Combating Caller ID Spoofing on 4G Phones Via CEIVE

Haotian Deng, and Chunyi Peng,
Purdue University

What is CEIVE?

CEIVE (Callee-only inference and verification) is an victim callee only solution against caller ID Spoofing without requiring additional infrastructure support or changes on telephony systems.

Call state ambiguity

• Standard stipulates the mechanism, but leaves implementation flexibility

Advanced spoofing attack

• Eve could manipulate Alice’s call state by making another call

How CEIVE works?

1. Infer call state of callee using caller’s view only

(Use VoLTE as an example)

➢ Rich set of signaling messages carry rich context information

How CEIVE works?

2. Two-phases verification strategy

 upon receiving an incoming call (inCall), make a callback (auCall)

➢ Inference the call state of Alice using unexplored call setup signaling messages

➢ Compare the call state of inCall and auCall to detect spoofing

What CEIVE achieves

Challenges have be solved

➢ Call state ambiguity

What CEIVE achieves

Evaluation

➢ Perfect accuracy under a variety of call network settings

Without CEIVE

With CEIVE

➢ 4 US major carriers: AT&T, T-Mobile, Sprint and Verizon, single-line landline

➢ Both VoLTE and CSFB call technology

➢ User friendlessness and responsiveness

➢ Single-phase inference: 4-10 seconds for VoLTE and 8-10 seconds for CSFB

➢ Finishes within 16 seconds (VoLTE) and 19 seconds (CSFB) for most case (>90%), up to 23 seconds.

Caller ID Spoofing

A Big Threat

Easy to launch

Hard to defend

Imposter Scams

1 IN 5 PEOPLE LOST MONEY

$328 million reported lost

$500 median loss

Top fraud in 2017

Billions of dollars loss

Not only in US, but globally

Caller can simply alter its caller ID contained in the call setup request to make spoofing.

Carrier ID Change

Carrier ID Change

Carrier ID Change

Caller’s carrier network

Voice conversation

Caller’s carrier network

Call setup request (with Alice’s ID) more call setup signaling messages

Caller’s carrier network

Call setup request (with Alice’s ID) more call setup signaling messages

Caller’s carrier network

Callee’s carrier network

1. Infer call state of callee using caller’s view only

(Use VoLTE as an example)

➢ Rich set of signaling messages carry rich context information

State match?

Output:

Spoofer

No-spoof

N/A

Signaling run-time collection

Pattern Extraction

Callee state inference

2. Two-phases verification strategy

inCall’s state \eq ual to auCall’s state?\n
match

mismatch

Spoofer

Last phase?

no

Ambiguity?

Yes

N/A

No

Easy to launch

.How CEIVE works?

Top fraud in 2017

Billions of dollars loss

Not only in US, but globally

Hard to defend

However, there is no practical solution in place:

• End-to-end global certificate authority: heavy deployment requirement

• Challenge-and-response: changes on both caller and callee side

• Caller ID App: based on user report, doesn’t work at beginning

 caller ID Spoofing

SIP response codes

RFC3261: e.g., 200 OK, 180 Ringing, 181 Call Is Being Forwarded, 182 Queued, 183 Session Progress, 301 Moved Permanently, 400 Temporarily Unavailable, 481 Call/Transaction Does Not Exist, 486 Busy Here, 487 Request Terminated, ... etc.

PIM

RFC5009: sendrecv, sendonly, recvonly, inactive

URN-Alert

RFC7462: normal (default), call-waiting, forward, recall:callback, recall:hold, recall:transfer, ... etc.

VoLTE

TS24.229, TS24.628, TS24.615: e.g., early-media value or alert-info in 180/183, call terminated by network when busy... etc.

FSM

Standardized call setup procedure gives enough hint to infer callee’s call state

Challenges have be solved

• Call state ambiguity

➢ Standard stipulates the mechanism, but leaves implementation flexibility

➢ Advanced spoofing attack

➢ Eve could manipulate Alice’s call state by making another call

Evaluation

➢ Perfect accuracy under a variety of call network settings

Without CEIVE

With CEIVE

➢ 4 US major carriers: AT&T, T-Mobile, Sprint and Verizon, single-line landline

➢ Both VoLTE and CSFB call technology

➢ User friendlessness and responsiveness

➢ Single-phase inference: 4-10 seconds for VoLTE and 8-10 seconds for CSFB

➢ Finishes within 16 seconds (VoLTE) and 19 seconds (CSFB) for most case (>90%), up to 23 seconds.