WIDIPAY: A CROSS-LAYER DESIGN FOR MOBILE PAYMENT SYSTEM OVER LTE DIRECT

Umut Can Çabuk[1], Georgios Kanakis[2], Feriştah Dalkılıç[3]

[1]*Department of Electronics Engineering, Erzincan University, Erzincan, Turkey*
[2]*Johannes Kepler University, Institute of Software Systems Engineering, Linz, Austria*
[3]*Dokuz Eylul University, Department of Computer Engineering, Izmir, Turkey*

Abstract

Long term evolution direct, plus its features of device-to-device networking and proximate discovery, are new and emerging technologies able to come out of the shadow to render a whole new perspective at mobile payments. In this work, we propose a new mobile payment system using long term evolution direct and its features. A sensitive mobile payment system would require high security requirements in order to be trusted by the users and the businesses. These requirements are taken into account in our proposed system design and solutions to security considerations are provided. The system's security and usability features are designed for implementation from physical to application layer to address the identified issues. Within the scope of this work, we provided the conceptual design solutions to allow the system to be as solid and secure as possible while they are convenient enough not to degrade user's experience when using the system.

Keywords: *LTE Direct, Mobile Payment, Internet of Things, Device-To-Device Networking*

----------***----------

1. INTRODUCTION

It has been not long time ago since the spotlight of research switched to a new direction towards device-to-device (D2D) networks and the possibility of providing services over them. A service, well distinguished and sensitive, is wireless and contactless payments [1] including the area of mobile payments. Mobile payment (and also contactless payment) is one of the hottest topics in the last decade. A field where major companies [2] have spent years of research to develop solutions and systems able to provide this type of service to the users. Therefore, we decided to conduct a research on the possibility of designing a system for mobile payments using a new emerging technology called long term evolution direct (LTE Direct) [3].

Our initial objective is to provide the necessary information about technologies and concepts like device to device networks, proximate discovery and LTE Direct. These technologies and concepts are the motive to think of a viable design for a mobile payment system that could be deployed in its initial state to cafés, bars, restaurants, etc. Furthermore, we are taking into consideration the work carried out by major companies [2], which they have already provided implemented solutions.

Our study provides a set of design decisions in different layers for an innovative mobile payment system and security features that are mandatory to build it to be secure. We do not provide an implementation for it since a real implementation would require the cooperation of all involved parties but we believe it will be a useful guide and/or a framework for the commercial implementation. The security features, in our point of view, which lead to the proposed design are the validation of parties, the communication's confidentiality, lost user device, low signal and lost signal case, existence of multiple merchants and denial of service (DoS) attacks. Every one of these issues is addressed and solutions are provided to ensure the system's security. Depending on the issue addressed, solutions are applied to the appropriate layers in order the system to become as secure as possible.

This work has been divided into six main sections. Section 1 is the introduction. The following section 2 gives the necessary background information and technology descriptions needed to understand the proposed system. Section 3 provides the most significant related work that exists in the field of contactless, mobile and wireless payments. Section 4 has the system design in high level and the main use case scenario of the system. Furthermore, in section 5, we provide the detailed security considerations and how these will be addressed by the proposed system. In section 6, we conclude this work by reflecting on our proposed system as well as we present ideas for further future work.

2. BACKGROUND INFORMATION

2.1 Device To Device Networking

Device-to-device communication is given by the notion of devices communicating directly between each other without the need of third party relay devices like access points or routers. The D2D communication can also be for human to human communication eg. two people talking on Skype™ with their mobile phones over WiFi, and/or for machine to machine communication eg. mobile phone and Bluetooth (BT) capable headset over BT. The most popular technologies used in the D2D networks nowadays are the

Bluetooth and the WiFi [4]. The weak security features, these technologies provide, do not allow a trusty payment system to be implemented [5]. Thus, the nowadays' dominant technologies are not suitable for the system we propose.

2.2 Proximate Discovery

Proximate discovery is quite new concept for end users in mobile networks, the ability for a device to passively and continuously search for relevant data or value in one's physical proximity or we can say ambience. Including but not limited to social media, proximate discovery is a platform fundamental in defining the next generation of services across an extensive set of use cases from advertising to Internet of Things (IoT). In a determined but moving area, it will connect people, objects (including even animals), government and business [6].

