RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: MBS-F02

MOBILE PAYMENT SECURITY RISK AND RESPONSE

Shaoliang Chen

Senior Security Expert
PwC

Aaron Turner

CEO & Founder
IntegriCell

Introduction – Shaoliang Chen

Shaoliang Chen
PwC
Senior Security Expert

Email: stevenchen2081@gmail.com
Twitter: @stevenchen2081
WeChat:

- **Position**: Senior Security Expert at PricewaterhouseCoopers(PwC) Beijing office.
- **Security experience**: A decade of experience in the information security area.
- **Finance Industry experience:** As a Chief Security Architect role in mobile payment system construction.
- **Social activities**: Presenter at security and financial conferences
- **Personal contributions:** A series of papers on mobile payment security.

Introduction – Aaron Turner

- **20 years of experience researching mobile payment system vulnerabilities**
  - Microsoft
  - US Government (DHS, Treasury)
- **Co-inventor of several contactless payment technologies**
  - Peer-to-peer contactless system based on elliptic curve cryptography
- **Inventor & Entrepreneur**
  - Founded Terreo in 2014 as one of the first broad-spectrum airspace monitoring systems to look for payment anomalies
  - Sold Terreo to Verifone in 2015

Email:stevenchen2081@gmail.com

Agenda

- Mobile Payment Ecosystem
- Mobile Payment Risk Analysis
- How to Improve Mobile Payment Security

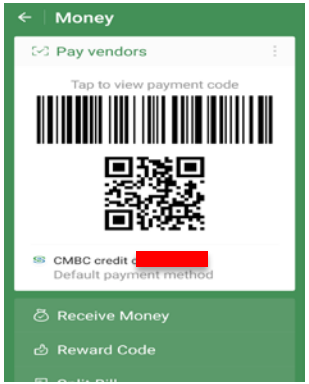
Part 1

Mobile Payment Ecosystem

Mobile Payment Definition and Methods

- Mobile Payment
  - QR code
  - NFC
  - Bluetooth
  - Magnetic Fields
- Near field communication scenarios:
  - Transit, urban commerce
  - Basis of Apple Pay and Google Pay

NFC



QR Code

Electronic bracelet

Smart watch

Email:stevenchen2081@gmail.com

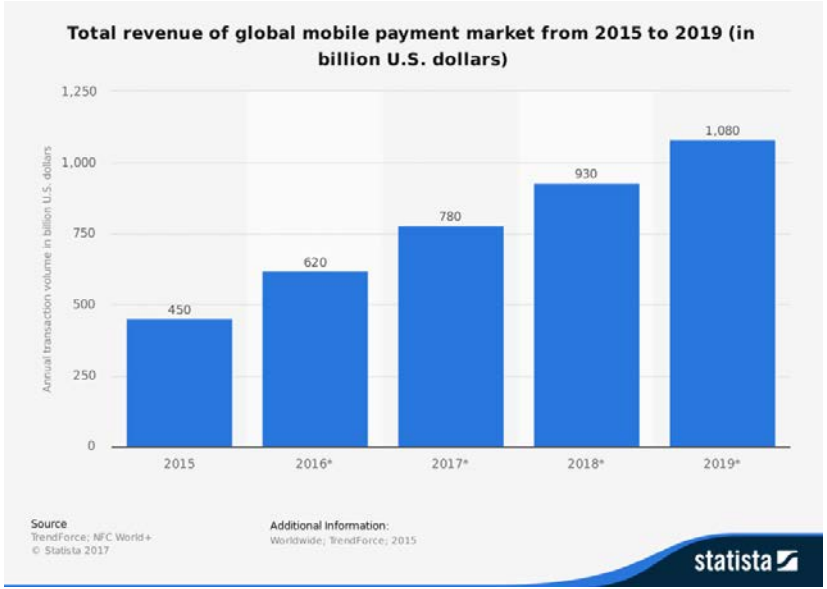
Global Mobile Payment Well-Known Brands

- China
  - Alipay: NFC, QR code
  - WeChat Pay: QR code
  - UnionPay: NFC, QR code
  - Hong Kong: NFC - Octopus
- United States
  - Apple Pay: NFC
  - Google Pay: NFC
  - Square: QR code
  - PayPal: QR code
- Other Brands
  - South Korea: Samsung Pay
  - India: Paytm
  - Europe: Wirecard

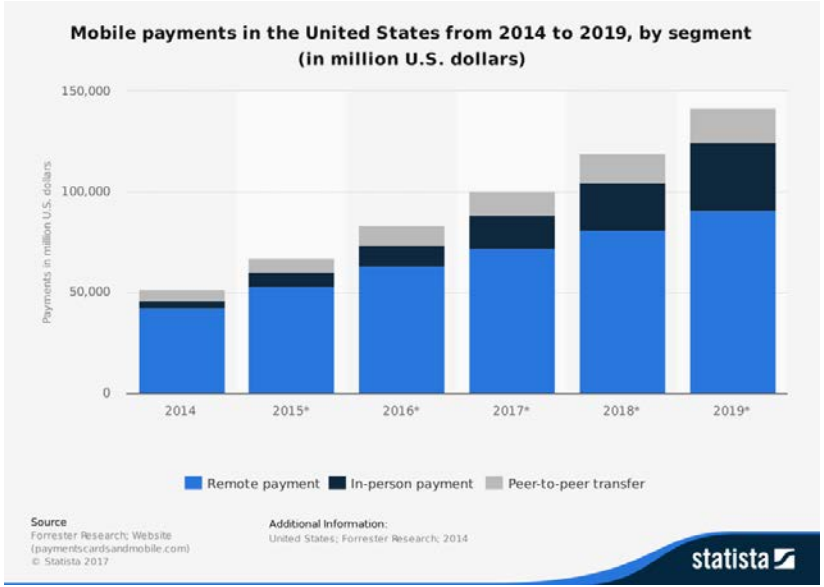
reference: xinhuanet.com, Chinadaily.com, various report

