A Survey of Technologies for Mobile Payment Security

Wenzheng Liu, *Student, NUDT,* John Doe, *Fellow, OSA,* and Jane Doe, *Life Fellow, IEEE*

***Abstract*—Nowadays, the rising penetration of smartphones and the important roles of them in peoples daily life make the smartphones an ideal medium to conduct payment transactions. The smartphones are capable to store everything that would normally be carried in a physical wallet and also allows the users to make payments anytime and anywhere. The potential added-values of mobile payments, such as generating new revenues, obtaining new users, increasing user stickiness attracted different players to expand their businesses to the mobile payment services, including financial institutions, mobile network operators, mobile device manufacturers, trusted third party providers. To compete in the market, they explored different technologies and business models which resulted in the complexity and dynamics of the mobile payment market. Consequently, mobile payments have only become a standard practice in a few countries. In terms of proximity payments, NFC is widely viewed as one of the most promising technologies due to its security features, compatibility with the existing financial infrastructures, and ease of use. In the Chinese market, compared with QR code, NFC was first introduced and supported by various players. However, the Chinese mobile proximity payment market has become the largest and fastest-growing mobile proximity payment market in the world in few years by utilising QR code. The market is highly concentrated with Alipay and Tenpay which are QR code-based mobile payment platforms. In other words, QR code overtook NFC and became the most popular mobile proximity payment technology in China.**

***Index Terms*—token, payment, offline, LATEX, online, TOTP.**

I. Introduction

IN this study, the research model is developed based on relevant business model, platform and business ecosystem theories. The final research model consists of three connected perspectives Chinese mobile payment platforms, namely, He Wallet, Alipay and QuickPass which have implemented one or several technological solutions based on NFC and QR code technologies. The data for the case studies is collected from the semi-structured interviews and the desk research. The results showed that although NFC technology was adopted first in the Chinese market, the enabling devices of both consumers and merchants were not widely ready at that time for NFC technology,but good enough for QR code technology. However, the early NFC adopters (both MNOs and financial institutions) were reluctant to make a huge investment in the enabling devices to realise the large-scale deployment in the early stage due to the uncertainties on the technology level and the unclear roles and benefits on the business aspect. Thereby, they missed the best time to capture user and develop users' habit. In contrast, Alipay strategically adopted the independent service provider mode to leverage its obtained platform resources and capabilities which significantly contributed the mass adoption of QR code in the Chinese market. Despite QR code currently dominated the Chinese mobile payment market, it is believed that NFC has its place in the Chinese mobile payment market as China UnionPay adopted an open platform strategy to incorporate all relevant players into its ecosystem to facilitate the development of NFC-based mobile payments.

M. Shell was with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332 USA e-mail: (see http://www.michaelshell.org/contact.html).

J. Doe and J. Doe are with Anonymous University.

Manuscript received April 19, 2005; revised August 26, 2015.

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Virtual Bank card binding technology

Virtual bank card instead of the real bank card binding in the payment account or mobile terminal and transfer in the transaction.In this section,the Virtual bank card binding technology will be told. First, It is need to know why the virtual bank card need bindind in the mobile phone.Accoding to the PCI DSS and China UnionPay standard,there three main reasons need to explain. First,If the magnetic stripe card is skipped, it can be easily copied into a fake card, which is used for fraudulent transactions and brings about capital losses to the cardholder.in addition,If the card number is expired and the validity period, it is easy to move in some e-commerce in fraudulent transactions, bringing the cardholder money losses.moreover,In the online payment and mobile payment environment,the card organization is even more hopeful that it will not change the usage habit of the cardholder completing the transaction with the card number and expiration date, and at the same time effectively improve the payment security.

A. The process of binding bank card.

The payment provider hands over the bank card account (PAN) which the user needs to bind to the corresponding bank server. If the corresponding virtual bank card for this PAN does not exist for this merchant in the public central database,a new virtual is generated and an entry is added to the public central database.At the same time return virtual bank card to the merchant. The merchant binds the token with the user's account as a virtual bank card corresponding to the PAN.

However, in order to prevent the payment provider to saving or leaking the user's real bank card information, Alipay has proposed a new virtual bank card binding scheme:

1, the merchant system pre-save the payment system server authorization certificate. And authorize the signature of the authorization certificate called its default instructions.

