ACM *MobiSys2021*

Discovering Emergency Call Pitfalls for Cellular Networks with Formal Methods

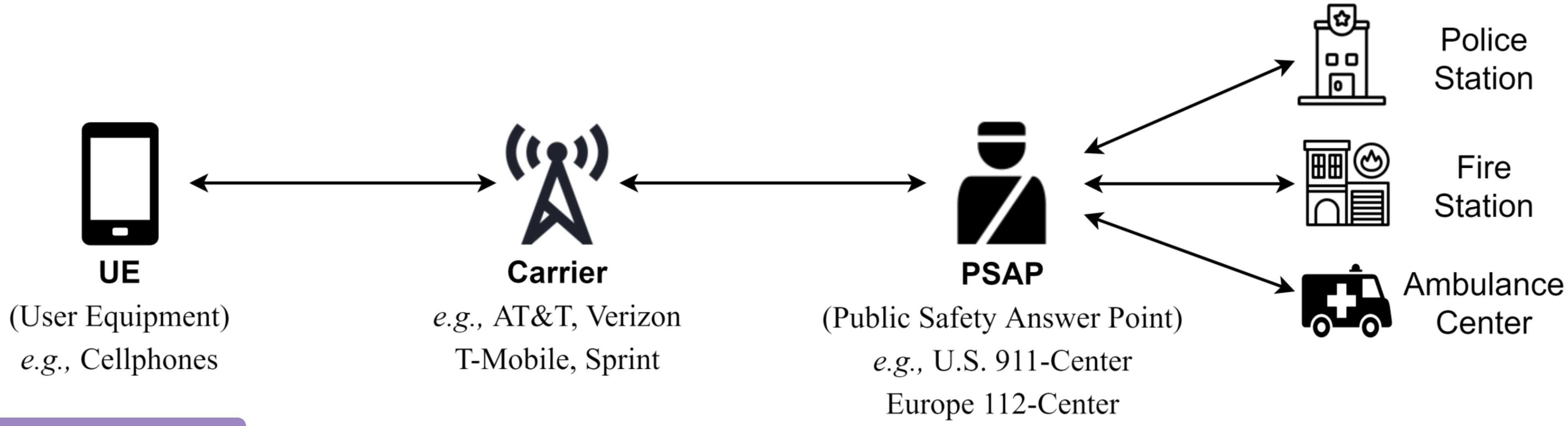
Kaiyu Hou[*†], You Li[*†], Yinbo Yu[‡], Yan Chen[†], Hai Zhou[†]

[†] Northwestern University

[‡] Northwestern Polytechnical University

[*] Both authors contributed equally to this research.

Cellular Emergency Call System



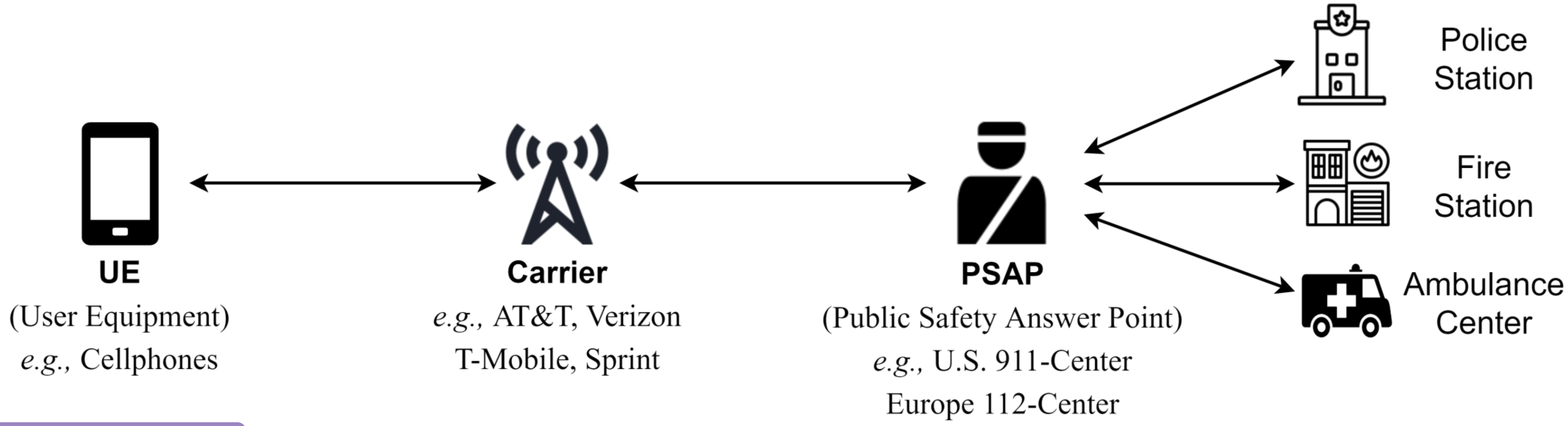
Importance

- 240 million emergency calls made to 911 each year
- 80% from cellular networks

Uncultivated

- No work thoroughly analyzes its correctness/vulnerabilities

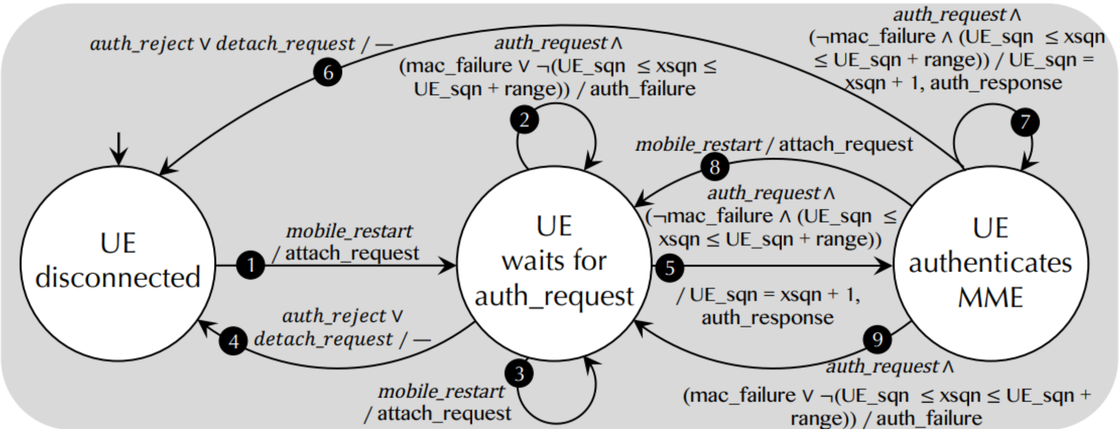
Cellular Emergency Call System

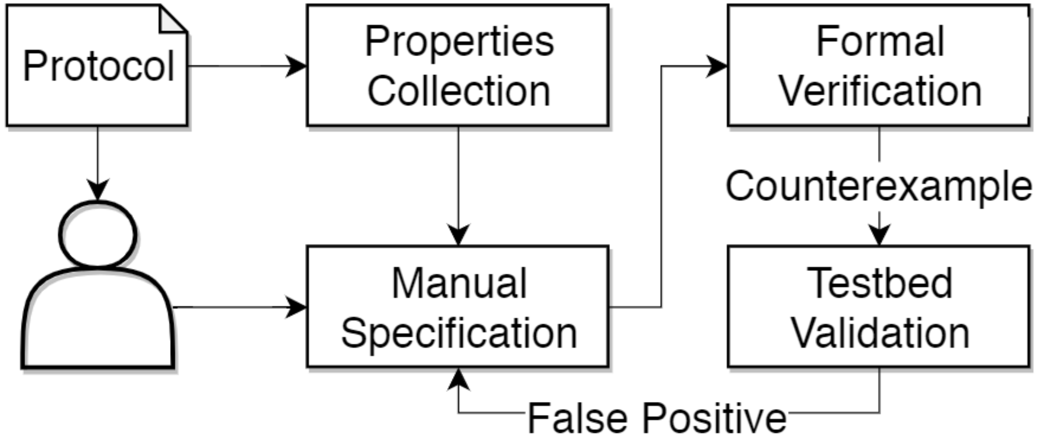


Goal

- Systematically discover the availability and security issues
- Explain underlying causal mechanisms

