NFC-enabled Attack on Cyber Physical Systems: A Practical Case Study

Fan Dang[1], Pengfei Zhou[1, 2], Zhenhua Li[1], Yunhao Liu[1]

1 School of Software, Tsinghua University, China
2 Beijing Feifanshi Technology Co., Ltd., China

Outline

01 **Introduction**

02 **Prior work**

03 **Our contributions**

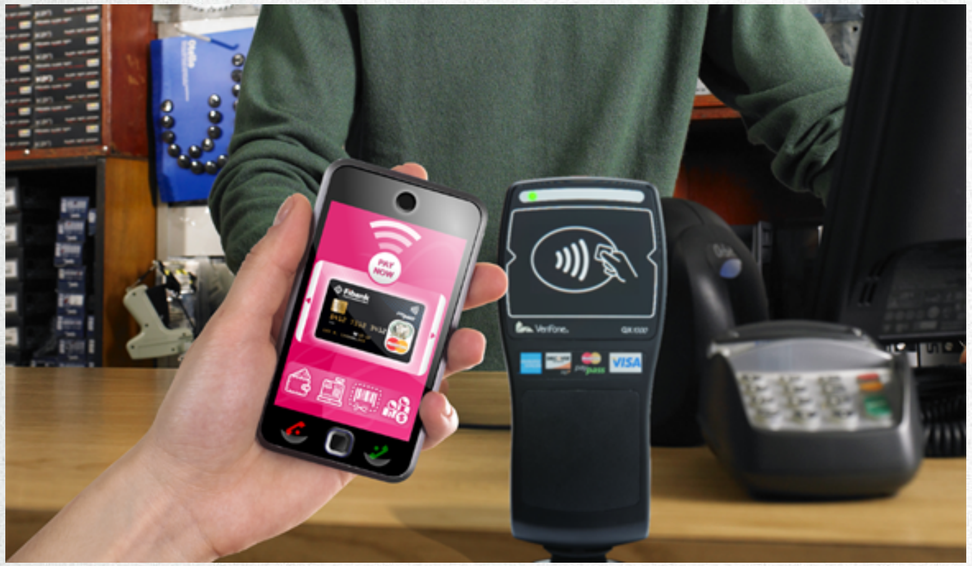
04 **Discussion and conclusions**

Introduction

MIFARE Classic

Processor Cards

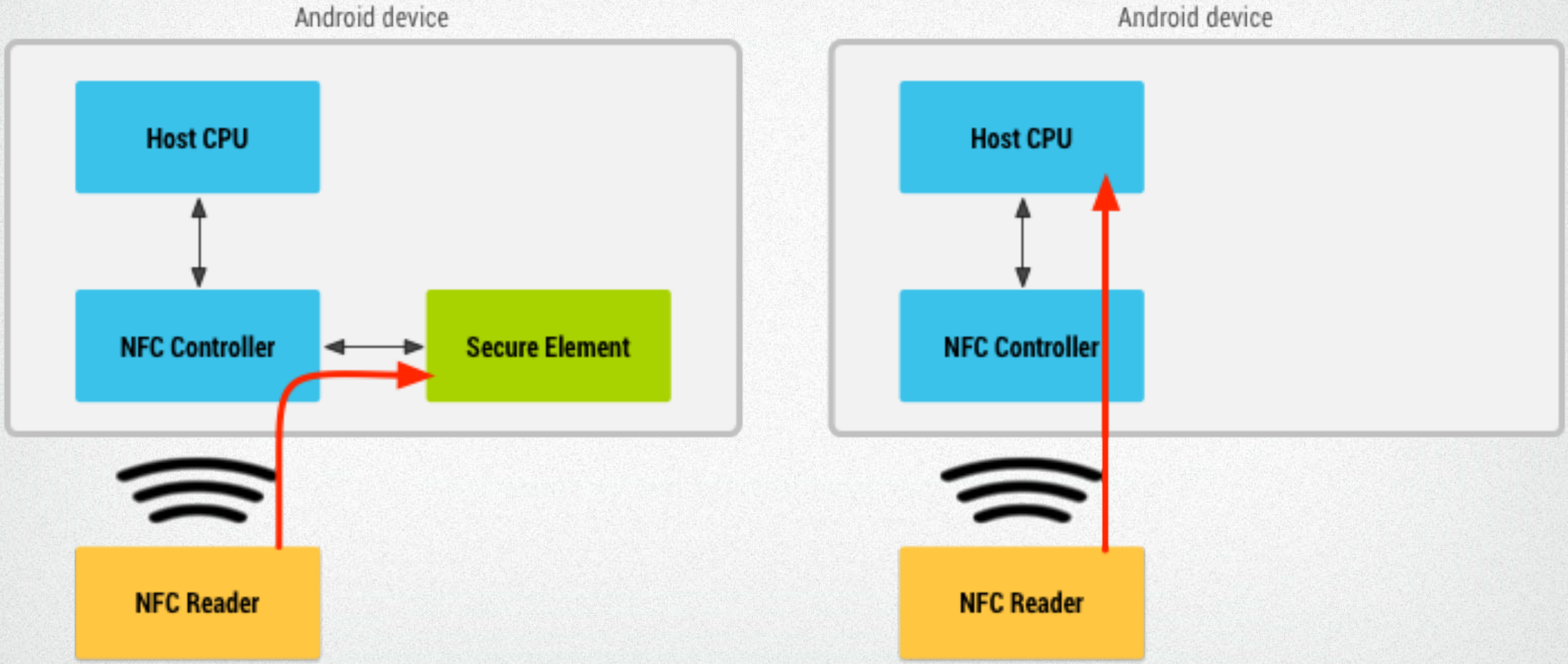
Introduction



NFC with external SE (SD/SIM)

NFC with embedded SE / HCE

Introduction



Prior work

Eavesdropping
credit cards…

Relay with
self-build hardwares…

Before HCE

Relay with
mobile phones

After HCE

Prior work

Experimental Setup

much work

[Hancke'09] [Francis'10] [Verdult'11] [Markantonakis'12]

