Eavesdropping one-time tokens over magnetic secure transmission in Samsung Pay

Daeseon Choi
Department of Medical Information, Kongju National University, Chungnam, Korea
Younho Lee
ITM Programme, Department of Industrial and Systems Engineering, SeoulTech, Seoul, Korea

Abstract

We have discovered a security vulnerability in the Samsung Pay app. The magnetic secure transmission in Samsung Pay emits too many magnetic signals that are excessively strong. Thus, we built a low-cost receiver to eavesdrop on the emitted magnetic signals. Using this receiver, we successfully eavesdropped the one-time token for a payment made on the Samsung Pay app around 0.6m $\sim$ 2.0m from where the payment was taking place, depending on the orientation of the magnetic field emitting antenna in the victim device. We verified that the collected one-time token could be used away from the victim device if the collected payment information was quickly transmitted over the Internet.

1 Introduction

The Samsung electronics company (SEC) released a new mobile payment platform, called 'Samsung Pay,' in August 2015 [1, 2]. Unlike competitors such as Apple Pay [3], Samsung Pay works with traditional point-of-sale (POS) devices that allow the use of magnetic card swipes [3]. Because of such backward compatibility, it is estimated that more than 95% of US retailers support Samsung Pay [3], compared with just 5% for Apple Pay [4]. The key technology that gives Samsung Pay such a superior position is called Magnetic Secure Transmission (MST) [5]. Under this technology, devices using the Samsung Pay app can generate a magnetic signal that contains the same payment information as that generated by swiping a magnetic card in the POS card reader. Thus, the POS device can recognize the Samsung Pay signal if the mobile device is sufficiently close, even though nothing is swiped on the card reader.

In this paper, we claim that the Samsung Pay service has a serious security vulnerability because of its implementation of the MST technology. There are two key findings:

- *The magnetic signal emitted during MST is too strong and is emitted too many times*: we can collect the magnetic signal containing the encoded one-time token information using a simple, low-cost receiver (less than US$200) at more than 2.0 m away from the victim device running the MST, if the receiver directly faces on the back part of the mobile phone or the screen of it. The distance goes down to 60cm if the receiver's face is perpendicular to the screen's direction. We can obtain the one-time token very quickly after decoding the signal with a laptop of moderate computing power. This result is against the claim of Looppay that the tranmission range is very short, 1 to 4 inches [6].
- *The collected token can be used away from the victim device*: a payment process can be successfully completed with a device using the sniffed one-time token information, even when the victim device that generated this one-time token is far away. We have found that the payment process using the eavesdropped one-time token should be executed within 60s of the victim device first emitting the magnetic signal for payment.

By exploiting the above vulnerabilities, we have successfully implemented a wormhole payment attack over Samsung Pay. After collecting a one-time token from a victim device and sending the decoded payment information to an attacker device away from the victim, we successfully paid money with the attacker device by emitting the magnetic signal with the encoded one-time token to a conventional POS device.

We provide a brief description of the payment protocol in Samsung Pay, including MST and the security features, in Section 2. The observed vulnerability of Samsung Pay and the proposed attack method are given in Section 3. The experiment to demostrate the feasibility of the proposed attack is given in Section 4. We introduce the related work at Section 5, which is followed by

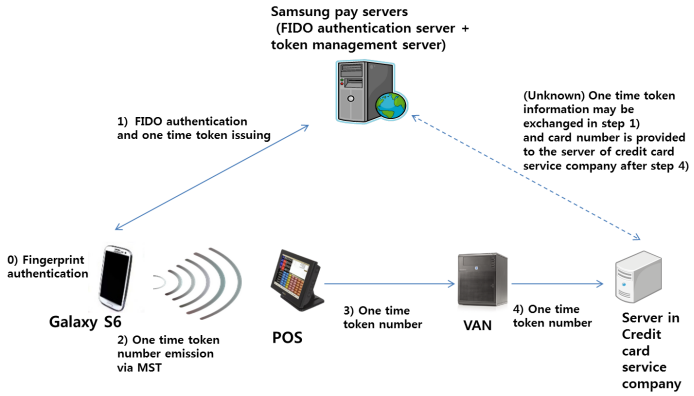

Figure 1: Overview of the payment protocol in Samsung Pay.

the conclusion in Section 6.

