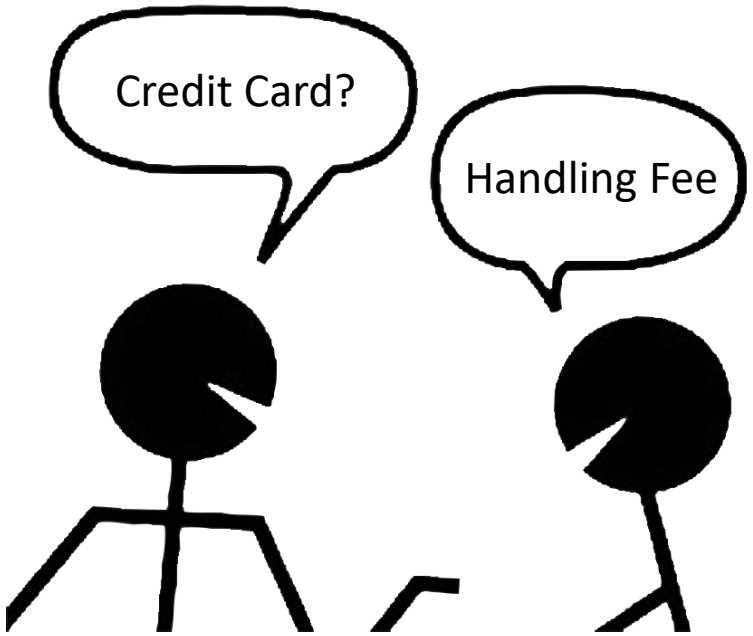
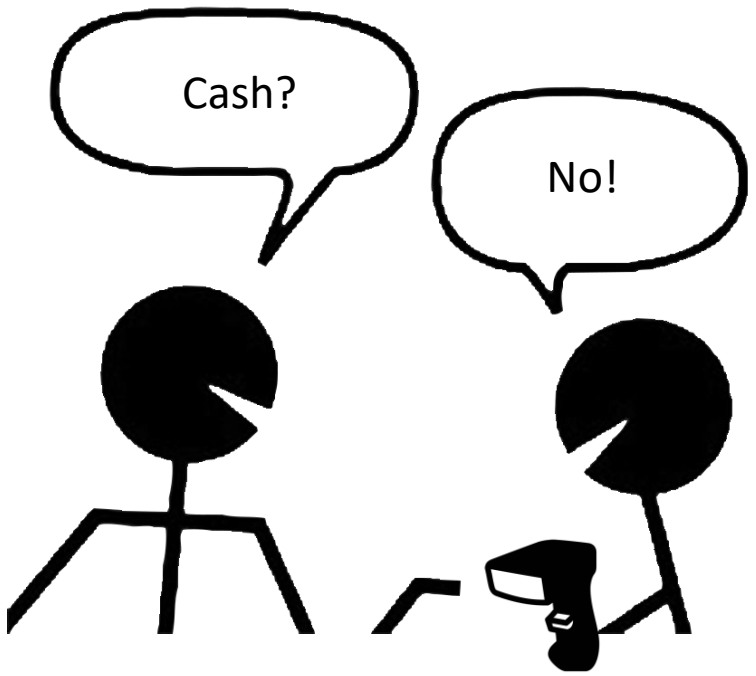
All Your Payment Tokens Are Mine: Vulnerabilities of Mobile Payment Systems

Speaker: Zhe Zhou, Fudan University, zhouzhe@fudan.edu.cn

Xiaolong Bai, Xiaofeng Wang, Zhou Li, Xianghang Mi, Nan Zhang, Tongxin Li, Shi-Min Hu, Kehuan Zhang

Mobile payment is so popular!



