Poster: Analyzing Ground-Truth Data of Mobile Gambling Scams

Geng Hong∗, Zhemin Yang∗, Sen Yang∗, Xiaolin Du∗, Min Yang∗, Haixin Duan‡
∗Fudan University, ‡Tsinghua University
∗{ghong17, yangzhemin, syang15, xldu20, m_yang}@fudan.edu.cn, ‡duanhx@tsinghua.edu.cn

What's the mobile gambling scams?

Two Roles:
- Scammer
- Victim

Three Vectors:
- Social Engineering
- Gambling Scam Apps
- Payment Channels

Four Stages:
- Connection Establishment
- App Delivery
- Gambling Deposit
- Scamming

Based on a valuable dataset: **1,461 incident reports** and **1,487 scam apps**

The question of mobile gambling scams

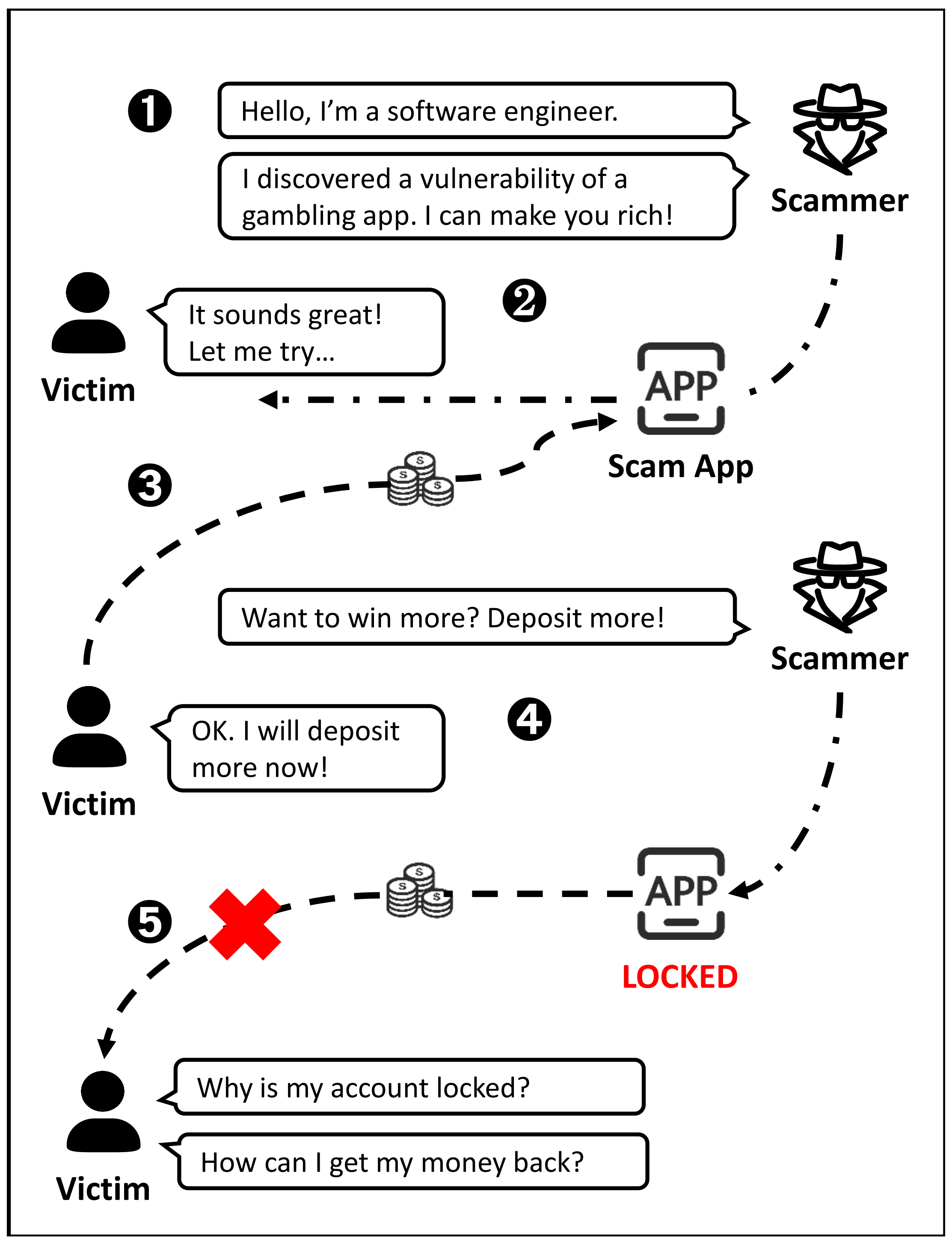
How does the scammer establish connection and earn my trust?