2 Samsung Pay

The Samsung Pay service was launched in the US on September 28, 2015. According to [7], the two major credit card companies (MasterCard and Visa) support Samsung Pay, as do most major wireless network service companies in the US, such as Sprint, AT&T, Verizon, and US Cellular. Additionally, major banks such as American Express, Bank of America, and Citibank provide payment services that work alongside Samsung Pay. According to [8], more than one million people have paid for items with Samsung Pay, with around 0.1 million using the app every day. On average, US$1.8 million per day is spent using Samsung Pay. According to [18], SEC announced that Samsung Pay has more than 5 million registered users in South Korea and the United States and it has processed over $500 million dollars in the first six months since its release.

2.1 Payment Protocol in Samsung Pay

Fig. 1 shows an overview of the payment protocol. The credit card registration step is performed in advance, before the payment begins. We do not describe the registration procedure, because its details are not known precisely and it is not relevant to the vulnerabilities we have found. According to [9], the registration procedure utilizes the standard EMV protocol [10]. Note that the payment procedure depicted in Fig. 1 is an estimate based on our experiments. In Fig. 1, the user is authenticated on their device in Step 0), using either a fingerprint or PIN. The FIDO authentication is then performed in step 1). After a data exchange between the server (maintained by the Samsung Pay system) and the user device to ascertain the user's credentials, the user's device obtains a one-time token for the current transaction. During step 1), it is estimated that the one-time token information that verifies the validity of the current payment transaction is sent from a Samsung Pay server to one controlled by the credit card company (see the unknown part in Fig. 1). We verified that the one-time token could not be used once a certain period of time had elapsed after step 1). From this, we could deduce that step 1) and the unknown step are executed simultaneously. Using MST, the user can then make a payment at a POS machine as if swiping a credit card through the machine's card reader. The payment information goes through a Value Added Network (VAN) to the credit card company's server. After some verification, such as checking the amount of time since the token was issued, the company either accepts or rejects the payment transaction. The result is returned to the POS machine through VAN.

2.2 Security Features in Samsung Pay

According to [9, 10, 11, 12], Samsung Pay uses many security features, such as tokenization, a hardware platform, and FIDO authentication. We now briefly introduce these features. Tokenization refers to the generation of a one-time token per transaction. The token contains a one-time card number. Thus, at every transaction, both the user's device and the credit card company's payment server share a freshly generated one-time token. Because this token does not contain any information about the original credit card and has a short lifetime, strong security is guaranteed [10]. Samsung Pay supports EMV standard-compatible [10] tokenization technology. According to [9], Samsung cooperates with VISA, MasterCard, and AMEX in using the tokenization specification [10]. Another security feature is the hardware security platform. Samsung Pay stores security-sensitive information in a secured zone (the so-called Trusted Zone, or TZ). This area is managed by a secure OS called KNOX. KNOX allocates dedicated computational resources for

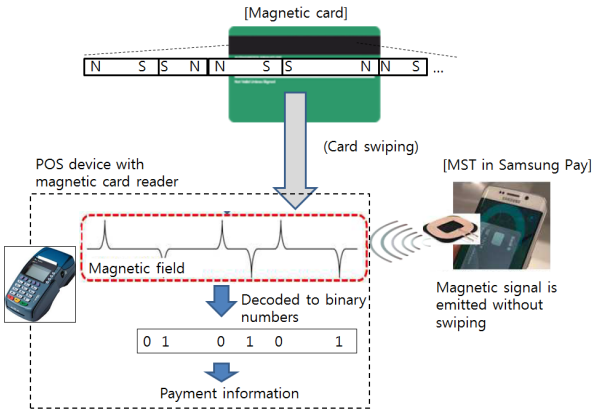

Figure 2: Overview of MST.