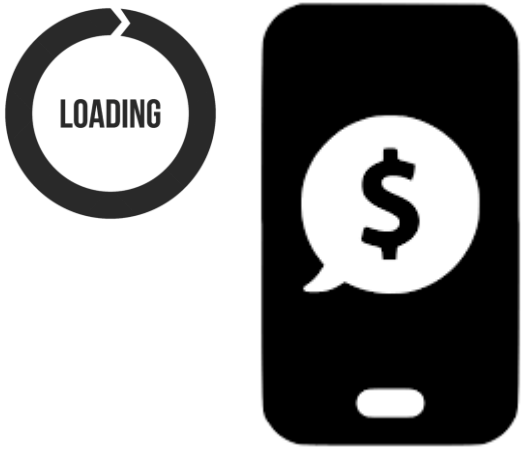


Mobile payment is so popular!

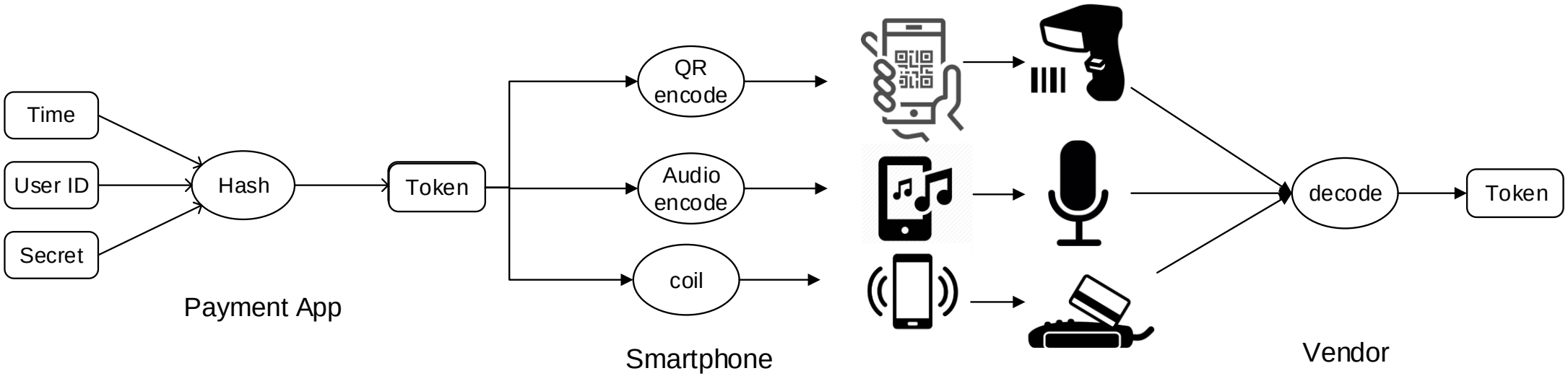
- 16.7 trillion USD transactions solely in China 2017
- China (including HK, Taiwan), India, USA, …
- Restaurant, Taxi, Shopping, …
- Financial Co., Internet Co.