In Practice

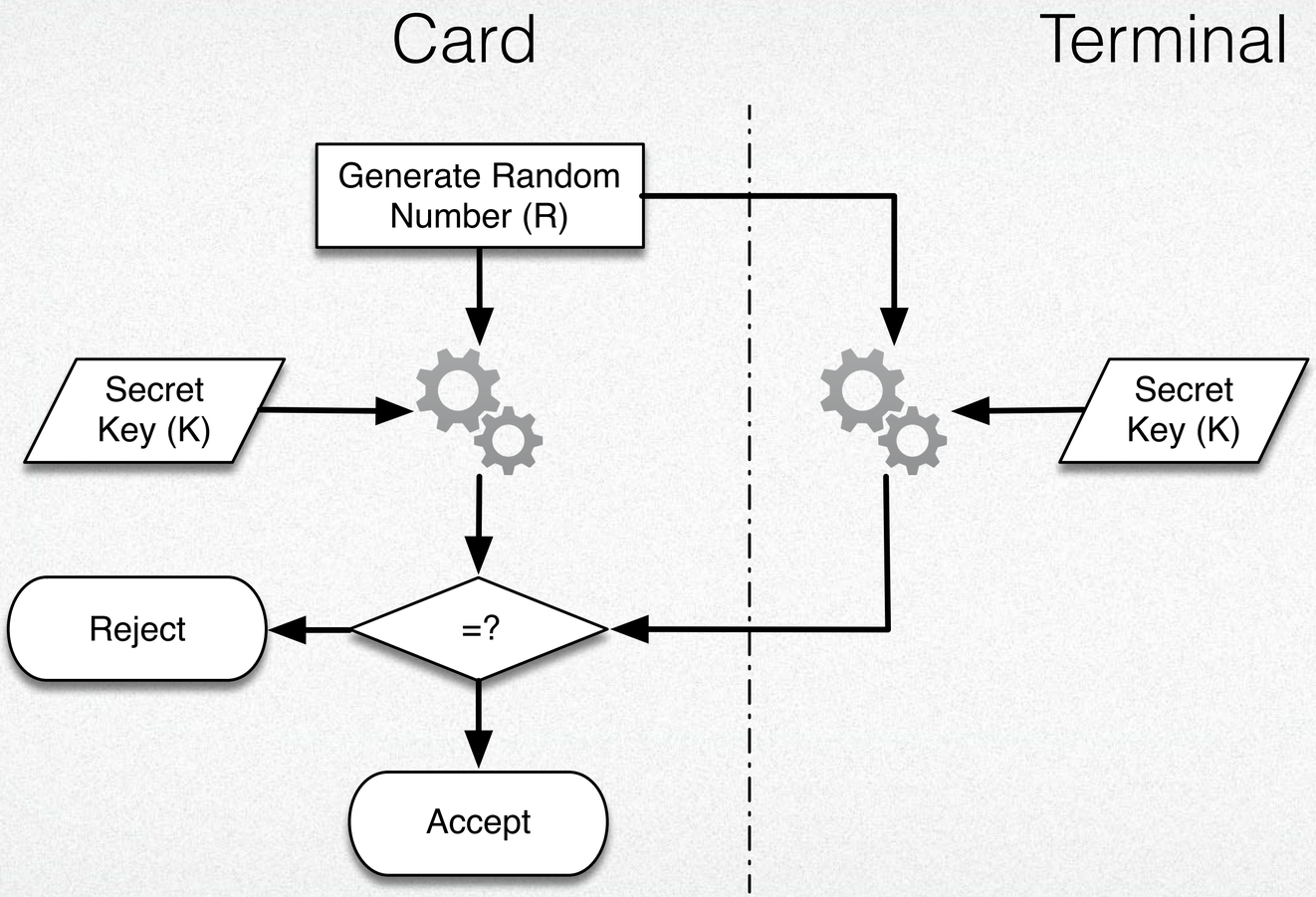
effort to prove feasible

[Bond'14]

