

Hermes: Hands-Free Authentication in Physical Spaces

Kulpreet Chilana^(✉) and Federico Casalegno

MIT Design Lab, 77 Massachusetts Avenue, Cambridge, USA
{kulpreet,casalegno}@mit.edu

Abstract. This paper presents Hermes, a hands-free authentication system that makes use of credentials stored on a users smartphone to authenticate them when they enter a physical space or the vicinity of a physical object. By combining Bluetooth LE and Kerberos, Hermes is a novel system that makes use of existing technology available in today's internet-connected devices. This makes a system like Hermes suitable for widespread adoption for a number of applications in kiosks, shared printers and access control systems.

A prototype was developed to assess how such a system could improve interactions with connected objects and reduce the friction before a user can interact with the object. Based on our preliminary user studies and performance tests, we show a considerable improvement in the time required to authenticate via Hermes, as opposed to traditional authentication methods. We also evaluate the accuracy of Bluetooth LE for use in such a system.

Keywords: Authentication · Kiosk · Intelligent environment · Security · Smartphones · Physical interaction

1 Introduction

The internet is increasingly being used as a medium for developing new interactions with physical objects. With this *internet of things* paradigm growing increasingly popular, it becomes critical to rethink legacy infrastructure and implement new systems that better fit the model of the interactions being developed. One system that directly impacts user experience is authentication. Most user authentication mechanisms involve typing a username and password on a virtual keyboard. This can be both insecure and cumbersome [9]. In physical interactions, a system is required that considers the tradeoffs between security and convenience to authenticate users when they enter a physical space or the vicinity of a physical object. Such a system should seamlessly integrate into the experience of the interaction and make use of existing infrastructure. Doing so significantly reduces friction for the user by decreasing the time it takes for them to interface with the physical interaction.

In this paper we present Hermes, a novel hands-free authentication system that uses a smartphone to authenticate a user when they enter a physical space.

As a starting point, aspects of architecture and technology were considered to develop a prototype with the goal of allowing users to simply walk up to a public kiosk and automatically be authenticated. There are a number of applications to this technology beyond the kiosk. For example, one can imagine restricting a bank teller's access to an account-holders records until the account-holder is in the physical branch or walking up to a personal computer and automatically log the user into the correct account.

By combining Bluetooth LE and Kerberos, we have developed a system that makes use of existing infrastructure. This makes the system suitable for widespread adoption for a number of applications. Based on our preliminary user studies and performance tests, we show a considerable improvement in the time required to use Hermes, as opposed to traditional authentication systems and show that Bluetooth LE is accurate enough for use in such a system.

2 Background

Current systems depend on existing authentication paradigms, which was observed in a preliminary study analyzing physical authentication systems around a college campus. The primary means of physical authentication involve RFID cards [10]. These cards, used more for access control than for authentication, were used by students to access dormitories and various buildings of the campus. However, the cards were not used when logging into campus computers or when interacting with other computer-based interactions such as point-of-sale terminals. Often times users had to input their username and a password. An example of an alternative approach to this interaction is being undertaken Knock, a system where the user is able to login to their OS X computer by walking up to their laptop and knocking on their iOS device¹.

Another physical system studied was the campus-wide printing system, which allowed students to print to a global print queue and release their print jobs at a small kiosk connected to the printer. While this system did use ID card for authentication, it required the user to print using their username and release the job using their ID card, making an otherwise simple process of printing directly to a printer unnecessarily complicated. A better experience could allow the user to simply walk into the vicinity of the printer and tap a button on the kiosk to release their print jobs, or automatically release the print jobs when the user is within range of the printer.