2. The merchant system receives a binding request sent by a terminal, where the binding request corresponds to a user account that the user logs in on the merchant system; and returns a preset instruction to the terminal;

3, the terminal to the payment system through the secure channel to send the default instructions and the real bank card number.

4, the payment system generates a virtual bank card number corresponding to the real bank card number. (For each real bank card number generated by the virtual card number is different)

5, the virtual bank card number returned to the terminal.

6, the terminal sends the virtual bank card number to the payment provider.

7, the payment provider bind the virtual bank card to the user accounts.

In this scheme, the payment provider can not get the user's real bank card account information.

B. Fundamental of virtual bank card: payment tokenization

Enterprises, merchants, and payment processors face severe, ongoing challenges securing their networks and high-value sensitive data such as payment cardholder data, to comply with the Payment Card Industry Data Security Standard (PCI DSS) and data privacy laws. Tokenization, which is used as a way of replacing sensitive data like credit card numbers with tokens, is one of the data protection and audit scope reduction methods recommended by the PCI DSS.

The principle is to verify the transaction by using a payment token instead of a real bank card number so as to prevent card number information leakage risk. Payment tokenization is the process of replacing a traditional bank card master account with a unique numeric value, while ensuring that the value's application is limited to a specific merchant, channel, or device. Payment tags can be used in all aspects of bank card transactions, and existing bank card number based on the same transaction, can be used across industries in the industry, has versatility. As the latest cutting-edge technology in the global payment field, payment tokenization technology has its advantages in three aspects:

First, there is no need to retain sensitive information, cardholder card number and the validity of the card does not appear in the transaction;

Second, payment tags can only be used in a limited transaction scenario, making payments more secure;

Thirdly, compared with the traditional bank card verification function, the payment tag integrates the functions of personal identification and device information verification, additional verification of payment information and risk rating to conduct transaction legitimacy identification and risk control. Therefore, the tokenization of the payment can not only prevent the leakage of sensitive information of cardholders in all aspects of transaction, but also reduce the probability of fraudulent transactions.

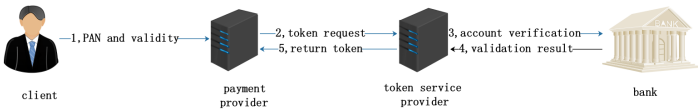

Fig. 1. Token application process.

1) Centralized tokenization technologies: Centralized tokenization is conventional, database-centric solutionswhich requst the token corresponding to the provided PAN from a common central database. If no token corresponding token exists in the common central database at the time of the request, a new token is generated and an entry will be added to the common central database.

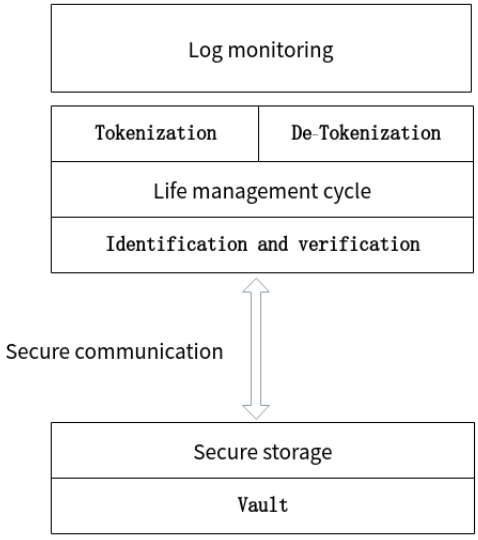

Fig. 2. token service provider

Card organizations are highly recommended centralized tokenization technologies. Centralized tokenization involves building a large-scale database (token vault), storing each PAN together with a generated token. Figure 3 shows the China UnionPay payment tokenization system framework

2) Distributed tokenization technologies:

III. Communication method

Mobile payment communication is mainly used for short-distance communication, especially for poor mobile network environment offline payment. Payment information is delivered via these means of communication. Many people regard communication as a means of payment. However, they are only responsible for transmitting payment information. The real means of influencing payment are payment encryption and authentication technologies.

