# Securing Bluetooth-based payment system using honeypot

Kiyana Zolfaghar, Shahriar Mohammadi
*K. N. Toosi University of Technology, Iran*
*kzolfaghar@sina.kntu.ac.ir, s.mohammadi@kntu.ac.ir*

## Abstract

*Wireless technologies provide a new channel for implementation of mobile payments systems. In this regard, the potential of short-range wireless technologies such as Bluetooth is enormous. These systems can be used for proximity payment to vending machines or offering banking service in the bank area. However, unsolved security issues are the biggest barriers to the growth of mobile payment. This paper is focused on the security of banking services which can be offered through Bluetooth technology. We propose a solution using honeypots in bank environment to mitigate the risk of Bluetooth-enabled payment transactions. In this paper, we try to elaborate how honeypot systems can be exploited to reduce the chance of Bluetooth enabled attacks' success by limiting the client device discoverability for attackers.*

## 1. Introduction

With the flourishing of electronic commerce and widespread use of mobile devices, a new type of service is emerging that extends e-business using wireless technology by enabling e-commerce services on mobile systems [1]. Mobile commerce is offering a new application domain for mobile devices and creating new opportunities for mobile users as well as for mobile service providers [2, 3]. Mobile payment is expected to become the killer application in mobile commerce [4]. There are wide ranges of options available to perform mobile payments due to the availability of network technologies. In this paper, we will focus on Bluetooth technology and it application in payment system while offering banking services. However, it is clear that many issues have to be resolved before mass adoption can occur. One of the biggest barriers to the growth of mobile commerce has been a lack of consistency in security of payment methods [5, 6]. Mobile banking must develop a security system that clients trust to provide the same level of confidence as obtained in a face-to-face transaction. This paper concentrates on the topic of secure mobile payments using Bluetooth technology. The main contribution of this paper is proposing a design solution for a Bluetooth-based honeypot system in bank environment to secure banking services offered via this technology.

The remaining part of this paper is organized as follows: in the next section, we make a small introduction on the honeypot concept, Bluetooth technology and provide a review of Bluetooth application in payment systems and banking services. In section 3, we will focus on various vulnerabilities that can impact the security of Bluetooth-enabled systems offering banking services, and then we propose our solution of using honeypots to mitigate these risks in section 4. We present our concluding remarks in section 5.

## 2. Background

This part introduces the reader to three concepts include the concept of a honeypot, the Bluetooth technology, and its application in payment system, which are referred to later in this paper.

### 2.1. Honeypot concept

Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of honeypots which are mainly used to attract attackers to study their behavior and to learn their tactics. For computing, a honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource [7]. By being a vulnerable and well-situated entity, the honeypot appears to have value and be an easy target for attackers. In other word, by standing up honeypot targets, we can distract attackers from more valuable machines on the network. Honeypots are closely monitored and any actions directed towards them are by default suspect [8]. These systems can be classified

based on different aspect such as their purpose, t and level of interaction with the attackers (Table 1).

**Table 1.** Honeypot classification

| Properties | | | |
|---|---|---|---|
| Environment: | Production | Research | |
| Interaction: | Low | Medium | High |
| Purpose: | Deception | Deterrence | Detection |
| Attacker Profile: | Script Kiddie | Professional Blackhat | |

Honeypots are a relatively new technology that is becoming increasingly popular as commercial solution. While recent work [9, 10] identifies Bluetooth payments as a potentially forthcoming area of security issues, we find honeypots to be tools that can help us in *prevention, early detection and Deterrence* of malicious attacks by studying malicious and unauthorized behavior. However, we need to ensure that the honeypots follow desirable characteristics to interact with attackers in Bluetooth network.