2.1 Prior Work

Using smartphones as a medium for authentication has been explored in different capacities in numerous studies. Hesselmann et al. explain how smartphones could be used as mediators between users and interactive tabletops to accomplish tasks such as authentication and information sharing. In doing so, they explain

¹ <http://www.knocktounlock.com>.

the shortcomings of wireless communications technologies to accomplish two-way communication between the smartphone and the tabletop, citing that they often require complex coupling procedures to establish the communication channel and are vulnerable to packet sniffing attacks [6]. Mayrhofer et al. describe a cryptographic approach to authentication based on accelerometer data and shaking two devices together to avoid the cumbersome task of inputting a PIN [8]. Greene et al. describe different authentication schemes in the context of password requirements. They conclude that device constraints must be considered before porting password requirements from one system to another (i.e. desktop to mobile). From this work, it makes sense that device constraints must also be considered when porting traditional authentication schemes to that of a physical interaction [5].

Most relevant to this publication is the work of Roalter et al., who also developed a smartphone-based authentication system for public kiosks [9]. Their work discusses a number of trends in authentication schemes used in industry today. In many ways, Hermes is an extension and improvement on their work in that it addresses many of the shortcomings of their system. Namely, that it requires active use of the smartphone rather than passively using the smartphone in the background. Hermes is a tested implementation that make use of existing infrastructure (Bluetooth LE and Kerberos) to accomplish something very similar with even less friction on the part of the user.

2.2 Technologies

Bluetooth LE (BLE) broadcasters or beacons can be used to detect proximity of a nearby device with an accuracy of $\approx 1m$. A number of studies have depicted the potential for vast applications of micro-location technologies such as BLE in enabling new experiences when interacting with physical spaces [4, 7]. Apple’s CLBeacon API documentation categorizes beacon proximity into four categories: immediate, near, far and unknown. [3] These classifications are used to determine how far a user is from a beacon device, such as a kiosk, and will be used to describe various steps in the user flow and the design of the system below.

During the initial design stages several authentication schemes were considered, taking into account ease-of-use, reliability and security. Traditional authentication schemes that were considered include LDAP and Kerberos protocols. Additionally, less clean approaches were explored such as session-hijacking and cookie-forwarding. Kerberos is the most widely deployed computer network authentication protocol used on the internet and makes use of tickets to allow users to prove their identity to a service or application. The system described below outlines one approach to a hands-free authentication system that uses Kerberos with the added benefit of never sending a user’s password over the air during authentication.

3 System Components

The system consists of three main components as shown in Fig. 1 above: a server, kiosk device, and the user's personal smartphone. First, the user stores their login credentials securely on their device when they download and install a mobile application. The kiosk device runs an application that connects to the server via a socket connection. Upon connecting to the server, the server supplies the kiosk with a UUID and a major and minor value. These three values are broadcast by the kiosk over Bluetooth LE and can be used by the server to uniquely identify the kiosk.

When the user enters the far field of any kiosk with that particular UUID, their smartphone authenticates them using their stored credentials against the authentication scheme. The result is an authentication credential (e.g. a Kerberos