A. QR code

QR code is a matrix QR code symbol that was invented in 1994 by Denso Wave, a Toyota subsidiary of Japan. The QR code not only has large information capacity, high reliability,

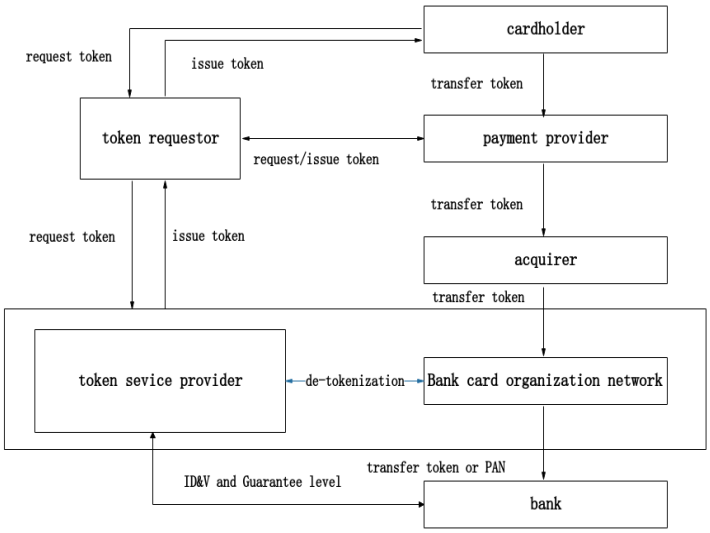

Fig. 3. China UnionPay payment tokenization system framework

and low cost, but also can represent various character information such as Chinese characters and images, and has strong security against fraud and is very convenient to use. Therefore, it quickly became popular in Japan and South Korea. Since then, European and American countries have begun to use it in large quantities.

QR code payment is very popular in China, people can almost go out without wallets and bank cards. You only need to show the QR code on your mobile phone to be able to pay in most places even without network. However, why is it possible to authorize payment with the QR code?

The QR code itself cannot make payment authorization, since the actual payment authorization is the payment certificate which encoded in the QR code. The payment certificate is a series of digits. You can authorize payment with this numbers. So the role of the QR code in mobile payment is to transmit this series of numbers. The specific technology of payment certificate will be told in section 4.

B. NFC:MST

MST is "Magnetic Secure Transmissions". The technology was developed and patented by LoopPay. Samsung previously acquired the company to deploy its Samsung Pay service.The biggest highlight of Samsung Pay and Apple Pay is support for magnetic stripe card payments.

Figure 3 shows the components of the payment accessory that LoopPay made for Samsung. By using AC current, the coil will generate a magnetic field.If the correct magnetic field is generated, the coil can communicate with a credit card reader.In fact, the principle of MST is to emit a magnetic field.

However, payment security is not solved by a copper coil.The MST application has three protection mechanisms: Payment Tokenization, eSE (hardware security module) bank card information protection, KNOX, and fingerprint/password authentication.

For Token, the user needs to enter the card information and send it to the card organization for verification. After the card organization passes the verification, a token will be generated for this card and the token will be sent to the device. The credit card information is not directly stored on the device. Token is stored in an independent security chip (SE chip) and used to replace the bank card number. It can be understood that the Token and the bank card number are equivalent, but even if the Token leaks, the bank card information cannot be reversed. Only when fingerprint or password authentication passes can the token be read out through the MST. Token's storage and management is governed by Samsung's own KNOX security platform.High-risk behaviors such as equipment modification occur, and KNOX can invalidate sensitive data on the device.

In other words, when using Samsung Pay's magnetic card payment mode, the key technical step is how this Token is sent. The MST generates a dynamic magnetic field through an induction coil and can be changed according to the user-defined time limit. If your mobile device is within 3 inches of the reader, you will be able to identify the magnetic field.

Like a traditional credit or debit card, magnetic fields include your payment information. The magnetic field only exists when the user chooses to send the payment information, and the magnetic field will automatically disappear once the distance between the mobile device and the reader exceeds 3 inches. This means that the attacker must be very close to the payment process to steal the payment data.

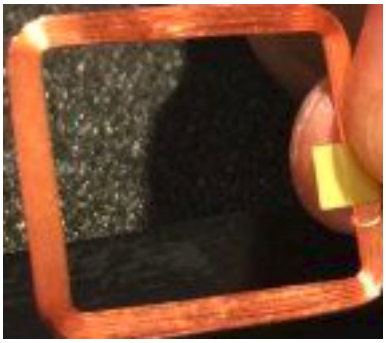

Fig. 4. token service provider

C. Audio

The audio protocol we are talking about today for sonic communication is generally from the technical documentation of chirp which is a novel application for "transmitting" files via voice issued by the American startup Animal Systems.

