# Large-Scale Invisible Attack on AFC Systems with NFC-Equipped Smartphones

**Fan Dang**[1], Pengfei Zhou[1, 2], Zhenhua Li[1], Ennai Zhai[3], Aziz Mohaisen[4], Qingfu Wen[1], Mo Li[5]

1 School of Software, Tsinghua University, China
2 Beijing Feifanshi Technology Co., Ltd., China
3 Department of Computer Science, Yale University, USA
4 Department of Computer Science and Engineering, State University of New York at Buffalo, USA
5 School of Computer Science and Engineering, Nanyang Technological University, Singapore

# Introduction



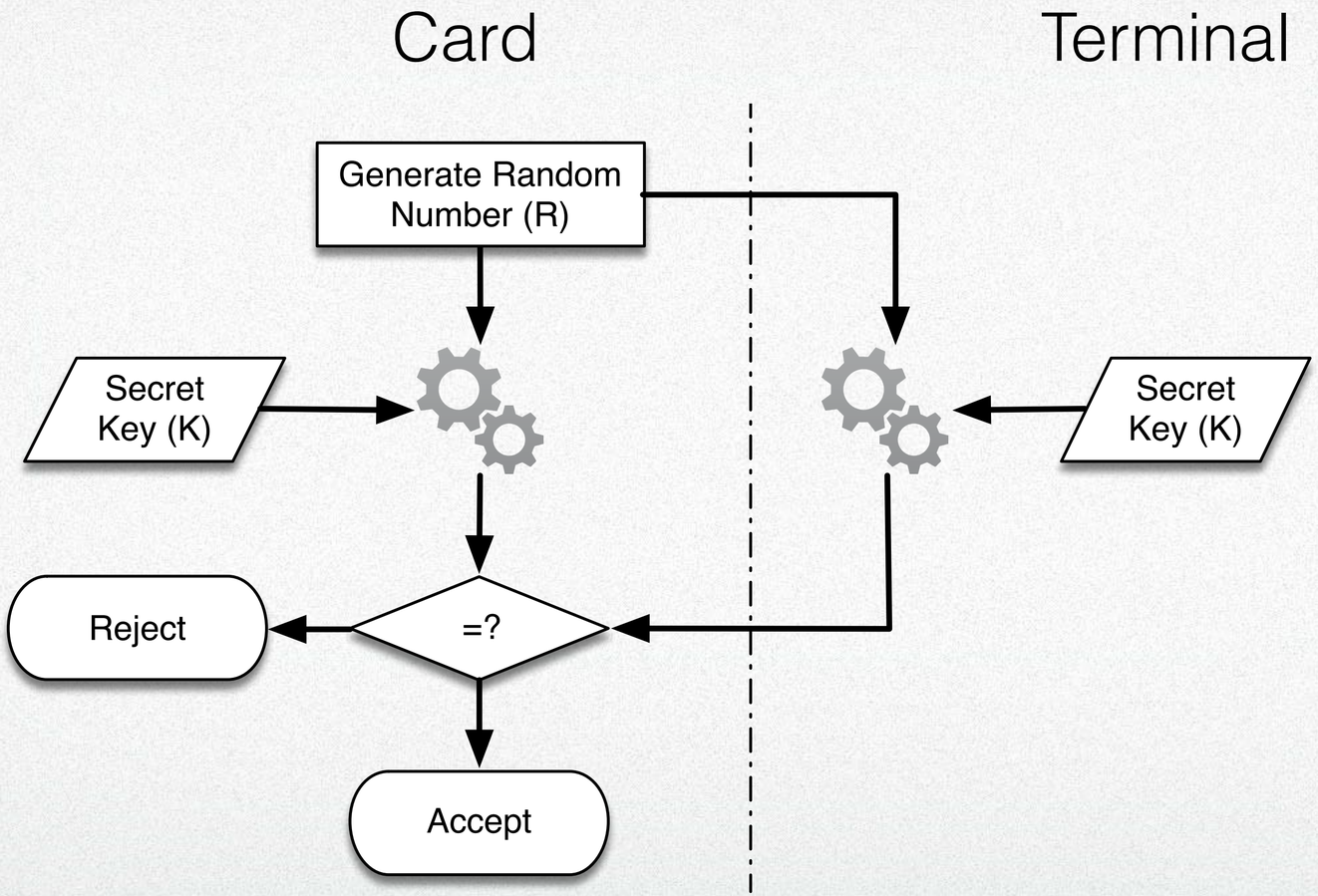
Automated Fare Collection (AFC) system

# Introduction

MIFARE Classic

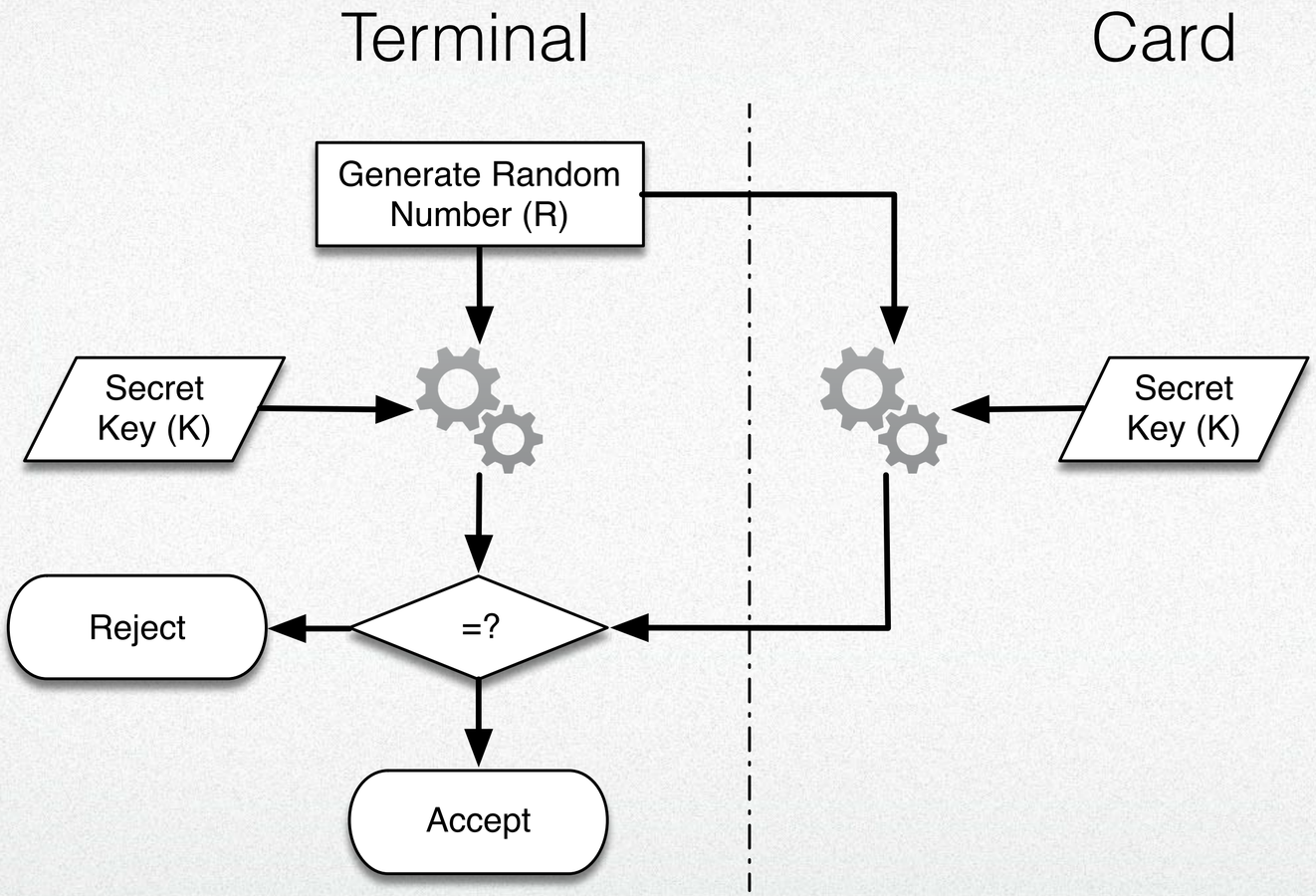
Processor Cards

# Introduction



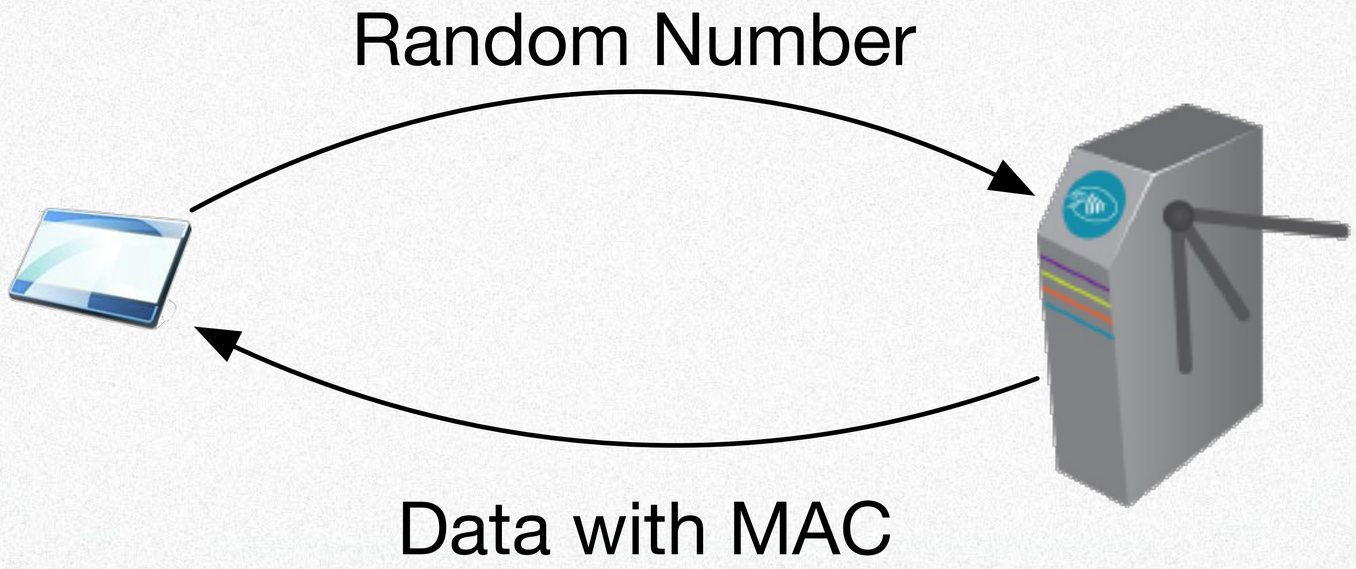

**External Authentication: a card verifies a terminal**

# Introduction




**Internal Authentication: a terminal verifies a card**

# Introduction




Message authentication code: MAC = Digest(*data*, rnd, key)