Here, we explicitly mention direct discovery which is different from some conventional localization technologies, for example the ones based on global positioning system (GPS) etc. The proximate discovery alongside with the above mentioned D2D communication is a core element in the way our proposed system shall operate and work. The way to discover a user's position, is essential to the payment system as we have envisioned it within the LTE Direct technology. LTE Direct proposes a unique built-in beacon based discovery feature using licensed radio spectrum for that beacon communication as well as regular data communication. iBeacon™, a similar discovery protocol [7] however, uses Bluetooth low energy (BLE), which is not the best solution to such a system because of energy efficiency problems, unlicensed spectrum and device specific non-standard coverage ranges. Additionally, in order to save energy, mobile users tend to keep Bluetooth features off when there is no peripheral device (i.e. headset) connected or no file transfer is needed.

2.3 Lte Direct

LTE Direct is a new and innovative device-to-device data communication technology, which was first announced in 2011, standardized in 2013, had trials in 2014 and 2015, and it is planned to be commercially deployed in 2016. It enables discovering thousands of devices and their services in the proximity of ~500m, in a privacy sensitive and battery efficient way [6, 8]. This allows the discovery to be "Always ON" and autonomous, without severely affecting the device battery life unlike other proximity solutions such as over-the-top (OTT) based that use GPS, or BLE and WiFi Direct [3]. It merges the OTT and peer-to-peer (P2P) features of conventional systems. Additionally, it makes use of the licensed LTE radio spectrum which already was assigned to existing mobile operators.

Device discovery is achieved by broadcasting (and listening) of tiny, 54 or 128-bit data packages, called "expressions", which contain device IDs and available services [6, 8]. This process consumes much less energy when compared to conventional methods especially in long term and it can even be done while some high data rate applications are running [6, 8]. In fact, another very comprehensive work was published by Mumtaza et. al. about LTE Direct energy consumption that verifies this claim with several comparisons [9].

3. Related Work

Since 2007, a large number of companies from various industries were interested in the development of the contactless and near field communication (NFC) payments [2]. The long list of names contains companies like Mastercard, Visa from the financial sector, JCB, Nokia, Cellular South from the communication sector, etc. Different approaches were taken by the various companies to implement new payment systems.

Visa developed the PayWay system [2], which is based on a smart card that is issued and verified by visa and the necessary equipment in the merchant side. The same in principle is the contactless system developed by Mastercard, named PayPass [10]. While easy to use and relatively secure, these payment methods are depended on the specific companies that issue the cards. The downside in this approach is the different equipment per card for the merchants while the users need to issue and carry different cards in case they need to switch from one system to the other. This discomfort can be bypassed by our proposed system which uses established technologies and the user is required to have only his mobile phone with him. A commodity that it is commonly used today as a tool for a large number of people around the world [11].

On the other hand, nowadays NFC (as a mobile phone feature) is being seen as a good solution to the contactless/mobile payment systems by parts of the telecoms and payment sector, thus quickly became widespread [2]. Yet we do not agree, since NFC can only have several centimeters of communication range, which allows it just to be contactless but not much more. Hence, it does not provide a true on-the-go style mobile shopping/dining experience and neither provide advanced customer-shop interactions like offers and ads. Last but not least, NFC lacks security protocols for such uses. For example, NFC payment gateway constitutes a potential risk for the users due to its weak encryption which is set by the businesses and the merchants. If they do not pay attention (i.e. use weak keys/passwords) then all transactions could be sniffed, decrypted and even be manipulated by rogue [12, 13]. Another disadvantage of NFC is brand specific hardware dependency. In example, Apple offers its own NFC payment system [14] and so does Samsung [15]. However, both rely on their unique hardware on both sides of the transaction.

Other less involved or better to say less adopted technologies were not taken into account because of the general and large scale adoption that we wish for a future mobile payment system.