Mobile phone needn’t network

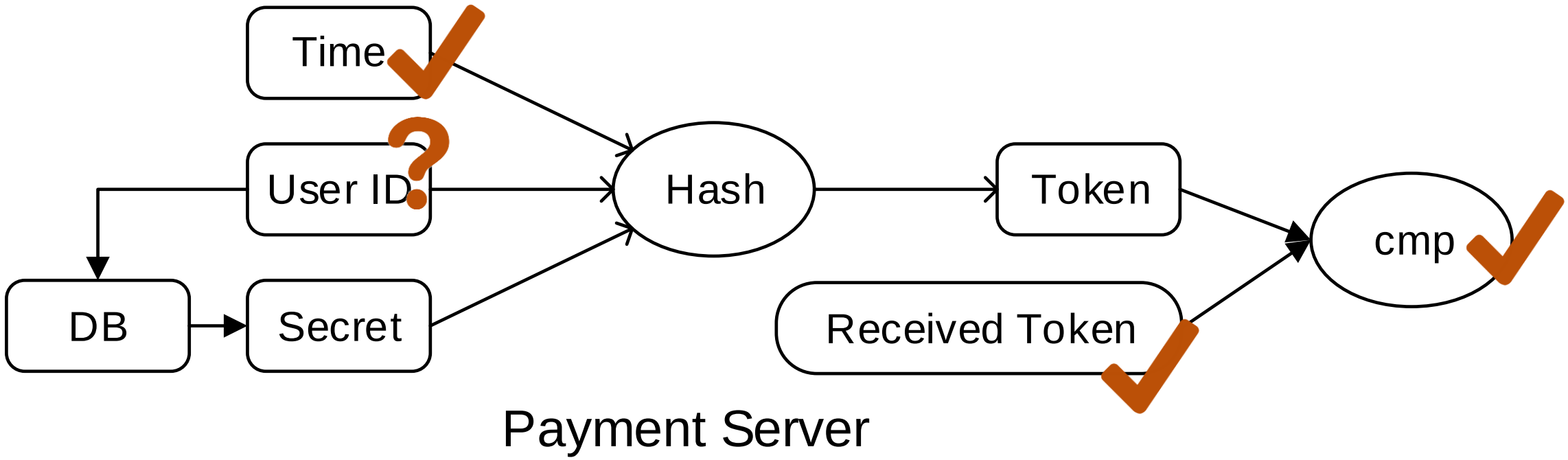
- A lot of transactions happen indoor, where cellular is poor.
- Rapid response.



