1)} + \log \frac{P_{L,1}(C)}{P_{L,-1}(C)} \ge \log \frac{P_{PIN,1}(1)}{P_{PIN,-1}(1)} + \log \frac{P_{L,1}(H)}{P_{L,-1}(H)} \quad (7)$$

Eq. (7) can be rewritten as Eq. (8), which quantifies the security criteria that an active factor $S$ should satisfy to meet the security of the legitimate user typing her PIN at home, given that the active factor $S$ authenticate the person at café.

$$\log \frac{P_{S,1}(1)}{P_{S,-1}(1)} \ge \log \frac{P_{PIN,1}(1)}{P_{PIN,-1}(1)} + \log \frac{P_{L,1}(H)}{P_{L,-1}(H)} - \log \frac{P_{L,1}(C)}{P_{L,-1}(C)}$$

$$= \log \frac{P_{PIN,1}(1)}{P_{PIN,-1}(1)} \frac{P_{L,1}(H)}{P_{L,1}(C)} \frac{P_{L,-1}(C)}{P_{L,-1}(H)} \quad (8)$$

A legitimate user is more likely to be at her home than to be at café. Thus, $P_{L,1}(H)/P_{L,1}(C) > 1$. In contrast, someone else is much more likely to be at the café than to be at the user's home, i.e., $P_{L,-1}(C)/P_{L,-1}(H) \gg 1$.

Therefore, Eq. (10) indicates that the active factor should be stronger than the PIN. Furthermore, Eq. (8) offers a quantitative guideline for the strength of the active identifier $S$ could be given the user's location. Our model can also include other passive factors, such as sensor data, time since last login, or number of times logged in at given places. We describe another example of selecting active factor in our field study.

## 4. USER STUDIES
CASA offers us a model for combining a variety of factors for user authentication. For our next step, we wanted to investigate how useful and feasible this framework might be in practice. To have strong reliability in the results, we opted to start from a relatively simple set of active and passive factors rather than combining many factors at once.

First, we investigated the potential of using location as a passive factor. Past work suggests that people spent most of their time in a few locations [7,21,22]. However, there is little empirical data on how frequently people used their smart phones at these locations. We collected this information to estimate usefulness of location information for CASA.

Second, we conducted a one-week field study with 32 participants, having them try out our prototype that modulates active factors based on their locations to understand how well our ideas might work in practice, as well as to obtain feedback from participants.

## 5. MOBILITY PATTERN ANALYSIS
We recruited multiple Android phone users through Craigslist and e-mails. Participants were asked to install our logging app from the Android Market. Participants were enrolled in a raffle for $50 Amazon gift cards as compensation. Over five months, we collected data from 128 participants. In this analysis, we focused on 36 participants with at least seven days of logs.

## 5.1 Data Collection
Our app sampled location every three minutes regardless of whether participants were interacting with their phones. Location was obtained through standard Android APIs using Wi-Fi and cell tower information. The standard API also provided expected error for each location estimate. We discarded location data when the expected errors were greater than 200 meters. Our app also logged the smartphone's running processes every 30 seconds when the smartphone was *not* in sleep mode. The timestamps of these logs let us infer when participants used their phones.

We analyzed location traces from 36 participants. The data collection periods varied from seven days to 140 days. The median length of the data collection was 26.5 days.

| Place | Time | | Activations | |
|---|---|---|---|---|
| | Mean [%] | SD [%] | Mean [%] | SD [%] |
| 1 (Home) | 38.9 | 20.2 | 31.9 | 15.6 |
| 2 (Workplace) | 18.7 | 12.6 | 28.9 | 18.1 |
| 3 | 9.9 | 8.4 | 18.5 | 13.7 |
| 4 | 5.5 | 4.8 | 10.8 | 8.5 |
| 5 | 4.3 | 4.7 | 5.2 | 4.7 |
| Other place | 22.6 | 13.1 | 4.5 | 4.6 |

**Table 1. The distribution of the time spent and the phone activation events at the places where participants spent most of their time. Place 1 to 5 denote the places where participants spent most time (1) to fifth most time (5).**

| Condition | Home | Workplace | Other places |
|---|---|---|---|
| None-PIN | None | None | PIN |
| PIN-Password | PIN | PIN | Password |

**Table 2. Active factors required at different locations. The prototype required the same active factors as participants were using at their homes and workplaces while required stronger active factors at other places.**

We divided the latitude and longitude space into discrete $0.002 \times 0.002$ latitude/longitude grids (each cell was approximately $200 \times 200$ meters in/near North America) as previously done in [13]. The particular choice of discretization was based on practical considerations balancing the accuracy of Android's positioning system with granularity of the analysis.