# Introduction

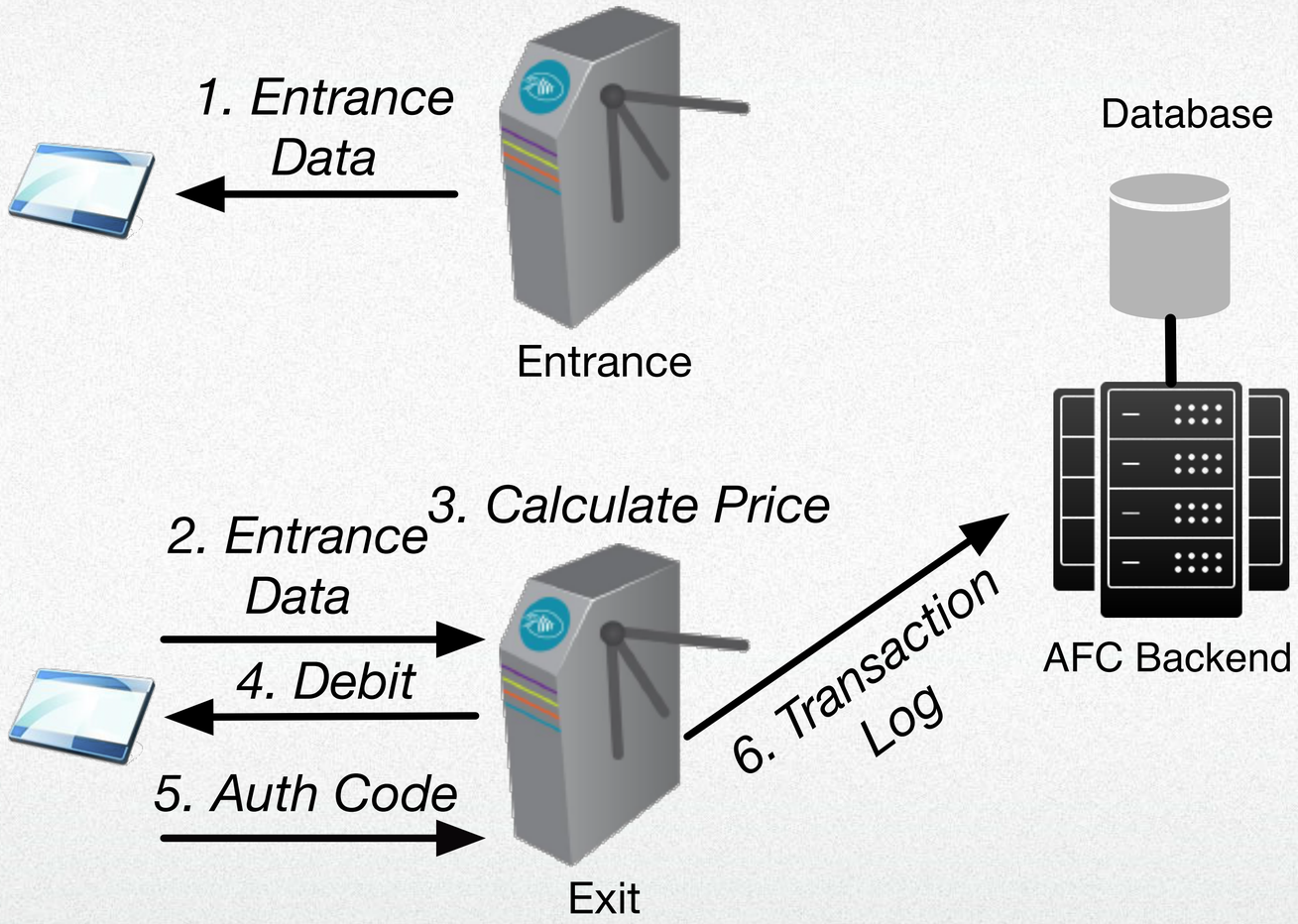
What is a possible flaw?

