# Friendly Authentication and Communication Experience (FACE) for Ubiquitous Authentication on Mobile Devices

Benjamin Halpert
*Nova Southeastern University*
*Graduate School of Computer and Information Sciences*
*bhalpert@nova.edu*

## Abstract

*Current wireless personal area network (WPAN) standards provide no method for two previously unacquainted parties to authenticate to one another in a trusted manner upon first encounter. The paper details the research leading up to the development of Friendly Authentication and Communication Experience (FACE). The FACE methodology will be developed to be independent of wirelessly enabled mobile device types, such as smartphones, personal multimedia devices, personal digital assistants (PDAs), and mobile gaming platforms. FACE will enable individuals that have never met before to communicate in a trusted manner on the first attempt. FACE development will advance human interaction via wirelessly enabled mobile devices.*

## 1. Introduction

Current wireless personal area network (WPAN) standards provide no method for two previously unacquainted parties to authenticate to one another in a trusted manner upon first encounter. A new authentication methodology is required to enable individuals that have never met to communicate in a trusted manner on the first attempt. The name given to the new authentication method is Friendly Authentication and Communication Experience (FACE). The target environment for FACE is wirelessly enabled mobile devices that form ad-hoc networks. Traditional authentication methodologies are inadequate for use in ad-hoc networks. The concept of enabling individuals that have never met before to communicate in a trusted manner on the first attempt is a departure from current authentication mechanisms.

Section 2 details the motivation that led to the commencement of research, section 3 describes the current methods available for authentication in ad-hoc environments that can be utilized by wirelessly enabled mobile devices, section 4 presents development requirements, and section 5 discusses future work areas.

## 2. Motivation

Many factors motivated the work on a new authentication methodology. One factor is reducing the passage of malicious code from one wirelessly enabled device to another, thereby reducing the vicious cycle of malicious code propagation. The *2004 CSI/FBI Computer Crime and Security Survey* noted that of all the respondents, 99% utilized anti-virus software. Anti-virus technology is the most widely used security technology, based on the survey results [15]. The survey only addressed organizational computing environments that rely on traditional computing technologies such as desktops, laptops, and servers. While anti-virus products are available to the mobile device market, the concentration is on traditional personal digital assistants (PDAs) and smartphones [34]. The category of wirelessly enabled mobile devices has been expanding over time to include devices such as portable gaming platforms and MP3 players [3, 24, 27]. The evolving capabilities of the aforementioned devices will require protection from malicious code. FACE will require authentication prior to connecting to a device, thereby halting malicious code. A second factor motivating the work is to bring people in contact with others they may not typically associate. An example would be two individuals that were traveling in a contained environment, such as on a commuter train, for an hour trip to work. Many wirelessly enabled mobile devices have the ability to inform a user if another similarly equipped device is within range. A user could initiate a probe of all other wirelessly enabled devices in the environment. At this

point, the proposed authentication process can begin, and upon agreement of the requested party, a new relationship can begin to form. A third factor is that the proposed ubiquitous authentication method can assist in reducing identity theft occurrences. Identity theft is a major concern for individuals. Over the last five years, more than 27 million individuals in the United States, have been victims [32]. Because wirelessly enabled mobile devices establish a connection to facilitate the exchange of data, information stored on either device, personal or business related, can potentially be extracted by a malicious entity. Reports of WPAN enabled devices being vulnerable to attack, potentially without a device owner's knowledge, have been reported in the media [12, 23]. Lastly, WPAN enabled mobile device applications are starting to be developed, such as [28], that enable users to exchange files with individuals that are within range that have similar preferences. These applications lack security measures that would allow requestors of a file to be properly authenticated to another individual's device.

# 3. Authentication

In this section, authentication methodologies are discussed. Section 3.1 provides a brief introduction to authentication and describes two traditional authentication examples. Section 3.2 introduces WPAN standards and provides an overview of the applicable authentication processes. Section 3.3 details prior work involving authentication for ad-hoc networks.