4. SYSTEM ARCHITECTURE

The main components of the proposed system are the application for the handheld smart device in the user side and the point of sales (POS) system on the merchant side. The system also involves different parties for the entire process to be completed. Even though, we focus on the use cases between the user and the merchant, we present our assumptions about the system in subsection 4.1 and the involved parties of the system in subsection 4.2. Afterwards, we continue our main focus on the system architecture and design.

4.1 Assumptions

In order to keep such a payment system stable and sustainable, some issues must be addressed before the deployment phase by the parties (introduced in section 4.2). First of all, all parties must establish a collaboration focused on data and authorization sharing [2]. Hence, all parties (especially customers and merchants as individuals) must sign a legally binding contract for privacy and confidentiality purposes. Figure 1 demonstrates the communication between the parties.

Another obvious need is special software/hardware requirements. For the customer side, a smartphone application must be created to make shopping transactions over LTE Direct and provide extra functionalities like storing credit card information. For the merchant side, a special POS device must be developed to process payment operations and transmit push ads/offers.

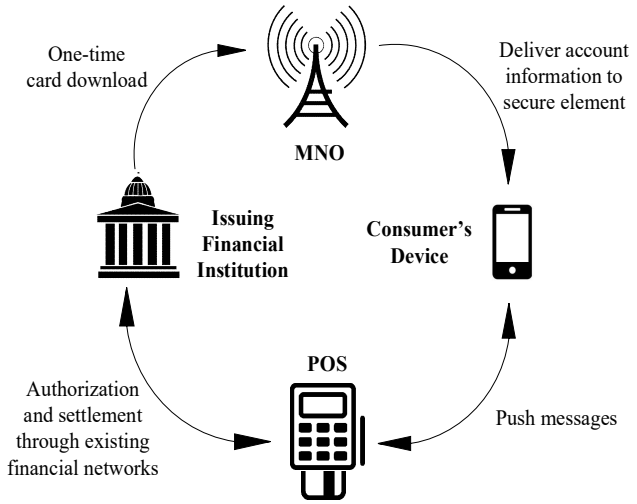

Fig -1: Collaboration scheme of the parties in the ecosystem

4.2 Parties Of The System

There are 4 main parties of the framework: The merchant, the customer, the bank and finally the accompanying mobile operators. All parties presumably have different subsystems, while mobile operators provide a secure communication infrastructure over their licensed radio spectrum.

The merchants are basically the shop owners. They will possess dedicated payment terminals. A payment terminal can be a smartphone (or any device with cellular phone capabilities) that is dedicated to this system or a special POS machine design like the current mobile payment system is also possible.

The customer is the end user, who has an LTE/LTE Direct enabled smartphone or tablet that has the suitable application(s). Interactions between the merchant and the customer will be handled by push notification messages over LTE Direct. Here, suitable applications stand for a proximity detection application and a payment application. These two applications can even be built as one software with the same functionality. Otherwise, these two should be able to share some information and prompts.

The bank is the issuing financial institution and responsible for user credentials, transfer accounts and the payment interactions with collaboration of payment brands [2]. Bank will provide the payment application on application markets (such as Google Play), that will store user's credentials and track payment requests. Fortunately, that application will be similar to the current mobile banking applications of several banks.

Mobile operators will provide secure data communication on LTE radio channel. All digital identities as well as confidentiality, integrity and authorization will be provided by LTE (or 3G, when/where LTE is not available) infrastructure of the operators.

4.3 Use Cases

This work considers cafés, bars and restaurants as merchants in an attempt to limit its scope to a set of similar business requirements, because different retail shops may require different approaches for mobile payment transactions. Focusing in these merchants, three different use cases are defined: Transfer of billing information, receiving special offers/coupons and making the payment. A typical use scenario including the use cases will be explained in this subsection.

The terminal always stands in the visible/discoverable mode (as an assumption), plus user device shall be able to list all places in the proximity, via the application. When a customer gets in the place, or gets in the range of that place's terminal, terminal shall request a unique device identifier (ID) (based on international mobile station equipment identity (IMEI)/international mobile subscriber identity (IMSI)/temporary mobile subscriber identity (TMSI)) from the user device. Right after sending the device ID, user device shall receive a session ticket that consists of five alphanumeric digits. This session ticket will be sent by a push message and stored in both terminal and the user device. User will be able to see it, and will use it as a customer ID. If available, ads, offers and coupons can be delivered to customers again via push messages. When the customer requests the bill from the staff, the cashier will send the total amount of the bill in a push message. After receiving that message, the customer can accept that payment or cancel it.