# Flaw

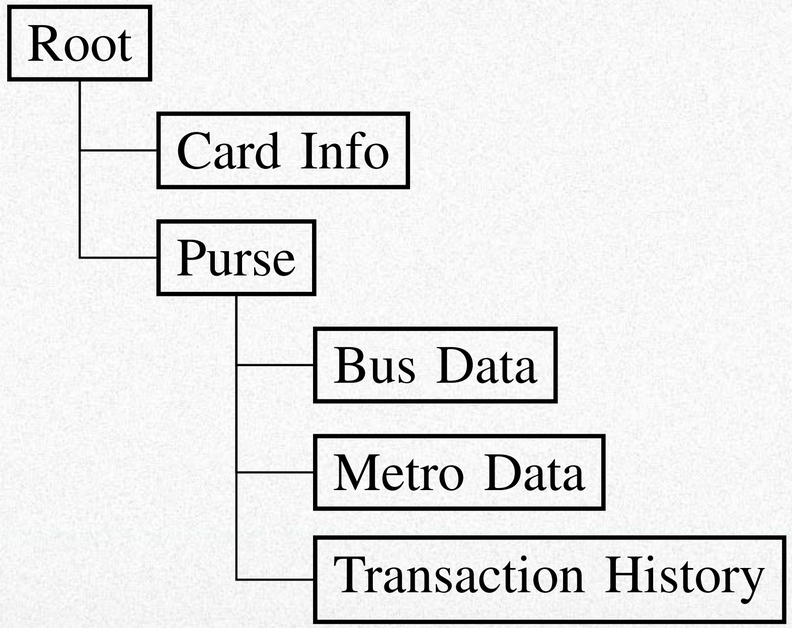
**City Traffic Card**

ISO/IEC 14443-4 based
Millions issued

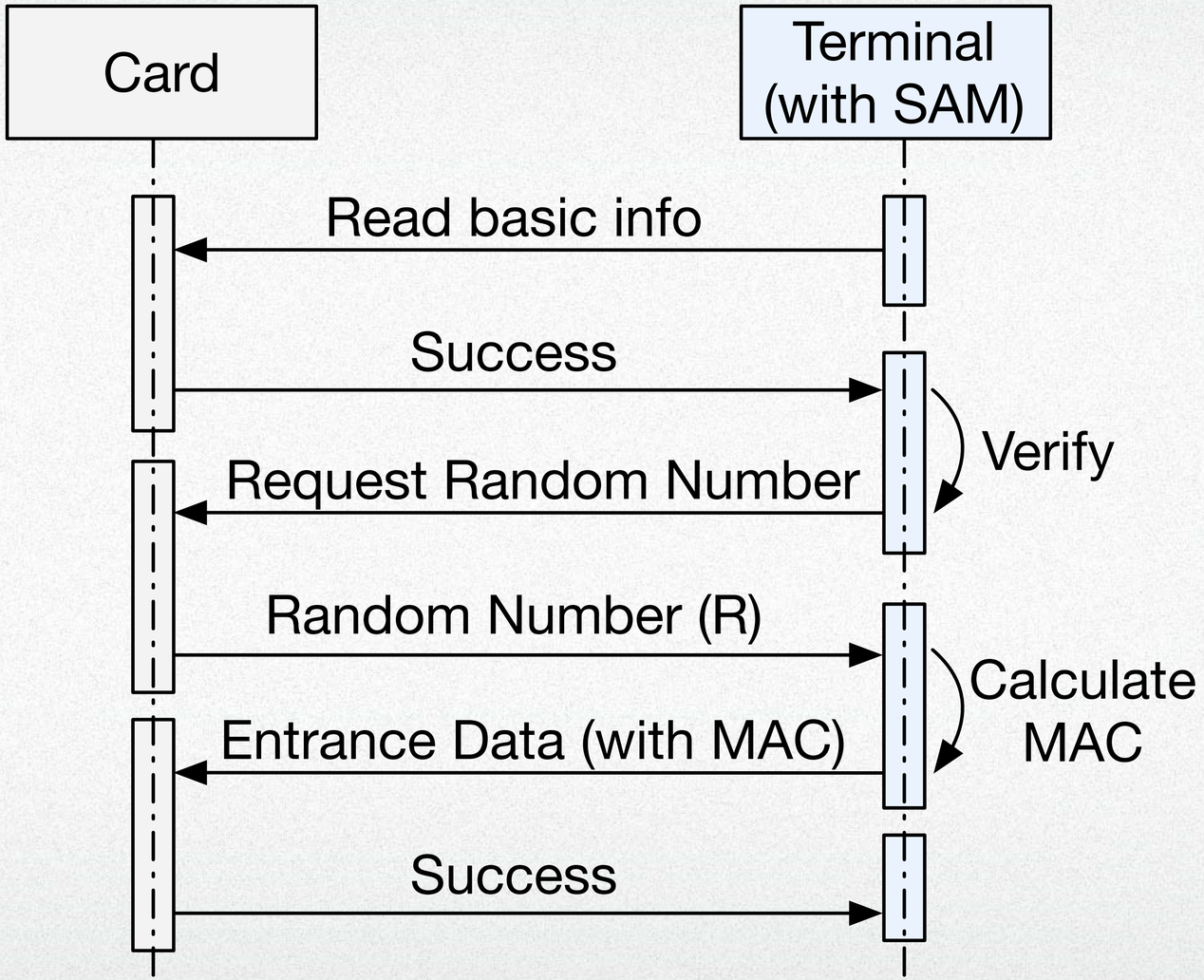
# Flaw


1. Entrance Data
Entrance
Database
2. Entrance Data
3. Calculate Price
4. Debit
5. Auth Code
6. Transaction Log
AFC Backend
Exit