Acoustic wave transmission is a set of technical solutions that use sound to achieve fast transmission of files: Cross-platform technology is used to implement data transmission between any device that can send sound waves and receive sound waves.There are also a large number of applications in mobile payments.

1) coding: The principle of the audio protocol is simple and easy to implement. Create a table with 32 characters and map each character to a frequency table. The frequency table is generated based on the music theory through the calculation of sound.Each character is represented by the pitch of one frequency, so there are 32 frequencies, 0 corresponds to 1760

Hz, 1 corresponds to 1864 Hz,..., v corresponds to 10.5 kHz, and the adjacent frequency differs by a half interval.

The audio produced by Chirp contains 20 characters. Each character is generated with a sine wave of the corresponding frequency. Each sine wave lasts 87.2 ms. If the sampling rate is 44.1 kHz, then each character is about 3846 samples. The whole audio is about 20*87.2ms=1.744s, because each character is represented by a different frequency, it sounds like music.

A complete sound packet contains 20 tones (ie 20 characters), one tone every 87.2 milliseconds. The first two bits are headers and use hj to notify the receiver to start receiving. The middle 10 bits are valid information bits, which are effective transmission information, that is, Key values are mapped after the frequency information. The last 8 bits are the RS check digits. The RS parity check algorithm calculates the middle 10 bits and generates 8-bit parity information.

2	10	8
information header	data bits	RS validity bits

Fig. 5. A complete sound packet.

2) decoding: Chirp describes the technical details of relying on sound for data communication between a smart device, but in fact, the audio protocol of the sound wave communication can be arbitrarily designed by itself, for example, changing the sound in the chirp audio protocol to double-frequency sound, even multi-tone sound. In order to increase the information capacity per unit time, thereby increasing the transmission speed, this is all possible, as long as there is a demand for this application.

The receiver needs to record the sound and perform it and fault-tolerant processing. Its relatively high requirements on the algorithm, noise reduction and fault-tolerant processing are critical to the correct information

IV. Internet transfer payment technologies

A. scan the QR code

B. Through email

PayPal is a Web-based e-commerce business that allows money transfers and payments to be made through the Internet. It offers a secure method to transfer funds between individuals or business electronically. A special feature of PayPal is that it does not transmit any financial information over the Internet as a bank would do. It is similar to an escrow service as PayPal acts as the middleman holder of the money between both parties involved in a transaction. In this paper I will focus on the specific case of Cross-Site Scripting attacks (XSS) against the security of web applications. The XSS attack is very similar to SQL Injection due to the fact that both attacks inject code into the web application that poses a threat. A study documented by Symantec in 2007 showed that roughly 84 of websites are susceptible to cross site scripting.

PayPal uses the public key cryptography technology to encrypt your PayPal button created from your account that is used in a website. Public key cryptography provides a way to prove the identity in the online world. This cryptographic algorithm uses two keys(public-key and private-key) which are bits of data that are mathematically related to one another. This type of cryptographic algorithm only works only if you keep the private key confidential, while the public key can be made available. The public keys are distributed inside a digital certificate. Digital certificates represents a file that contains information about the public key (name of the company that owns the public key, the third party company that distributed the certificate and the certificate expiration date) and the key itself. The third party involved in signing the certificate is referred as a certificate authority (CA). The CA signs the digital certificate, and the consumers can validate that the public key is valid by using the public certificate of the CA to verify the digital signature.

Even though you can generate an encrypted PayPal button either from your PayPal account or through the PayPal API, many websites still use the standard HTML form for a Buy Now button or Subscription button. The code for the encrypted PayPal button is presented in the image below. You can see in Figure 1 that the input with the name $hosted_button_id$ holds the encrypted value for the product. This includes the business name. item name, price, currency shipping and tax values entered in PayPal.

This type of PayPal button is secure because it does not display any information about the merchant or about the item itself. Another type of PayPal button is the one where you can enter all the variables in plaintext as seen below (Figure 2).