Email:stevenchen2081@gmail.com

Mobile Payment Market Development Trend



Global Market



USA Market

reference: statista.com

Mobile Payment Security Incidents

Fraud , Mobility , Payments Fraud

Apple
Authe
Mobile a Bree
Tracy Kitten (Fra

zed Numbers,

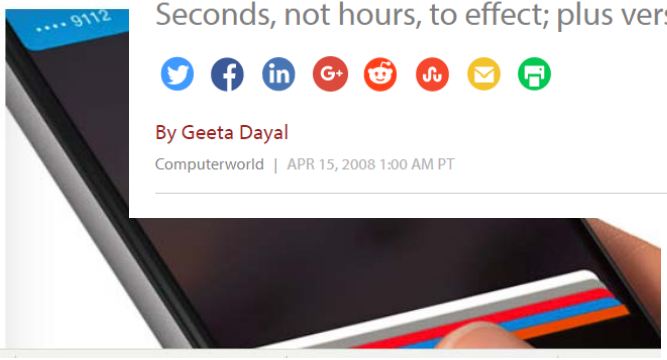
NEWS

MiFare RFID crack more extensive than previously thought

Seconds, not hours, to effect; plus version tappable too

By Geeta Dayal

Computerworld | APR 15, 2008 1:00 AM PT



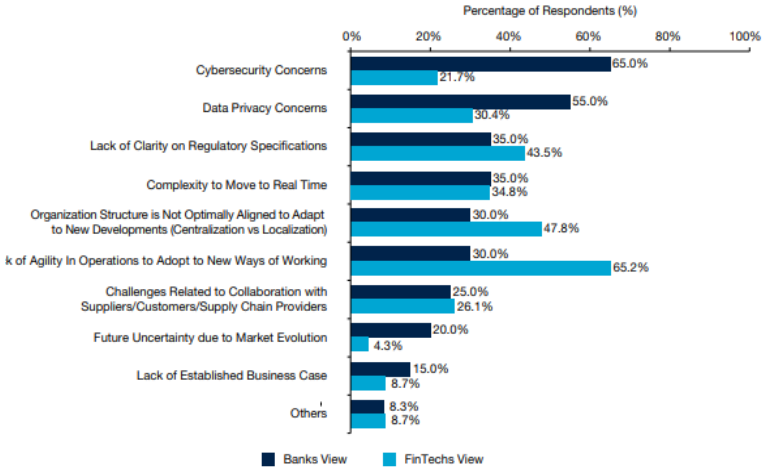
reference: bankinfosecurity.com

reference: zdnet.com/blackhat.com

Security Issues for Payment

Capgemini & BNP Paribas 2017 World Payments Report

Survey revealed that bank executives are most concerned about cybersecurity(65.0%) and data privacy(35.0%)



Cyber Security	*Data Privacy*
65%	35%

More and more people focus on cyber security for payment

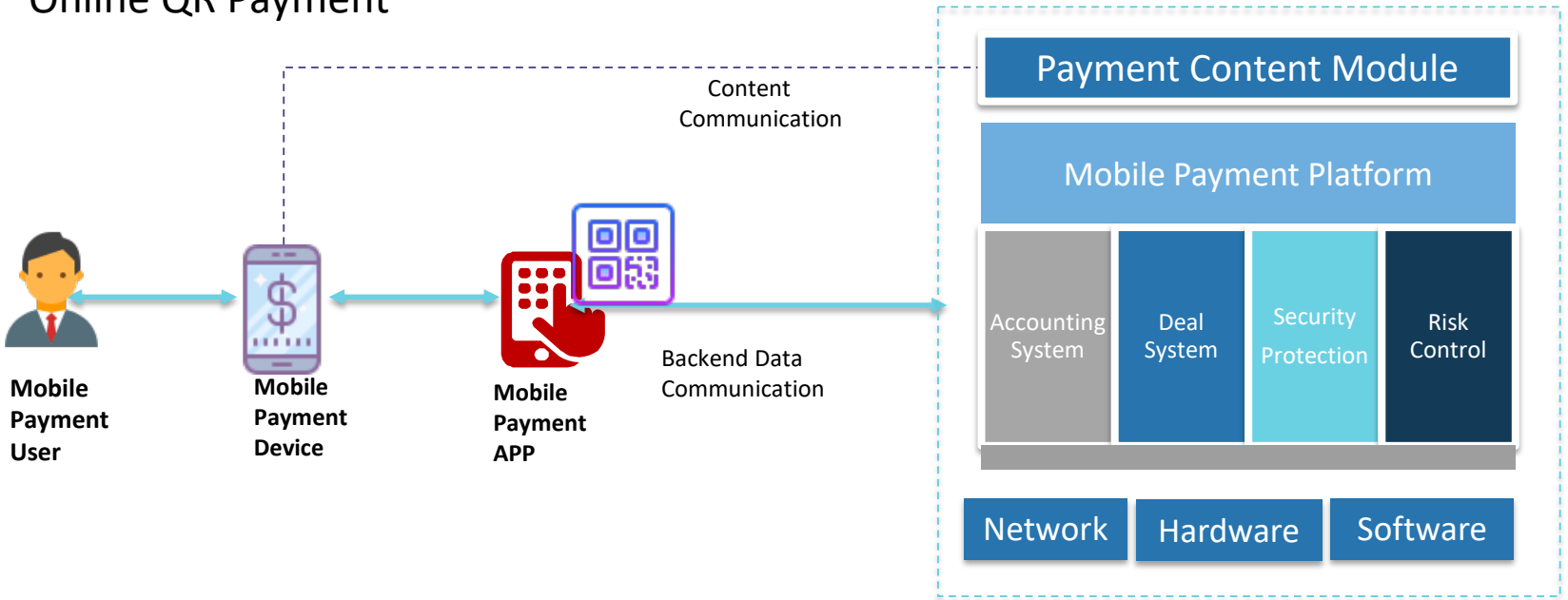
Can mobile tech help?