How does the scammer deliver a scam app to me?

Victim

How do I get lured to deposit money continually?

What is the logic of mobile gambling scams?



Hello, I'm a software engineer.

I discovered a vulnerability of a gambling app. I can make you rich!

It sounds great! Let me try…

Want to win more? Deposit more!

OK. I will deposit more now!

Why is my account locked?

How can I get my money back?

Operational Pipeline

Main Findings of the Study

- Reveal social engineering techniques used by miscreants via a qualitative analysis on 1,461 incident reports.
- Characterize both Android and iOS gambling scam apps, including their development frameworks, declared permissions, compatibility, and backend network infrastructure.
- Reveal that public online app generators have been abused to develop gambling scam apps.
- Uncover a new type of money mule-based payment channel and measure its revenue.

Social Engineering Tricks

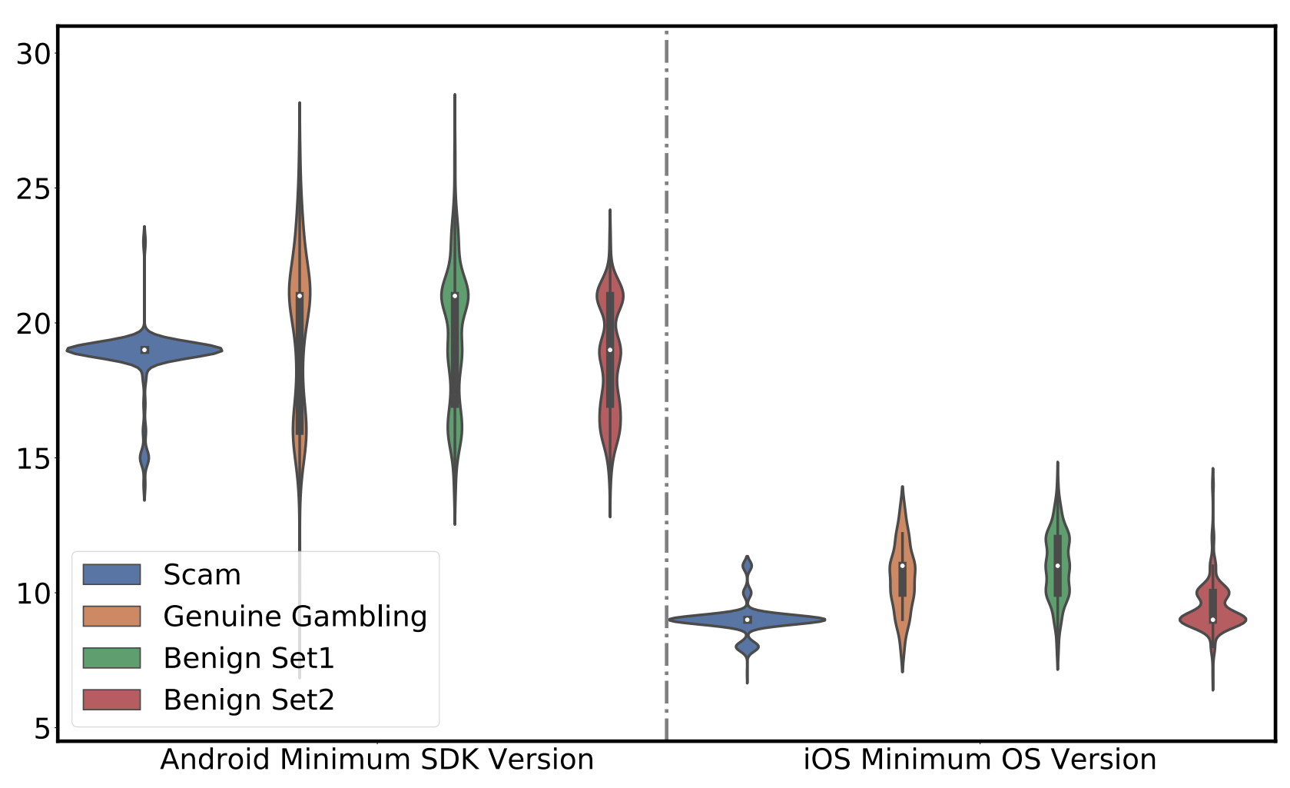
Scammer " When establishing connections with victims, I tend to palm myself off as holding roles with high social statuses or intimate relationships."