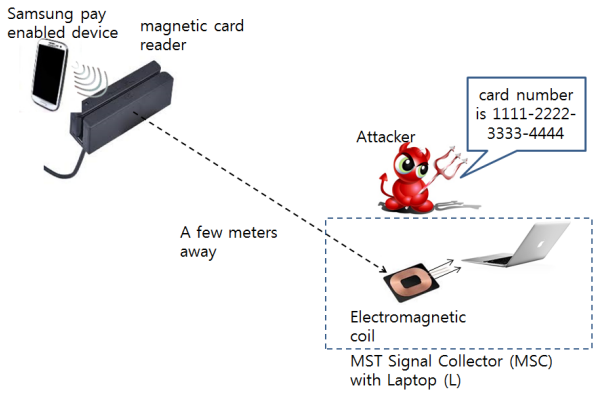

Figure 3: Vulnerability in Samsung Pay: magnetic signal in MST is too strong and its transmission direction is too wide

security operations, and does not allow access to conventional applications. The third feature is authentication. Samsung Pay utilizes the FIDO specification [11], which enables fingerprint-based authentication to be used in an online manner. Additionally, a conventional PIN can be used [11]. The one-time token is only generated after successful authentication.

2.3 MST

Fig. 2 compares the payment information transmission using a conventional magnetic card with that of Samsung Pay using MST [9]. When a user swipes their card in a card reader, a magnetic signal is generated. The card reader records and decodes this magnetic signal to obtain the payment information. In Samsung Pay, MST generates the same type of magnetic signal, which can then be decoded as a valid one-time token by the POS device. Because the sensor that detects the change in magnetic signal is in the slot where the card is swiped, the strength of the signal transmitted by MST must be above a certain threshold.

3 Observed Vulnerability and Proposed Attack

This section describes a vulnerability that occurs under the Samsung Pay protocol, and constructs an attack scenario that was realized by our implementation. We also provide the implementation details, and present the results of two real-attack experiments.

3.1 Vulnerability and Wormhole Payment Attack

We observed that a Samsung Galaxy S6 device emits the magnetic signal too strongly and too often while performing MST in the Samsung Pay protocol. Thus, we are able to build a laptop-connected magnetic signal collector (**MSC**) that can record the magnetic signals in MST by the victim's Samsung Pay device from 0.6m $\sim$ 2.0 m away. We also have found that a software decoder can be implemented for the received magnetic signals, and can be used to obtain the one-time token information. This is illustrated in Fig. 3. We refered to [13] to build MSC. Using the networking facility of the laptop, we can send the one-time token information to another device, called the Remote Malicious Payment Device (**RMPD**), which can be suitably distant from the victim device. After receiving the one-time token, the RMPD can make a payment using this one-time token by emitting the equivalent magnetic signal to a conventional POS machine with a swipe-based credit card reader. We call this a 'wormhole payment' attack; the procedure is illustrated in Fig. 4.

Because MST is normally used in a step for making a payment, the attacker can collect one-time token when the victim user is on making a payment. Thus, the eavesdropped one-time token should be spent earlier than the victim user completes the payment procedure. Otherwise, the attacker cannot use the collected token because it already becomes obsolete. However, unfortunately, our observation is that users waste non-trivially much time while running MST on their devices in order to wait for providing the payment information to a POS device or making a hand-written signature on an electronic pad, as a step for the payment. Thus, attackers have enough time to make a payment with the collected token.