In Figure 2 you can see that the personal information about your account is now visible: business (the merchant account), amount (the price of the item), first name, last name, address 1, address 2 city, zip (information about the buyer). All the above information is in plaintext and can be easily altered for malicious intents.

For example using a man-in-the-middle attack as seen in Figure 3, the attacker intercepts the communication between the victim and the Web Server. Using different techniques, the attacker can split the original connection into two new connections, one between the victim and the attacker and the other between the attacker and the Web Server. Once the connection is intercepted, the attacker can read and alter the data from the intercepted connection. Once the attacker intercepts the connection he can alter the merchant account by adding his own

users browser allows an attacker to perform the following types of attack: Cookie theft: the attacker can access the victims cookies associated with the website, send them to his own server and use them to extract sensitive information like session ID, which can be used to enter PayPals website (PayPal uses cookies when a user loges in with his account) as though he was the actual owner of the account

Keylogging: the attacker can register a keyboard event listener, and then send all of the users keystrokes to his own server, potentially recording personal or financial information Phishing: the attacker can insert a fake login form into the page, set the forms action attribute to target his own server and then trick the user into submitting sensitive information.

For security purposes PayPal introduced an option for using a PayPal Security Key during the login process. This security measure is actually an OTP authentication system that generates a random temporary security code (which is displayed on the PayPal Security Key card) that must be used together with the accounts holder username and password to complete the sign in process. is ignored and therefore the attack was successful. Further, the attackers establish a separate HTTPS connection with the server to complete the request, and the result of the response is delivered to the victims browser. This gives the attackers full control over the SSL traffic and helps them steal personal information. Since the attackers are not breaking the request-response chain, this kind of attack becomes tough to detect the data theft. 2.3.1 NSA Man in the middle NSA (National Security Agency) is known for using man in the middle attack. Because NSA has a secret partnership with the US telecoms companies, NSA placed secret servers at key places in the internet backbone. This placement

ensured that they can react faster then any other websites can. Exploiting these speed differences these servers could impersonate a visited website to the victim before the legitimate website could respond, thereby tricking the victim into thinking they are on the right website. This kind of attack is very difficult to execute for any other attackers because it requires a privileged position in the internet backbone. NSA uses these fast servers to execute a packet injection attack that redirects the victim to one of the NSA servers. 2.3 The SSL Man in the middle attack In this case, the attackers intrude into the network and establish a successful man in the middle connection. The attackers can watch the HTTPS traffic and wait for the targeted website to respond to some browsers HTTPS request. When a browser sends a HTTPS request, the server responds by sending its digital certificate as part of the SSL handshake protocol. At this moment, the attackers can grab this certificate and note down various information as the domain name, expiration date etc. The attackers can now create their self-signed certificate using the information from above. From this point forward, the attackers intercept each browser request and respond with the fake certificate. As a normal response to this situation, the browser pops up a warning to the user, which in most cases 2.4 Packet Crafting Packet crafting is a task that is methodically carried out to penetrate into a networks infrastructure. There are four steps involved in crafting a packet: Packet assembly; Packet editing; Packet playing; Packet analysis. 2.4.1 Paced assembly This is the first step in the crafting process, where an attacker decides which network needs to be cracked, tries to gather possible vulnerability information and creates the packets to be sent. The packet is then checked for accuracy, especially to ensure that the attack is as invisible on the network as possible, to go undetected.