## 2.2. Bluetooth technology

Bluetooth is an open standard for short-range digital radio frequency for wireless connection of devices such as Pocket PCs, mobile phones, and desktop computers. Bluetooth makes it possible for these devices to communicate with each other when they are in range. Because the devices use a radio (broadcast) communications system, they do not have to be in line of sight of each other. This technology is enabling users to create Wireless Personal Area Networks and *ad hoc* connections between wide ranges of personal electronic devices such as mobile phones, laptops and so on [11]. The main advantages of Bluetooth technology are its low power, low cost, ease of use, and its ability to give high connection reliability in a crowded area of the spectrum [9]. That is why many researchers will now examine the potential of Bluetooth technology for mobile payments systems and financial transactions.

## 2.3. Bluetooth application in payment systems

Mobile payments represent an opportunity for the mobile industry and for financial service companies. It has been welcomed in most of the countries as a new branch in electronic banking while it has some superiority over e-banking due to its availability, High penetration coefficient and being fully personalized. Financial establishments have also begun implementing mobile banking applications utilizing Bluetooth. According to recent research by the Celent financial advisory firm, 200,000 US households use some form of mobile banking. By 2010, the market is expected to grow to 17 million US households. In Mexico, BBVA Bancomer has deployed more than 13,000 Bluetooth-enabled payment terminals [10]. EUROCARD is another form of Bluetooth based wireless payment has been used in Sweden [12]. Mobile payment provides flexibility and convenience for consumers. However, mobile banking via Bluetooth presents a risk. While no generic profile for mobile banking exists for Bluetooth, application developers must design systems with security in mind and require a protection mechanism for detecting malicious Bluetooth traffic. In this part, we elaborate some application of Bluetooth technology in mobile payment.

**2.3.1. Proximity payments using Bluetooth.** Mobile proximity payments are predicted as the best medium term revenue opportunity. One of the main applications of Bluetooth technology can be defined in proximity payments which involve the use of wireless technologies to pay for goods and services over short distances. Proximity transactions develop the potential of mobile commerce, for example, using a mobile device to pay at a point of sale, vending machine, ticket machine, market, parking, and so forth. Through short range messaging protocols such as Bluetooth, the mobile device can be transformed to a sophisticated terminal that is able to process both micro and macro payments. In proximity [6]

**2.3.2. Banking services using Bluetooth**. Mobile banking is considered one of the most popular m-commerce applications. Banking services are generally divided into the four categories which all of them can be offered through Bluetooth technology. These services includes Notifications and alerts services which are offered to inform the customer of the transactions done or to be done with his account, Information services concerning transactions and the amount of money available in customer's account are sent at certain intervals, Applications services in which an application is sent to the server concerning the account or special transaction and services through which banks can transfer amount of money between customer's accounts or pay an amount to a third party such as paying bills [13]. The main goal of using Bluetooth in m-banking is to offer banking services in bank area through mobile phone without paying for any costs in order to decrease the rush hours and amount of banking operations done by the bank clerks .In this method bank customers can be connected to server

installed inside the bank through Bluetooth technology and to handle their banking affairs through their mobile phones. This server will be capable to offer banking services through Bluetooth technology by which the server can be connected with other devices equipped with Bluetooth lying in 100-meter scope [9]. Offering banking services through Bluetooth can have many advantages:

- Mobile phones are widely used by people all the time and Most of them are equipped with Bluetooth technology (Availability).
- Security of this service is higher than internet, and SMS because of its limited Scope [9].
- Due to low-speed and high-cost of internet for mobile phones in some countries like Iran, using this service is almost fast and does not incur any cost.
- Bluetooth technology makes it possible to offer m-banking services to several people in accordance with the number of servers [11].
- Payment systems using Bluetooth not only decreases visits to interior of the banks but also can decrease some visits to ATMs for handling such affairs as inspection and checking of account balance and alleviate problems of these appliances.[9]

## 3. Security issues in Bluetooth-enabled payment applications

Security and privacy are essential elements for the success of mobile commerce and its applications specifically in payment area. As with any wireless technology, Bluetooth has several inherent security risks because access to any Bluetooth device is potentially open to anyone in the range of the device. Thus Bluetooth security is a huge concern for wireless applications [14]. In this part, we introduce some of the known vulnerabilities toward Bluetooth application and then we propose our solution based on honeypot systems to detect and delay some of these attacks.