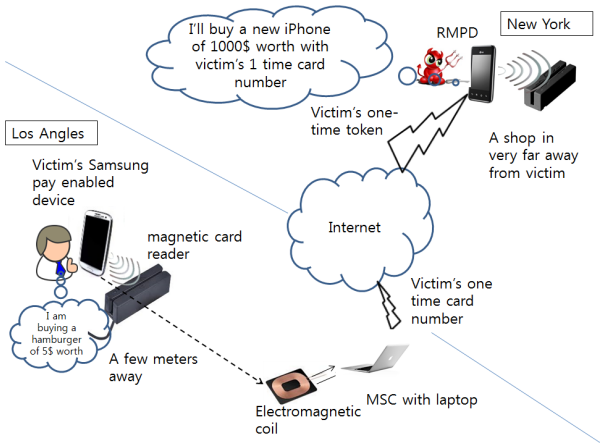

Figure 4: Wormhole payment attack against Samsung Pay

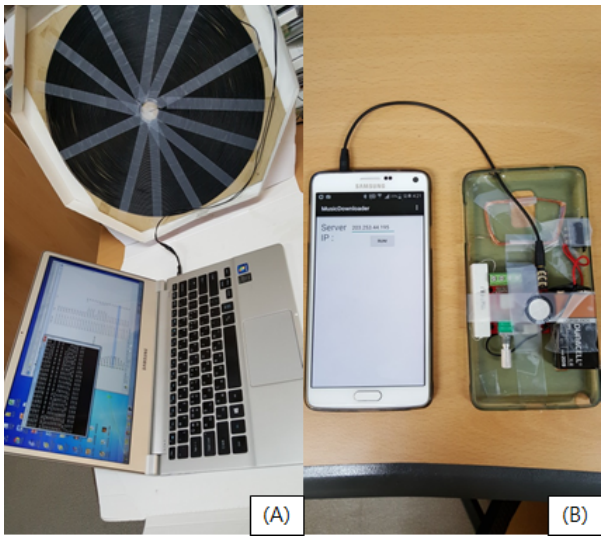

Figure 5: Devices used in our experiment: (A) MSC and laptop (Samsung NT900X3K-K716C). (B) RMPD.

3.2 Implementation of the Attack

Fig. 5 shows the devices used in our actual implementation. Their roles are described in the figure caption. For the experiment shown in Fig. 9, a mobile POS device was used in the step (C) in Fig. 9 to verify that the RMPD works well with the sniffed one-time token.

In the upper part of (A) in Fig. 5, there is the MSC we made. It is made with a long insulated wire. We wound the wire several tens of times to have the MSC make the same effect as a magnetic coil when it collects magnetic signal. The MSC is connected into laptop's microphone jack. It converts captured magnetic signal into sound signal. Actually it works as a microphone. The laptop runs a software that decodes the sound signal and extracts one time payment information, we developed a software that sends the payment informtion to RMPD. The (B) in Fig. 5 shows the proposed RMPD. It consists of an android smartphone, an amplifier that is powered by a DC battery and a loop of copper wire that produces the electro magentic signal. The smartphone runs a software that receives the one time payment information sent by the laptop in (A) through the Internet. The smartphone encodes the payment information into sound signal of 0.5-second length. Then the smartphone plays the sound through the headphone jack to the amplifier that is connected to the loop of copper wire. Finally the loop of copper wire emits magnetic signal.

Fig. 6 shows the details of the proposed wormhole attack procedure. The detailed encoding/decoding and modulation/demodulation methods are described in the figure. In the final step, we used an amplifier in RMPD to make the signal stronger, increasing the success probability of the attack.

4 Experiments

To verify the validity of the proposed attack methods, we conducted two experiments. The first is in-the-lab experiment for measuring the success rate of sniffing one-time token. The second is a real-attack experiment to verify the existence of vulnerability and show that the proposed attack is feasible.

In the first experiment, we measured the success rates of eavesdroppings in various distances and angles between MSC and victim's smartphone. Fig. 7 explains the four experiment settings.