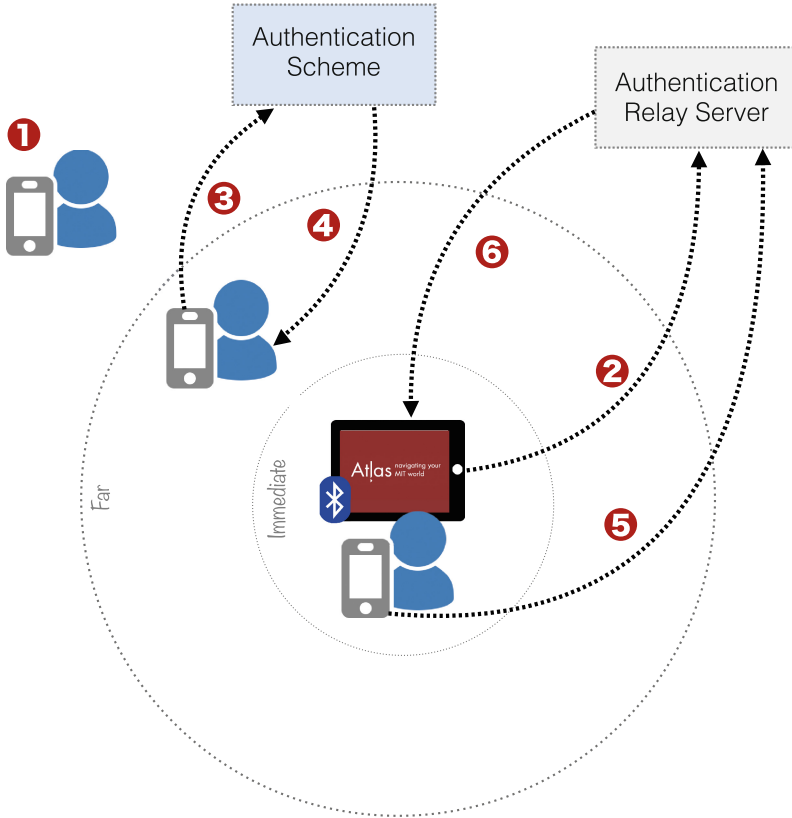


Fig. 1. A high-level overview of Hermes. (1) The user *logs in* and effectively stores their credentials on their smartphone. (2) The kiosk connects to the authentication relay server (3) The user enters the *far* field and (4) exchanges the stored credentials for a token. (5) The user enters the immediate field posting the token to the authentication relay server. (6) The server relays the token to the kiosk.

ticket, certificate, or session cookie) stored on the user’s device. This secure information remains on the user’s device until they enter the immediate field of a kiosk, at which point the authentication credential is forwarded to the server along with the major and minor value of the nearby kiosk. The authentication relay server uses this information to forward the authentication credential to the right kiosk, which can use the token to pose as the user until the user walks away from the kiosk or leaves the immediate field.

4 Design and Implementation

A prototype was developed that made use of the Bluetooth and Kerberos APIs included in the Apple iOS SDK. The kiosk was developed as a tablet application and a mobile client was written for the user to store their username and password. To sidestep the security issues with wireless communication outlined by Hesselmann et al. [6], the kiosks and the mobile client interfaced with each other through an authentication relay server. This server was written as a simple TCP socket, using the Python Twisted library and maintained connections to kiosks and clients separately.

An alternative approach could have the tablet and the mobile device communicating directly over Bluetooth LE link-layer, but this would require an additional mechanism to verify the identity of the kiosk to the mobile device to prevent an adversary from broadcasting the same UUID as the kiosks and intercepting the user’s authentication credential. The iOS SDK provides such a mechanism to establish a secure link-layer connection, but it requires pairing the two devices. This additional step creates another level of friction in the user experience and defeats the purpose of hands-free authentication:

If the central and the peripheral are iOS devices, both devices receive an alert indicating that the other device would like to pair. The alert on the central device contains a code that you must enter into a text field on the peripheral device’s alert [2].

An authentication relay server acts as an effective mediator between the kiosk and client, with many mechanisms already existing to establish secure connections and verifying the identity of connected clients over TCP without requiring pairing. In our tests, the added time required to reroute through the authentication relay server as opposed to establishing a direct link-layer connection is negligible.

The kiosk and the client made use of the Generic Security Service Application Program Interface (GSS-API) for Kerberos authentication. The GSS-API is an IETF standard that provides a common API for authenticating against a large number of authentication schemes including Kerberos, NTLM, DCE, SESAME, SPKM and LIPKEY. This API makes adjusting a prototype built around one of these schemes easily adaptable to any of the others. Despite being a low-level API, the GSS-API comes bundled with the iOS SDK and is also written in C.

Two particular APIs can conveniently be used in this system: `gss_export_cred` and `gss_import_cred` [1].

The authentication process starts in a callback that is triggered when the user enters the far field of the kiosk with their mobile device. The mobile device uses the stored username and password to acquire an initial credential, in this case a forwardable Kerberos Ticket Granting Ticket (TGT). When the user enters the immediate field, another callback is called which serializes the acquired credential using `gss_export_cred` and send the credential to the authentication relay server over the TCP socket along with the major and minor value of the nearby kiosk. The server then blocks any other requests to authenticate to that kiosk and forwards the credential. The kiosk can import the credential using `gss_import_cred`. When the user exits the immediate field, another callback is triggered which signals the server to stop blocking requests and signal the kiosk to log out the user and destroy the imported credentials.