Once the payment is accepted, there are two ways to proceed with the transaction: First way is the direct transfer of the user's bank credentials to the terminal, using LTE Direct and complete the rest of the transaction the same as the NFC based current implementations [2]. Bank credentials are initially considered as credit card or debit card information, which are saved to the application by the customer. However, other methods like electronic fund transfer (EFT) can be implemented. Second way is an Internet connection over LTE or 3G network and treating the transaction as an online/mobile banking prompt. Implementation is up to the banks, developers and vendors. But one should take into account that, the EFT option may require additional protocols since commerce has legal regulations different than plain fund transfers mainly for taxation. Figure 2 shows the use cases from the point of view of the merchant's terminal.

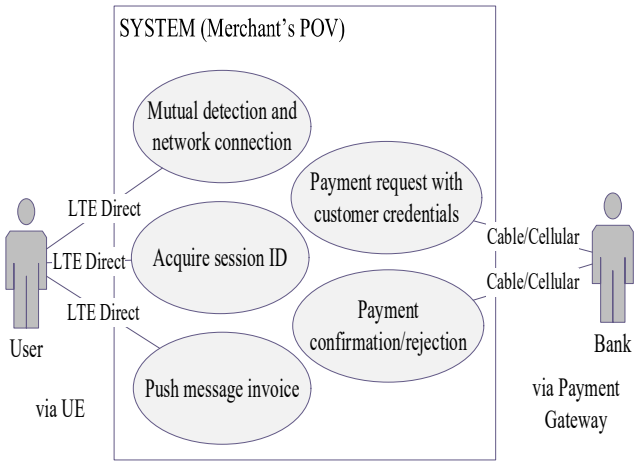

Fig -2: Use case diagram of WiDiPay from a merchant's point of view

4.4 Application Features

The system design requires a POS terminal with LTE Direct capability installed in the merchant's shop. This POS terminal will include an information screen and the LTE Direct terminal. The LTE Direct terminal will be responsible for tracking and establishing communication with the user device in range. It will also be able to create and send the unique session ID to the user's device.

The screen will be able to present a list with all the connected IDs and the ability to drop or renew one's ID. The screen will also be the mean of communication between the merchant's part and the user's device regarding payment notifications and offers messages. The procedure will be as simple as selecting one's ID from the list and, then, it will possible to perform the described actions with the user's device.

During the ordering process, the customer should only provide his unique ID to the waiter or the assistant and the items wishing to order. The assistant or waiter will simply select the customer's ID from the list and will register the order to that ID in order to push the payment notification and the invoice later on.

On the customer side, there will be the mobile application responsible for the communication with the merchant's terminal. The communication will be exclusively established only if the mobile application is up and running. The application will initially receive the unique ID generated by the terminal and that ID will be presented to the user when the user selects the merchant's terminal.

Later, this ID will be used by the customer to place the order, request to pay for the order and receive the invoice or other possible notifications from the merchant terminal. Also, the application will have a list of all connected (in range) merchant terminals by signal strength order. This will provide the user with the flexibility to select the appropriate terminal easier regarding to its location.

5. SECURITY CONSIDERATIONS

5.1 Validation of The Parties

In order to increase the security and trust level within the system, we have to ensure that all users are real people and all devices are legal registered products - no clone or modified device should be allowed - a 4G/LTE (or 3G if not available, because LTE security functions are backward compatible with universal mobile telecommunications system (UMTS) security functions [16]) network connection with a valid universal integrated circuit card (UICC, formerly called as the SIM card) is required. By this way, all users of the system will be authenticated by the network operators and personal information about the user will be available but not visibly disclosed to merchants or third party companies and applications.