## 3.1. Traditional authentication

There are two general types of authentication, symmetric and asymmetric. The difference between the two being that the former involves a shared secret and the latter uses different, although related, secrets [10]. For traditional authentication processes to function, the two entities must have some prior knowledge of each other. An example of shared secret, or symmetric, authentication is the process Bluetooth devices engage in when they are paired for the first time. Authentication of two or more Bluetooth enabled devices is based on a static PIN code. The PIN codes are typically 4 digits in length, too short for a secure pin that is also used in the encryption process. Additionally, many Bluetooth devices do not have a user interface to enable a user to create their own PIN. In such instances, the default PIN of 0000 is used [6].

Public Key Infrastructure (PKI) is an example of an asymmetric authentication process. For PKI, one user has the private key and another user or system has the corresponding public key. An example of a PKI based authentication system, is when a user connects to a website and has to present their private key credential in order to log into the site. The backend server then verifies whether the public-private key pair matches and is still valid. Many authentication methods have been introduced in the past, each with varying degrees of success. Other examples of asymmetric authentication methods are, email-based identification and authentication (EBIA), user name password systems, Identity-Based Encryption (IBE), Internet Identity Solution from Authentify, Pretty Good Privacy (PGP), RSA Mobile, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), 802.1x, and biometrics [14].

## 3.2. WPAN authentication

Current wireless personal area network (WPAN) standards do not include a method for two unknown users to authenticate in a trusted manner. A partial listing of current and proposed WPAN technology standards and industry consortiums, also referred to as trade associations or alliances, appears in Table 1 [11, 16, 18, 35, 36, 37]. While each WPAN standard includes a design for authentication, the methods rely on both parties either having a previous relationship or allowing a connection to an unknown device without adequate security measures [2, 4, 8, 9, 17, 19, 20, 21].

**Table 1. WPAN consortium and standard relationship**

| Consortium | Standard |
|---|---|
| WiMedia Alliance | 802.15.3 |
| Zigbee Alliance | 802.15.4 |
| Bluetooth Special Interest Group | 802.15.1 |
| Infrared Data Association | IrDA |
| Wireless USB Promoter Group | WUSB |

## 3.3. Ad-hoc authentication

While research has been conducted with the goal of developing an authentication method for mobile devices that form ad-hoc networks, all of the work relies on prior knowledge of the connecting device or physical contact of one device to another. The premise of [5] is that all of the device owners have a pre-established relationship. The example scenario provided includes a group of individuals in a meeting that wish to set up an ad-hoc wireless network so all of the computers can communicate securely. All ad-hoc

users must be physically in the same room and trust each other prior to connecting their devices. As illustrated, the research focuses on how to authenticate in an environment where the individuals know and personally trust each other.

Another example of research that has been conducted targeting ad-hoc authentication is described in [1]. As with the prior example, all participants must physically be in the same room and trust each other prior to connecting their devices. The method described involves one person in a group creating a shared key that is then beamed via infrared to all other participants in a clear text manner.

In [31] the authors propose verification of credentials in an ad-hoc network where a prior knowledge of one peer to another is a given. The solution is based on using a public-key crypto system where at least one node has access to the Internet. However, when one node cannot connect to the Internet, a peer may vouch as to the authenticity of the requestor. If a peer can verify a certificate, then the certificate will be accepted as valid to others. The authors state that revocation issues for public-key systems in ad-hoc networks are difficult.

[7] builds on previous work dealing with authentication for mobile devices in ad-hoc networks. According to the authors, all previous work has centered around some type of data exchange using an out-of-band method prior to the establishment of a wireless connection between two or more wireless enabled ad-hoc devices. The authors explain how an earlier proposed solution, known as the Resurrecting Duckling method, involves imprinting data in devices during manufacture. Pretty Good Privacy's (PGP's) web of trust authentication method was also discussed. The PGP out of band authentication method involves a phone call, email, or physical meeting of individuals to validate a PGP fingerprint and therefore trustworthiness of another party. The author's solution uses a location-limited side channel. The location-limited solution can either involve a user touching a device to a printer to exchange some pre-authentication data at the point of contact or a device can transmit pre-authentication data in a limited area that a user can select to authenticate with. Here again is an example of where a device user has some form of a pre-established relationship with another device prior to joining an ad-hoc network.