users browser allows an attacker to perform the following types of attack: Cookie theft: the attacker can access the victims cookies associated with the website, send them to his own server and use them to extract sensitive information like session ID, which can be used to enter PayPals website (PayPal uses cookies when a user loges in with his account) as though he was the actual owner of the account Keylogging: the attacker can register a keyboard event listener, and then send all of the users keystrokes to his own server, potentially recording personal or financial information Phishing: the attacker can insert a fake login form into the page, set the forms action attribute to target his own server and then trick the user into submitting sensitive information. For security purposes PayPal introduced an option for using a PayPal Security Key during the login process. This security measure is actually an OTP authentication system that generates a random temporary security code (which is displayed on the PayPal Security Key card) that must be used together with the accounts holder username and password to complete the sign in process. is ignored and therefore the attack was successful. Further, the attackers establish a separate HTTPS connection with the server to complete the request, and the result of the response is delivered to the victims browser. This gives the attackers full control over the SSL traffic and helps them steal personal information. Since the attackers are not breaking the request-response chain, this kind of attack becomes tough to detect the data theft. 2.3.1 NSA Man in the middle NSA (National Security Agency) is known for using man in the middle attack. Because NSA has a secret partnership with the US telecoms companies, NSA placed secret servers at key places in the internet backbone. This placement ensured that they can react faster then any other websites can. Exploiting these speed differences these servers could impersonate a visited website to the victim before the legitimate website could respond, thereby tricking the victim into thinking they are on the right website. This kind of attack is very difficult to execute for any other attackers because it requires a privileged position in the internet backbone. NSA uses these fast servers to execute a packet injection attack that redirects the victim to one of the NSA servers. 2.3 The SSL Man in the middle attack In this case, the attackers intrude into the network and establish a successful man in the middle connection. The attackers can watch the HTTPS traffic and wait for the targeted website to respond to some browsers HTTPS request. When a browser sends a HTTPS request, the server responds by sending its digital certificate as part of the SSL handshake protocol. At this moment, the attackers can grab this certificate and note down various information as the domain name, expiration date etc. The attackers can now create their self-signed certificate using the information from above. From this point forward, the attackers intercept each browser request and respond with the fake certificate. As a normal response to this situation, the browser pops up a warning to the user, which in most cases 2.4 Packet Crafting Packet crafting is a task that is methodically carried out to penetrate into a networks infrastructure. There are four steps involved in crafting a packet: Packet assembly; Packet editing; Packet playing; Packet analysis. 2.4.1 Paced assembly This is the first step in the crafting process, where an attacker decides which network needs to be cracked, tries to gather possible vulnerability information and creates the packets to be sent. The packet is then checked for accuracy, especially to ensure that the attack is as invisible on the network as possible, to go undetected.

V. OFFLINE PAYMENT TECHNOLOGIES

A. Time-Based One-Time Password:The key to offline payment

B. IC card and NFC payment

C. Mobile phone imitate IC card

With the gradual deployment of Android Pay, Apple Pay and Samsung Pay, mobile payments have returned to the public eye and the comparative articles on several types of payment have not been uncommon in recent days. This article mainly discusses the similarities and differences between several payment methods from a technical point of view.

Apple Pay and Android Pay each serve as a system-level payment application (Apple Pay by iOS, Android Pay by Android), not only play the role of application, but also has a God perspective, as a system feature for other applications developers A unified payment gateway. In other words, other shopping and service applications can invoke APIs of Apple Pay or Android Pay in the development code to charge consumers, for example, purchasing a movie ticket. Before the application is almost always linked to VISA or MasterCard online payment allows users to fill in the cardholder name, card number, expiration date, code and other safety information, each time you have to fill in the shopping (the site should not and can not be saved), or combined with OTP (one-time password) certification, This is a hassle and a safety hazard (previously PC-based cookies were hacked, or consumer websites saved user-card information, such as previous Ctrip, resulting in theft of credit card information); application developers can now call Pay, allowing users to choose their own credit card has been added to pay, users do not need to fill in a form, a key shopping, the real charge to pay to do.

Relative to the online payment (in short, that is connected with the Internet, the payment of data through the network transmission), offline payment is a physical payment, you need a terminal device chargeback, in most cases, POS machines. In order to replace the traditional credit card with credit card spending, NFC + Pay way allows consumers to use a cell phone, rather than a variety of cards for ”flash” consumption. Pay only needs the POS machine to support NFC without any other modification. Therefore, offline entity merchants accept this payment method exactly as the acceptance of non-connected bank cards such as MasterCard Pay Pass, Visa Pay Wave, China Union Pay Flash Quick Pass , There is no promotion barriers, but also to speed up the deployment of wireless POS machines coupled with a heavy weight.

1) sumsung pay:

2) Android pay:

3) apple pay:

VI. DISSCUSION AND SECURITY COMPARISON

VII. CONCLUSION

The conclusion goes here.

APPENDIX A
PROOF OF THE FIRST ZONKLAR EQUATION

Appendix one text goes here.

APPENDIX B

Appendix two text goes here.

ACKNOWLEDGMENT

The authors would like to thank...

REFERENCES

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.