Formal Methods in Cellular Network Protocols





Succeeded Aspect

Crypto-related protocols:

Authentication and Key Agreement (AKA)

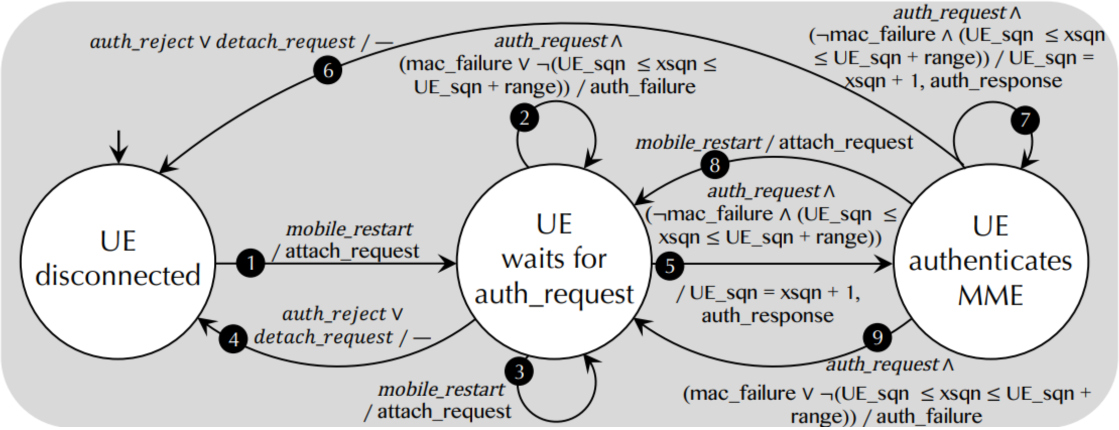
Still Challenging

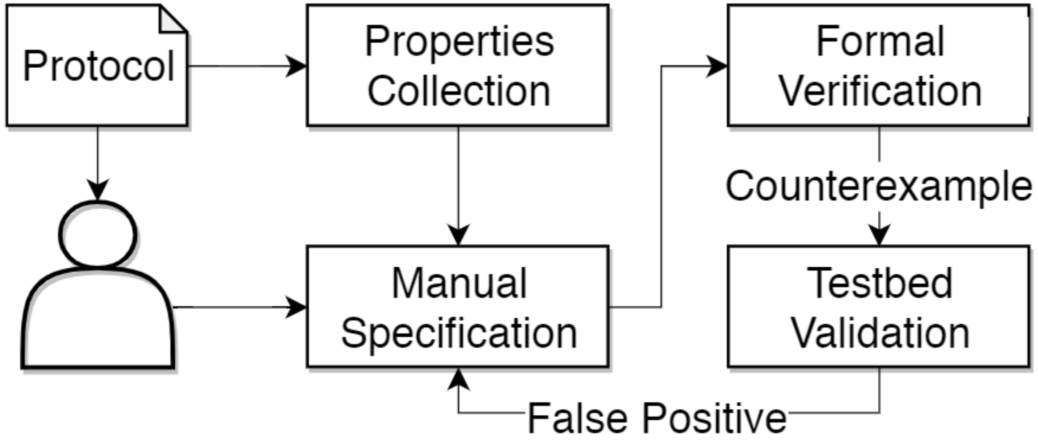
Formally verify:

General cellular network protocols

*Top figure referred from: Hussain et al, *LTE Inspector: A Systematic Approach for Adversarial Testing of 4G LTE*, NDSS'18

Problems in Existing Works





1 Modeling Granularity

2 Misrepresentation

Always Gaps

- Protocol Definition
- Formal Specification
- System Implementation

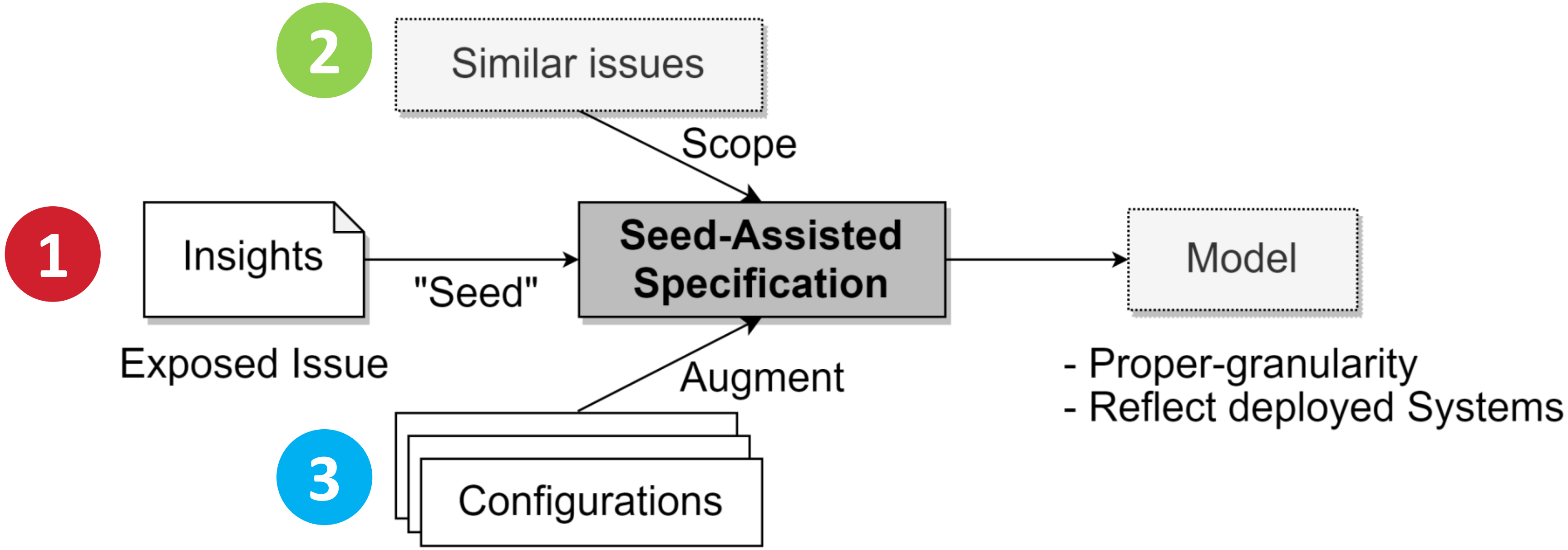
*Top figure referred from: Hussain et al, *LTE Inspector: A Systematic Approach for Adversarial Testing of 4G LTE*, NDSS'18