### 3.1. Bluetooth-Enabled Attacks

Bluetooth-Enabled Attacks can be classified from different points of view. One of the major weaknesses of any wireless technology like Bluetooth is that its physical medium is based on radio frequency (RF). Because Bluetooth transmissions must travel through the air in the form of RF waves, they are prone to Denial of Service (DoS) attacks. An attacker simply needs to generate enough RF noise in the Bluetooth network frequency to saturate the medium and made impossible the establishment of any communication [15]. In disclosure threats for example, Bluetooth air sniffers make it possible to sniff the raw data being exchanged between two devices. Such attacks could have a serious impact on the security of m-payment schemes. But the most important attacks in Bluetooth networks is *wardriving* which refers to any type of attack that attempts to gather information about a Bluetooth-enabled device in order to proceed with further attacks. Successful wardriving detection allows targets to take countermeasures prior to follow-on attacks [16].There is several different ways to prevent Bluetooth-based devices from being the target of any of the attacks launch via Bluetooth. Fortunately not every Bluetooth device is susceptible for every attack and most of these treats cannot be launched unless the devices are discoverable to attackers. So the best defense against these threats is to limit device discoverability and connectability [17]. In the next section, we present a honeypot system which can be used as a deception to make the discovery process much longer.

## 4. A solution for Security issues in Bluetooth-enabled applications

As we mentioned before, honeypot is a kind of intrusion detection system which is exploited broadly as a resource whose value lies in its unauthorized use. From a conceptual perspective, any traffic going to or coming from the Honeypot is likely a probe, attack or compromise attempt, except the self-generated traffic that simulates the Honeypot clients [7]. This paper focused on building honeypot solutions for Bluetooth network to distract mobile attackers from the Bluetooth-enabled clients.

As it mentioned in previous section, most of the Bluetooth-enabled attacks cannot be launched unless the attacker would be able to discover the target devices in Bluetooth network. An advantage of Bluetooth attacks over typical wireless attacks is the relatively quick time in which an attacker can find and comprise a target. So we should increase the time required for an attacker to find a target device [18]. To achieve this, in this paper we suggest using honeypots in Bluetooth network to use its capability in distracting attackers from the real client connect to bank servers via Bluetooth and trapping them in honeypot systems to delay any potential attacks. Honeypots in this system should be employed randomly in different locations so as not to give an attacker obvious knowledge of the boundaries of system [19]. Figure 2 shows a

Conceptual diagram of how Bluetooth honeypot can operate in bank environment.