In [25], a security architecture for ubiquitous ad-hoc computing is presented, named SHAD (Secure Human-centered Architecture for Distributed Systems). SHAD introduces specific aspects that should be considered when developing secure communications methods for wireless ad-hoc environments. Prior knowledge of users trying to gain access to a specific wirelessly enabled mobile device is assumed. The prior knowledge can be accomplished by a physical meeting of individuals to determine if they agree to exchange the data necessary to pair their devices.

## 4. Development requirements

FACE development will be carried out with specific requirements in mind. Face will be designed to ensure low resource consumption, to include battery life, processing power, and application footprint. Device owners will determine who to trust prior to granting a connection request by being afforded the time to make a decision. It has been shown that given the right information, data owners will make appropriate risk based decisions [29]. The authentication interface will be designed to minimize cognitive load while displaying clear and pertinent information. As exemplified by [26], focus has been lacking with regard to authentication interface designs. FACE will be encryption algorithm independent, allowing a user to select an appropriate level of protection, depending on the sensitivity of the data to be transmitted. The FACE methodology will be developed to be independent of a specific wirelessly enabled mobile device type, such as smartphones, personal multimedia devices, PDAs, and mobile gaming platforms.

## 5. Future work

The development of FACE will rely on the following assumptions. The first assumption is that all devices within the ad-hoc network have already agreed on a given routing protocol to communicate via the "best connected" device [30]. The second assumption holds that at least one device in the ad-hoc network has access to the Internet via wired or wireless means. Cellular carriers have announced the availability of new devices that include the capability to function on more than one type of wireless network at a time [33], effectively turning the device into a bridge. Example network types that are now included on one mobile device include wireless wide area networks (WWAN), wireless local area networks (WLANs), and wireless personal area networks (WPANs). A third assumption is that the user has already been authenticated to the actual device in-hand and granted access to the data contained therein. Numerous papers have been published on a myriad of methods, including [13, 22].

## 6. Conclusion

FACE development will enable ubiquitous authentication for individuals in mobile ad-hoc networks that have never met before to communicate in a trusted manner on the first attempt. The innovative work will have positive implications for expanding secure communication between previously unacquainted parties. As previously stated, the proposed authentication method will limit malicious code propagation and instances of identity theft. Additionally, FACE will enable individuals that share similar interests to communicate with others in range of their wirelessly enabled device. Existing authentication methods require some form of prior relationship between two individuals that wish to communicate. FACE development will advance human interaction via wirelessly enabled mobile devices in an unprecedented manner.

## 7. References


[1] Ahlgren, B., Feeney, L.M., & Westerlund, A. (2001). Spontaneous Networking: An Application-oriented Approach to Ad Hoc Networking. IEEE Communications Magazine, 39(6), 176-181.

[2] Allen, J. & Gandolfo, P. (2002). *802.15.3 Overview/Update*. The WiMedia Alliance. http://www.wimedia.org/

[3] Apple Computer, Inc. (2005). *Apple iPod.* http://www.apple.com/ipod/

[4] Arbaugh, W. (2001). Security/Privacy Introduction and Overview (IEEE 802.15-01/245r0). www.ieee802.org/15/pub/2001/May01/01245r0P802-15_TG3-Security-Privacy- Introduction-and-Overview.ppt

[5] Asokan, N. & Ginzgoorg, P. (2000). Key Agreement in Ad-hoc Networks.

[6] Bakker, D.M. & Gilster, D. M. (2002). Bluetooth End to End. New York: Hungry Minds, Inc.

[7] Balfanz, D, Smetters, D.K., Stewart, P. & Wong, H.C. (2002). Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. Network and Distributed System Security Symposium Conference Proceedings.

[8] Barr, J. (2002). *IEEE 802.15 Working Group for Wireless Personal Area Networks.* IEEE 802.15-02/096r5. http://www.ieee802.org/15/pub/2002/Mar02/02096r5P802-15_TG3-Opening-Report-March02.ppt

[9] Bisdikian, C. & Siep, T. (2001). *IEEE P802.15.1 Tutorial.* http://ieee802.org/15/pub/2001/Jan01/01046r0P802-15_WG-802-15-1-TG1-Tutorial.ppt

[10]Bishop, Matt. (2003). *Computer Security: Art and Science*. Boston, MA: Pearson Education, Inc.