Key Features: Security Analysis for Cellular

1 *Exposed Security Issue: worthy to investigate underlying causes*

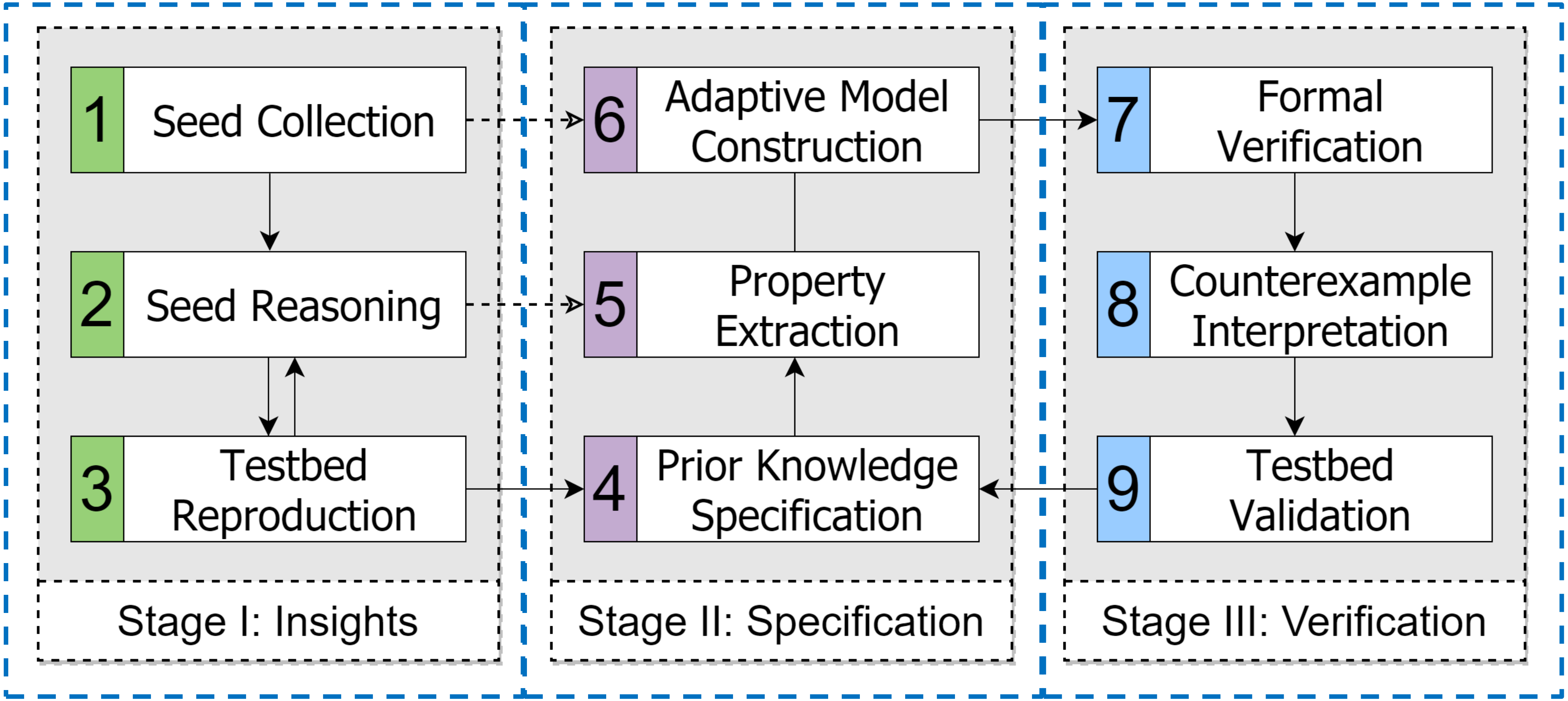
2 *Potential Similar Issues: systematically searching under similar causes*

3 *Configurations: can be measured on-air or at UE side*



- Proper-granularity
- Reflect deployed Systems

Framework of Seed-Assisted Specification



The Seed: A Piece of Shocking News

The victim tried to dial 120, the ambulance emergency number, from her Meizu MX6 UE

Valid SIM for a Chinese carrier was inserted
UE was covered by good signal

All 120 calls were failed: neither from locked screen emergency panel nor normal panel

She only head repeated dialing instructions:
110 for police, 119 for fire, 120 for ambulance…

Father suffered a brain hemorrhage, and her mother couldn’t dial the emergency number.

Step 1: Seed Collection

Cellular Network Protocols

- Developed by 3GPP, consists of more than 1,000 documents
- Narrow to call setup protocols and emergency call-related protocols

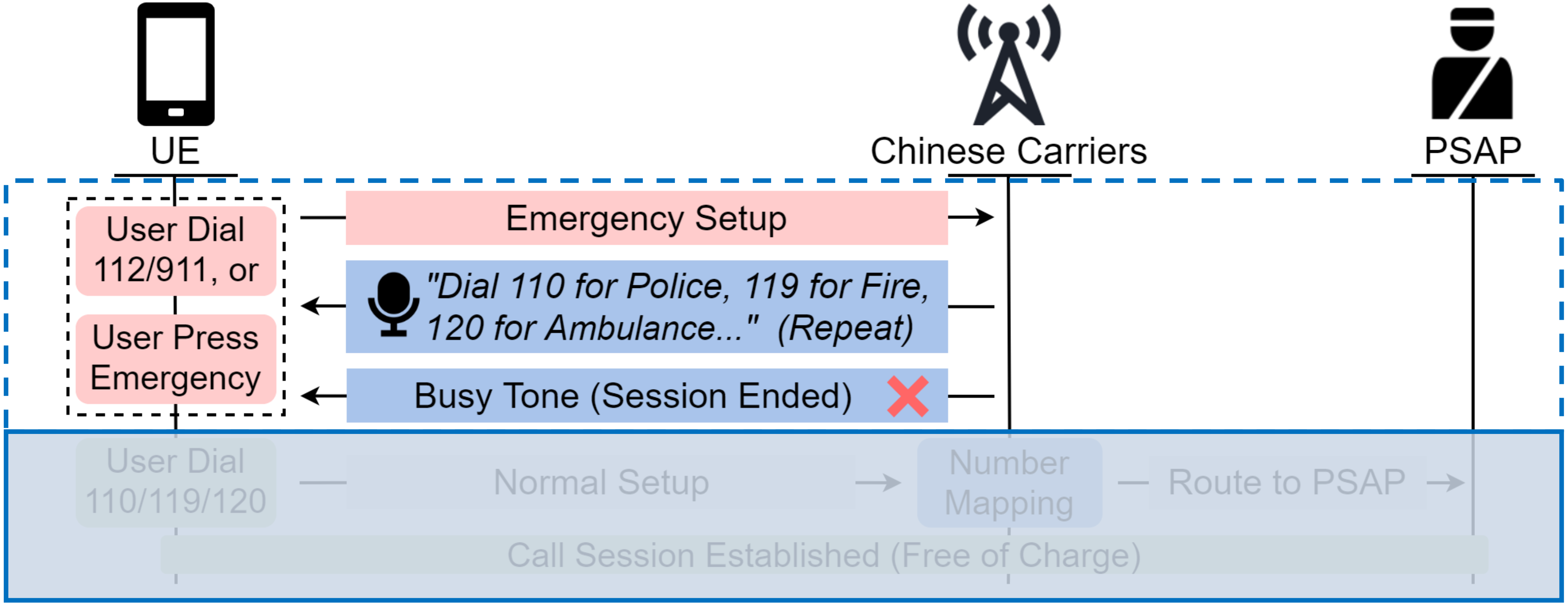
Implementation of UEs

- Analysis source code from Android Project (AOSP) and Meizu ROMs
- Focus on telephony functionality

