Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment

-- Xiaolong Bai¹, Zhe Zhou²*, XiaoFeng Wang³, Zhou Li⁴, Xianghang Mi³,
Nan Zhang³, Tongxin Li⁵, Shi-Min Hu¹, Kehuan Zhang²

¹Tsinghua University, ²The Chinese University of Hong Kong
³Indiana University Bloomington, ⁴IEEE Member, ⁵Peiking University

*Alphabetically Ordered Authors
Mobile Payment – A Convenient Life Style

• Mobile payment is everywhere.

• Over 5 Trillion US Dollar Transactions.
Offline Mobile Payment

• A Mobile Payment Method Without Network.
  • Mobile phone does not need network.
  • POS machine must be connected.

• Advantages.
  • Short delay.
  • Avoid poor network connection inside rooms.

• Simple to use.
  • No need to enter password
  • Simple approach a phone to POS.
Offline Mobile Payment Working Flow

- Hash value inside token.
- Security based on the synchronized secret key.

![Diagram showing the working flow of mobile payment offline.](image-url)
Security Guarantees

• Through hashing, a token is bonded to
  • The time when being generated.
  • The user ID.
  • It cannot be **forged** without the synchronized secret.

• Tokens are hard to sniff.
  • Token transportation is designed to be distance bonded.

• Even if a token is sniffed.
  • A token, once received by the provider, is invalidated immediately.
  • A token is only valid in a short period of time.
Assumption: Passive Adversaries

- Passive attackers are already defended, because tokens, once sniffed, are also received by the provider, is invalidated immediately.
Break it with an active adversary

• But it is vulnerable to an active adversary!
Attacks against Offline Payment

• STLS Attacks.
  • Synchronized Token Lifting and Spending.

• Steps
  • Acquire a live token.
  • Prevent it from being legally used.
  • Spend it at another place, before it expires.

• Targets
Samsung Pay
Known Attacks against Samsung

- Previous paper sniffing and replaying Samsung pay tokens.
  - Assumption: Passive attackers.
- Legal transaction is not interrupted.
- The sniffed token is not alive.
- Users are still enough secure.
STLS Attack against Samsung Pay

- Assumption: Active Attackers.
- Standing close to the POS, can jam the network.
STLS Attack against Samsung Pay

- Token replay.
Devices to launch the attack
Sound Pay
Attacking Sound Pay – Adversary Model
Attacking Sound Pay – Sniffing and Jamming
Attacking Sound Pay – Colluder Side
STLS Attacks – QR Pay

• An extremely popular payment method.

• Payment Mode
  • B2S mode: A phone scans QR code on a paper to pay.
  • B2L mode: A phone presents QR code under POS scanner to pay.
Adversary Model – QR Pay

• Payer’s phone is infected with attacker’s malware.
• The malware has the front camera privilege.
  • For sniffing.
• The malware can display a floating window.
  • To prevent tokens from being legally used.
STLS Attacks – QR Code Sniffing
Prevent Legal Scanning

• 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.
P2P Mode Attacks

• What if you use iPhone instead of Android Phone?
  • iPhone does not support background front camera photo shooting.
• What if your phone is not infected?
• P2P mode: A phone scans QR code on another phone to pay.
• The QR code can also be used in B2L mode to pay to the merchants.
P2P Mode Attack Adversary Model

- The victim (payee) is not infected.
- The payer is infected with attacker’s malware.
  - Has an exactly same UI with legal payment app.
  - Will be used to sniff the QR code token.
- The victim has turned on the Bluetooth.
  - Can be exploited by attacker to keep the token alive.
STLS Attacks – QR Code Sniffing
Preventing sniffed QR code from legal scan
STLS Attacks – Alipay’s Action

• Alipay ceased P2P transfer through QR code in this Feb.
• Face to face money transfer moved to printed QR code.
  • Users get an exclusive QR code for receiving money after application.
POSAUTH, restrict the use of sniffed tokens

• Live token can be spent at anywhere, with the upper bound amount.
• Sniffed token cannot be spent remotely, once bonded to the POS ID.
POSAUTH

• Get the POS ID
  • By a front scan.
  • Hash it into token.
  • Token is bonded.

• No hardware upgrade.
Q&A

• Offline payment schemes only considered passive attackers.
• Active attackers can keep the sniffed token alive by interrupting the transaction.
• Attackers can spend the token before it expires.
Security Vulnerabilities

• A token is bond to
  • The time when being generated.
  • The user ID.
  • But **not** a specific transaction (Amount, Merchant ID, etc.).

• A live token can be spent by the attacker, once sniffed.
  • At anywhere.
  • With the upper bound amount.
STLS Attacks – B2L Mode Attacks

• The white block prevents QR code from being legally recognized.
• The font camera captures a picture containing the QR code.
• The background app can decode the QR code to get the token.
• The token can be spent at another place.