reference: www.worldpaymentsreport.com

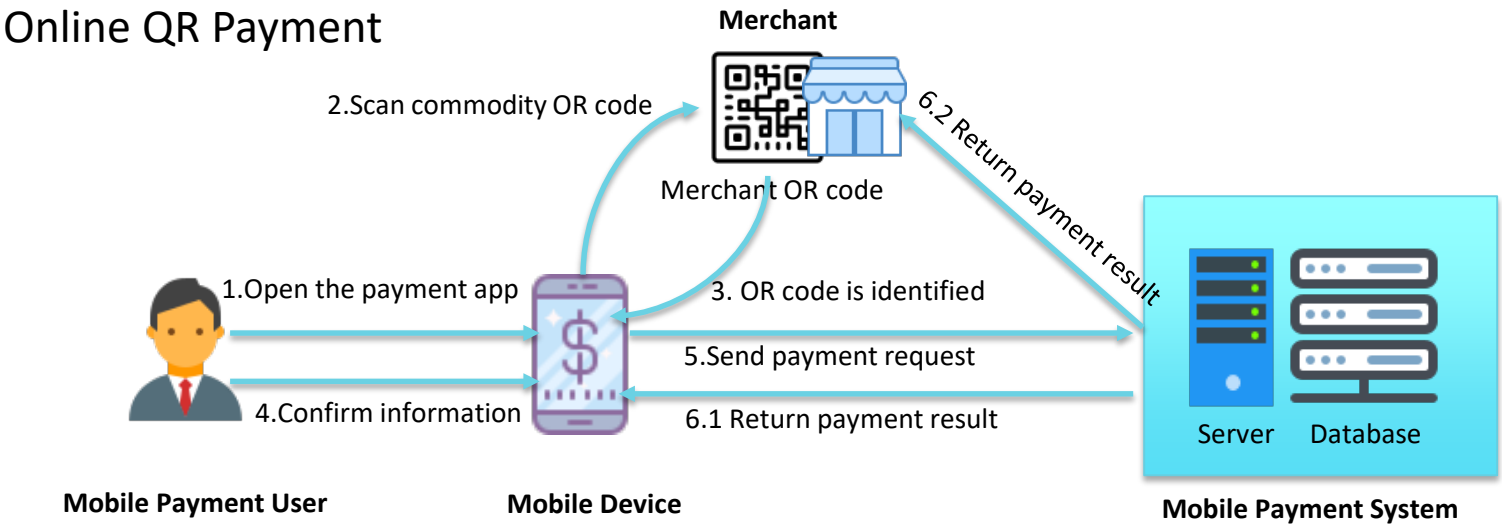
Email:stevenchen2081@gmail.com

Mobile Payment Architecture—QR payment

Online QR Payment

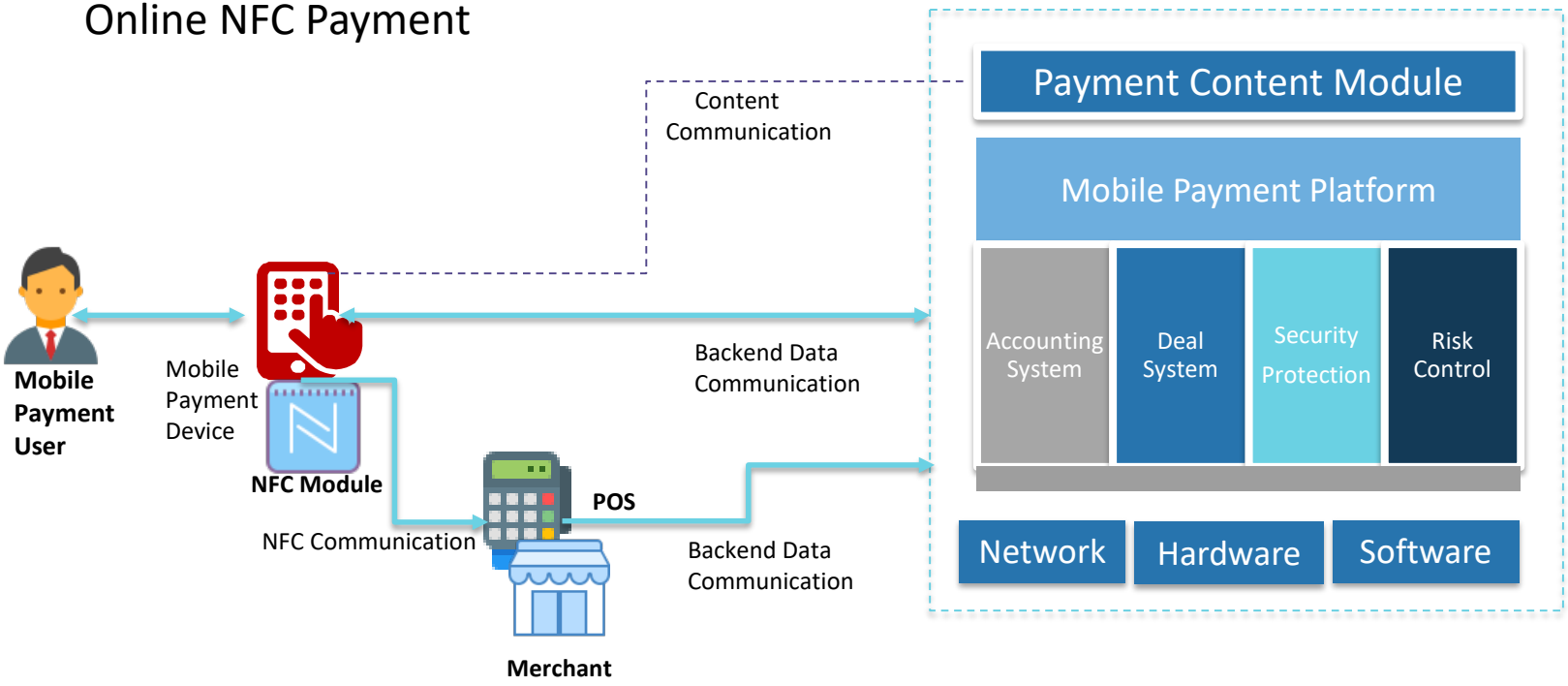


Mobile Payment Process—QR payment



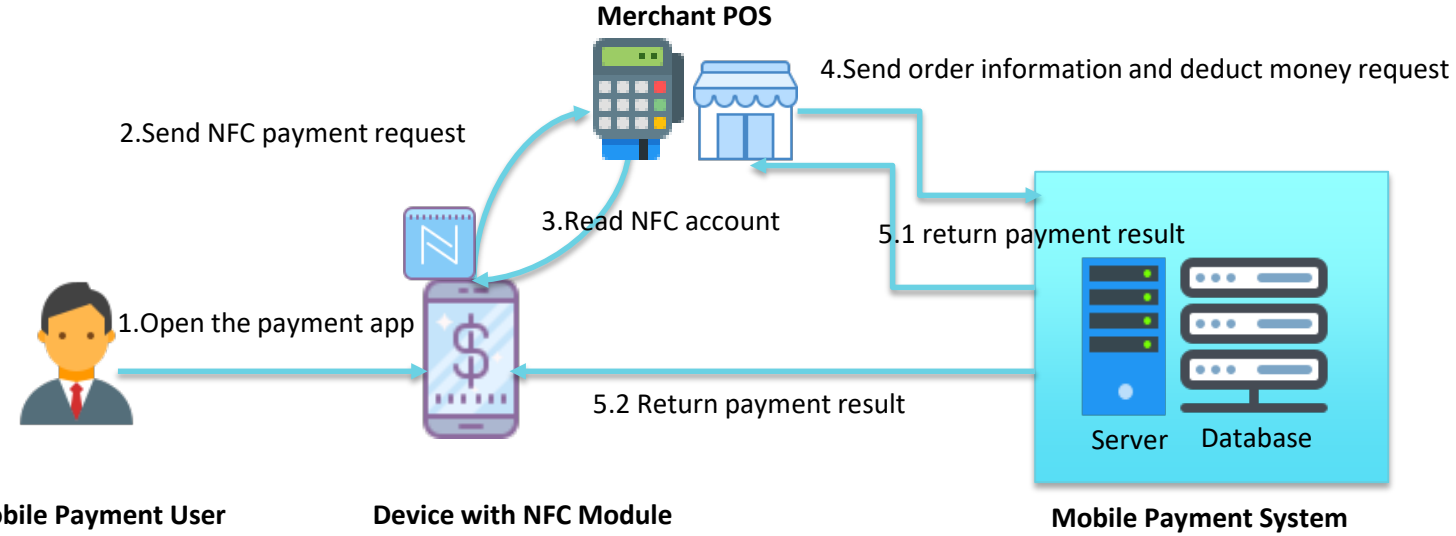
Mobile Payment Architecture—NFC payment

Online NFC Payment



Email:stevenchen2081@gmail.com

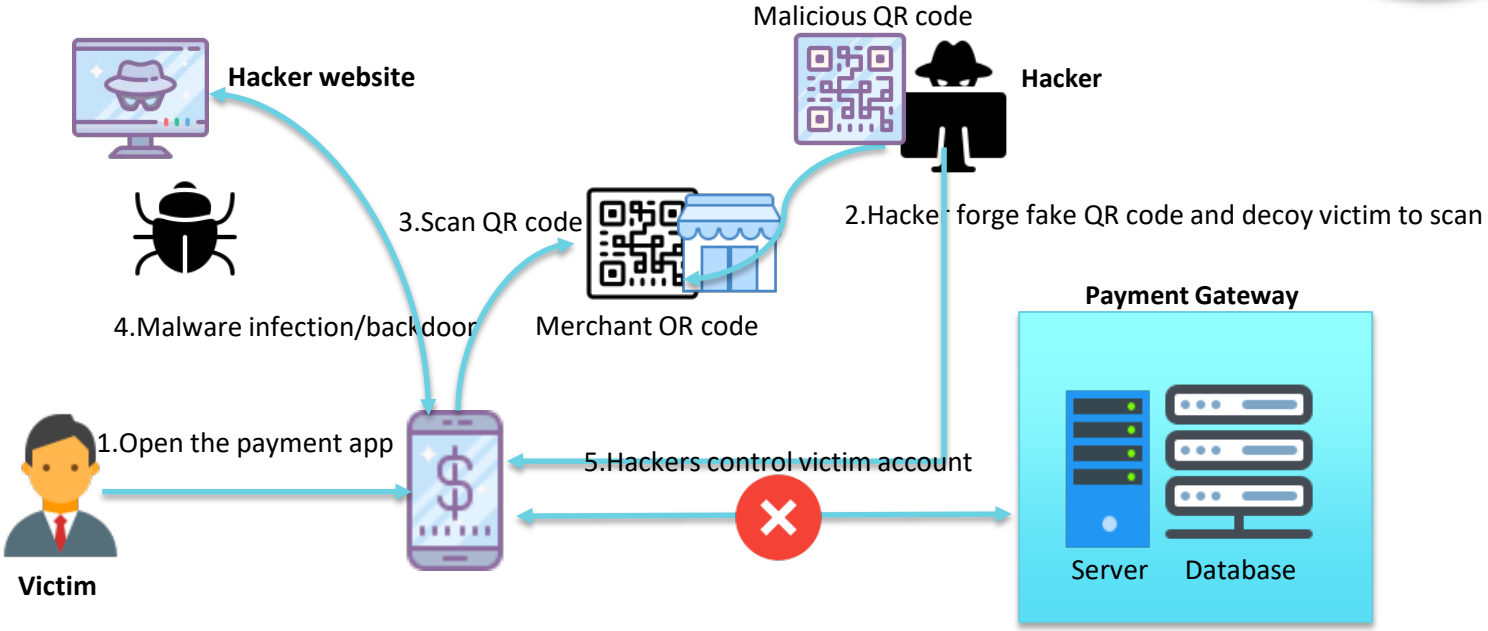
Mobile Payment Process- NFC payment



Part 2

Risk and Analysis

Mobile Payment Risk Demo—QR Payment



Mobile Payment Risk Demo – Phishing

The Register®
Biting the hand that feeds IT

ENTER SOFTWARE **SECURITY** DEVOPS BUSINESS PERSONAL TECH SCIENCE

licious base station