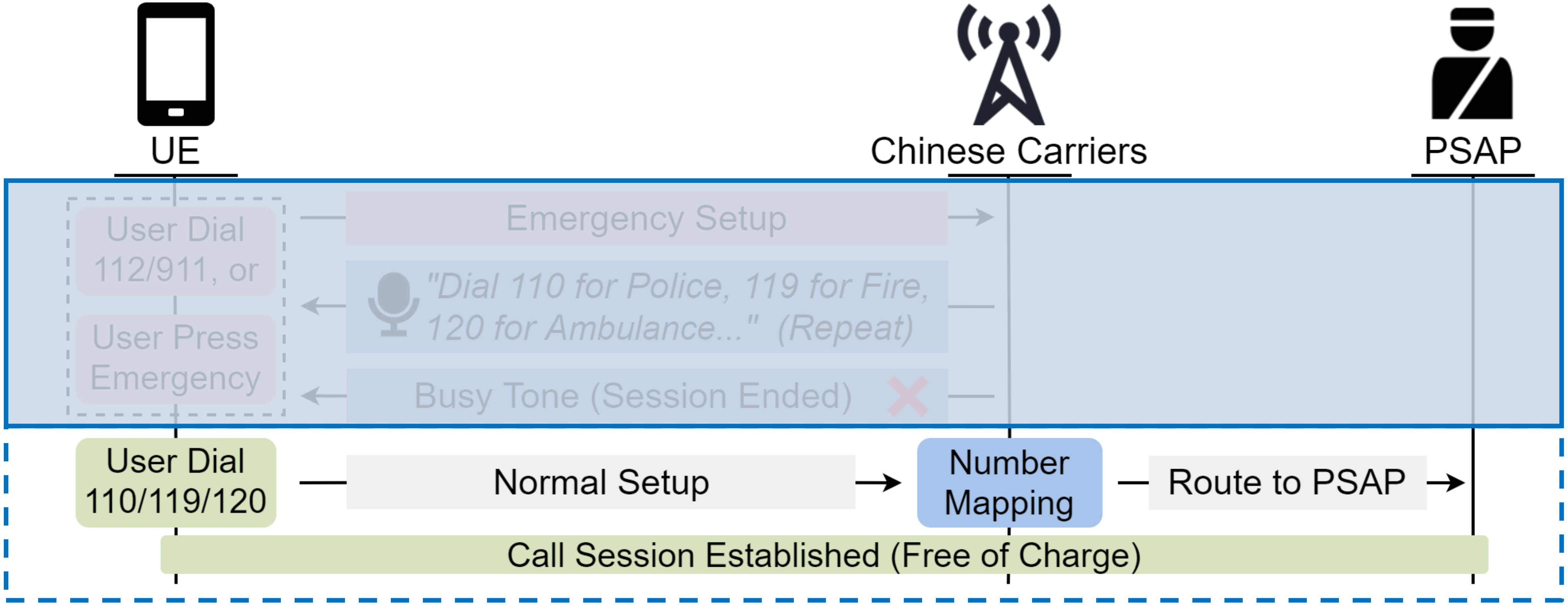
Configurations of Carriers

- Measure on UE side and sniffer packets on-air
- Infer from the solution provider documentation