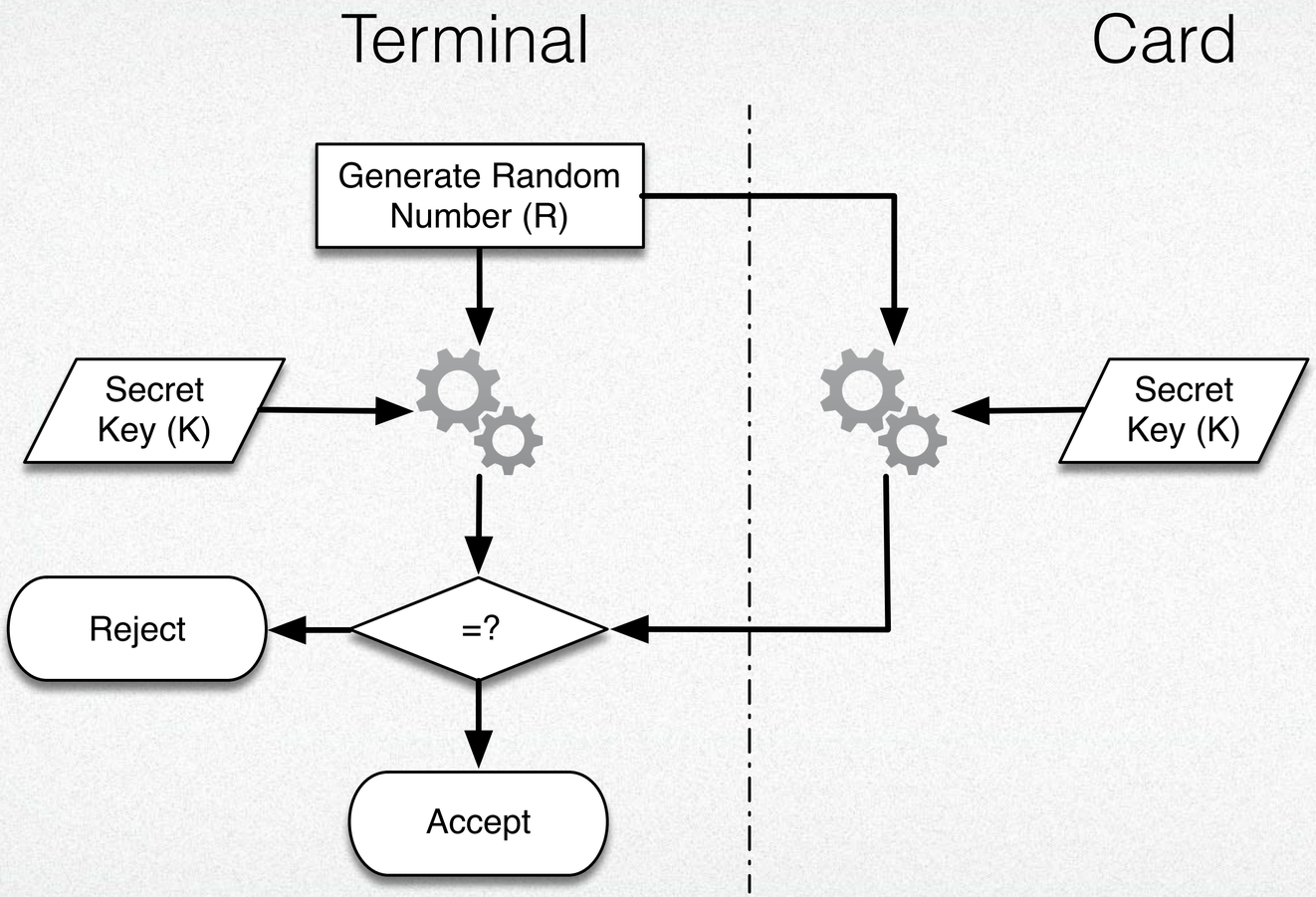
Beijing Municipal Traffic Card

ISO/IEC 14443-4 based

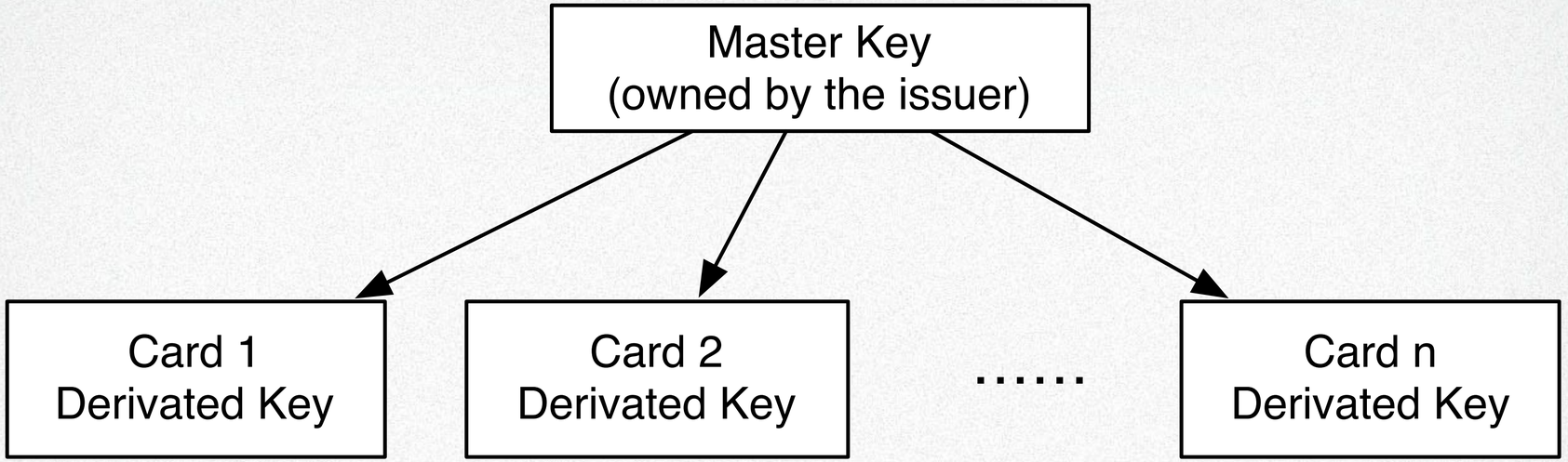