[11] Bluetooth Special Interest Group https://www.bluetooth.org/

[12] Brandt, A. (2004, December). Privacy Watch: Cell Phones Get Chatty With Hackers. http://www.pcworld.com/howto/article/0,aid,118236,00.asp

[13] Corner, M.D. (2003). Transient Authentication for Mobile Devices. Dissertation Abstracts International, 64 (9), 4518. (UMI No. AAT 3106037)

[14] Garfinkel, S. (2003). Email-Based Identification and Authentication: An Alternative to PKI? IEEE Security & Privacy, 1, 6.

[15] Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William and Richardson, Robert. (2004). 2004 CSI/FBI Computer Crime and Security Survey.

[16] Institute of Electrical and Electronics Engineers, Inc. (2004, November 17). *IEEE 802.15 Working Group for WPAN.* http://ieee802.org/15/

[17] Institute of Electrical and Electronics Engineers, Inc. (2002). *802.15.1Part 15.1:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).* http://standards.ieee.org/getieee802/download/802.15.1-2002.pdf

[18] Infrared Data Association. (2005). http://www.irda.org

[19] Infrared Data Association (IrDA). (2000). *Infrared Data Association Point and Shoot Profile.* www.irda.org/standards/pubs/PointandShootv1p1.pdf

[20] Infrared Data Association (IrDA). (2001). *Infrared Data Association Serial Infrared Physical Layer Specification*. www.irda.org/standards/pubs/IrPHY_1p4.pdf

[21] Intel Corporation. (2004). *Wireless USB.* http://www.intel.com/technology/ultrawideband/downloads/wirelessUSB.pdf

[22] Jansen, W.A. (2003, May). Authenticating Users on Handheld Devices. Proceedings of the Canadian Information Technology Security Symposium.

[23] Kelly, S. (2004, April 15). *Bluesnarfing*. http://www.bbcworld.com/content/clickonline_archive_15_2004.asp?pageid=666&co_pageid=3

[24] Nintendo of America, Inc. (2005). *Nintendo DS*. http://www.nintendo.com/systemsds

[25] Salvador, E.S. (2004). SHAD: A Human Centered Security Architecture for Partitionable, Dynamic, and Heterogeneous Distributed Systems, Proceedings of the 1st International Doctoral Symposium on Middleware, pp. 294-298. New York, NY: ACM Press.

[26] Smith, S.W. (2003). Humans in the Loop: Human-Computer Interaction and Security, IEEE Security & Privacy, 1(3), 75-79.

[27] Gerstmann, J. (2004, May 12). Hands-On with the PSP. http://www.us.playstation.com/news.aspx?id=328

[28] Rojas, P. (2004, July 12). IcyPole: Using Bluetooth to Sample Other People's Music Collections. http://www.engadget.com/entry/3621730184116930/

[29] Sasse, A. M. & Weirich, D. (2001). Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 137-143). New York, NY: ACM Press.

[30] Schilit, B.N. & Sengupta, U. (2004). Device Ensembles. Computer, 37(12), 56-64.

[31] Sye, L. K. & Emil, L. (2002). Towards flexible credential verification in mobile ad-hoc networks. Proceedings of the second ACM international workshop on Principles of mobile computing, 58-65.

[32] Synovate. (September 2003). Federal Trade Commission – Identity Theft Survey Report.

[33] T-Mobile USA. (2004). HP iPAQ h6315. http://www.t-mobile.com/business/products/overview.asp?phoneid=228503&class=pda

[34] Trend Micro. (2004). *Trend Micro Mobile Security.* http://www.trendmicro.com/en/products/mobile/overview

[35]WiMedia Alliance. (2005). *Welcome to the WiMedia Alliance.* http://www.wimedia.org/

[36] Wireless USB Promoter Group. (2005). *Our Mission Statement.* http://www.usb.org/wusb/home

[37] Zigbee Alliance. (2005). *Information Resources*. http://www.zigbee.org/en/resources/