## 5.2 Identifying Phone Activation
To track phone use, the system ran a low level thread that logged active processes every 30 seconds. When the phone was in sleep mode, the thread was automatically paused and no log entries were made. Thus, by examining the timestamps of log entries, the phone state could be determined.

Theoretically, intervals between log entries that exceed 30 seconds signified a phone activation event after being in sleep mode once. However, initial trials of this log analysis identified two common sources of error. The first issue was the low priority of the logging thread leading to fluctuations in the sequentially logged times - variations typically in the region of 5 seconds. To deal with this, we considered valid differences between log time stamps to be in the range 30-35 seconds. The second issue was phone activations caused by push notifications (e.g. email arrival). We adopted a conservative approach to mitigate false positives relating to this issue. Essentially, phone activation events were counted only when there were two successive log timestamps after observing at least a 35 seconds gap. This filtered out short phone activations due to push notifications because the phone went back to the sleep mode quickly after the automatic activations. A consequence of these manipulations was that a certain proportion of valid user activations (e.g. very brief glances and interactions) of the phone would not be counted. However, despite this cost, we believe that these manipulations ensured the validity of the study by counting only real user activations of their phones.

## 5.3 Results of Mobility Pattern Analysis
We identified 55840 phone activation events in our dataset. Participants activated their phones 27.4 times a day on average (SD=19.7). Table 1 shows the distribution of time spent and logins at the places where the participants spent most of their time. We first calculated each participant's top five places based on the amount of time spent using location data alone (see the two columns under label "Time"). Then, for each participant, we calculated the number of phone activations at each of these places

using location data and process data (see the two columns under label "Activations").

The results indicated that people spent 57.8% of their time at two locations, presumably home and work. Before conducting this study, it was unclear to us how often people would use their smartphones at home and work, since these would be places where people would most likely have easy access to other devices with network connectivity and larger displays (e.g., desktop and/or laptop computers) at these locations. Nevertheless, our results showed that these top two places accounted for 60.8% of phone activation events on average (SD=14.5%).

This result provides supporting evidence that people exhibit strong patterns in where they use their smartphones, suggesting that location could be a very useful passive factor. This result also indicates that we can positively impact both usability and security if we adjust the active factor based on location data coupled with a very trivial user model (home and work). As mentioned previously, this analysis assumes reasonably good physical security at home and work.

## 6. FIELD STUDY
In this field study, we deployed a prototype that dynamically selected active factors based on participants' location (i.e., whether they are at home, work, or some other places) to investigate users' reactions to CASA. Another purpose of this study was to investigate how much effort our participants could reduce in user authentication when using our prototype, using authentication logs collected by our prototype.

## 6.1 Participants
We recruited 32 participants using our university's participant recruitment website. Their age ranged from 18 to 40 years old with a mean age of 24 years. Our participants consisted of 26 students, 5 full-employed and 1 non-employed. Twenty-three out of 32 participants were living with others in their homes. We compensated participants $40 for their participation in the study.

Participants were assigned to one of two conditions based on whether they used any security lock on their phones prior to this study. Participants *not* using a security lock (e.g., PIN, Draw-A-Secret or password) were assigned to the *none-PIN* condition. Those already using a security lock were assigned to the *PIN-password* condition. In essence, participants used the same authentication they already used at home and work, and had stronger active authentication at other places.

## 6.2 Procedure
In the first session, we installed our prototype on participants' Android phones. We asked participants in the none-PIN condition to choose a PIN. For participants in the PIN-password condition, we asked them to choose a password in addition to a PIN.

During the study period, when the participants turned on their phone displays, the prototype selected an active factor based on the participant's location (home, work, and other) and condition (the none-PIN or PIN-password condition) (see Table 2). After participants authenticated, the prototype asked the participants to answer if they were at home, work, or other places. After one week, we had a second session where we asked participants to complete a post-survey, and conducted a follow up interview that lasted about 15 minutes.