5.2 Communication Confidentiality

Since sensitive information [2] will be transmitted between devices, to prevent eavesdropping (i.e. packet sniffing) and data manipulation (i.e. man in the middle attack), system shall provide encryption to all data communication, by using the power of 4G security within LTE Direct. LTE Direct uses IPsec in both core network and the serving network as well as advanced encryption standard (AES) based encryption standards [1, 17]. This is also one of the main reasons why LTE is chosen from a set of different radio technologies (another two are performance and energy efficiency). The use of password every time a device needs to connect to a merchant's terminal is not convenient and user-friendly, therefore an auto generated key system is required. There are two main approaches in the context of key acquisition for data encryption: the pre shared key (PSK) and the public key infrastructure (PKI).

In the case of PKI, to exchange the auto-generated encryption keys between devices, a special key exchange method like Diffie-Hellman-Merkle (DHM) [18] or Rivest-Shamir-Adleman (RSA) [19] should be implemented. Since communication is totally direct, this choice will provide performance advantages, but to avoid man-in-the-middle attacks, additional protections may be required.

On the other hand, a PSK method can be deployed, based on the cellular network data connection as a one-time secure channel to exchange auto-generated keys between the devices. Later, the communication will again be directly between WiDiPay devices. Here, the phone number validated IP addresses can be used to verify parties. The use of the UICC that contains IMSI and TMSI to generate keys, will ensure the end-to-end security and the confidentiality between the communicating parties. The mentioned approach is described in the specification designed by the 3GPP consortium and analyzed by Forsberg in [16]. The downside of this approach is the possibility of causing performance degradation due to the external connection.

However, we tend not to choose any of these options because this decision should be taken after the completion of 3GPP standardization for LTE Direct. Furthermore, future work may reveal more efficient and powerful methods to exchange keys over the network.

5.3 User Authorization

The potential issue of the user losing his/her device or any kind of unauthorized access to the user's device could be easily addressed by implementing an optional user defined short (i.e. four digits) PIN lock protection on the application. The application will require the PIN before an upcoming payment request is shown on the screen in a pop-up window, if that option is enabled. Other procedure will be the same as a regular credit card loss or similar situations. User has to contact the bank to secure his/her account, additionally it would require to contact his mobile service provider to deactivate his UICC.

5.4 Low Signal during Discovery

If parties have long distance in between, particularly when the customer device is at the border of coverage range of the shop's terminal; in order to prevent starting multiple sessions for the same device in indistinctive and unstable discovery situations, merchant's terminal shall wait for 5 seconds to produce a delay before sending session ticket. The same strategy will be applied to cases where the signal is lost while the connection is already established by the communicating parties.

5.5 Temporary Signal Loss While Connected

Session ticket for each user device will be stored both in merchant's terminal and in user device for a (predetermined) time period of 6 hours. The specified time frame is based on customer's behaviour in cafes and restaurants [20, 21]; after the 6 hours time frame, if the user is still in the proximity (i.e. sits in the café) the session ticket (a.k.a user code) will be renewed and it will be send to the user's device by the terminal. On the terminal side any unpaid billing information will be transferred to the new session ticket, but the merchant also has the option, on his POS device, to request the payment to be completed by the customer before ticket renewal. Within the 6 hour period, any connectivity loss will not be a problem since all ticket data are stored in both ends, user's device and the POS terminal.

5.6 Existence Of Multiple Merchants

The application on the user's device must be able to list all places in the proximity according to their received signal strength indicator (RSSI) value and the user will be able to see them all (a limit may be applied i.e 50 to reduce the memory requirements). Thus, this kind of situations would not be a problem. Facebook and Foursquare use a successful way to achieve a similar goal but they use a centralized database based approach with a place database and GPS (or cellular) connection to estimate the distance. Our proposal is a direct D2D proximity solution which will be much more effective in terms of energy efficiency and reflection speed.

5.7 Dos Attacks

While no solution can be exclusively applied to situations where DoS attacks are taking place [2, 22, 23]; we can still set an upper limit to the possible simultaneous connections a terminal can have to prevent the case where service is not available. The upper limit could be decided while taking the usual customer rate of each merchant and giving a logical margin greater than the observed rate. This strategy will potentially provide discomfort to the merchant, but we believe it is necessary until we investigate and determine a viable solution to the intended DoS attacks. Besides, WiDiPay utilizes the licensed radio spectrum which is less prone to physical attacks than the unlicensed industrial, scientific, and medical (ISM) bands because of its regulated nature and lesser device diversity.