The TGT on the kiosk can be used to authenticate to any service that supports Kerberos authentication. Once the user is authenticated to this service on the kiosk, the TGT is no longer needed. For this reason, it makes sense for the mobile device to acquire and forward a TGT with a short expiration time as an added security measure in case the TGT gets intercepted. The use of the GSS-API greatly simplifies the process of acquiring, destroying, exporting, and importing Kerberos credentials, abstracting away complicated lower-level Kerberos APIs. The credentials acquired using the GSS-API can also be stored in the sandboxed application Keychain and integrates well with NSURLSession and its higher-level APIs such as UIWebView in the iOS SDK. This comes in handy for web authentication, as the imported TGT can be used to easily authenticate via the HTTP-Negotiate protocol to access secure corporate websites, for example.

5 Performance Tests

This section discusses several tests that were performed to determine the system's reliability and performance. The first set of measurements was taken in a large open space to get a sense of the broadcast range of the tablet kiosk. This range was measured to be between 40 and 50 m, greatly exceeding the 30 m described in the Bluetooth LE specification. This is most likely due to the higher power and frequency of broadcast of the tablet device as opposed to the much lower-power Bluetooth peripherals or beacon devices.

At the lower extreme, with default parameters and conditions, the immediate field callback was triggered when the subject walked within approximately 80 cm of the tablet. Being able to adjust this parameter is important for a system of this sort: since the user is logged in when they enter the immediate field, it should be feasible to adjust this parameter from 0.8 m to 2.0 m if the physical setup of the interaction requires it. Every beacon broadcasts a measured power value with each advertisement. This measured power value corresponds with the received signal strength indication (RSSI) of the beacon calibrated to be one meter away from the device. This calibration process can be used to adjust the

distance at which the immediate field is triggered. A set of measurements were taken to determine the granularity of the RSSI signal at different distances and how well the measured power of a tablet placed at desk-level and face-level could be adjusted. The results are summarized in the Fig. 2.

These results show a similar signal strength measurement for a tablet at face-level and desk-level and a linear relationship between RSSI and distance. In collecting this data, a small anomaly was also discovered. One subject placed the mobile device used to measure RSSI into their back pocket. For this subject, shown by the yellow line in the figure above, the RSSI reading was much lower than the subjects who put the device in their front pocket. As the subject walked closer to the kiosk, the immediate field was not triggered; thus they were not authenticated. Upon further investigation we learned that the human body is a source of interference for Bluetooth LE signals and the subject's body was effectively shielding the signal. This presents a usability issue as many smartphone users prefer to keep their device in their back pocket. However, we also consider a future where wearable technology is more prevalent. Existing smartwatches on