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May 2017 at 20:02 48 SHARE ▼

way

ase

Risk Analysis — Device

- Phishing
- Cross Frame
- Clickjacking
- Man-in-the-Middle
- Buffer Overflow

- No Passcode
- Weak Passcode
- Operating System Vulnerability
- Software Vulnerability
- No Encryption
- Weak Encryption

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Certificate Validation
- Dynamic Runtime Injection
- Incorrect Default Permissions
- Escalated Privileges
- Malware

- Side Channel Attack
- Baseband Attack
- SMS Phishing
- Device Lost

Risk Analysis — Network

Network Surface Risk Analysis

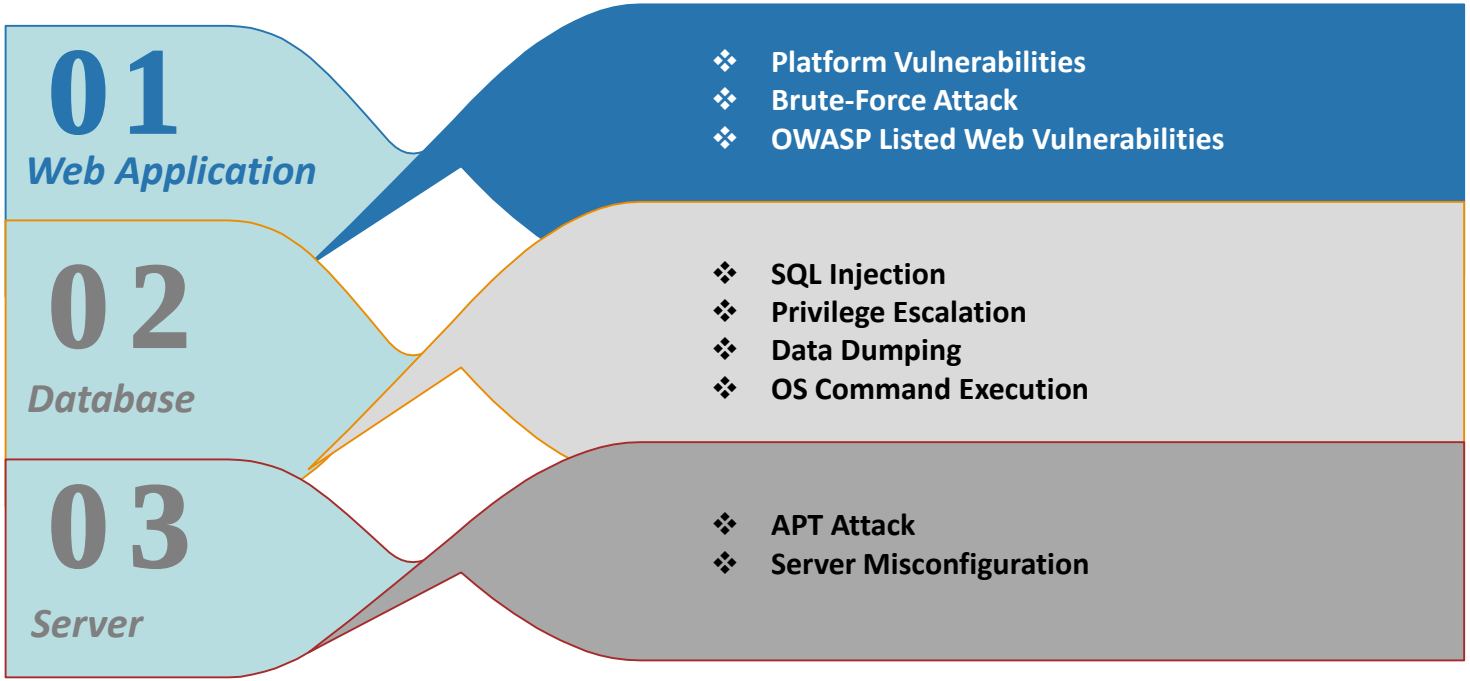
Protocol

- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS (Domain Name System) Poisoning
- Fake SSL Certificate