Step 2: Seed Reasoning



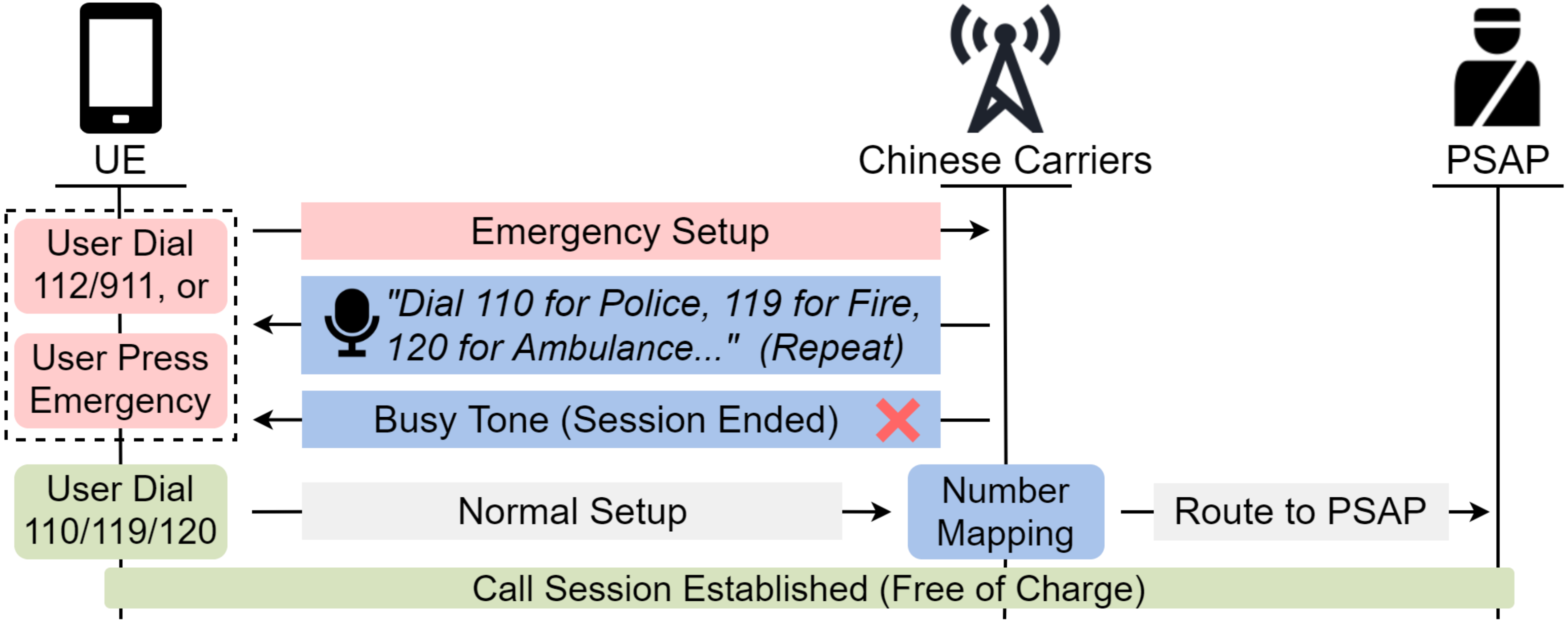
Step 2: Seed Reasoning



Tradition Landline System

- Using ITU signaling system
- Does not support 3GPP Emergency Setup

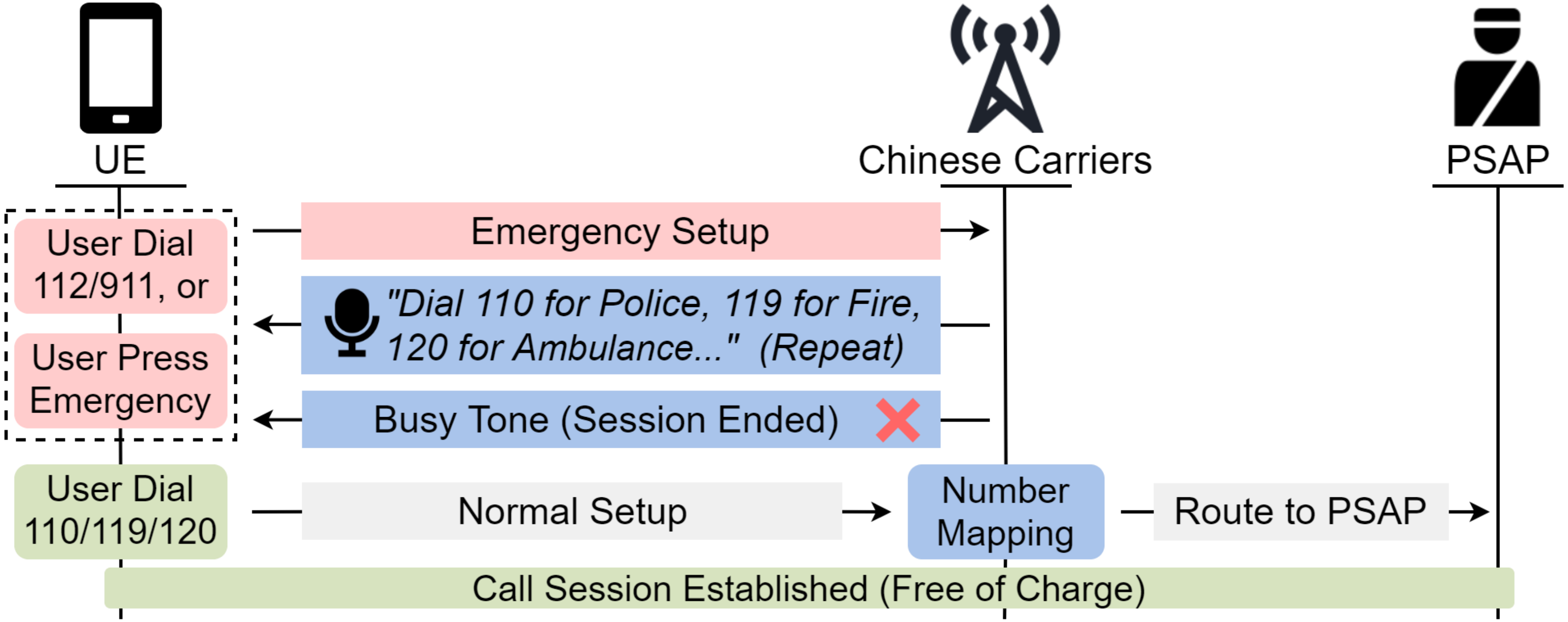
Step 2: Seed Reasoning



Current Solution

- Backwards compatible with the traditional system
- Also “respond to” Emergency Setup to some extent

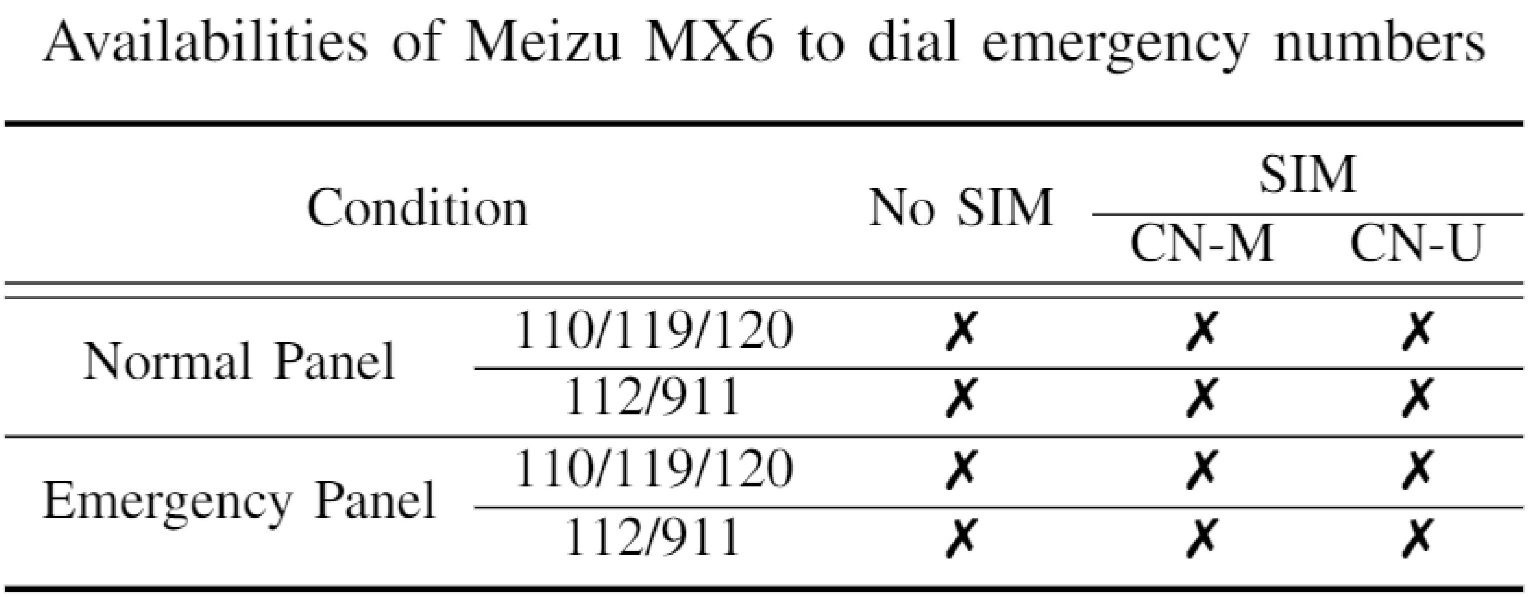
Step 2: Seed Reasoning



Speculate: when dial 120

Meizu MX6 UE falsely initiated calls with Emergency Setup

Step 3: Testbed Reproduction



Availabilities of Meizu MX6 to dial emergency numbers

Condition		No SIM	SIM	
			CN-M	CN-U
Normal Panel	110/119/120	✗	✗	✗
	112/911	✗	✗	✗
Emergency Panel	110/119/120	✗	✗	✗
	112/911	✗	✗	✗