## 6.3 Prototype with Active Factor Selection
Our prototype used location as a passive factor and selected an active factor from three options: no active factor, a PIN and a

password. First, we describe how we can utilize the CASA in selecting active factors using the PIN-password condition as an example. In the PIN-password condition, we selected active factors to provide the same evidence as typing a PIN at workplace.

Because location is the only passive factor in our prototype, Eq. (6) can be simplified to Eq. (11) and (12). These equations denote the conditions that active factors should satisfy to provide no less evidence than being at home (Eq. (11)) or at other places (Eq. (12)), where W, H and O denotes *workplace*, *home* and *other* places respectively, and $f(l_1, l_2)$ and $g(S)$ is defined as shown in Eq. (13). Intuitively, $\log(f(l_1, l_2))$ means the likelihood that a person is a legitimate user when she is at $l_2$ compared to when she is at $l_1$. If it is less likely, $\log(f(l_1, l_2))$ becomes positive. Then, the evidence provided by the active factor (the term on the left side) should be greater than that of PIN. If it is more likely, $\log(f(l_1, l_2))$ becomes negative. Then, the active factor could be weaker than PIN. As $\left|\log(f(l_1, l_2))\right|$ increases, the user's location provides stronger evidence towards authentication. $g(S)$ denotes how strongly an active factor S indicates users' identities.

$$\log g(S) \geq \log g(PIN) + \log(f(W, H)) \tag{11}$$

$$\log g(S) \geq \log g(PIN) + \log(f(W, O)) \tag{12}$$

$$f(l_1, l_2) = \frac{P_{L,1}(l_1)}{P_{L,1}(l_2)} \frac{P_{L,-1}(l_2)}{P_{L,-1}(l_1)}, g(S) = \frac{P_{S,1}(1)}{P_{S,-1}(1)} \tag{13}$$

We estimated $g(S)$ based on the entropy of four-digits PINs (~9 bits) and passwords (~18 bits) according to the estimations by NIST [9]. Assuming that the authentication system allows three trials and that a legitimate user always type a PIN and a password correctly, then we have $P_{PIN,1}(1)=1$, $P_{PIN,-1}(1)=3/2^9$, $P_{Pwd,1}(1)=1$, $P_{Pwd,-1}(1)=3/2^{18}$ and $P_{None,1}(1) = P_{None,-1}(1) = 1$. Thus, $g(PIN) = 2^9/3$, $g(Pwd) = 2^{18}/3$ and $g(None) = 1$.

To calculate $\log(f(W, H))$ and $\log(f(W, O))$ accurately, we need further empirical data collection. However, because our primary purpose in this study was to investigate participants' responses to our concept rather than applying CASA precisely, we approximated these values. We approximate the values in a way that $\left|\log(f(l_1, l_2))\right|$ becomes smaller to avoid overestimating the strength of the evidence provided by location information. We discuss the data collection issue more in the discussion section.

For $P_{L,1}(H)$ and $P_{L,1}(W)$, we used 0.389 and 0.187 that were obtained in the first study (Table 1). For $P_{L,1}(O)$, we used 0.099 to be conservative. Additionally, we assumed that $P_{L,-1}(l)$ was proportional to the number of people who can physically come into the location. Because we do not have empirical data about $P_{L,-1}(l)$, we make assumptions after showing its effect on the active factor selection.

In Figure 1, the diagonal plots show how the right sides of the Eq. (11) and (12) change along with $P_{L,-1}(l_2)/ P_{L,-1}(l_1)$. The horizontal lines show $\log g(S)$ for each factor. Thus, satisfying Eq. (11) is equivalent to the condition that the lower diagonal plot is below one of the horizontal lines at given $P_{L,-1}(l_2)/ P_{L,-1}(l_1)$. We assume that the number of people who can access *home* is less than that of *workplace* and more than 1/10 of that of workplace. The lower diagonal plot in the segment $P_{L,-1}(l_2)/ P_{L,-1}(l_1)$ =[0.1, 1] is between the horizontal lines representing *PIN* and *None* under this assumption. Therefore, we select PIN as an active factor that satisfies Eq. (11). Similarly, we assume that the number of people who can access *other places* is more than that of *workplace* and less than 100 times of that of workplace, the upper diagonal plot in the segment $P_{L,-1}(l_2)/ P_{L,-1}(l_1) = [1, 100]$ is between the horizontal
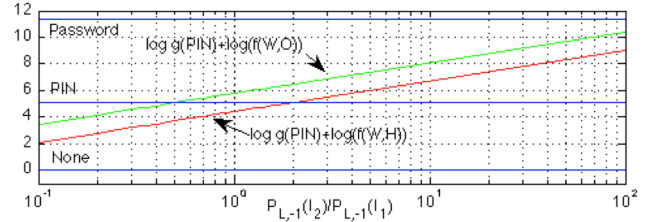