Access

- Wi-Fi (No Encryption/Weak Encryption)
- Rogue Access Point
- Packet Sniffing

Risk Analysis — Backend System

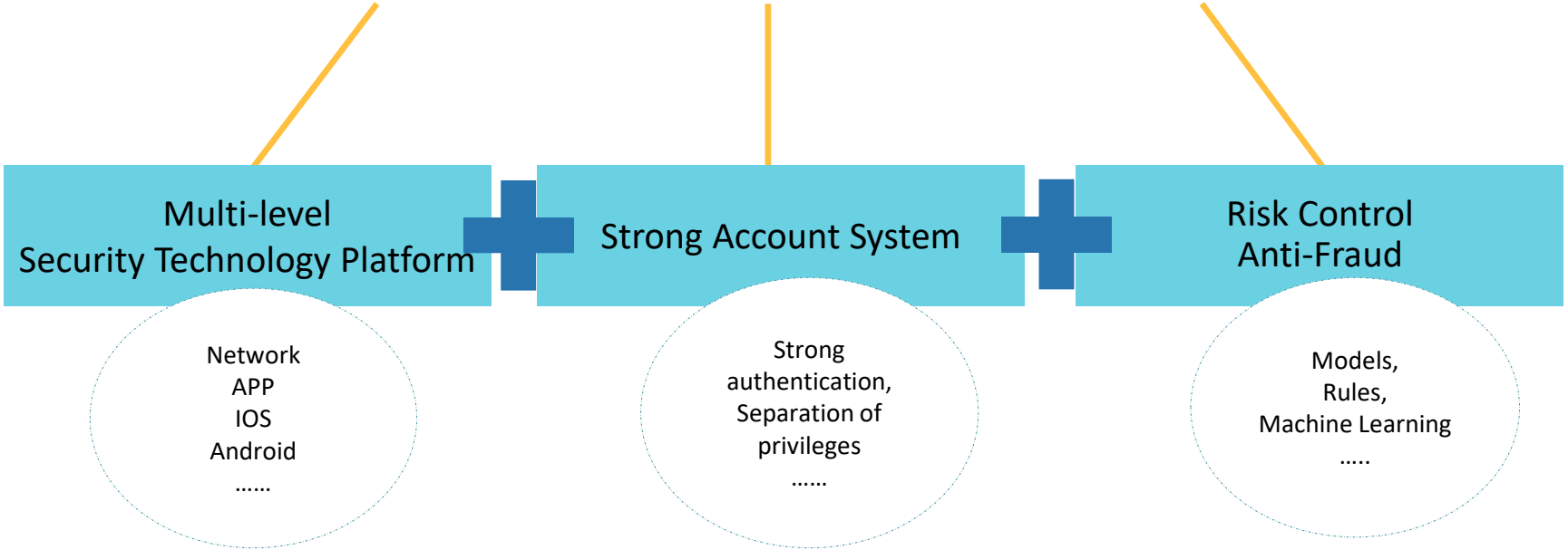


Part 3

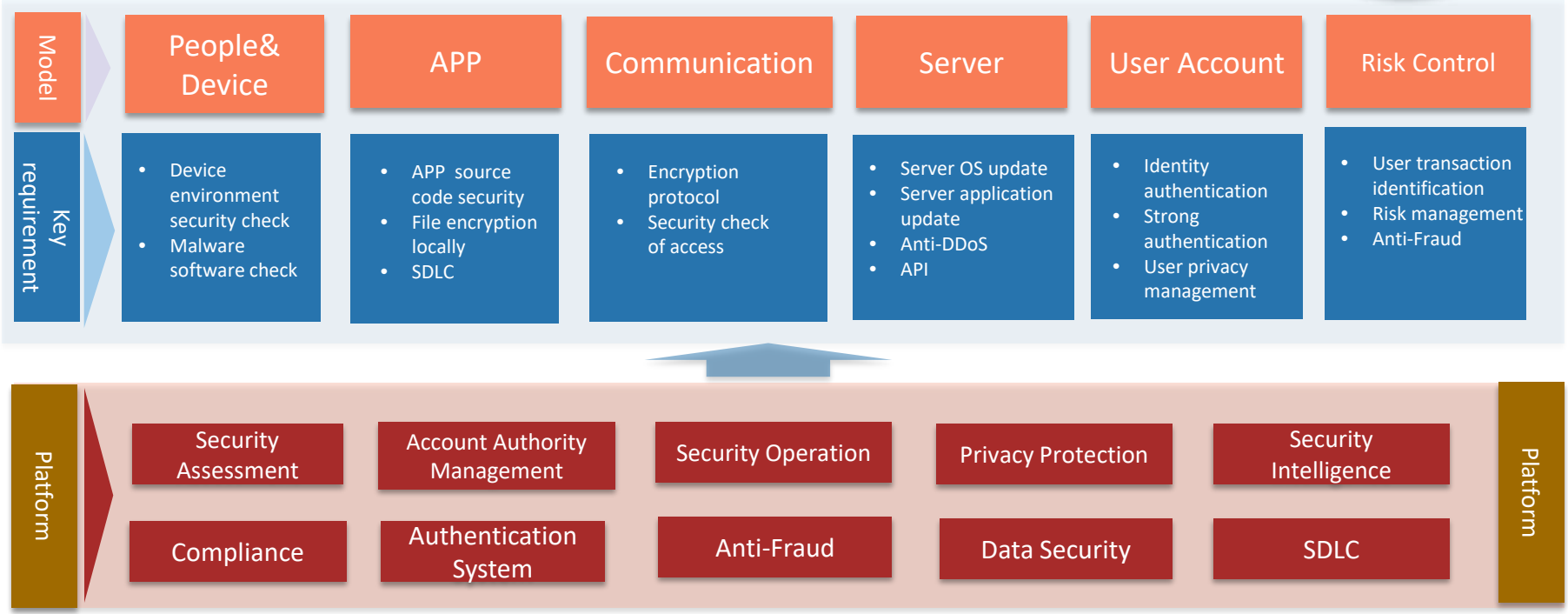
How to Improve Mobile Payment Security

Where are the weaknesses today?

End-to-End Mobile Payment Security?