Weakness in top-up



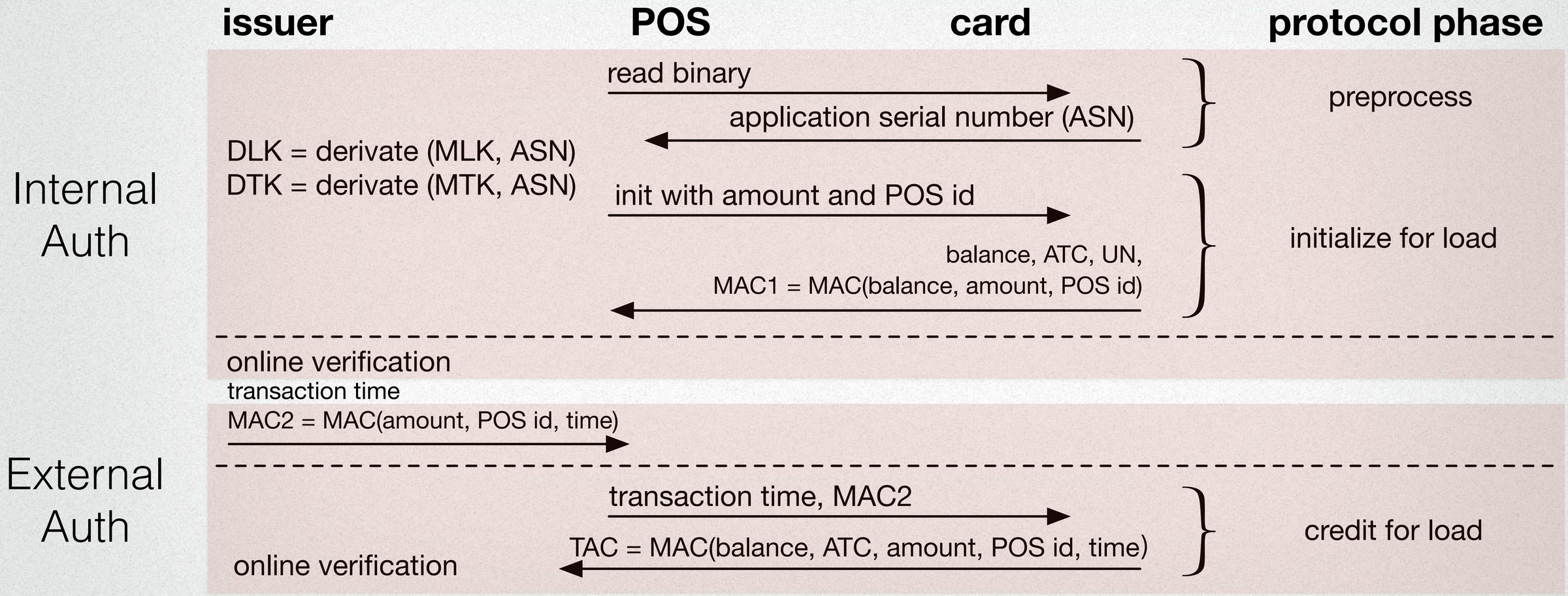
External Authentication: a card verifies a terminal