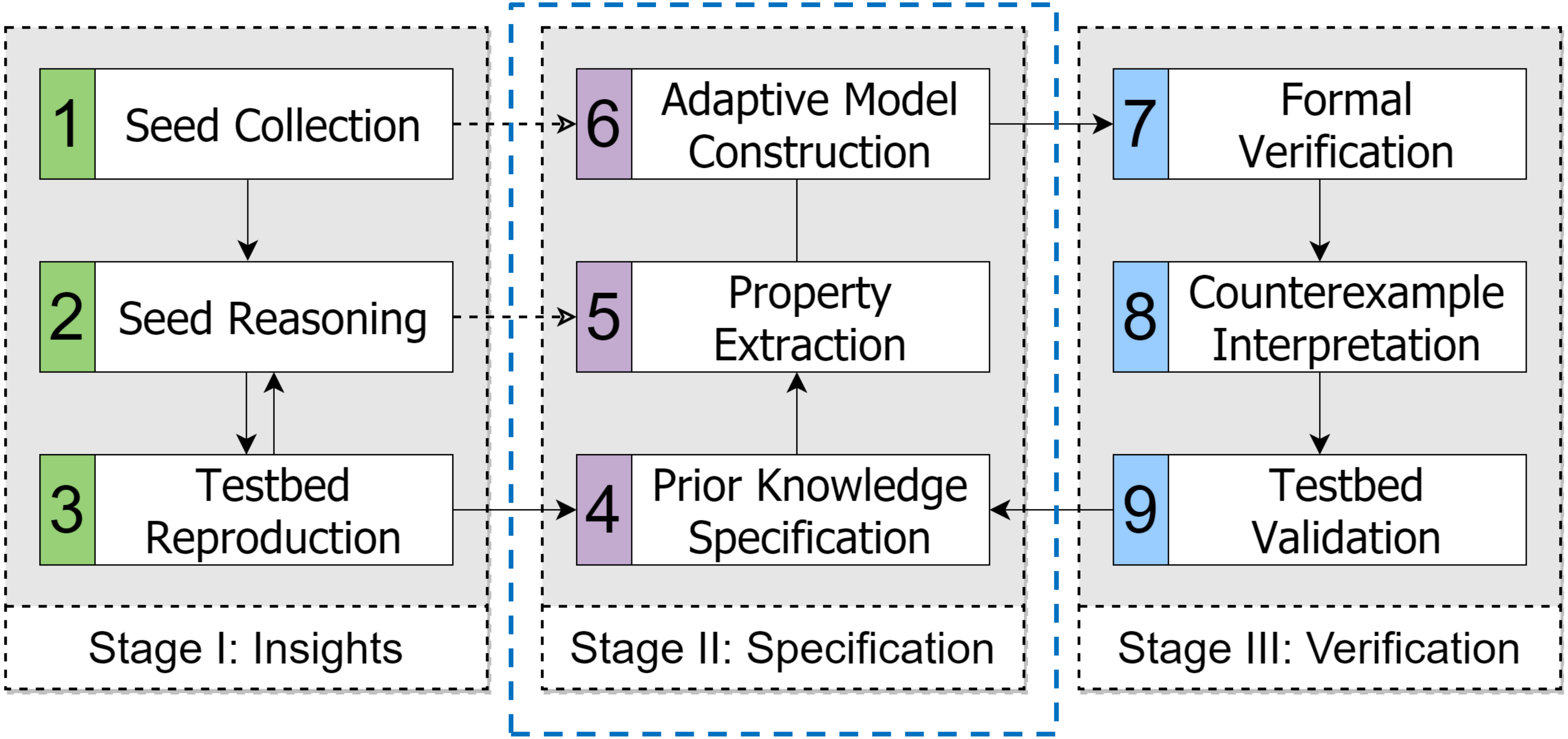
Packet Sniffer

Meizu MX6 uses Emergency Setup to initiate these calls

Other UEs

Initiate Calls by Emergency Setup, all of them fail

Stage II: Specification



Step 4: Prior Knowledge Specification

Specified by **TLA+**

2 Parts UE⟷Network

36 configurable variables

10.6 Billion Distinct States

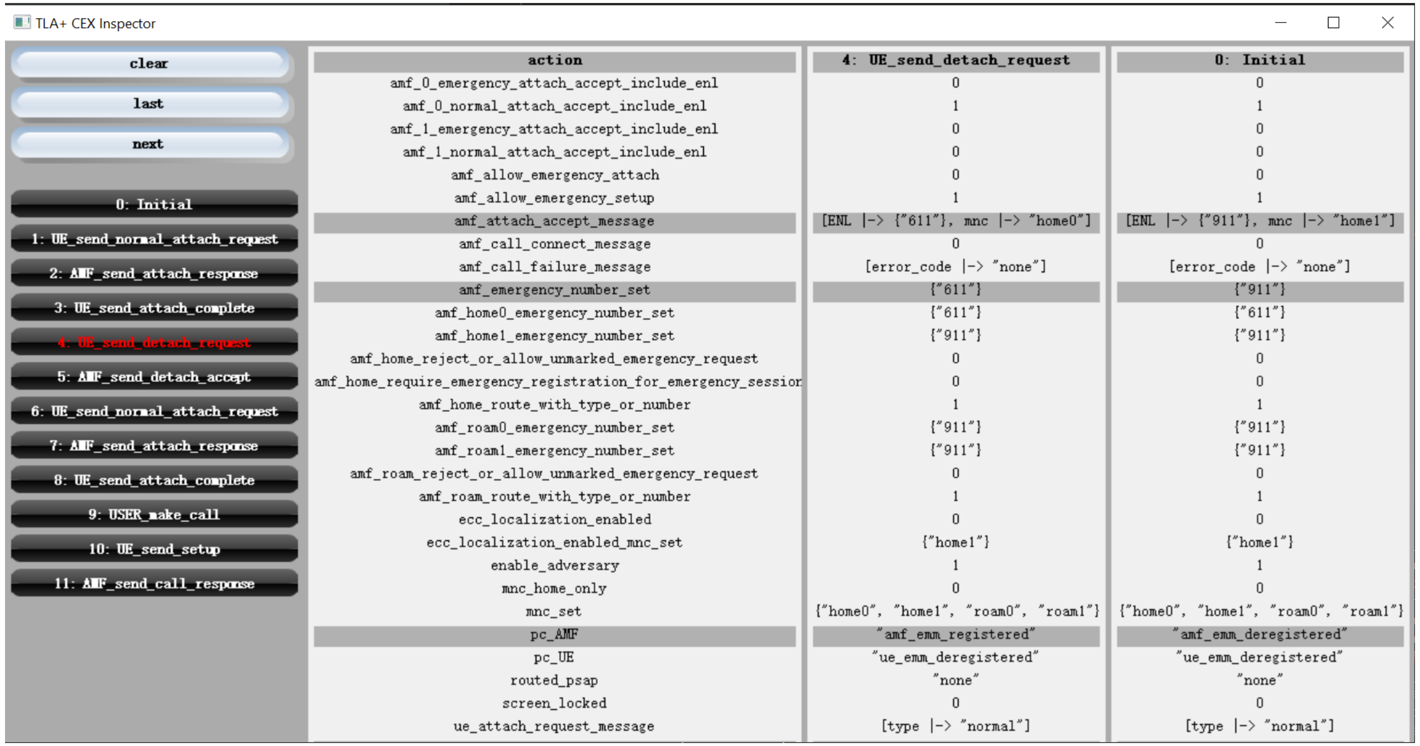
26 Max Diameter

github.com/FormalCellular/EmergencyCall

Formal Model
cellular emergency call systems

Model Checking
auto execution tools

GUI
CEX interpretation utilities



0: Initial
1: UE_send_normal_attach_request
2: AMF_send_attach_response
3: UE_send_attach_complete
4: UE_send_detach_request
5: AMF_send_detach_accept
6: UE_send_normal_attach_request
7: AMF_send_attach_response
8: UE_send_attach_complete
9: USER_make_call
10: UE_send_setup
11: AMF_send_call_response

action	4: UE_send_detach_request	0: Initial
amf_0_emergency_attach_accept_include_enl	0	0
amf_0_normal_attach_accept_include_enl	1	1
amf_1_emergency_attach_accept_include_enl	0	0
amf_1_normal_attach_accept_include_enl	0	0
amf_allow_emergency_attach	0	0
amf_allow_emergency_setup	1	1
amf_attach_accept_message	[ENL |-> {"611"}, mnc |-> "home0"]	[ENL |-> {"911"}, mnc |-> "home1"]
amf_call_connect_message	0	0
amf_call_failure_message	[error_code |-> "none"]	[error_code |-> "none"]
amf_emergency_number_set	{"611"}	{"911"}
amf_home0_emergency_number_set	{"611"}	{"611"}
amf_home1_emergency_number_set	{"911"}	{"911"}
amf_home_reject_or_allow_unmarked_emergency_request	0	0
amf_home_require_emergency_registration_for_emergency_sessior	0	0
amf_home_route_with_type_or_number	1	1
amf_roam0_emergency_number_set	{"911"}	{"911"}
amf_roam1_emergency_number_set	{"911"}	{"911"}
amf_roam_reject_or_allow_unmarked_emergency_request	0	0
amf_roam_route_with_type_or_number	1	1
ecc_localization_enabled	0	0
ecc_localization_enabled_mnc_set	{"home1"}	{"home1"}
enable_adversary	1	1
mnc_home_only	0	0
mnc_set	{"home0", "home1", "roam0", "roam1"}	{"home0", "home1", "roam0", "roam1"}
pc_AMF	"amf_emm_registered"	"amf_emm_deregistered"
pc_UE	"ue_emm_deregistered"	"ue_emm_deregistered"
routed_psap	"none"	"none"
screen_locked	0	0
ue_attach_request_message	[type |-> "normal"]	[type |-> "normal"]

Step 5: Property Extraction

Liveness Property

If a user dials a local emergency number, the call should eventually be routed to the corresponding PSAP.

Safety Property

Any call should not be routed to a non-corresponding callee.

Step 6: Adaptive Model Construction

Liveness Property

If a user dials a local emergency number, the call should eventually be routed to the corresponding PSAP.