**Figure 1. The diagonal plots show how the right sides of the Eq. (12) and (13) change along with $P_{L,-1}(l_2)/ P_{L,-1}(l_1)$. The horizontal lines denote $\log g(S)$.**
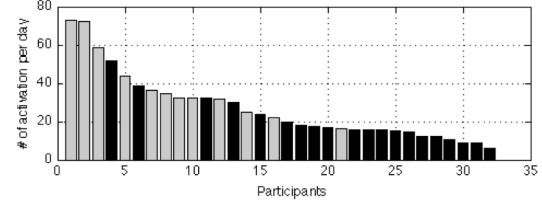


**Figure 2. The number of phone activations per day. Gray and black bars denote participants in the PIN-password condition and none-PIN condition respectively.**

lines representing *Password* and *PIN*. Therefore, we select passwords as an active factor that satisfies Eq. (12).

We made two assumptions above; however, we believe that these assumptions are safe to make considering the ranges. Additionally, our choice of active factors (Table 2) made active authentication more secure than what our participants used prior to the study. Our prototype required the same active factors as what they used prior to this study at their homes and work, and required more secure active factors at other places. Thus, we made the authentication more secure than what our participants used prior to our study.

## 6.4 Location Classification
Our prototype estimated the phones' locations using the network positioning system provided by Android OS every 150 seconds. The positioning system returns latitude, longitude, and estimated error. When the error was greater than 200 meters, our prototype discarded the location as unreliable information.

When the participants turned on their display, our prototype took the latest location information and then classified the location as home, workplace, or other using the 5-nearet neighbors within 100 meter radius.

## 7. RESULTS
## 7.1 Location Classification
In the study, our prototype asked for the ground truth of locations after each authentication and trained the 5-nearest neighbor classifier using all the ground truth data collected up to the classification. The classification accuracy was 92%. Most of the misclassifications happened when the participants transitioned from one location to another because location information was sampled every 150 seconds.

## 7.2 User Authentication
Our participants activated their phones a median of 20.7 times a day. Figure 2 shows the distribution phone activations per day. The gray and black bars represent participants in the PIN-password condition and in the none-PIN condition respectively. The participants in the PIN-password and the none-PIN condition activated their phone median of 33.6 times and 15.8 times a day respectively. The difference between the two distributions was statistically significant ($p<0.05$ in $\chi^2$ test). This result might be because those who use their phones more frequently are more

| Condition | Home | Workplace | Other places |
|---|---|---|---|
| None-PIN | 10.4 | 1.9 | 5.7 |
| PIN-password | 13.4 | 4.3 | 14.1 |

**Table 3. The median number of the phone activations per day at each location. Both the security lock group and the no security lock group activated phones more than 50% of time at homes or workplaces.**

likely to configure security locks on their phone because they are more likely to have sensitive data on their phone.

Participants in the PIN-password condition activated their phones 55% of the time at home or work, and none-PIN participants 68% of the time (see Table 3). Table 3 shows that for participants in the none-PIN condition, 32% of phone activations required authentication (PIN), and 68% of phone activations did not (at home or work). Similarly, for participants in the PIN-password condition, 45% of phone activations required the stronger authentication (password), and 55% used the equivalent to what participants were already using (PIN at home or work).

## 7.3 Participants' Receptiveness

In the post-survey, we asked participants to answer questions about their perceptions of our prototype using a 5-point Likert scale (higher scores being more positive). Participants in both conditions were very receptive to our prototype. In the followings, the number in the parentheses denotes the median of their ratings.

The participants in the none-PIN condition reported that the concept of not requiring a PIN at home and work while requiring a PIN at other places was useful (4) and very easy to understand (5). They also reported that they felt our prototype was secure (4) compared to not having any security lock on their phone. They also somewhat agreed (3.5) to the statement that they would use our prototype if it was available on their phones. One of the participants commented, "I don't normally use a security lock, but I would be much more inclined to use one if it didn't require constant unlocking."