5.8 Non-Repudiation

Non-repudiation is the case that a customer ignores or refuses the incoming payment request sent by the shop and intentionally leaves the WiDiPay coverage area of the shop without paying the bill. This case is legally equivalent to the regular shopping/dining scenario where conventional order and payment methods are used. Nevertheless, WiDiPay allows the merchant to identify the abusive customer by customer's LTE provider. Hence, the merchant may transfer customer's information (including personal ID and TMSI) to the local police. Moreover, in countries where legislation allows, the debt can be forwarded to that customer's LTE provider to be billed in the upcoming monthly subscription bill, like value added services offered by many providers. Another forward destination can be tax or (liability execution) authorities if there is such legal procedure in the home country.

6. CONCLUSION AND FUTURE WORK

In this work, we explain the notions of D2D communication, the proximate discovery and the LTE Direct. Afterwards, we present a design for a future payment system using the new and emerging LTE Direct technology. The system's assumptions are described before we proceed in the description of the involved parties of the system. Later, we provide a use case from a merchant's perspective.

Furthermore, we explain the scenario in which the system can be utilized within the context of a cafe, a bar or a restaurant. Finally, we describe the potential security risks for a sensitive mobile payment system as the WiDiPay is. The risks are expanding in very different context. Thus, each described security risk is addressed with solutions being applied at different layers of the system. Meanwhile, we were considering usability of the system when we provided a possible solution to each risk.

Since the LTE Direct is a fairly new technology, not much research has been contacted and only few resources are still available, further research is possible on both the context of the WiDiPay and in the LTE Direct D2D communication as well. For the WiDiPay expansion to other type of businesses, the possibility of adding quick response (QR) codes, radio-frequency identification (RFID) and NFC smart tags can be investigated and their interaction with a LTE Direct based WiDiPay system can be observed. Furthermore, the system uses air as its medium which it will always be open to malicious activities. Hence, new public key methodologies can be implemented that will not degrade the system's performance. As far as the D2D communication is concerned, better avoidance techniques and mechanisms can be developed in order to protect it against DoS attacks. Even though, it is known that complete protection is not possible from DoS attacks, we expect further progress to occur in this sensitive area of D2D communication.

Finally, we believe that international organizations, standardization bodies and companies will soon promote the use of the LTE Direct technology and prepare standards concerning it, which will create a big opportunity for others to be involved in this research area. This will reveal new options for possible improvements to our work that presents a pioneer contacless/D2D payment methodology.

ACKNOWLEDGEMENT

We want to thank Dr. Rune H. Jacobsen from Aarhus University, Department of Engineering, for providing us the opportunity to study this topic by arranging a state-of-the-art level master's course "Security in 4G/LTE Cellular Networks" in Spring 2014.

REFERENCES

[1]. S. Kungpisdan. "Modelling, Design, and Analysis of Secure Mobile Payment Systems", PhD thesis, Monash University, Melbourne, 31 Oct. 2005.

[2]. Smart Card Alliance. "Proximity mobile payments: Leveraging NFC and the contactless financial payments infrastructure", Smart Card Alliance, Princeton Junction, NJ, Technical Report, CPC-07002, September 2007.

[3]. Deutche Telecom, Qualcomm, Samsung etc. "LTE Direct Workshop White Paper", Qualcomm, https://www.qualcomm.com/media/documents/files/lte-direct-whitepaper.pdf, May 2013.

[4]. L. Lei, Z. Zhong, C. Lin, and X. S. Shen. (2012). "Operator controlled device-to-device communications in LTE-advanced networks", IEEE Trans. Wireless Commun., 19(3):96–104.

[5]. M. J. Callaghan, J. Harkin and T. M. McGinnity. (2006). "Case study on the Bluetooth vulnerabilities in mobile devices", IJCSNS International Journal of Computer Science and Network Security, 6(4):125-129.

[6]. LTE Direct Overview: The Case for Device-to-Device Proximate Discovery, White Paper, Qualcomm Research, 2013.