Offline payment schemes



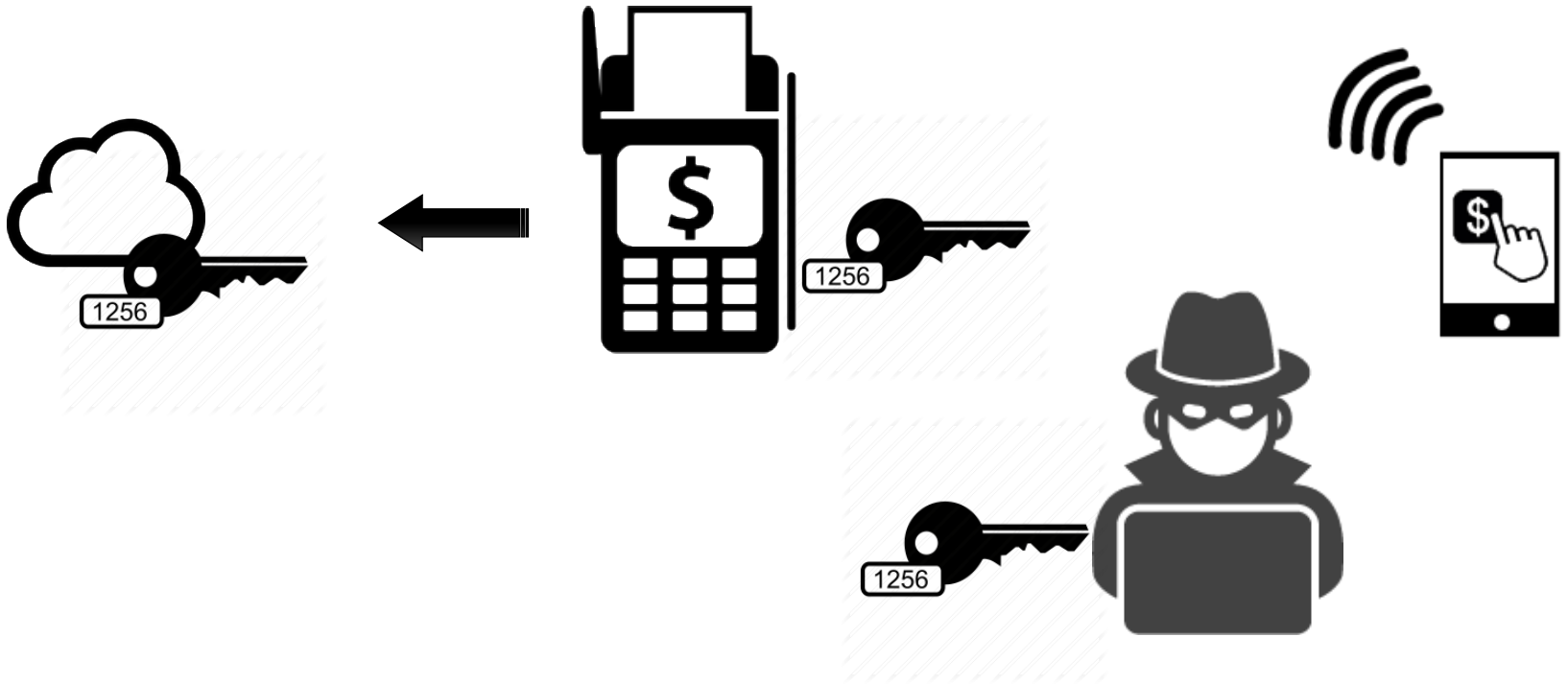
Offline payment schemes



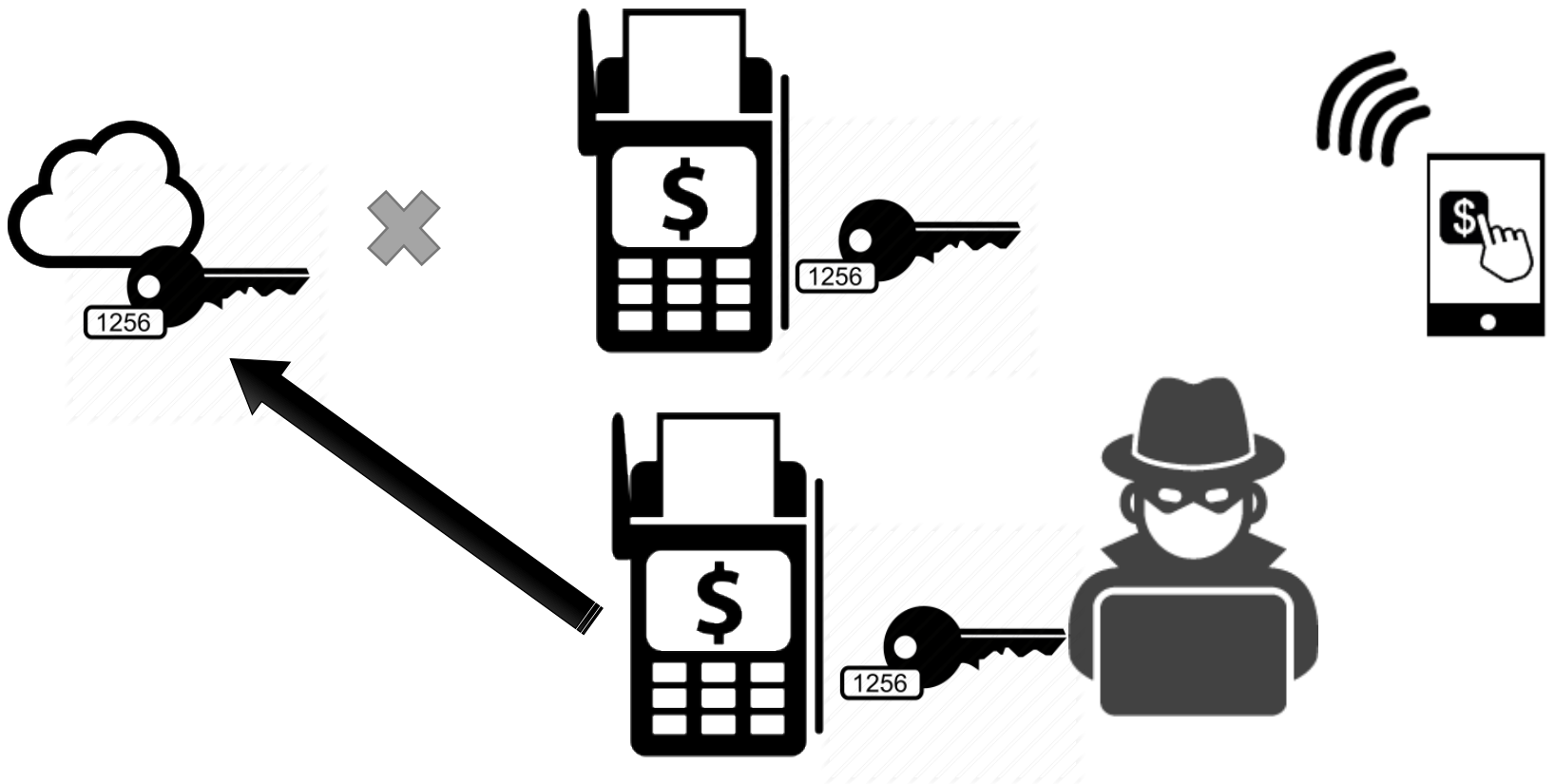
Security weak points

- Token transmission in broadcast channel.
  - No encryption during transmission.
  - It can be sniffed.
- Token is not bound with specific transaction.
  - A sniffed token can be spent at another place.