Chinese Carriers

Configuration of all major carriers

The availability of cellular emergency calls

Safety Property

Any call should not be routed to a non-corresponding callee.

U.S. Carriers

Configuration of two major U.S. carriers

The security of cellular emergency calls

Step 7: Formal Verification

Liveness Property

If a user dials a local emergency number, the call should eventually be routed to the corresponding PSAP.

Chinese Carriers

Configuration of all major carriers

The availability of cellular emergency calls

Four Failures

Safety Property

Any call should not be routed to a non-corresponding callee.

U.S. Carriers

Configuration of two major U.S. carriers

The security of cellular emergency calls

Two Attacks

Step 8: Counterexample Interpretation

A tourist who is

roaming in China

Inserts valid SIM

Uses localized UE

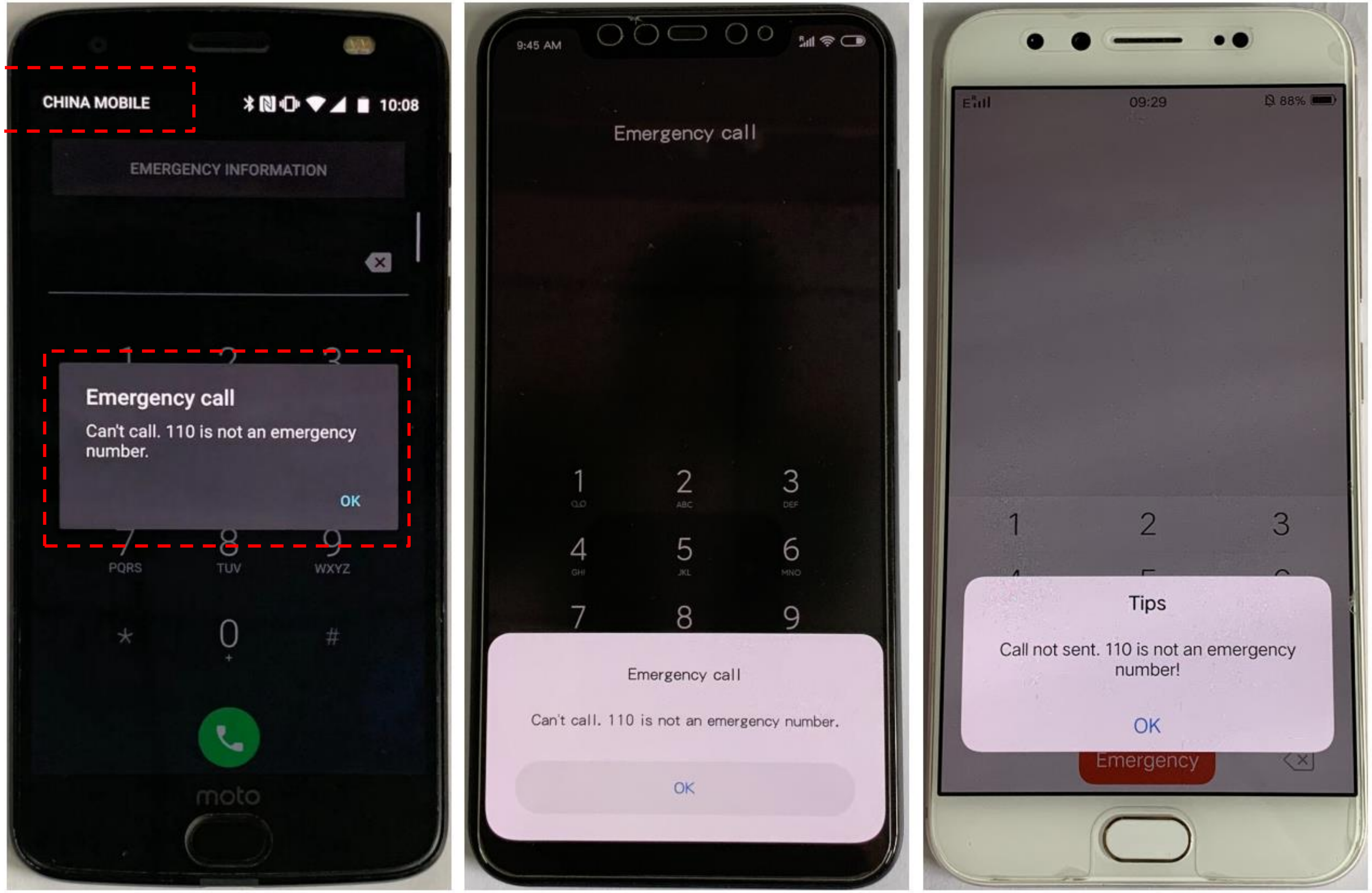
Has roaming subscription

F-4 *A roaming UE cannot initiate an emergency call in China by the emergency panel of the locked screen, even with a valid subscription, if its home local emergency number is different from China.*

Power of Formal Methods

- Hard to discover without systematic study
- Easy to reproduce once found

Step 9: Testbed Validation



Emergency call

Can't call. 110 is not an emergency number.

OK

Emergency call

Can't call. 110 is not an emergency number.

OK

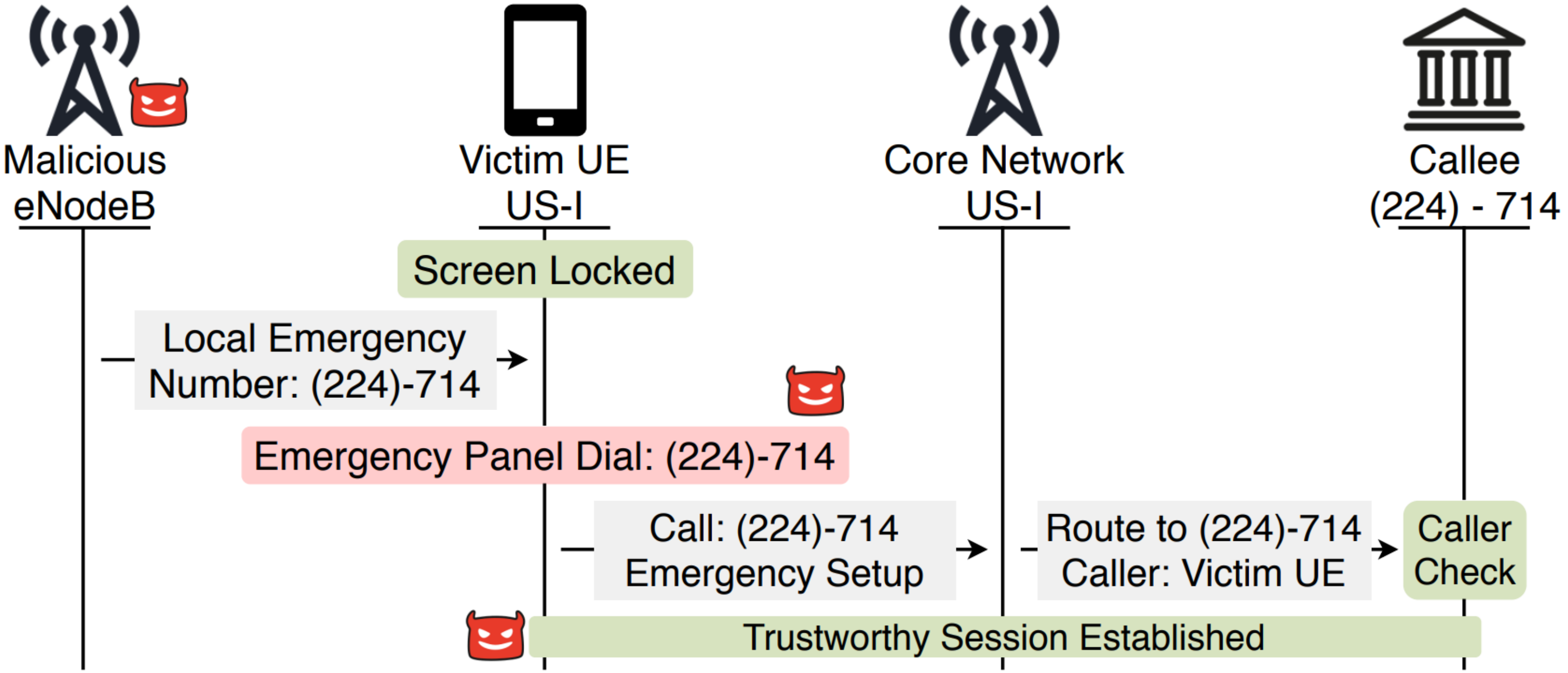
Tips

Call not sent. 110 is not an emergency number!