Internal Authentication: a terminal verifies a card



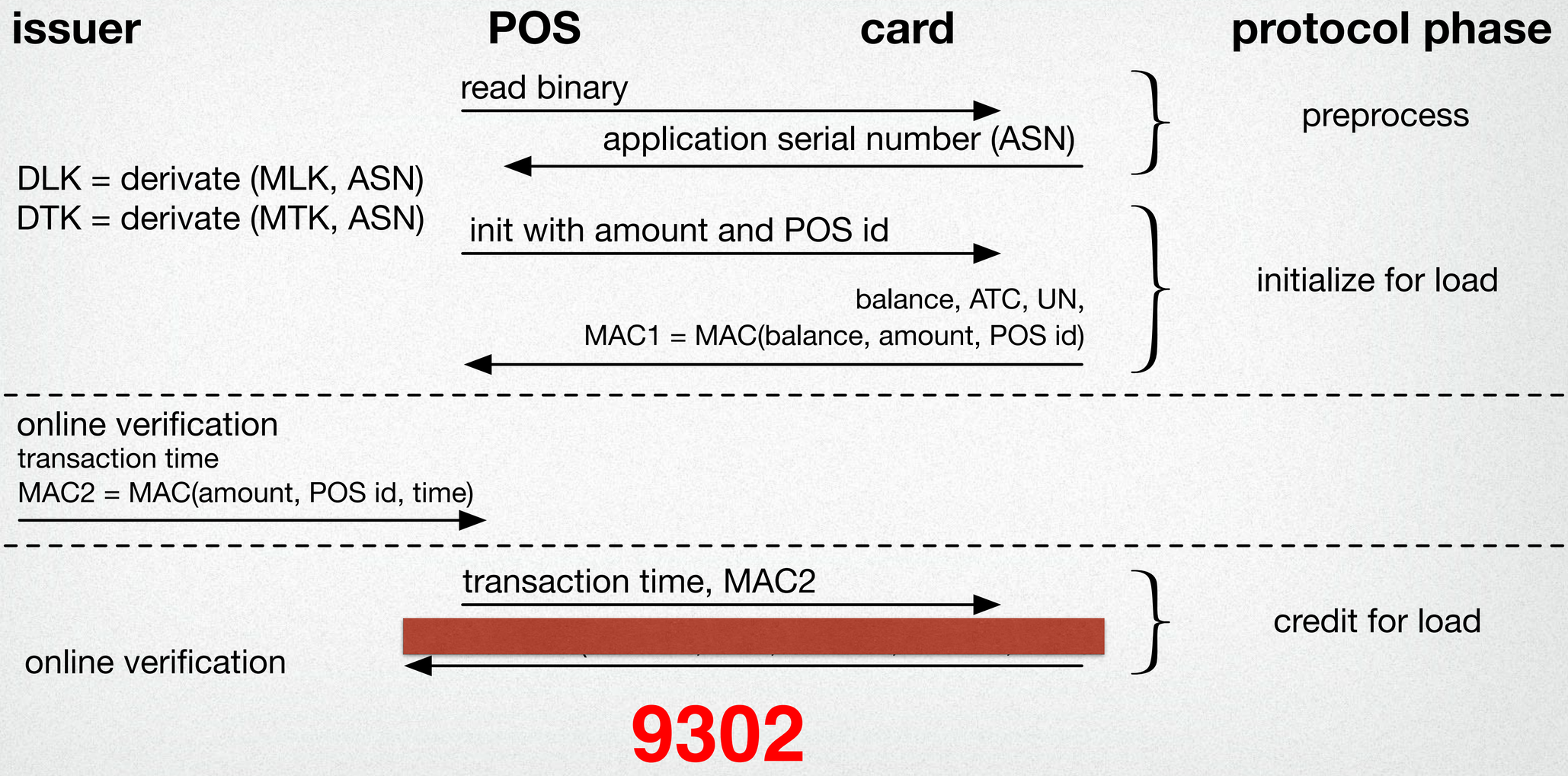
$$DK = \mathrm{3DES}(ASN, MK) + \mathrm{3DES}(\sim ASN, MK)$$