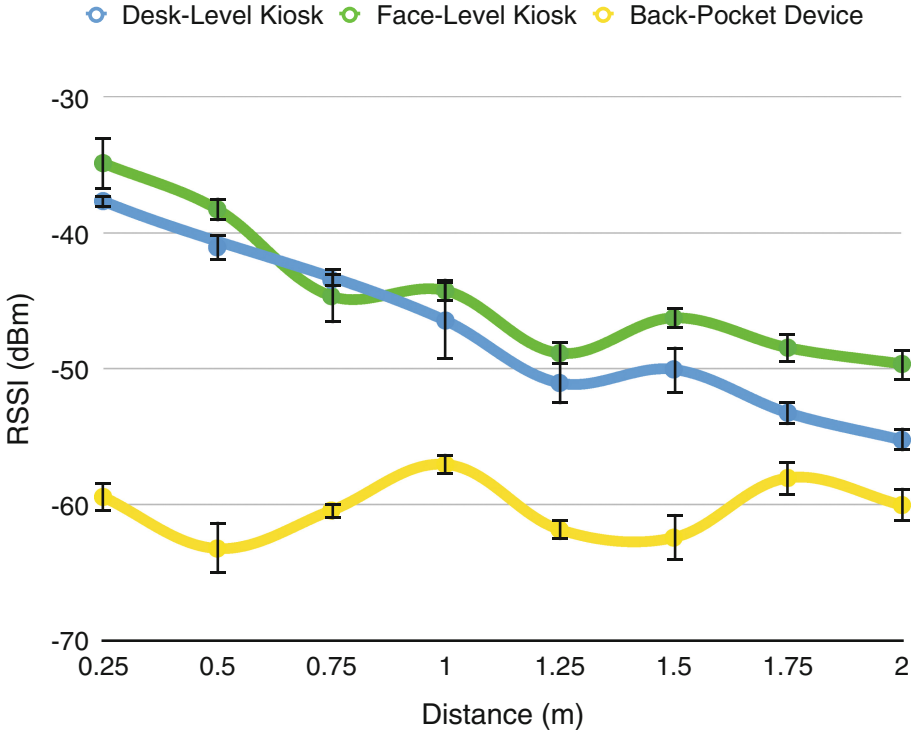


Fig. 2. A plot of distance from the kiosk and measured signal strength at that distance. Such a plot could be used to calibrate the distance that triggers the *immediate* field and thus the authentication. The yellow plot depicts the result of shielding that occurs when the user keeps their smartphone in their back pocket. (Color figure online)

the market today are equipped with the necessary technology to perform all the operations required by the mobile device in this system, so users could theoretically use them to authenticate from their exposed wrists rather than their back pockets.

5.1 User Study

A user study was also conducted, using a technique similar to that of Greene et al., to compare the time taken to authenticate through this hands-free system with that of a conventional password-based system [5]. Subjects were given an 8-character password comprised of letters, numbers and special characters to memorize. They were then timed from a starting position four meters away from the tablet device until they were successfully authenticated on the device. This was measured using a virtual keyboard on the tablet device, a physical keyboard attached to the tablet, and using the Hermes hands-free system developed in this paper. The results shown in Fig. 3 show a marked improvement from both the virtual and physical keyboard:

Despite this improvement, when interviewed many of the subjects felt that the hands-free authentication took longer because there was a short delay when they approached the kiosk while they waited for the authentication to complete and were not occupied typing their password. This is a minor concern, given that

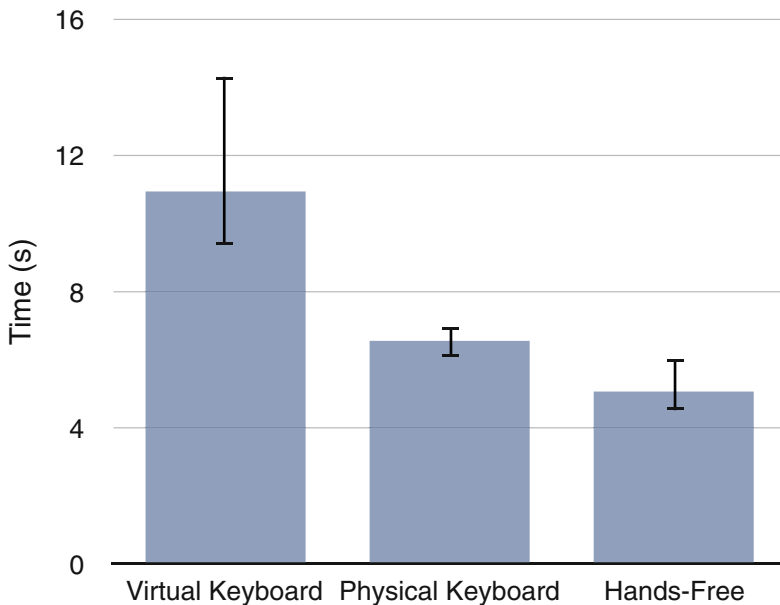


Fig. 3. Hermes, hands-free authentication performs markedly better than traditional authentication systems that use a keyboard, reducing the friction before a user can interface with an interaction.

this is an early prototype and the system design and network configurations could be further optimized to improve latency.