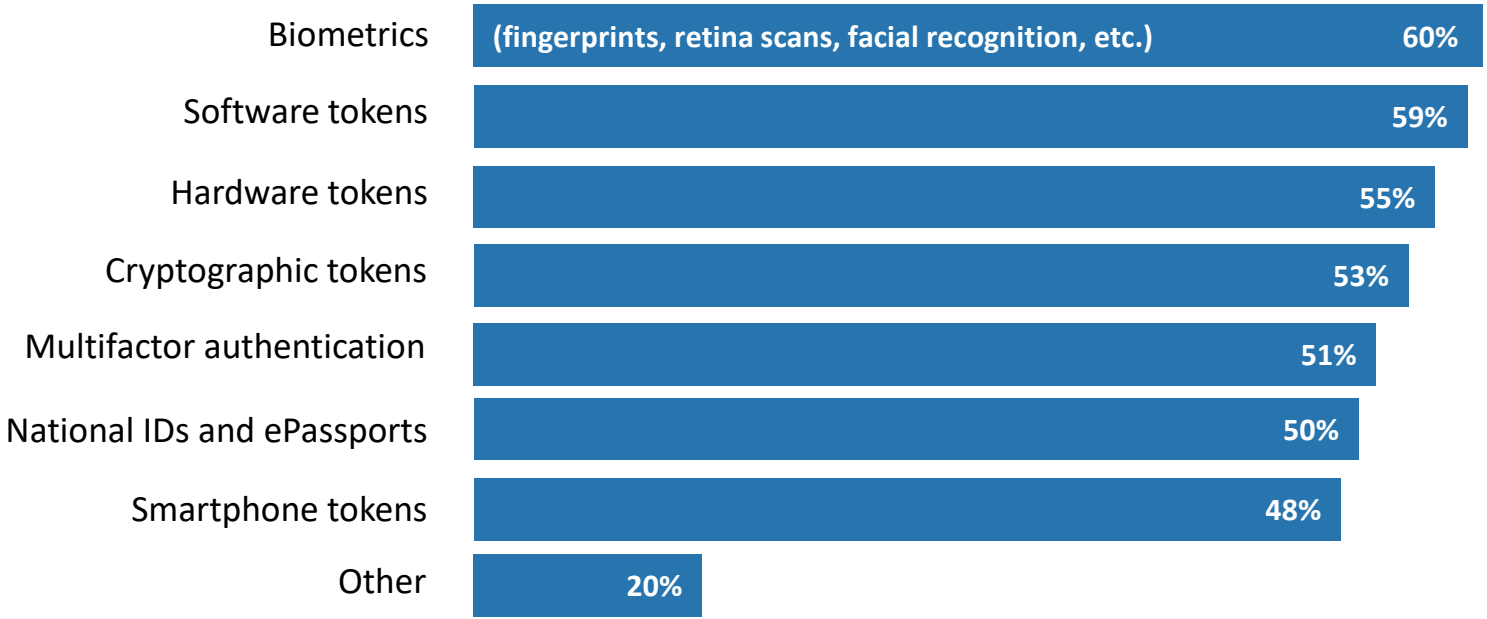
Mobile Payment Security Architecture



Email:stevenchen2081@gmail.com

Statistics for Authentication

Companies are adopting advanced authentication technologies

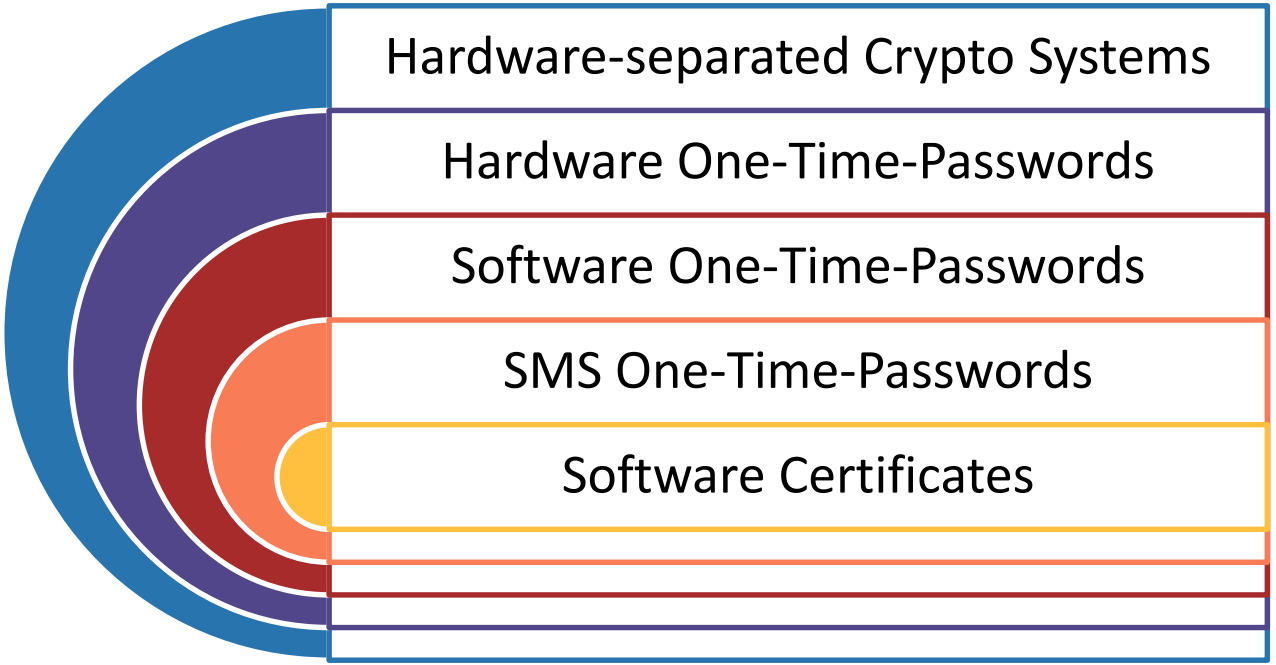


reference: PwC, CIO and CSO, The Global State of Information Security Survey 2018 Base 9500 respondents

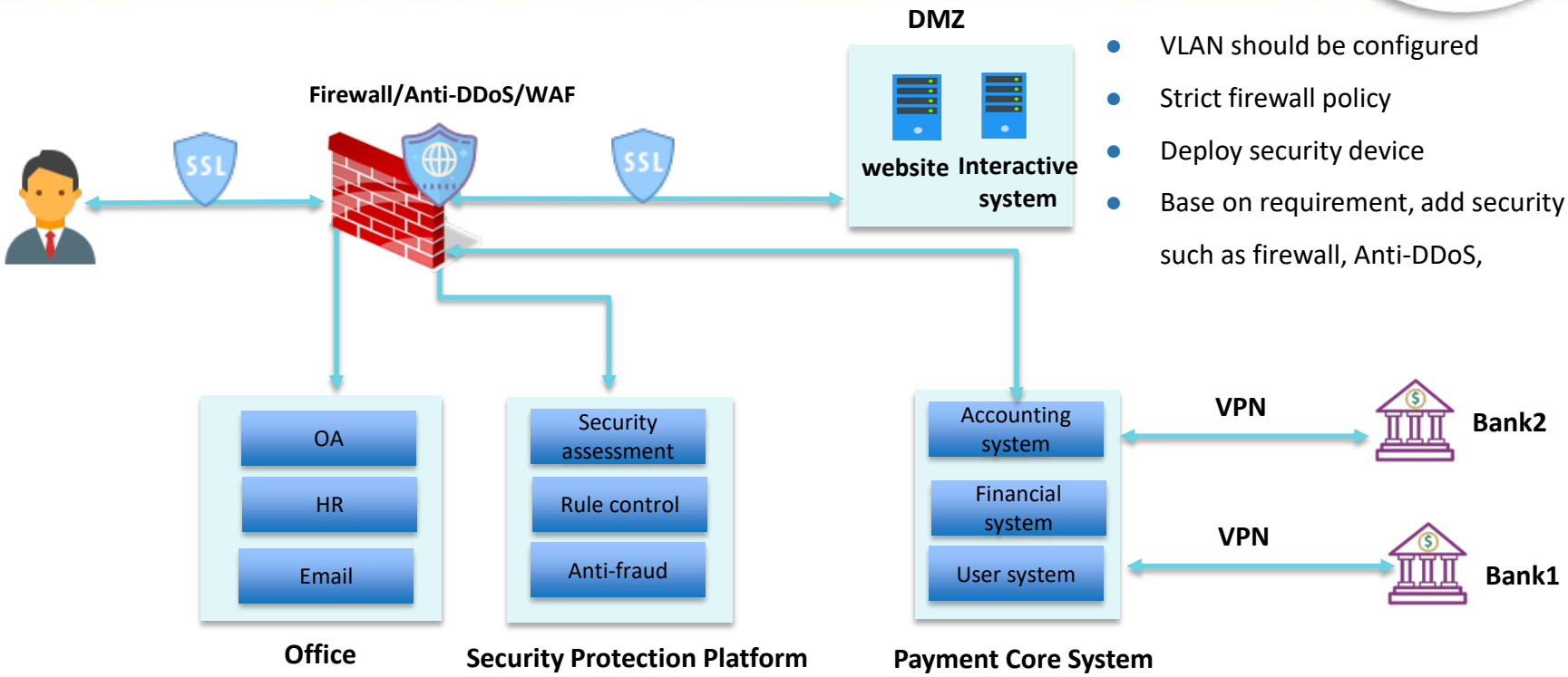
Best Practice – Authentication Technology Comparison

