Instructions Unclear: Undefined Behaviour in Cellular Network Specifications

Daniel Klischies, Moritz Schloegel, Tobias Scharnowski
Mikhail Bogodukhov, David Rupprecht, Veelasha Moonsamy
Cellular baseband

RF communication (e.g., LTE)
Cellular baseband

Network services

RF communication (e.g., LTE)
FLASH FLOOD WARNING issued across cell phones in Massachusetts

Story by Amy Phillips • Tuesday

CHICOPEE, Mass. (WWLP) – The National Weather Service issued a Flash Flood Warning for parts of western Massachusetts Tuesday afternoon that may have caught you by surprise on your cell phone.

Weather Alert: Possible strong thunderstorms Tuesday
The Wireless Emergency Alert (WEA) system is activated when the National Weather Service (NWS) issues a warning for your location. Destructive thunderstorm warnings and higher-end flash flood warnings trigger these alerts.

At approximately 1:42 p.m. the National Weather Service issued a FLASH FLOOD WARNING alert on cellular devices indicating, “This is a dangerous and life-threatening situation. Do not attempt to travel unless you are fleeing an area subject to flooding or under an evacuation order.

A Flash Flood Warning is in effect for Hampden County until 4:45 p.m. and in Hampshire and Franklin Counties until 5:15 p.m. Live radar indicates thunderstorms producing heavy rain up to 3 inches in some locations.

Emergency Alert 43m ago
National Weather Service: A FLASH FLOOD WARNING is in effect for this area until
FLASH FLOOD WARNING issued across cell phones in Massachusetts

Story by Amy Phillips • Tuesday

HICOPREE, Mass. (WWLP) – The National Weather Service issued a Flash Flood Warning for parts of western Massachusetts Tuesday afternoon that may have caught you by surprise on your cell phone.

Weather Alert: Possible strong thunderstorms Tuesday

The Wireless Emergency Alert (WEA) system is activated when the National Weather Service (NWS) issues a warning for your location. Destructive thunderstorm warnings and higher-end flash flood warnings trigger these alerts.

At approximately 1:42 p.m. the National Weather Service issued a Flash Flood Warning alert on cellular devices indicating, “This is a dangerous and life-threatening situation. Do not attempt to travel unless you are fleeing an area subject to flooding or under an evacuation order.

A Flash Flood Warning is in effect for Hampden County until 4:45 p.m. and in Hampshire and Franklin Counties until 5:15 p.m. Live radar indicates thunderstorms producing heavy rain up to 3 inches in some locations.

Emergency Alert 43m ago

National Weather Service: A FLASH FLOOD WARNING is in effect for this area until
How your phone receives emergency alerts
How your phone receives emergency alerts

Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.
How your phone receives emergency alerts

**Emergency Alert**
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Instructions Unclear: Undefined Behaviour in Cellular Network Specifications (Klischies et al.)
Behaviour of MediaTek’s PWS implementation

Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

- Text: INBOUND TO HAWAII
  - Segment #: 2
  - lastSegment: yes

- Text: BALLISTIC MISSILE THREAT
  - Segment #: 1
  - lastSegment: no
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Baseband memory

Received segments: 0  Target segments: ?

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Instructions Unclear: Undefined Behaviour in Cellular Network Specifications (Klischies et al.)
Behaviour of MediaTek’s PWS implementation

Text:

BALLISTIC MISSILE THREAT  |  INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Baseband memory

Received segments: 1
Target segments: ?
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Baseband memory

Received segments: 1
Target segments: 2
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Received segments: 2  Target segments: 2

Baseband memory

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no
Behaviour of MediaTek’s PWS implementation

Text:
BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Baseband memory

BALLISTIC MISSILE THREAT INBOUND TO HAWAII

Received segments: 2  Target segments: 2
Undefined behaviour of MediaTek’s PWS implementation

Baseband memory

Received segments: 0  Target segments: ?

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 3
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes
Undefined behaviour of MediaTek’s PWS implementation

Baseband memory

Received segments: 1  Target segments: 2
Undefined behaviour of MediaTek’s PWS implementation
Undefined behaviour of MediaTek’s PWS implementation
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19

5.2.2.19 Actions upon reception of SystemInformationBlockType12

Upon receiving SystemInformationBlockType12, the UE shall:

1> if the SystemInformationBlockType12 contains a complete warning message:

   2> forward the received warning message, messageIdentifier, serialNumber and dataCodingScheme to upper layers;

   2> continue reception of SystemInformationBlockType12;

1> else:

   2> if the received values of messageIdentifier and serialNumber are the same (each value is the same) as a pair for which a warning message is currently being assembled:

       3> store the received warningMessageSegment;

   3> if all segments of a warning message have been received:

       4> assemble the warning message from the received warningMessageSegment;

       4> forward the received warning message, messageIdentifier, serialNumber and dataCodingScheme to upper layers;

       4> stop assembling a warning message for this messageIdentifier and serialNumber and delete all stored information held for it;

3> continue reception of SystemInformationBlockType12;
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19

Is the incoming segment a complete warning message? Yes

Show message
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19

Is the incoming segment a complete warning message? Yes
No

Is there currently a message being assembled? Yes

Have all segments been received? Yes

Show message
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19

- Is the incoming segment a complete warning message? Yes → Show message
  No → Is there currently a message being assembled? Yes → Have all segments been received? Yes → Show message
  No → No
  No → Store segment
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19

- Is the incoming segment a complete warning message?
- Is there currently a message being assembled?
- Have all segments been received?
- Store segment

Show message

BALLISTIC MISSILE THREAT INBOUND TO HAWAII
Specification as a state machine

- Last segment
- Not last segment
Specification as a state machine

- Last segment
- Not last segment
Specification as a state machine

- Last segment
- Not last segment

Undefined State
Specification as a state machine

- Last segment
- Not last segment

Undefined State
Specification as a state machine

- Last segment
- Not last segment

Undefined State
Specification as a state machine

- Last segment
- Not last segment

Undefined State
Key challenges

Dependencies within a network packet, like segment number and type
Key challenges

**Dependencies** within a network packet, like segment number and type

Packet **sequences** for state setup, fragmentation & reassembly
Key challenges

**Dependencies** within a network packet, like segment number and type

Packet **sequences** for state setup, fragmentation & reassembly

**Timers** for deduplication, timeouts & expiry
Our proposed approach: Using a model checker
Model defined behaviour

- Using mathematical notation → Dependencies
- And temporal logic → Sequences & Timers

} TLA+
Our proposed approach: Using a model checker

Model defined behaviour

- Using mathematical notation \(\rightarrow\) **Dependencies**
- And temporal logic \(\rightarrow\) **Sequences & Timers**

Amend model to cover undefined behaviour

- Add an **undefined state**
- By negating the transitions for defined behaviour
Results

Public Warning System

SMS

Radio Resource Control
Results

Public Warning System
14 million states
8 undefined behaviours

SMS
8.5 million states
22 undefined behaviours

Radio Resource Control
955 states
28 undefined behaviours
Over-the-air evaluation
Over-the-air evaluation

5 exploitable undefined behaviours
→ 3 CVEs
Summary

Cellular specifications contain undefined behaviour

Undefined behaviour can be discovered from a model of defined behaviour

Undefined behaviour promotes insecure implementations