In the experiment, a player who is of a victim role held smartphone and ran a samsung pay transaction. The smartphone emitted magnetic signal to the back cover direction. The MSC was located following one of the settings in Fig. 7. The Samsung Pay device emitted magnetic signal 13 times for a single transaction. We measured how many times among the total 13 magnetic pulse tranmission the MSC could successfuly eavesdrop the magnetic signal. If the collected-then-decoded one-time token's LRC (Longitudinal Redundancy Check) was correct, the eavesdropping was considered as a success. We measured the success rates on various distances from 0.4m to 2.2m.

Fig. 8 shows the results of this experiment. Except the 90 degree case, the eavedroppings were successful with higher than 80% probability in any settings. In the case of 'Front' and 'Back', the attacker was successful with greater than 70% probability even he/she was 1.6m away from the victim device. Also, we would like to emphasize that a low success rate does not means that the

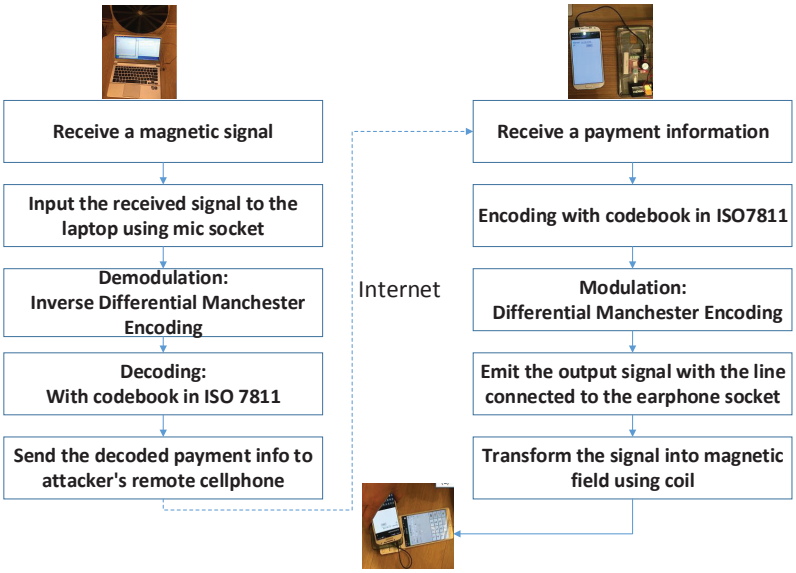

Figure 6: Details of the proposed wormhole attack

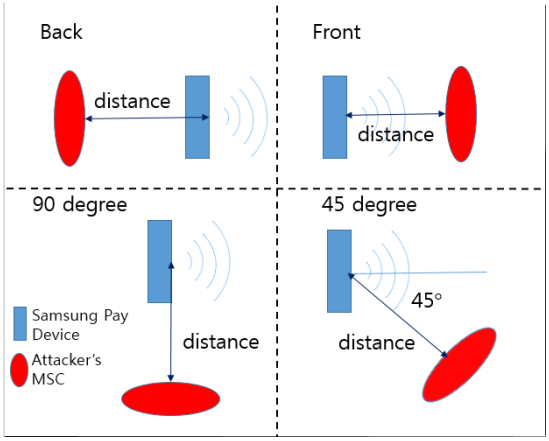

Figure 7: Experiment settings

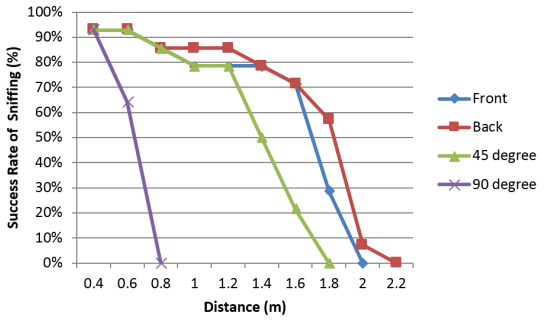

Figure 8: Success rates of sniffing in various distances and angles between MSC and victim's smartphone

attack is difficult to succeed: only one success in sniffing one-time token from total 13 transmitted signal per a transaction is enough to make the proposed attack successful.