Technology	Features	Key Points
Security key	• Strong encryption • Hardware key/USBkey • Key file (*.key….)	• Build the key management system and ensure security • Hardware key/USBkey is proved more secure by now
Biometric(fingerprint, facial recognition)	• Higher identification rate • User unique	• Risk of permanent leakage • Natural person property • Privacy protection and legal compliance
Two-Factor Authentication	• Hardware tokens • Software tokens • Smartphone tokens • Email, SMS	• Mandatory to use when register • Anti-fraud combination
Multi-factor Authentication	• Multi-dimension • Knowledge, possesion • Various technologies (Security key, SMS, and etc.)	• Backend analysis • Risk model judgement
National IDs and ePassports	• Name • ID number	• Verified by public security department • Response whether match between name and ID number • Privacy

- Turner's Hierarchy of MFA
  https://portal.iansresearch.com/content/2774/enhancing-the-integrity-of-privileged



Best Practice – Network Architecture

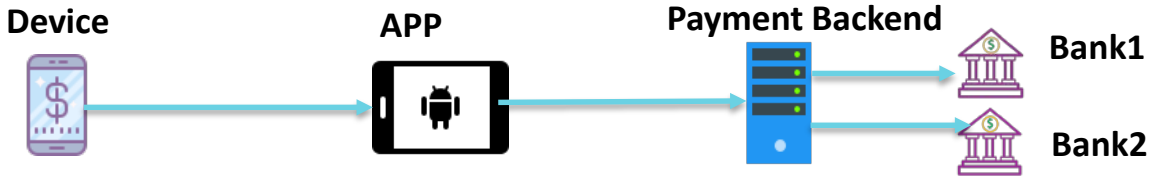


- VLAN should be configured
- Strict firewall policy
- Deploy security device
- Base on requirement, add security device, such as firewall, Anti-DDoS,

Best Practices

- SMS Verification?
  - When to use it and when NOT to use it
- Human ‘not a bot’ verification
  - How effective versus captcha-sweatshops?
- Account recovery?
  - What real-world processes can you implement to drive integrity to prevent account hijacking?
- Avoiding social engineering attacks?
  - How far upstream can you get with mobile payment system designers?

Best Practice – Key Points for Security Testing



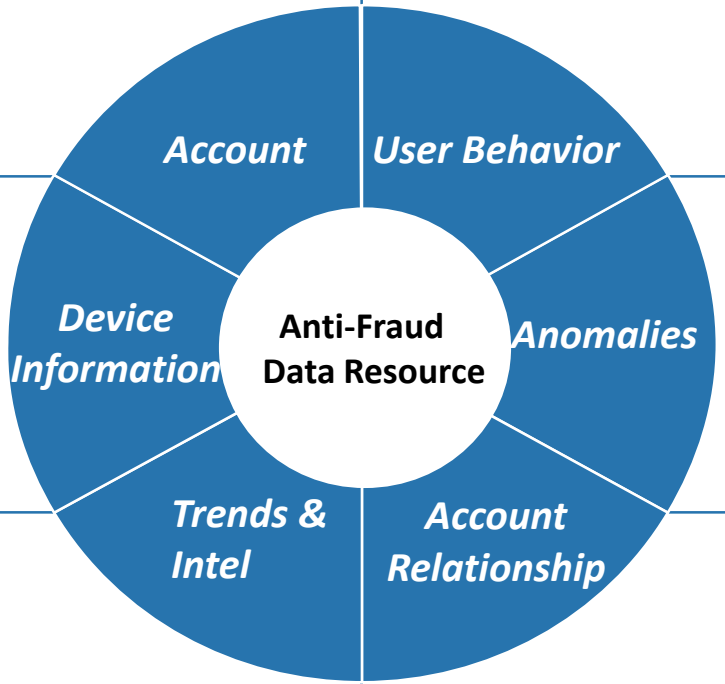
- Root
- OS version
- Access point/wireless/4G
- Proxy
- SSL certificates
- Malware

- Communication
- Secret protection
- Authentication
- Logic check

- SQL Injection/OWASP
- Database permission
- Interfaces
- Transaction quota
- Data Encryption
- Blacklist (IP address or high risk account)
- PCI-DSS

Test for failures at each stage – how does the system respond to malicious input?

Best Practice – Anti-Fraud 1



Account

- Account status, active account or not
- Black account list
- Account risk rate

User Behavior

- Trade time
- Trade device
- Trade amount number
- Trade bank credit card

Device information

- Device serial number
- Device network MAC address
- Device IMEI number
- Device MEID number

Anomalies

- Abnormal operation, such as quickly transfer to multiple accounts.
- Change account payment password in late night