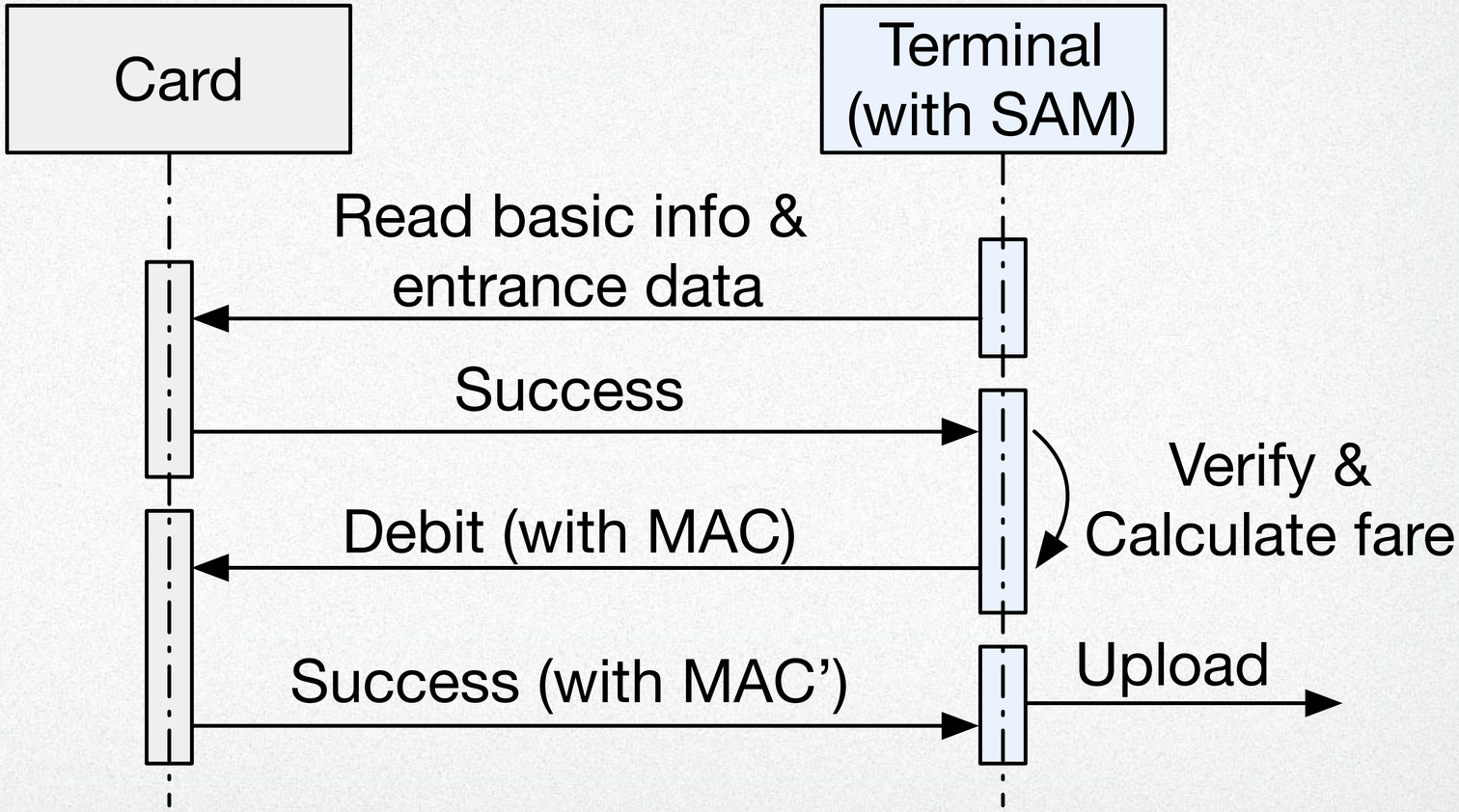
# Flaw


Root
Card Info
Purse
Bus Data
Metro Data
Transaction History

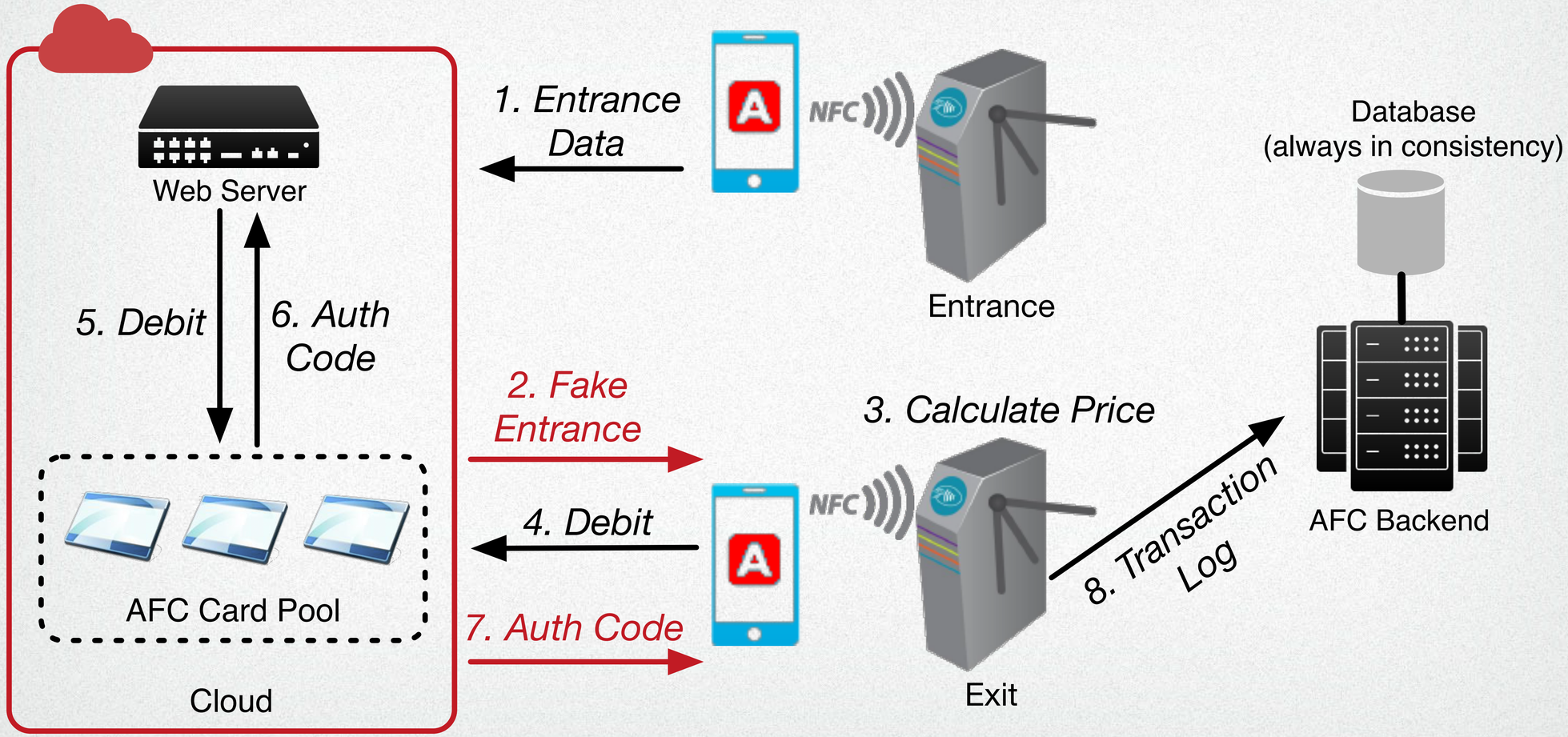
# Flaw


Card
Terminal (with SAM)
Read basic info
Success
Verify
Request Random Number
Random Number (R)
Calculate MAC
Entrance Data (with MAC)
Success

# Flaw


Card
Terminal
(with SAM)
Read basic info &
entrance data
Success
Verify &
Calculate fare
Debit (with MAC)
Success (with MAC')
Upload