In the second experiment, we excuted an real payment that shows feasibility of the proposed attack in a real environment. In this experiment, an eavedropper who has MSC and a laptop in her shoulder bag sniffed a victim's one-time token at a restaurant then sent the sniffed one-time token to her experiment colleage who has RMPD in a different place. The bottom side of Fig. 9 shows the photos capturing the moment when the attack is being executed. In (A) of Fig. 9, the locations of MSC and RMPD are indicated on a map, respectively. In the experiment, the worm-hole attack was successful: the experiment colleage could buy some cookie with the victim's payment information. This means that *there is no validation procedure for consistency between the position of one-time token issurance and that of where the payment with the token is taking place in the Samsung Pay system*.

We need to mention that, after the one-time token signal was emitted, the victim and the checkout staff spent a few seconds in talking about price and payment options before the staff pressed enter key in the POS device to send the price information and one-time token to the credit card company server. While they were talking with each other, the attack colleage could complete her payment using the evaesdropped one-time token before victim's payment transaction was sent to the credit card company server. In the case where the attackers use

their own POS device, they can complete a payment as soon as they receive the sniffed one-time token from the evaesdropper, thus less amount of time is needed so the attack success probability may increase.

Figure 9: Execution of the real attack with a conventional POS device: (A) A map shows the location of a victim and attack payer (B) An eavesdropper runs the MSC and sniffs the samsung pay one-time token. (C) An attack Payer performs a payment with RMPD at a conventional POS machine in a coffee-shop.

5 Related Work

In this section, we introduce some previous works that are related to ours. In [15], the authors consider employing short-range wireless technologies for mobile payment systems, such as Bluetooth, RFID, and Nearfield Communication (NFC). The authors compare and analyze them in terms of communication range, cost, frequency range, and the organizations which considers employing the technology. Also, they show the problems of the technologies on various aspects such as conflict of interests, interoperability, security and reliability, and availability. Unfortunately, they do not consider magnetic signal as a communication medium for a mobile payment system. [16] discusses the security vulnerabilities on NFC-enabled mobile phones and suggests attack methods based on them. It deals with the vulnerabilities on the software that processes the data of NFC Data Exchange Format (NDEF). It also shows the attacks leveraging them such as an URI spoofing based on the data from the tag and the worms that can propagate through NFC. Unfortunately, it also does not consider the vulnerabilities on the mobile payment system with magnetic signal. [17] is the most recent work to the best of the authors knowledge. It classifies the mobile payment systems into five types: mobile payment at the POS (Point of Sale), mobile payment as the POS, mobile payment platform, independent mobile system, and direct carrier billing. Then, it introduces the security components that are employed for the mobile payment systems, such as password-based authentication, multi-factor authentication, SSL/TLS, and Secure elements. It also shows the possible threats against the mobile payment systems, such as malware, SSL/TLS vulnerabilities, and data leakage, and possible solutions for remediation. It does not mention the eavesdropping issues on the mobile payment at the POS, which belongs to the method in Samsung Pay. We think [13] is the most relevant work. This work addresses the security vulnerabilities on magnetic credit cards, such as untrusted magnetic card readers and skimming devices. To resolve them, the authors suggest a similar type of a device that Samsung Pay-enabled phone has: a device that obtains a credit card number of electronic signal from the connected smartphone and emits it as magnetic signal to a magnetic card reader. It also suggests one-time credit card number. This number is issued by the credit card issuer to a users smartphone for each transaction and the user uses the received one-time number with the help of the proposed device for payment. It deals with the sniffing issue that we are tackling now. However, it only considers the case where the collected card number is used again later by the malicious entity, after the current transaction has been completed. However, it does not consider the case where the collected card number is used for payment before the user completes the current payment as our work.