Trends & Intel

- Frequency statistics
- Biggest statistic

Account Relationship

- Multiple accounts with the same identified individuals
- Geographical position

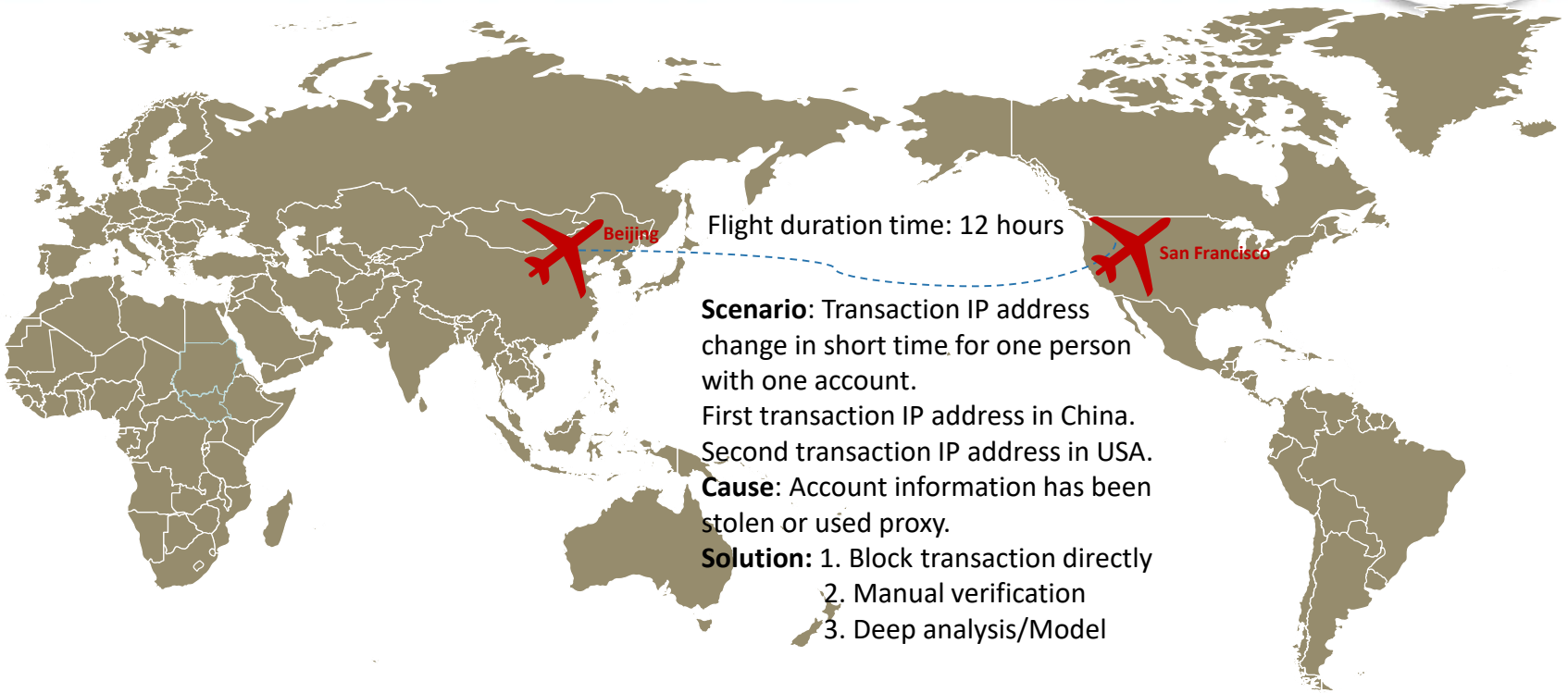
Best Practice – Anti-Fraud 2

Rule Samples

Rule Number	Rule description	Rule formula
Rule 1	A account has been changed password more than three times a day, which requires a SMS verification code to verify.	When single account has been changed password times>3, then send SMS verification code.
Rule 2	The transaction takes place between 1 a.m. and 5 a.m., and the device is associated with two accounts, sending SMS verification codes.	When transaction time between 1 a.m. to 5 a.m., one device is associated with the account number≥2, then send SMS verification code.

Email:stevenchen2081@gmail.com

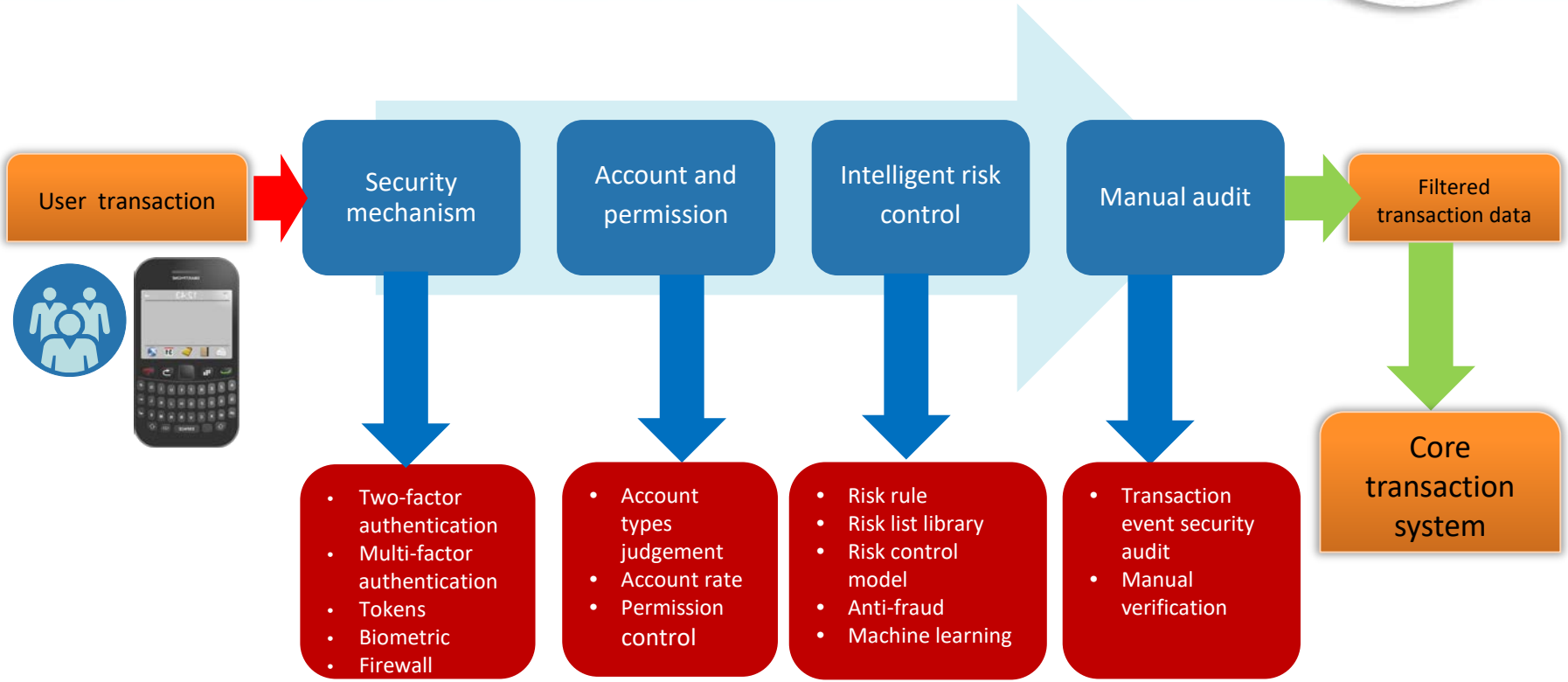
Best Practice – Anti-Fraud 3



Scenario: Transaction IP address change in short time for one person with one account.
First transaction IP address in China.
Second transaction IP address in USA.
Cause: Account information has been stolen or used proxy.
Solution: 1. Block transaction directly
2. Manual verification
3. Deep analysis/Model

Email:stevenchen2081@gmail.com

Transaction Security Control Stream



Email:stevenchen2081@gmail.com

Mobile Payment Challenge—Method Selection

- Which is more secure?
  - NFC & QR code (Two principles)
    - Transaction size?
    - User experience?

NFC VS QR code ?

Method	Security Authentication mode	Security Control	Reference Standard	Main Risk Scenarios
NFC	• Security SE • Security chip • Password	• Small amount transaction(no password and signature) • Backend quota one day one account	• GSMA Organization • ECMA Organization	• Lost device
QR code	• Encrypted URL • Security software	Transaction amount control one day with one account<500 CNY	China UnionPay has independent QR code standard and ecosystem, “EMVCo QR Code Specification for Payment Systems: Consumer Presented Mode 1.0”	• Malware • Phishing

URL:https://www.emvco.com/emv-technologies/qrcodes

Email:stevenchen2081@gmail.com

Mobile Payment Challenge-Privacy Protection

- What kind of data should be protected
  - China Cyber Law
  - GDPR
  - Reference to law and standard, such as 《Privacy Act》
  - Other sensitive data
- What methods are used to protect data?
  - DLP
  - Reference to PCI-DSS
  - Encryption is necessary, ID number

Mobile Payment Challenge – Smart Device

- Various payment methods
  - i.e. wearable device payment

- More complicated ecosystem
- More interfaces
- More dimensional attacks
- More risk points

Home › Security

NEWS

Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture

Reference: csoonline.com

Conclusions

- Identification authentication is the key factor for mobile payment security.
- New authentication technology does not mean that it is more secure.
- Pay more attention to privacy protection.
- Accumulating bad samples is the key to building a risk control model.
- Machine learning will become good solution to against mobile payment attack in the future.
- Rules and risk control models must be worked together now.

Poll the Audience

- Session ID:MBS-F02
- What other security topic you want to know in terms of mobile payment in the future?
  - A-Architecture/New Technology
  - B-Development/App
  - C-Anti-Fraud/Compliance

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3806

THANK YOU

Email: stevenchen2081@gmail.com
Twitter: @stevenchen2081
WeChat:

Follow Aaron Turner on LinkedIn:

https://www.linkedin.com/in/aaronrturner/