# Attack model



# Tampering Entrance Data

1. Collecting entrance data
   We developed a lightweight app (different from LessPay app) to specifically collect data.
2. Obtaining data structure of entrance data

| # | Entrance Data | Enter Time | Metro Line | Station | Balance When Entering |
|---|---|---|---|---|---|
| 1 | 1512051417043D014C1D | 2015-12-05 14:17 | 4 | Station A | 75.00 |
| 2 | 151130113502080 1B009 | 2015-11-30 11:35 | 2 | Station B | 24.80 |
| 3 | 15112215225E1D01AC0D | 2015-11-22 15:22 | X | Station C | 35.00 |
| 4 | 15112009560A11016612 | 2015-11-20 09:56 | 10 | Station D | 47.10 |
| 5 | 151112200904010 15203 | 2015-11-12 20:09 | 1 | Station E | 8.50 |

3. Obtaining station information
   Reverse an app E-Card Tapper（e卡贴）
4. Tampering the entrance data
   Location based

# System Implementation

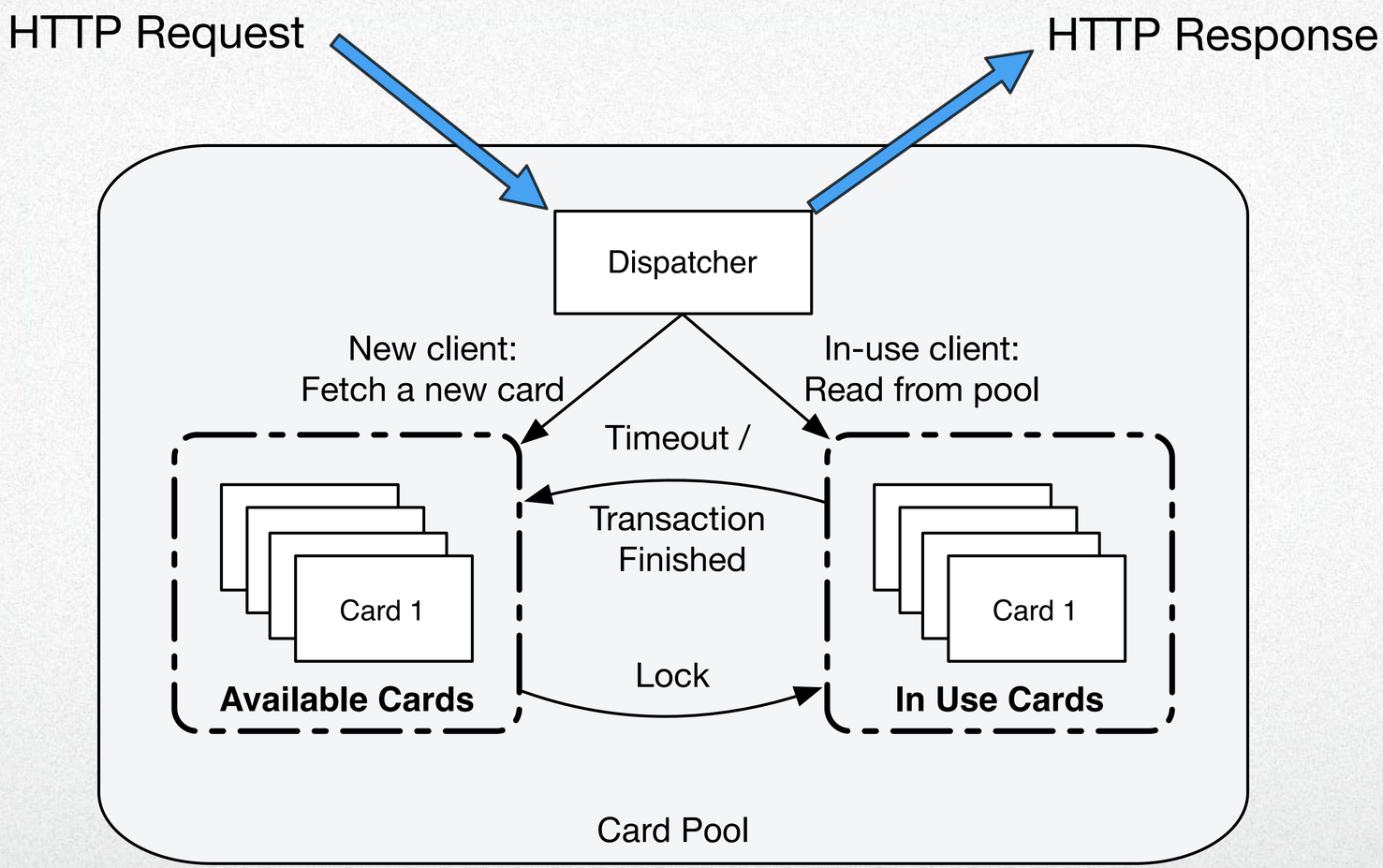
Server with 100Mbps network

5 ACR 122u readers with 5 CTC cards

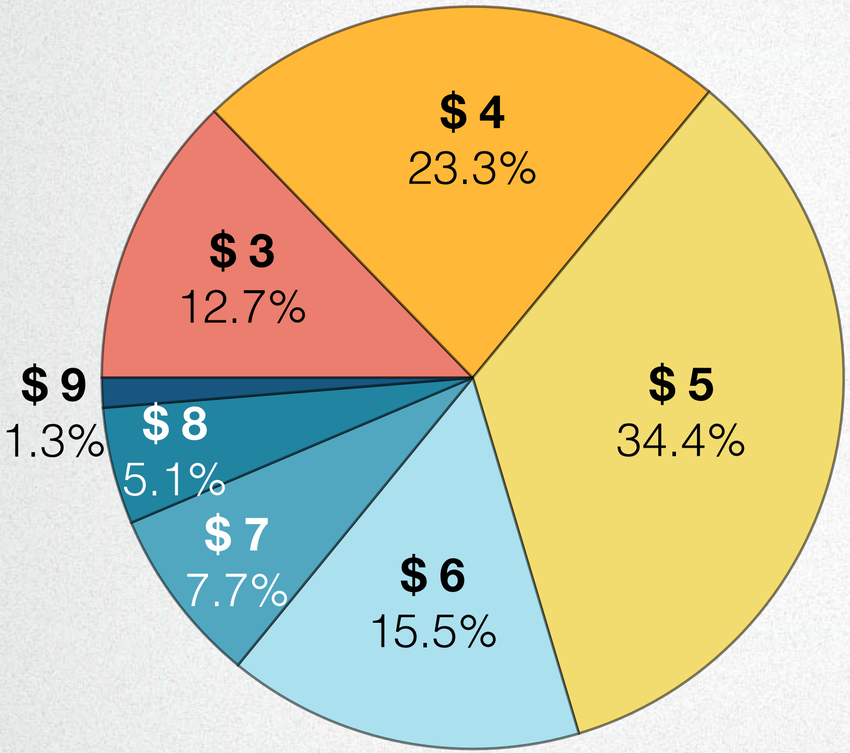
Cellphones:
- Samsung Galaxy S5
- Huawei Mate 7
- Moto XT1095
- LGE Nexus 5X