OK

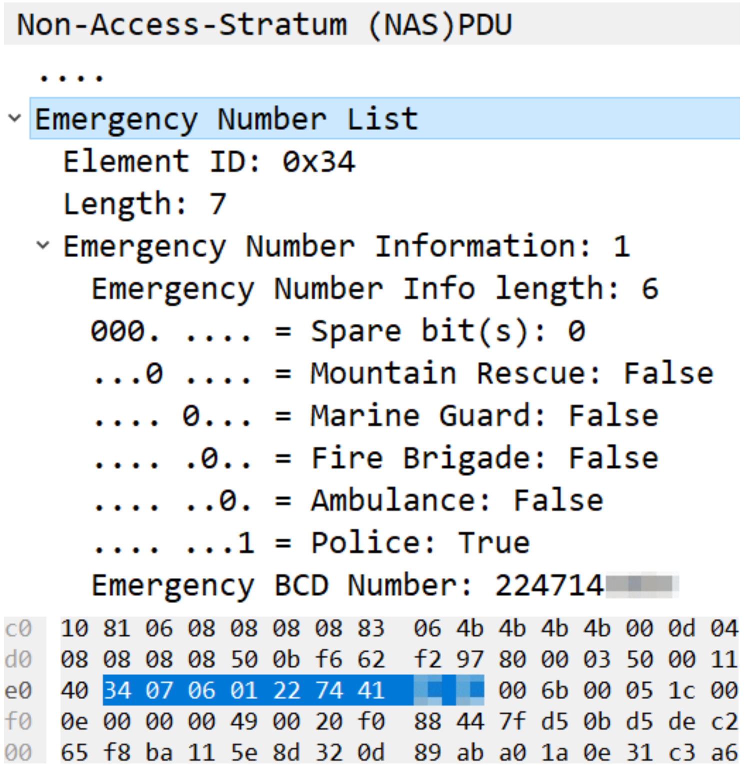
(a) Moto Z2 (b) Xiaomi 8 (c) Vivo x9s

Attack-1 UE Screen Lock Bypassing on US-I


Malicious eNodeB
Victim UE US-I
Core Network US-I
Callee (224) - 714
Screen Locked
Local Emergency Number: (224)-714
Emergency Panel Dial: (224)-714
Call: (224)-714 Emergency Setup
Route to (224)-714 Caller: Victim UE
Caller Check
Trustworthy Session Established

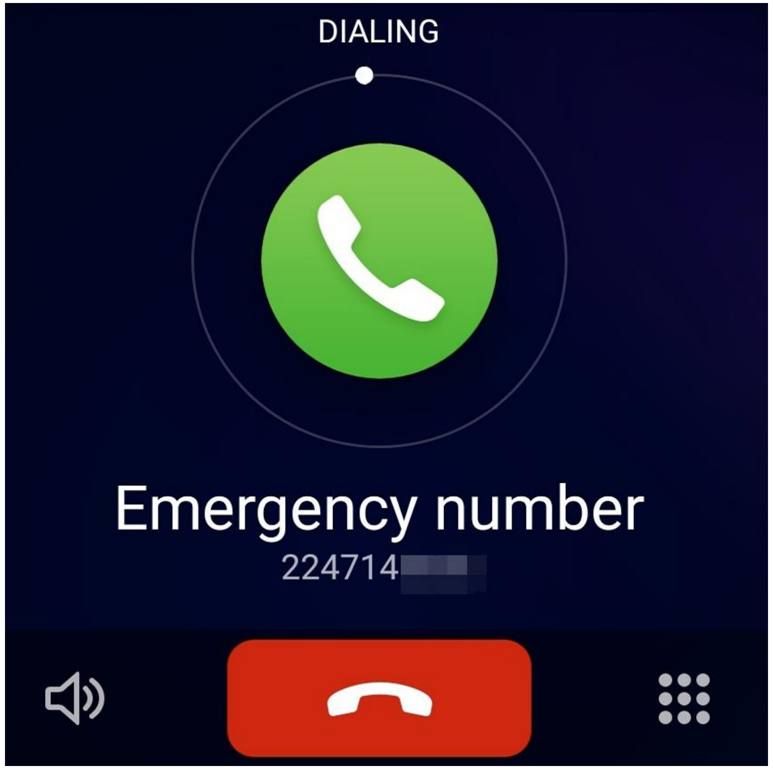
Attack-1 *The adversary can dial any normal number on the emergency panel of the victim's UE and get routed to the callee, without unlocking the UE, if the UE is a subscriber of carrier US-I.*

Attack-1 Deployment



```
Non-Access-Stratum (NAS)PDU
  ....
⌄ Emergency Number List
    Element ID: 0x34
    Length: 7
  ⌄ Emergency Number Information: 1
      Emergency Number Info length: 6
      000. .... = Spare bit(s): 0
      ...0 .... = Mountain Rescue: False
      .... 0... = Marine Guard: False
      .... .0.. = Fire Brigade: False
      .... ..0. = Ambulance: False
      .... ...1 = Police: True
      Emergency BCD Number: 224714[redacted]
c0  10 81 06 08 08 08 08 83  06 4b 4b 4b 4b 00 0d 04
d0  08 08 08 08 50 0b f6 62  f2 97 80 00 03 50 00 11
e0  40 34 07 06 01 22 74 41  [redacted] 00 6b 00 05 1c 00
f0  0e 00 00 00 49 00 20 f0  88 44 7f d5 0b d5 de c2
00  65 f8 ba 11 5e 8d 32 0d  89 ab a0 1a 0e 31 c3 a6
```

(a) Wireshark Log: the fake local emergency number list we pushed. It contains (224)-714-*



DIALING

Emergency number

224714[redacted]

(b) Screenshot: UE identifies the normal number (224)-714-* as an emergency number. We are dialing this number without unlocking the UE.

- The first attack that can bypass the UE password to make calls
- Bypass state-of-the-art caller ID spoofing defense mechanisms

Recommendations

Technical Solution

- Pushing Local Emergency Number List
- Accepting Emergency Setup Signaling
- Store Emergency Numbers in SIMs
- Filtering Non-emergency Numbers

Social Economic Solution

We argue that cellular network features, which have high social impacts but make no profits, e.g., emergency calls, shall be seriously considered and clearly defined by protocol designers.

Conclusion

Method

We propose the *seed-assisted specification* method, a novel approach applying formal methods to cellular network system.

Model

We specify a formal model and conduct the first research to study the availability and security issues in cellular emergency call system.

Four Failures and Two Attacks

We discover 4 failure scenarios of emergency calls for all major Chinese carriers. We find 2 new attacks affecting two major U.S. carriers.

Solution

We devise a solution addressing all failures and attacks and show its correctness. The overhead of the solution is marginal.

Thanks

Kaiyu Hou

kyhou@u.northwestern.edu

LIST Lab, Computer Science Department
Northwestern University