[7]. E. Bouchet. "iBeacon & location-based marketing", Whitepaper, Paris, May 2014.

[8]. Qualcomm. "LTE Direct Always-on Device-to- Device Proximal Discovery", Qualcomm Technologies, San Diego USA, August 2014.

[9]. S. Mumtaza, H. Lundqvistb, K. M. Huqa, J. Rodrigueza, and A. Radwana. (2014). "Smart Direct-LTE communication: An energy saving perspective, Ad Hoc", Networks, 13(B):296–311.

[10]. VeriFone. "A Cashless Future on the Horizon", Whitepaper, http://www.verifone.com/media/1420610/VeriFone_Cashless_Future_Contactless.pdf Sep 2010.

[11]. R. Thomas and H. Deacon. "4G Gathers Momentum as Smartphones Smash One Billion Units in 2013", Internet:www.ccsinsight.com/press/company-news/1724-4g-gathers-momentum-as-smartphones-smash-one-billion-units-in-2013, 2013 [Feb 02, 2016].

[12]. nearfieldcommunication.org. "Security Concerns with NFC", Internet:www.nearfieldcommunication.org/nfc-security.html, [Feb 02, 2016].

[13]. E. Haselsteiner and K. Breitfuß. "Security in near field communication (NFC)", in Proc. Workshop on RFID security, 6 Jul. 2006, pp. 12-14.

[14]. Apple Inc. "iOS Security: iOS 9.0 or later", White Paper, https://www.apple.com/business/docs/iOS_Security_Guide.pdf Sep 2015.

[15]. Canadian Bankers Association. "Payments Security", Whitepaper, http://www.cba.ca/contents/files/submissions/misc-2015-paymentssecurity-whitepaper-en.pdf Jul 2015.

[16]. D. Forsberg, G. Horn, W. Moeller, and V. Niemi. "LTE Security", 2nd Edition, New York: John Wiley & Sons, 2012.

[17]. IP Encapsulating Security Payload (ESP), IETF RFC-4303, December 2005.

[18]. W. Diffie and M. E. Hellman. (1976). "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654.

[19]. R. L Rivest, A. Shamir, and L. Adleman. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communication of the ACM, 21(2):120-126.

[20]. K. Fisher and J. Robinson. "Daily Routines in 22 Countries: Diary Evidence of Average Daily Time Spent in Thirty Activities", Tech. Paper, Centre for Time Use Research, Oxford University, 5 Feb. 2010.

[21].K. Hamrick, M. Andrews, J. Guthrie, D. Hopkins, and K. McClelland. "How Much Time Do Americans Spend on Food?", US Dept. of Agriculture, Economic Research Service, Economic Information Bulletin Number 86, Nov. 2011.
[22].M. Choi, R. J. Robles, C. Hong, and T. Kim. (2008). "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, 3(3):77-86.
[23].R. P. Jover. "Security attacks against the availability of LTE mobility networks: Overview and research directions", in Proc. Wireless Personal Multimedia Communications (WPMC), 16th International Symposium on, Atlantic City, NJ, pp. 1-9, 2013.

BIOGRAPHIES

Umut Can Çabuk received his B.Sc. degree from Uludag University, Turkey, in 2012 and M.Sc. degree from Aarhus University, Denmark, in 2015. He is currently a project assistant in Dokuz Eylul University Dept. of Computer Engineering. His research interests include mobile and wireless networks, internet of things and security.

Georgios Kanakis received his bachelor's degree from Technological Educational Institute of Athens in 2011. He received his Master's Degree from Aarhus University, Denmark, in 2015. Currently, He is a Ph.D. student at Johannes Kepler University in Linz, Austria. His research interests are cloud computing, networks, software modelling and code generation.

Feriştah Dalkılıç received her bachelor's, M.Sc., and Ph.D. degrees in computer engineering from Dokuz Eylül University, Izmir, Turkey in 2006, 2009, and 2015, respectively. Since 2009 she has been a Research Assistant with the Department of Computer Engineering, Dokuz Eylül University. Her research interests include data mining, genetic algorithms, naturel language processing, and intelligent transportation systems.