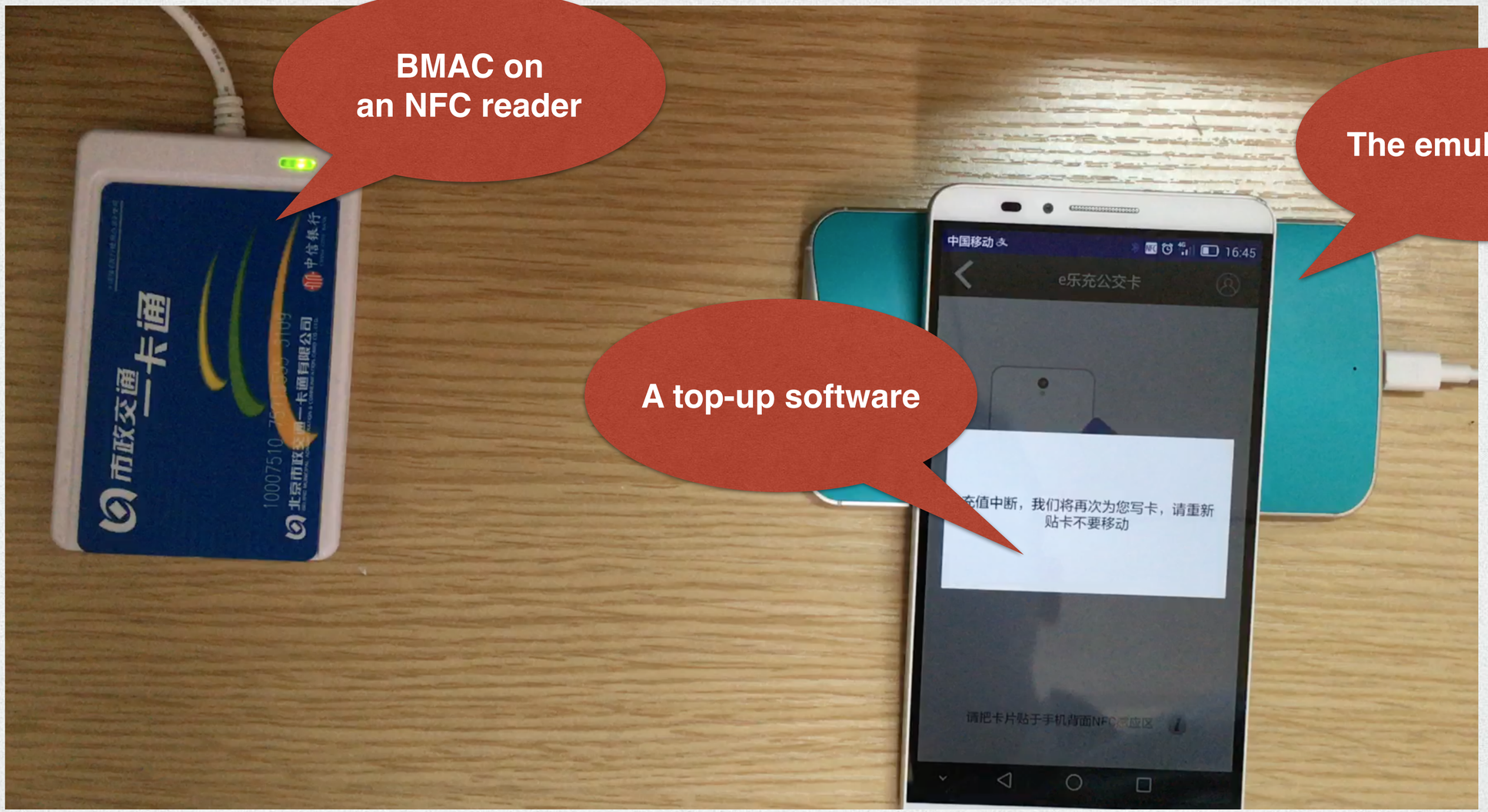

issuer
POS
card
protocol phase
Internal Auth
read binary
application serial number (ASN)
preprocess
DLK = derivate (MLK, ASN)
DTK = derivate (MTK, ASN)
init with amount and POS id
balance, ATC, UN,
MAC1 = MAC(balance, amount, POS id)
initialize for load
online verification
transaction time
MAC2 = MAC(amount, POS id, time)
External Auth
transaction time, MAC2
TAC = MAC(balance, ATC, amount, POS id, time)
credit for load
online verification

Command APDU						
CLA	INS	P1	P2	L_c	Data Field	L_e

Response APDU		
Response	SW1	SW2

Status Words	Explanation
9000	Success
6E00	CLA incorrect
9302	MAC invalid
9303	Application locked


issuer
POS
card
protocol phase
read binary
application serial number (ASN)
preprocess
DLK = derivate (MLK, ASN)
DTK = derivate (MTK, ASN)
init with amount and POS id
balance, ATC, UN,
MAC1 = MAC(balance, amount, POS id)
initialize for load
online verification
transaction time
MAC2 = MAC(amount, POS id, time)
transaction time, MAC2
online verification
credit for load
9302


BMAC on
an NFC reader
The emulated card
A top-up software
中国移动
16:45
e乐充公交卡
充值中断，我们将再次为您写卡，请重新
贴卡不要移动
请把卡片贴于手机背面NFC感应区


NFC
市政交通一卡通
10007510
北京市政交通一卡通有限公司
中信银行

The problem

Message passing through **unreliable channels**
cannot create **common knowledge**.

Common Knowledge and Common Belief
Hans van Ditmarsch, Jan van Eijck, Rineke Verbrugge

Defenses

1. No refund after generating MAC
2. Try detecting relay attack

Discussion

1. EZ-Link (Singapore)
   `CREDIT` command has a failure status
2. Oyster (London)
   A `CREDIT` command is wrapped in a `TRANSACTION` command, which also has a failure status.
3. CIPURSE (Barcelona, Perm, Medellin)
   Similar to Oyster.
4. Octopus (Hong Kong)
   FeliCa, impossible to relay currently.

Conclusions

1. We analyze the weakness of ISO/IEC 14443-4 when facing a relay attack. The flaw appears quite general to all kinds of AFC systems following this standard globally.
2. We design a relay experimental method and perform the relay attack. The result shows that the protocol is vulnerable.
3. We propose two attack countermeasures, and discuss the feasibility and practicality of these countermeasures.


Q&A