The final user study involved multiple subjects approaching and attempting to authenticate at the same kiosk. In this case, the subject who approached the kiosk first was authenticated on the kiosk at almost every trial. This situation could present some awkwardness in a deployed system but could easily be remedied with the two-factor authentication extension described in the next section.

6 Limitations and Extensions

There remain several limitations and areas for exploration. One of the first concerns is whether walking up to a physical device should be sufficient to authenticate a user. Other proposed models include a two-factor authentication model that requires the user to walk up to the physical interaction and also confirm their intention to authenticate by tapping on a smartwatch, scanning an ID card, or providing some other quick form of identification such as a thumbprint or facial scan. Another model proposes splitting the data in an application or service so that the user only be prompted for the second authentication factor when they need to access sensitive or secure information.

There are also several considerations concerning security and privacy. An authentication system involving beacons placed all around a campus could also be used to triangulate a user's location. While there are many interesting use cases such as tracking when a worker physically arrives at work and when they leave to get a more accurate clock in and clock out, the assumption is that a large majority of users would not be fond of allowing an organization to track their position. The final consideration is infrastructure, as this system requires all users to have a smartphone. There is no way of knowing with certainty if enough users of a particular physical system have smartphones to justify requiring it in this system; thus, the assumption is that a majority of systems will have a fallback method of authentication.

7 Contributions

In this paper, we have developed Hermes, a novel authentication system for physical interactions and demonstrated how it quantitatively and qualitatively performs better than traditional authentication systems. Hermes was developed mainly as a proof-of-concept prototype to show it's possible to build such a system and assess how well it performs in a variety of different scenarios. While it was shown that the system performs much better in certain situations than others, it remains a promising option for a future where remembering passwords and password-based security vulnerabilities are a thing of the past.

References

1. MIT Kerberos Documentation, Chapter Developing with GSSAPI, 20 March 2015
2. Core Bluetooth Programming Guide, chapter Best Practices for Setting Up Your Local Device as a Peripheral. Apple, Inc. (2013)
3. CoreLocation Framework Reference, chapter CLBeacon Class Reference. Apple, Inc. (2013)
4. Casado-Mansilla, D., Foster, D., Lawson, S., Garaizar, P., López-de Ipiña, D.: ‘close the loop’: An ibeacon app to foster recycling through just-in-time feedback. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA 2015, pp. 1495–1500. ACM, New York (2015)
5. Greene, K.K., Gallagher, M.A., Stanton, B.C., Lee, P.Y.: I can’t type that! P@\$\$word entry on mobile devices. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 160–171. Springer, Heidelberg (2014)
6. Hesselmann, T., Henze, N., Boll, S.: Flashlight: Optical communication between mobile phones and interactive tabletops. In: ACM International Conference on Interactive Tabletops and Surfaces, ITS 2010, pp. 135–138, New York, NY, USA. ACM (2010)
7. Jamil, S., Basalamah, A., Lbath, A.: Crowdsensing traces using bluetooth low energy (ble) proximity tags. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, UbiComp 2014 Adjunct, pp. 71–74, New York, NY, USA. ACM (2014)
8. Mayrhofer, R., Gellersen, H.-W.: Shake well before use: authentication based on accelerometer data. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 144–161. Springer, Heidelberg (2007)
9. Roalter, L., Kranz, M., Möller, A., Diewald, S., Stockinger, T., Koelle, M., Lindemann, P.: Visual authentication: a secure single step authentication for user authorization. In: Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia, MUM 2013, pp. 30:1–30:4, New York, NY, USA. ACM (2013)
10. Walton, C.: Portable radio frequency emitting identifier, 17 May 1983. US Patent 4,384,288

Human Aspects of Information Security, Privacy, and Trust

4th International Conference, HAS 2016, Held as Part
of HCI International 2016, Toronto, ON, Canada, July
17-22, 2016, Proceedings

Tryfonas, T. (Ed.)

2016, XV, 289 p. 83 illus., Softcover

ISBN: 978-3-319-39380-3