" I happily chatted with him (the scammer), and soon he became my boyfriend. He informed me that there was a quick way to make money in mid-May... " **Victim**

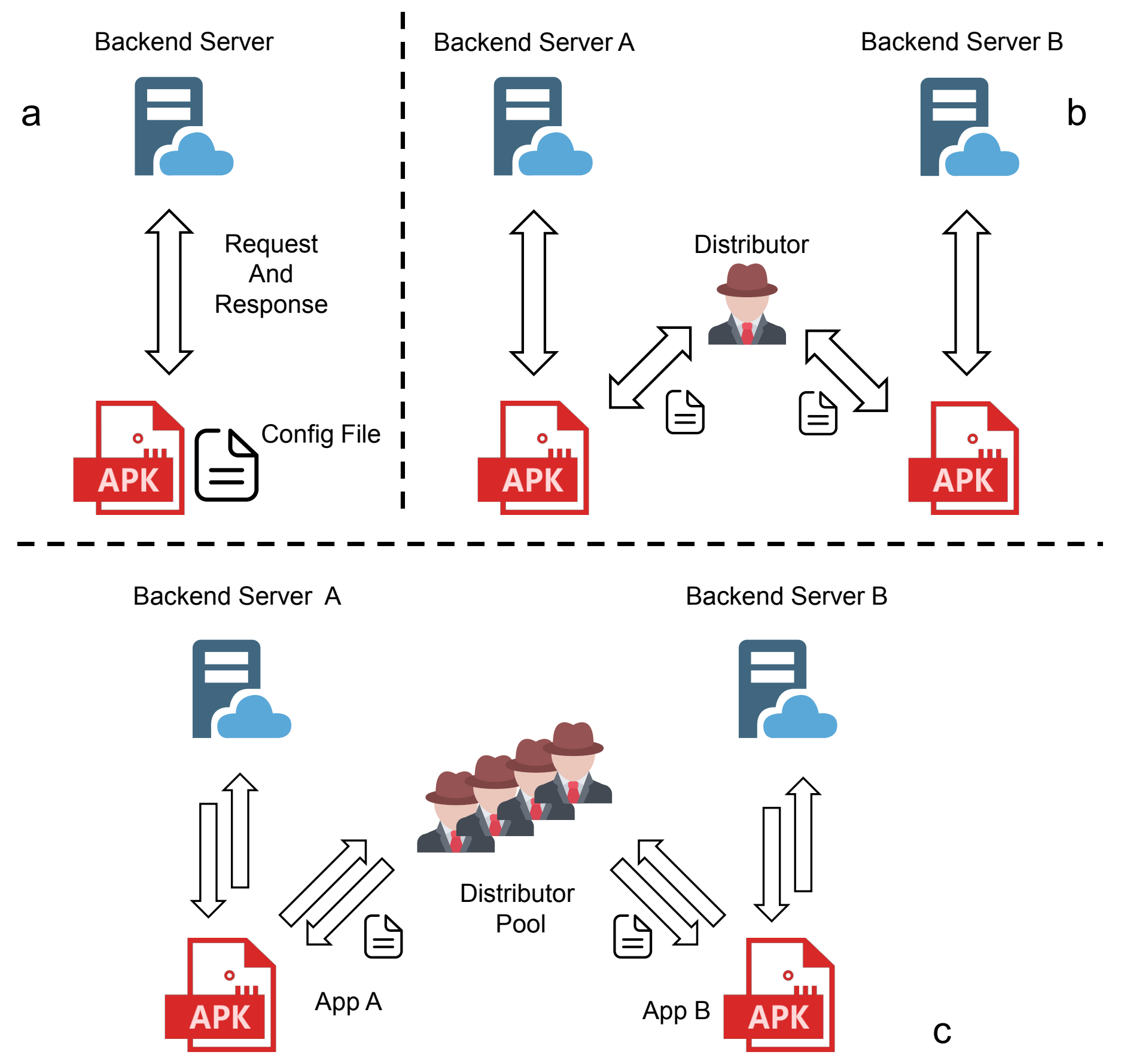
Scammer " To ensure victims make deposits, I tend to leverage incentive strategies instead of imposing psychological pressures. "