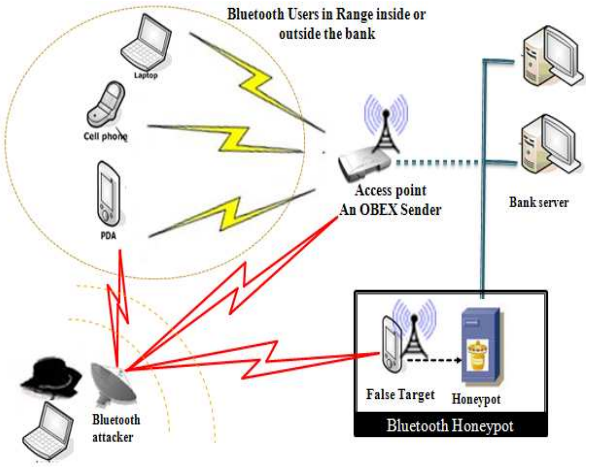


**Figure 1.** Conceptual diagram of Bluetooth honeypot in bank environment

There are different methods of discovering devices in Bluetooth networks which can be exploited by attackers to finds real servers or clients which communicate through Bluetooth. The common method is broadcasting inquiries in which the attacker continually broadcasts inquiry requests until receiving successful acknowledgments from the bank client. Due to presence of Bluetooth honeypots in bank environment, these inquiries receive by honeypots too. Responding this malicious attempt, honeypot acknowledge them immediately to initiate a communication with attackers and distract them from the real bank clients whom use Bluetooth services. Another method which can be used by attackers to find target devices is brute-force detection. In contrast with the former method, brute-force detection is able to detect non-discoverable Bluetooth devices too. In this way, the attacker attempts to predict the unique 48 bit Mac address of the target clients. To mitigate the risk of discovering the target devices, honeypots can flooding the attackers with a range of false targets whose their Mac Address is in the range of physical addresses of real client. By this way, they can increase the possibility of conducting the attacker toward the false targets instead of real clients and delay the attacks. These reconnaissance attacks can also be utilized against banks servers. Neutering them, the Roaming Properties of Honeypot should be used as a mechanism that allows the locations of honeypots to be unpredictable, continuously-changing and disguised within a server pool [20], this mechanism not only confusing the attacker in detect of the active server but also mitigating the effects of DoS attacks against the bank servers. After detecting the presence of attackers in the system, honeypots can analyze the data gathered from the interaction of honeypots with attackers through false application. According to this information and data from previous attack which are existed in the reference database, the system designs an appropriate response to counter the attackers effectively. Figure 2 demonstrates this Organization of a generalized Honeypot system in bank environment.

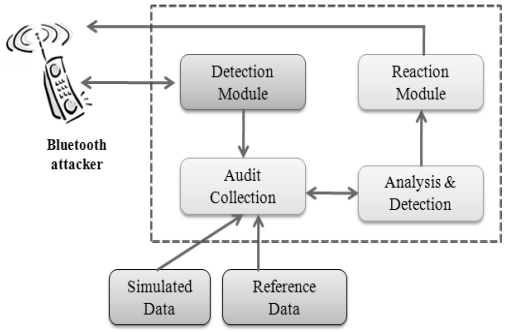


**Figure 2.** Organization of a generalized Honeypot system in Bluetooth environment

### 4.1. A simple Scenario

In this section, we describe a simple scenario which illustrates how honeypots can be can be exploited to reduce the chance of Bluetooth enabled attacks' success by limiting the client device discoverability for attackers (figure 3). In the first step, consider bank customers are connecting to the server installed inside the bank through Bluetooth technology to handle their banking affairs through their mobile phones (1). This server will be capable to offer banking services through Bluetooth technology (2). Now imagine that an intruder wishes to attack the client which is connected to the server to transfer money. Launching the attack, the intruder should be able to discover the target devices at a first step, so continually broadcasts inquiry requests until receiving successful acknowledgments from a bank client(3). Due to presence of Bluetooth honeypots in bank environment, these inquiries receive by honeypots too (4). After collecting the required data from detection module (5), Honeypots then analyze the gathered data and performs the correlation of collected attacking information to predefine attack scenarios in order to detect the attack type(6). Upon finishing the analysis, the system designs an appropriate response to counter the attackers effectively (7).Most of the time, honeypot reaction is initiating direct communication with the attacker to distract him from the real client (8).