Similarly, participants in the PIN-password condition reported that the concept of requiring a PIN at home or work while requiring a password was neither useful nor useless (3) and easy to understand (4). They also reported that they felt the prototype was more secure (4), as easy to use as requiring a PIN at all the places. They were neutral to using our prototype if it was available on their phones. In the PIN-password condition, our prototype required a PIN at homes and work while requiring passwords at other places. The configuration might have made participants less positive about our prototype.

We further asked about the configuration where our prototype did not require PINs at homes or work while it required a PIN at other place (i.e., the same configuration as one used in the none-PIN condition). The participants reported that the configuration would be easy to use (4) and as secure as a requiring a PIN at all places (3), and they agreed (4) that they would use the system if it were available on their phones.

As these results indicate, participants were receptive to our prototype. Although the participants in the PIN-password condition were neutral to use our prototype with the PIN-password configuration, our participants rated the none-PIN configuration as easier to use than the security lock that they used prior to our study, and more or equally secure to the security lock. Furthermore, more than half of the participants preferred to use our prototype on their phones.

## 8. DISCUSSION AND FUTURE WORK

We investigated the feasibility of a user authentication system that changes active factors based on users' locations. However, our work has several limitations. For example, for each factor, CASA needs estimates of $P(s|u = -1)$, the probability that a person trying to be authenticated is not legitimate. As exemplified in the field study, there are cases where rough estimates are sufficient. Additionally, for some passive factors, such as behavioral biometrics, it is easy to estimate. However, the estimation could be challenging for other passive factors.

Our participants rated our system as being as secure as using PIN at all places. However, since users are not always good at evaluating security, it is necessary to conduct a more formal security evaluation. Furthermore, over half of our participants were university students, potentially biasing our results.

One line of future work is to evaluate other passive factors and user models. Prior work has investigated the security of some passive factors, such as behavioral biometrics. However, the security of other passive factors is not clear, especially when malicious attackers try to impersonate legitimate users. Furthermore, in this paper, we used a very simple model (one passive factor modeling home, work, other). This model had the benefit of being simple to implement and simple to understand. It is clearly possible to build more sophisticated models, combining more passive factors and incorporating more information about the user (e.g. last login time, number of times logged in at a given location). However, this approach raises new questions about how well users can understand what the system is doing, and could lead to frustration if it is hard to predict.

Furthermore, we believe it is worth investigating different combinations of active factors as well as new "good enough" forms of active authentication. For example, most active authentication schemes today are designed for high accuracy in differentiating between legitimate and illegitimate users. By leveraging multiple passive factors, it is possible to relax this constraint, requiring only "good enough" accuracy.

## 9. CONCLUSION

In this paper, we introduced Context-Aware Scalable Authentication (CASA), which envisions combining multiple passive and active factors to authenticate users. We also proposed a quantitative way of choosing active factors to provide desirable security given passive factors.

We also demonstrated the feasibility of selecting an active factor based on passive factors through two user studies. In the first user study, we observed that the participants logged into their phone 60% of the time at their homes or workplace. This data indicated that there was substantial potential to improve both the usability and the security of a user authentication by choosing active factors based on users' locations. In the second study, we developed a user authentication system that changes active authentication schemes (no authentication, PIN, and password) based on users' locations. Through a field study, we observed that our prototype improved 32% to 45% of the user authentication at less frequently visited places without affecting usability of the rest of the user authentication at home or workplaces.

Although there is ample opportunity for further investigation, we believe that this paper proposed a novel authentication framework and demonstrated its feasibility and the usefulness. We hope this stimulates future researches towards our vision of developing user authentication systems that require minimum but sufficient active factors.

# 10. REFERENCES

1. eToken. http://www.aladdin.com/etoken/.

2. RSA securID http://www.rsa.com/node.aspx?id=1156.

3. Advanced sign-in security for your Google account. http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html

4. Facebook Social Authentication. http://facebook.com/blog/blog.php?post=486790652130

5. Adams A. and Sasse A. M. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (December 1999), 40-46.

6. Allan A. 2004. Passwords are near the breaking point. Gartner Research Note

7. Amini S., Lindqvist J., Hong I. J., Mou M., Raheja R., Lin J., Sadeh N., and Tochb E. 2010. Caché: caching location-enhanced content to improve user privacy. In Proc. of *SIGMOBILE Mob.*

8. Bardram J. E., Kjær R. E., Pedersen MØ. 2003. Context-Aware User Authentication Supporting Proximity-Based Login in Pervasive Computing. In Proc. of UbiComp.