MNOs:
- LTE-TDD
- LTE-FDD

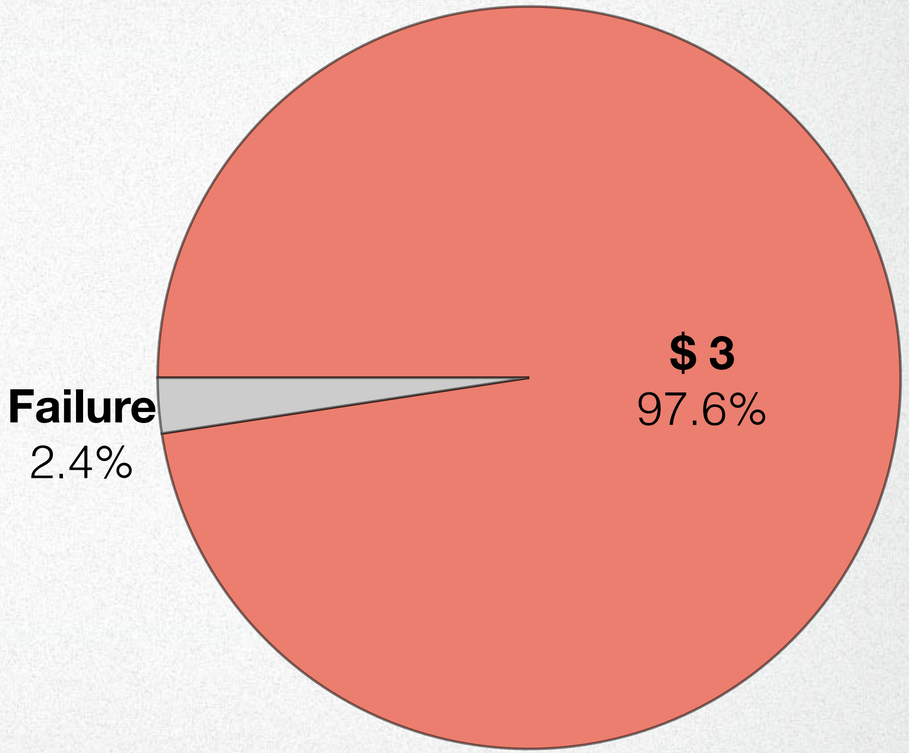
# System Implementation



# Performance

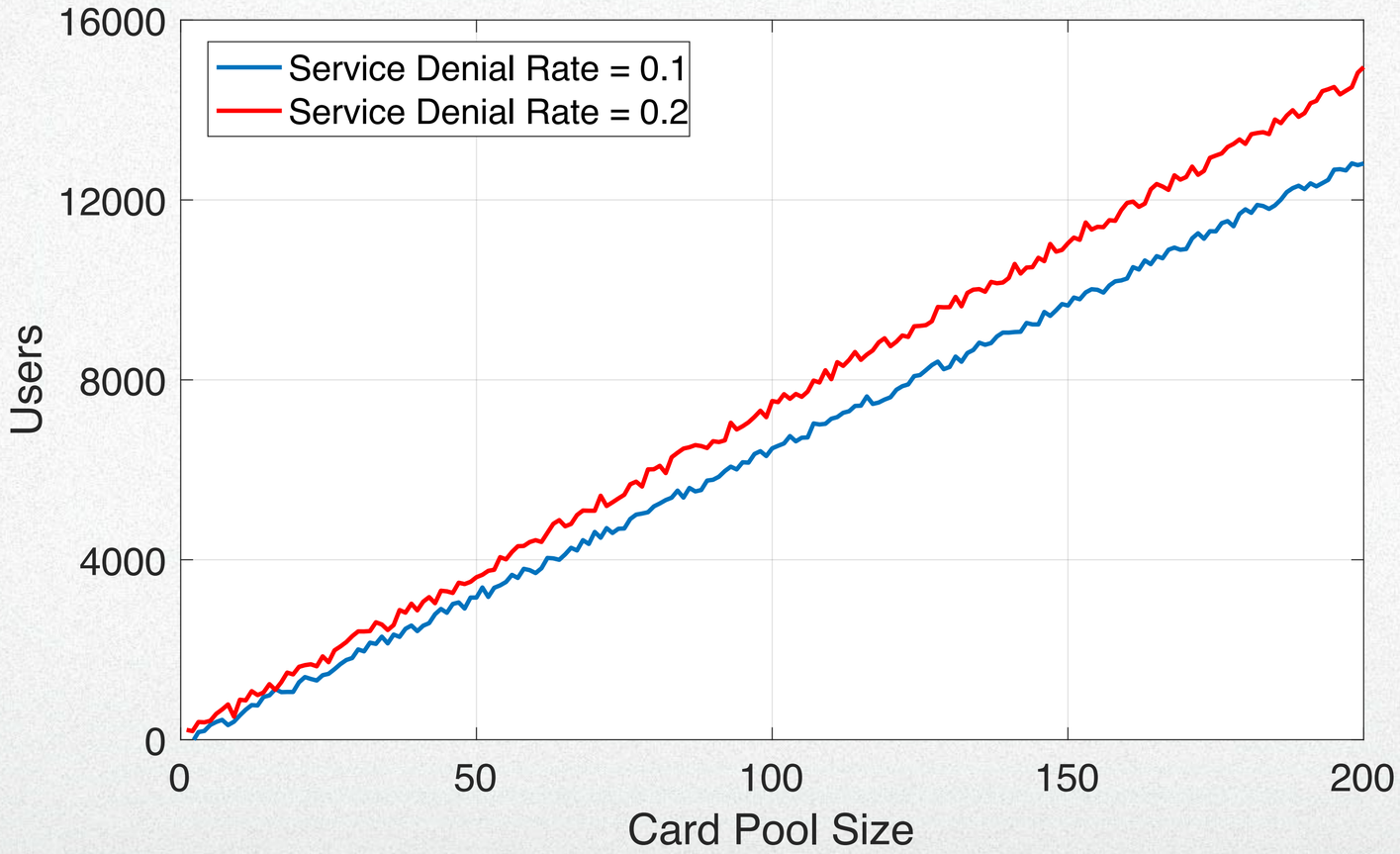



Users should pay the fares from $3 to $9.

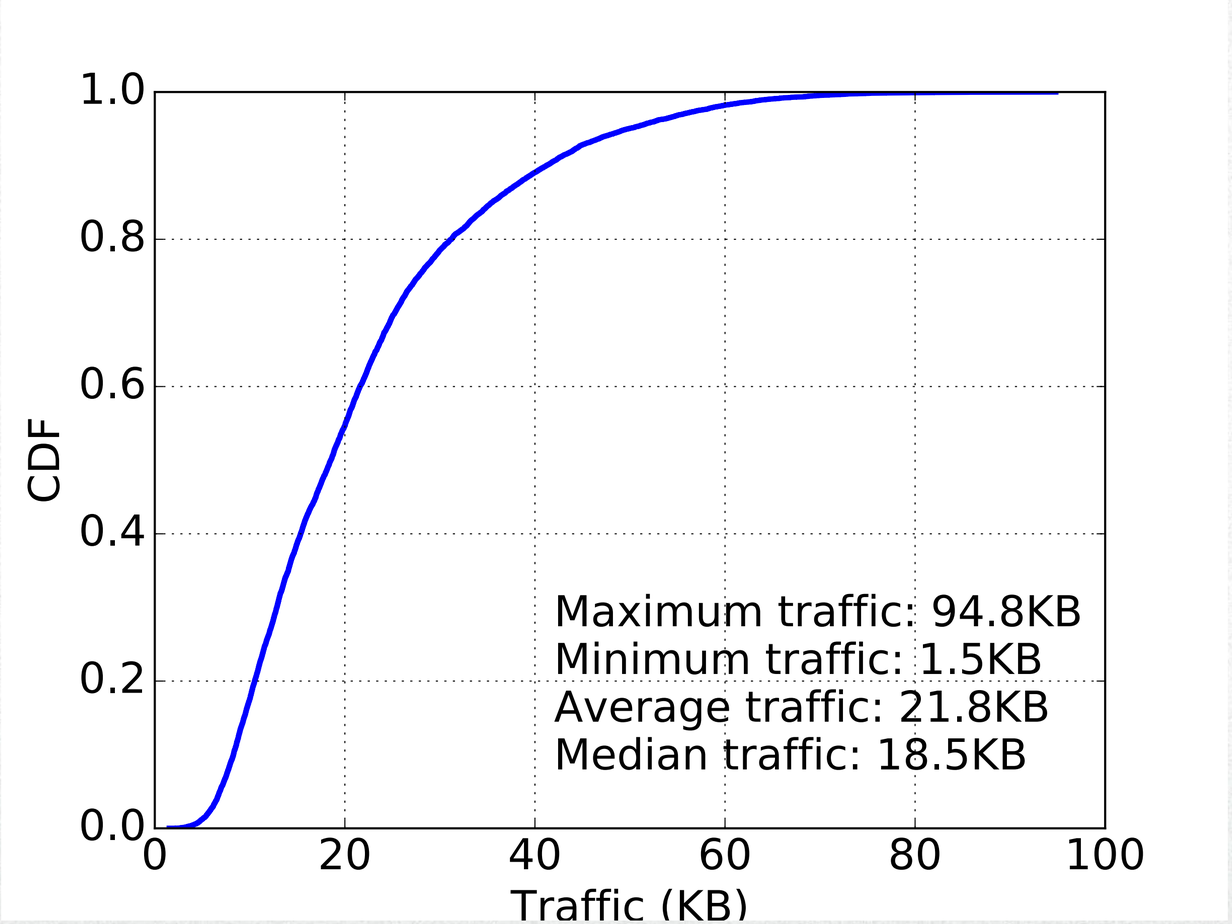



Except for 2.4% failures, users actually paid only $3.

# Performance



# Performance



# Countermeasures

1. Switch to online transactions
2. Encrypt/sign data
3. Use secure messaging in ISO/IEC 7816-4
4. Detect relay attack

# Conclusions

1. We construct a large-scale invisible attack on AFC systems with NFC-equipped smartphones, thus enabling users to pay much less than actually required.
2. We develop an HCE app, named LessPay, based on our constructed attack.
3. We evaluate LessPay with real-world large-scale experiments, which not only demonstrate the feasibility of our attack, but also shows its low-overhead in terms of bandwidth and computation.


Q&A