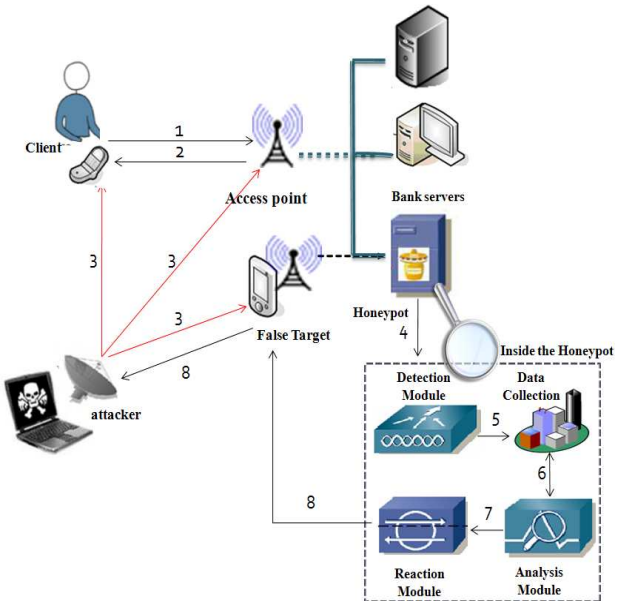


**Figure 3.** A Simple Scenario

## 5. Conclusion

Considering the promising future of mobile payment, this paper investigate Bluetooth network as a short-range wireless technology for mobile payments systems. Due to widespread growth of mobile phones, this system can cover a wide range of users. These Bluetooth-enabled systems can be used for offering banking services such as notification services or transferring money between customer's accounts in the bank area. However, M-Commerce will not prosper without reliable and usable security concepts. Consistently, Bluetooth security is a huge concern for Bluetooth-enabled payment systems. Several attacks exist that successfully target and exploit Bluetooth enabled devices however many of them cannot launched successfully unless the devices are discoverable to attackers. In this paper, a solution is proposed that aims at relieving these security problems using Bluetooth honeypots. Achieving this, the honeypot systems can be deployed in bank environment to distract the attackers from real clients by flooding attackers with a range of false targets. This solution has some advantages. First, by trapping the attacker in honeypots, the time required for an attacker to find a target device will be increased and the system have more time to respond it appropriately. Second, it can monitor the attacker behavior thorough his communication with honeypot and find his attack motivation and the tactics which the attacker uses to compromise the systems. The limitation of this solution is that attacks against clients will not be captured unless the honeypot is threatened also. So if the attacker know the exact Mac address of the client, detecting the attack is too hard.

## 6. References


[1] Pousttchi k. (2007), A modeling approach and reference models for the analysis of mobile payment use cases, Electronic Commerce Research and Applications.

[2] Leung, K.(2001). Improving returns on m-commerce investments. Journal of Business Strategy, 22(5), 12−13.

[3] Turowski, K.; Pousttchi, K.(2003): Mobile Commerce – Grundlagen und Techniken. 1. Ed., Heidelberg.

[4] Hu,X., Li W., Hu Q.(2008), Are Mobile Payment and Banking the Killer Apps for Mobile Commerce?, Proceedings of the 41st Hawaii International Conference on System Sciences.

[5] Lee C., Kou, W., and Hu W.C. (2005), Advances in security and payment methods for mobile commerce, Idea Group Publishing,USA.

[6] Agarwal S., Khapra M., Menezes B. and Uchat N. (2007), Security Issues in Mobile Payment Systems.

[7] Spitzner, L. (2003). Honeypots - tracking hackers. Boston: Pearson Education Inc.

[8] Barfar A. and Mohammadi S. (2007). Honeypots: Intrusion deception, ISSA Journal.

[9] Shahreza,M. and Shahreza M. H. (2007), Mobile Banking Services in the Bank Area, SICE Annual Conference, Japan.

[10] Mexican bank deploys hypercom bluetooth-enabled payment stations. Mobile Enterprise Magazine.Oct 2007.

[11] Chen J.J., Adams C. (2004), Short-range Wireless Technologies with Mobile Payments Systems, ACM..

[13] Gustafsson L. (2004), Eurocard Bluetooth Payments interview, J. Chen, Ed.

[14] K. Pousttchi, and M. Schurig (2004), Assessment of today's mobile banking applications from the view of customer requirements, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 5-8.

[15] Potter B. (2003), "Bluetooth - Security Optional," *Network Security*, no. 5, pp. 4-5.

[16] Suen Yek (2003), Measuring the Effectiveness of Deception in a Wireless Honeypot, 1st Australian Computer, Network & Information Forensics Conference, Australia.

[17]Johnson K., Zuroff M., Whitaker J., Bluetooth Security, By MJK Group

[18] Connor M.T, Reeves D. (2008), Bluetooth Network-Based Misuse Detection, Annual Computer Security Applications Conference.

[19] Siles R. (2007), HoneySpot: The Wireless Honeypot Monitoring Attacker's Activities in Wireless Networks A design and architectural overview, http://www.honeynet.org, Last Modified: December 17, 2007

[20] Khattab S.M. , Mosse D., Melhem R. (2004), Roaming honeypots for mitigating service-level denial-of-service attacks, Distributed Computing Systems.