9. Burr W. E., Dodson D. F., and Polk. W. T. 2006 Electronic authentication guideline. Tech report, NIST

10. Chiasson S., Biddle R., and Oorschot P. C. 2007. A second look at the usability of click-based graphical passwords. In *Proc. of SOUPS.*

11. Corner M. D. and Noble B. D. 2003. Protecting applications with transient authentication. In Proc. of MobiSys.

12. Dhamija R. and Perrig A. 2000. Déjà Vu: a user study using images for authentication. In *Proc. of USENIX.*

13. Cranshaw J, Toch E., Hong J. I., Kittur A., and Sadeh N. 2010. Bridging the gap between physical location and online social networks. In *Proc. of UbiComp.*

14. Dunphy P., Heiner P. A., and Asokan N. 2010. A closer look at recognition-based graphical passwords on mobile devices. In *Proc. of SOUPS.*

15. Everitt K. M., Bragin T., Fogarty J., and Kohno T. 2009. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proc. of SIGCHI.*

16. Florêncio D., Herley C., and Coskun B. 2007. Do strong web passwords accomplish anything?. In *Proc. of HOTSEC.*

17. Froehlich J. and Krumm J. 2008. Route Prediction from Trip Observations. Society of Automotive Engineers.

18. Kalamandeen A., Scannell A., Lara E., Sheth A. and LaMarca A. 2010. Ensemble: cooperative proximity-based authentication. In Proc. of Mobisys.

19. Komanduri S., Shay R., Kelley P. G., Mazurek M. L., Bauer L., Christin N., Cranor L. F., and Egelman S. 2011. Of passwords and people: measuring the effect of password-composition policies. In Proc. of SIGCHI.

20. Krumm J. 2008. A Markov Model for Driver Turn Prediction. Society of Automotive Engineers.

21. González M. C., Hidalgo C. A., Barabási L. A. 2008. Understanding individual human mobility patterns. Nature 453, 779-782.

22. Hayashi E. and Hong J. I. 2011. A diary study of password usage in daily life. In Proc. of SIGCHI.

23. Herley C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proc. of NSPW.

24. Hulsebosch J. R., Salden H. A., Bargh S. M., Ebben P. W. G, and Reitsma J. 2005. Context sensitive access control. In Proc. of SACMAT.

25. Inglesant P. G. and Sasse A. M. 2010. The true cost of unusable password policies: password use in the wild. In Proc. of SIGCHI.

26. Jermyn I., Mayer A., Reiter F. M. M., Rubin A. 1999. The design and analysis of graphical passwords. In Proc. of USENIX.

27. Jakobsson M., Shi E., Golle P., and Chow R. 2009. Implicit authentication for mobile devices. In *Proc. of USENIX.*

28. Orr, R.J. and Abowd, G.D. 2000. The Smart Floor: A Mechanism for Natural User Identification and Tracking. ACM Press, New York, New York, USA.

29. Peacock, A., Xian K., Wilkerson, M. 2004. Typing patterns: a key to user identification, *Security & Privacy, IEEE* , vol.2, no.5, pp.40-47, Sept.-Oct. 2004

30. Buthpitiya S., Zhang Y., Dey A. K., Griss M. 2011. n-Gram Geo-trace Modeling. In Proc. of Pervasive

31. Shepard R. 1967. Recognition memory for words, sentences and pictures. J. Verbal Learning and Verbal Behavior, 113(1):95-121.

32. Shay R., Komanduri S., Kelley P. G., Leon P. G., Mazurek M. L., Bauer L., Christin N., and Cranor L. F. 2010. Encountering stronger password requirements: user attitudes and behaviors. In *Proc*. of SOUPS.

33. Seifert J., De Luca A., Conradi B. and Hussmann H. 2010. TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones. In Proceedings of Pervasive.

34. Wiedenbeck S., Waters J., Birget J. C., Brodskiy A., and Memon N. 2005. Authentication using graphical passwords: effects of tolerance and image choice. In Proc. of SOUPS.