" ...the customer service said that my bank card number was incorrect... Only with one more deposit could I change the card number. " **Victim**

Apps empower scamming attacks



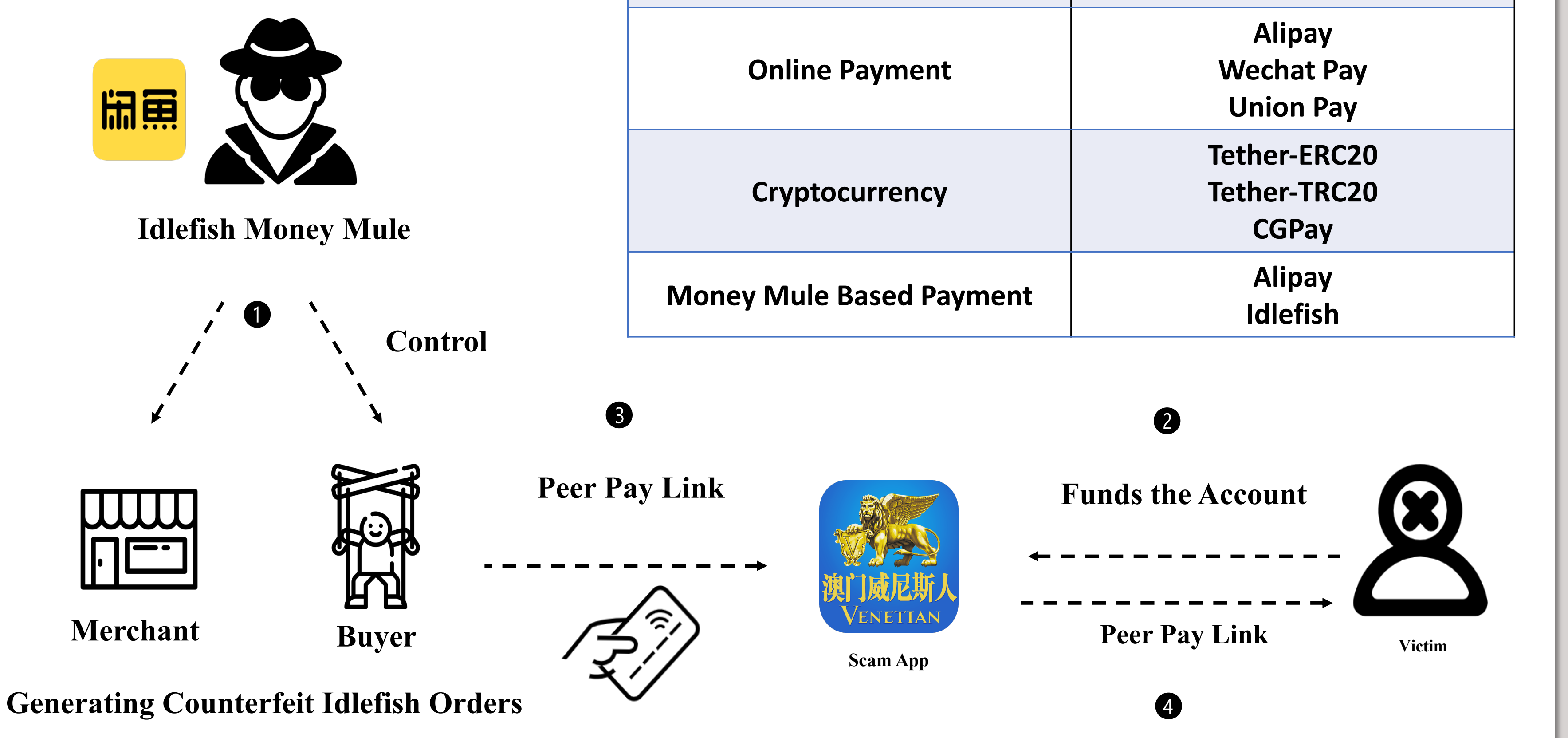
Development SDK version distribution



Typical backend network architectures

Various Payment Instruments

Category	Sub Category
Bank Transfer	Direct Debit
Online Payment	Alipay Wechat Pay Union Pay
Cryptocurrency	Tether-ERC20 Tether-TRC20 CGPay
Money Mule Based Payment	Alipay Idlefish



The operational pipeline of Idlefish Money Mules

Poster: Analyzing Ground-Truth Data of Mobile Gambling Scams

Published Paper

Authors:
Geng Hong, Fudan University, ghong17@fudan.edu.cn
Zhemin Yang, Fudan University, yangzhemin@fudan.edu.cn
Sen Yang, Fudan University, syang15@fudan.edu.cn
Xiaolin Du, Fudan University, xldu20@fudan.edu.cn
Min Yang, Fudan University, m_yang@fudan.edu.cn
Haixin Duan, Tsinghua University, duanhx@tsinghua.edu.cn

Date: May 22-26, 2022
Venue:
43rd IEEE Symposium on Security and Privacy
Link: https://www.dropbox.com/s/m6w24wthtxl9clz/Gambling_Scam_camera_ready.pdf

Abstract

With the growth of mobile computing techniques, mobile gambling scams have seen a rampant increase in the recent past. In mobile gambling scams, miscreants deliver scamming messages via mobile instant messaging, host scam gambling platforms on mobile apps, and adopt mobile payment channels. To date, there is little quantitative knowledge about how this trending cybercrime operates, despite causing daily fraud losses estimated at more than $522,262 USD.

This paper presents the first empirical study based on ground-truth data of mobile gambling scams, associated with 1,461 scam incident reports and 1,487 gambling scam apps, spanning from January 1, 2020 to December 31, 2020. The qualitative and quantitative analysis of this ground-truth data allows us to characterize the operational pipeline and full fraud kill chain of mobile gambling scams. In particular, we study the social engineering tricks used by scammers and reveal their effectiveness. Our work provides a systematic analysis of 1,068 confirmed Android and 419 iOS scam apps, including their development frameworks, declared permissions, compatibility, and backend network infrastructure. Perhaps surprisingly, our study unveils that public online app generators have been abused to develop gambling scam apps. Our analysis reveals several payment channels (ab)used by gambling scam app and uncovers a new type of money mule-based payment channel with the average daily gambling deposit of $400,000 USD. Our findings enable a better understanding of the mobile gambling scam ecosystem, and suggest potential avenues to disrupt these scam activities.