6 Conclusion

In this paper, we have reported a security vulnerability in Samsung Pay, which is a widely-used mobile payment service. We also demonstrated the feasibility of a wormhole attack, in which a payment is made at some distance from the victim Samsung Pay device after eavesdropping the MST signal. For public interest, we believe our result should be made known to the millions of Samsung Pay users across the world [14].

7 Acknowledgments

We thank you for anonymous reviewers and the program committe members who give us very helpful review comments to improve our paper. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (2016R1A4A1011761). Younho Lee is the corresponding author of this paper.

References

[1] Official Samsung Pay website. Available at http://www.samsung.com/us/samsung-pay/ [Visited at 2015].

[2] Saumsung Mobile Press, "Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay", Aug., 2015. Available at:http://www.samsungmobilepress.com/2015/08/13/Samsung-Announces-Launch-Dates-for-Groundbreaking-Mobile-Payment-Service:-Samsung-Pay

[3] Fortune, "Heres why Samsung Pay is way better than Apple Pay and Android Pay", http://fortune.com/2015/09/30/samsung-pay-review/, Sep., 2015.

[4] John Gessau, ''Samsungs LoopPay Deal Leaves Some Technology Loopholes", Payments Source, Feb. 2015. Available at: http://www.paymentssource.com/news/paythink/samsung-looppay-deal-leaves-some-technology-loopholes-3020667-1.html

[5] G. Wallner, System and Method for A baseband nearfield magnetic stripe data transmitter, US Patent No: US 8628021 B1, Jan., 2014.

[6] Looppay, "Frequently Asked Questions - Security - Is the LoopPay device safe when transmitting? Can LoopPay provide added dynamic security?", Available at:https://www.looppay.com/faqs

[7] Malarie Gokey, "Samsung's Cheaper mobile devices will support Samsung Pay in The near future", Digital Trends, Nov., 2015. Available at:http://www.digitaltrends.com/mobile/samsung-pay-news/

[8] Nirave Gondhia, "Samsung Pay crosses 1 million users", Android Authority, Oct., 2015. Available at:http://www.androidauthority.com/samsung-pay-crosses-1-million-users-651621/

[9] Security Technology Research Team, Analysis on Samsung Pay service and its security features, Federal Security Agency, Korea, Mar., 2015. (Written in Korean)

[10] EMVCo, "EMV Payment Tokenization Specification Technical Framework", available at https://www.emvco.com/specifications.aspx?id=263 , Mar.,2014.

[11] FIDO (Fast Identity Online) Alliance. Available at: https://fidoalliance.org/ [Visited at Nov. 2015]

[12] Samsung electronics America, "What is tokenization?" available at: http://www.samsung.com/us/support/answer/ANS00043866/997410219/ork

[13] Y. Cao, X. Pan, and Y. Chen, "SafePay: Protecting against Credit Card Forgery with Existing Card Readers", in Proc. IEEE Conference on Communications and Network Security, pp. 164-172, Sep. 2015.

[14] Korea IT News, "It is expected that Samsung Pay Will Be Registered In More Than 2 Million Cards By End of The Year", Sep., 2015. Available at: http://english.etnews.com/20150923200003

[15] J. Chen and C. Adams, "Short-range Wireless Technologies with Mobile Payments Systems", in Proc. ACM 6th International Conference on Electronic Commerce, pp. 649-656, 2004.

[16] C. Mullner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones", In Proc. International Conference on Availability, Reliability, and Security (ARES09), pp. 695-701, 2009.

[17] Y. Wong, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges", in Proc. 2nd International Conference on Mobile and Secure Services, pp.1-5, 2016.

[18] Ken Yeung, "Samsung pay now has 5M users, processed over $500M in first 6 months", Feb. 19, 2016. Available at:http://venturebeat.com/2016/02/19/samsung-pay-now-used-by-5m-users-processing-over-500m-in-first-6-months/ [Visited at May, 2016]