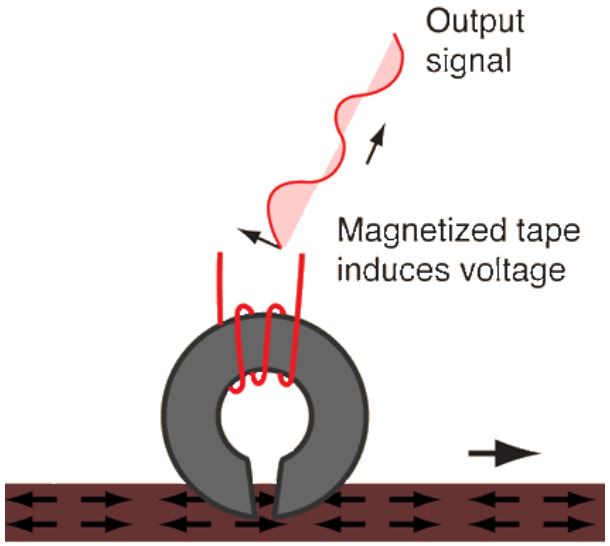
Security is not that bad

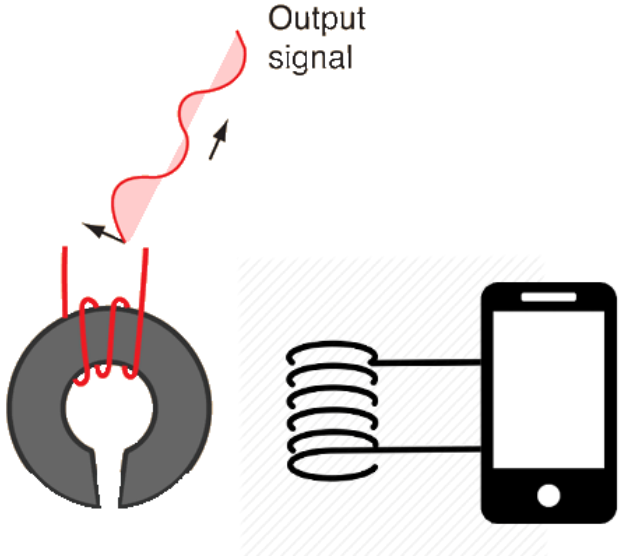


Our attacks



MST based mobile payment

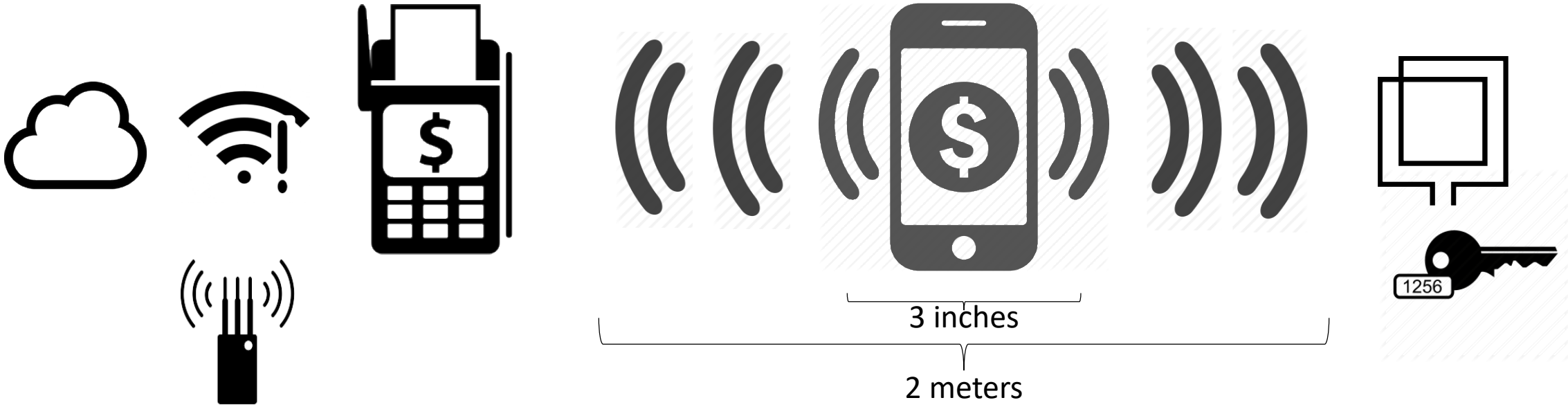




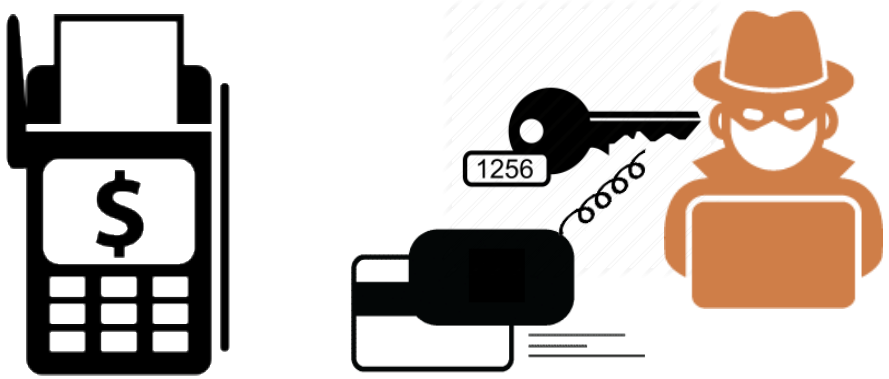
SAMSUNG

MST based mobile payment

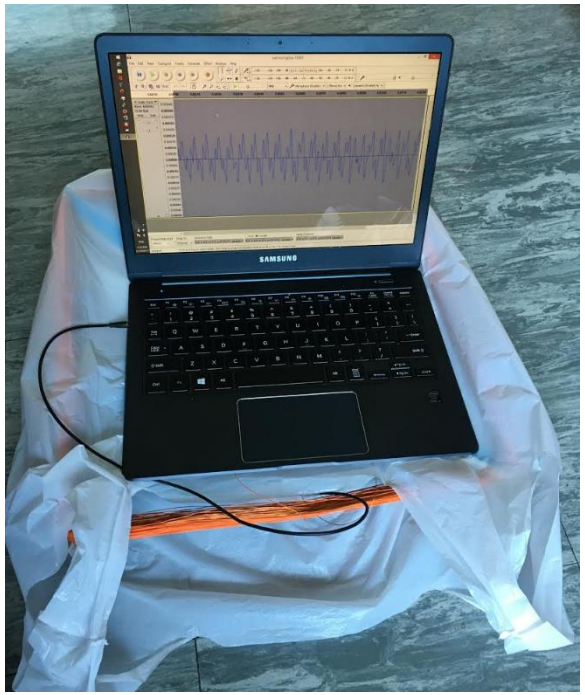
Attack MST



Attack MST

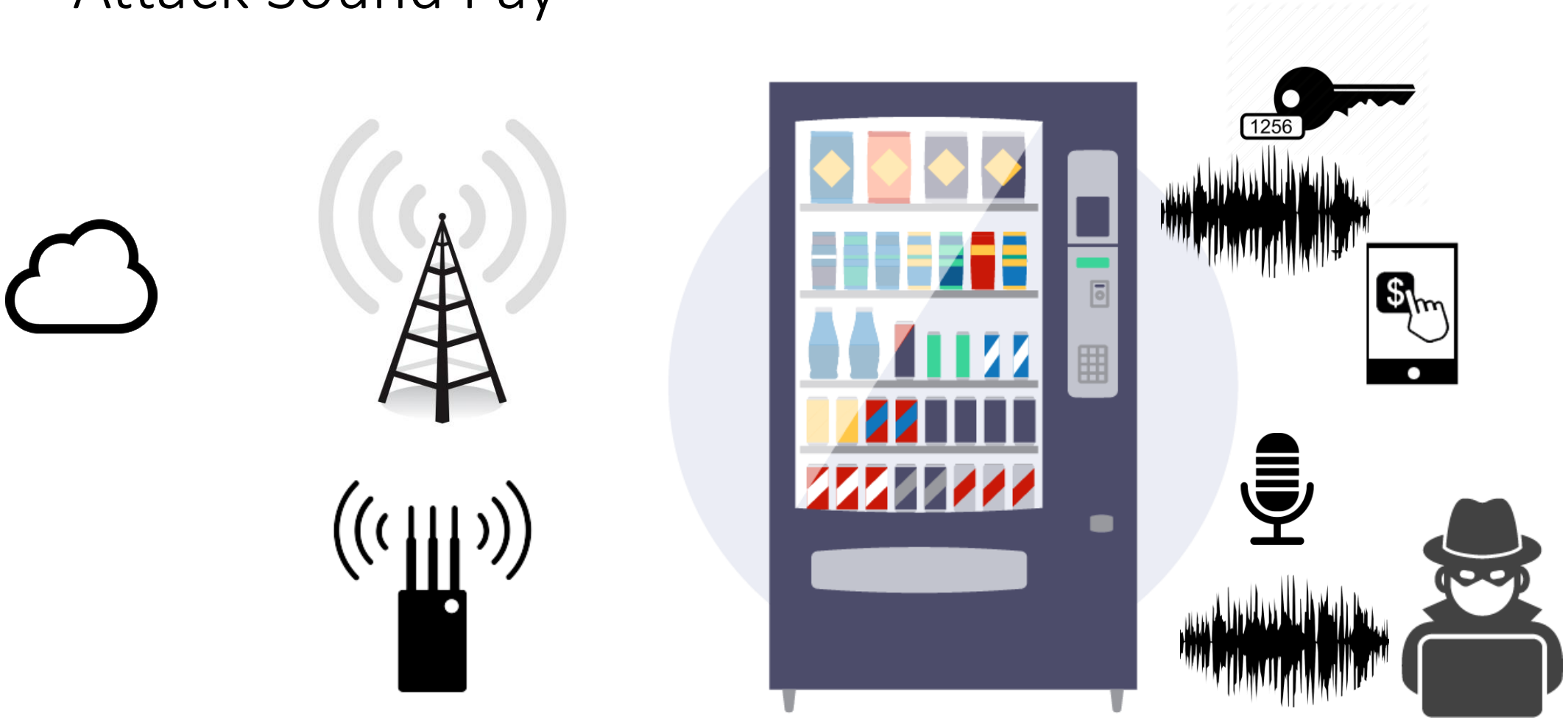


Devices used to attack MST

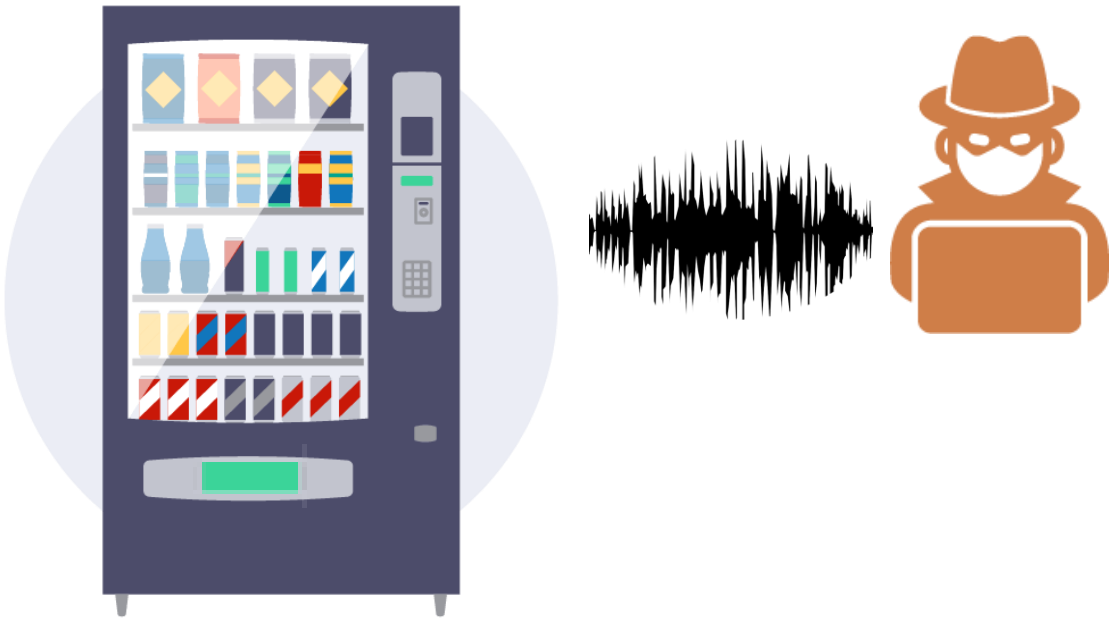


Sound Pay

Attack Sound Pay



Attack sound pay



QR code payment

- An extremely popular payment method.
- Payment Mode
  - B2S mode: A phone scans QR code printed on a paper to pay.
  - B2L mode: A phone presents QR code under POS scanner to pay.

Attack QR code payment, sniffing

Attack QR code payment, interrupting

- A malware a draw a white block.
- To prevent the code from legally recognized.
  - Positioning mark is critical for decoding.
  - POS machine can no longer decode the QR code.
- The sniffed QR code token is kept alive.
  - Attackers spend the token during the period.

Bonus attack

- Payment QR code is meant to be sensitive.
- But can also be used as **name card for transfer**.

Bonus attack, token sniffing

Payee, victim

Payer, infected

Quit? Token will be consumed.

Stay? User will notice.

Bonus attack, token protection

Payee, victim

Payer, infected

Initiate a Bluetooth pairing.
Then quit.

Bonus attack, token protection

Payee, victim

Payer, infected

A window **flashes** in victim's phone.
Some hundreds of ms.
Normal transaction goes on.

Remedy

- Report the attack to the service provider (the No.1 provider in China).
- The service provider revoked payment QR code as name card.

Lessons from the attacks.

- Payment token is so sensitive.
- Token should be bound to a transaction when being generated.

Q&A

- Thank you for your time.