CERIAS

The Center for Education and Research in Information Assurance and Security

Combating Caller ID Spoofing on 4G Phones Via CEIVE

Haotian Deng, and Chunyi Peng,
Purdue University

What is CEIVE?

CEIVE (**C**all**e**e-only **i**nference and **ve**rification) is an victim callee only solution against caller ID Spoofing without requiring additional infrastructure support or changes on telephony systems.

Highlights

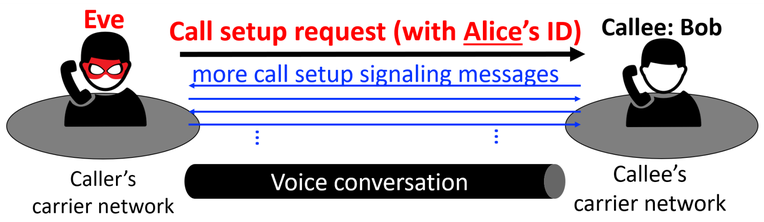
- ✓ Callee-only solution
- ✓ Without requiring any additional infrastructure update or caller-side cooperation
- ✓ Utilize unexplored call setup signaling messages
- ✓ Effective, responsive, user friendly

Caller ID Spoofing

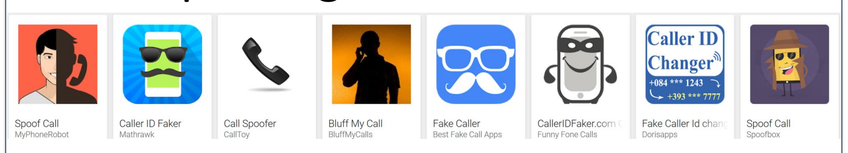
A Big Threat

- Top fraud in 2017
- Billions of dollars loss
- Not only in US, but globally

Easy to launch



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

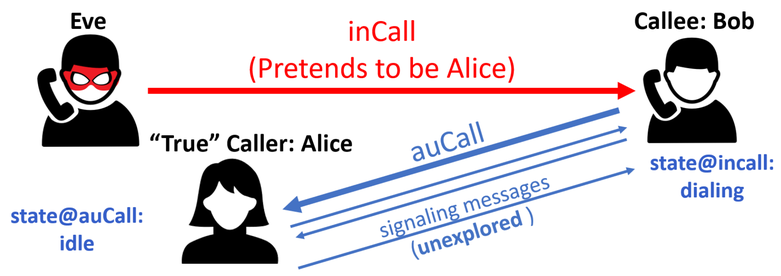


Hard to defend

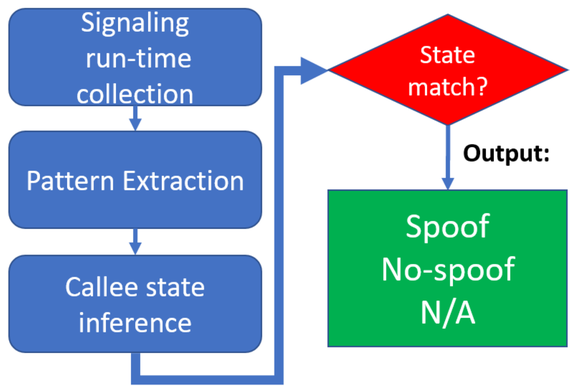
However, there is no practical solution in place:

- 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

How CEIVE works?



- 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



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

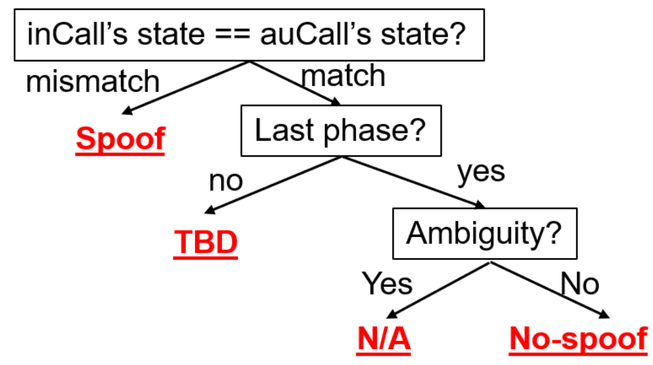
(Use VoLTE as an example)

- Rich set of signaling messages carry rich context information

Field	Reference: Values (examples)
SIP response codes	RFC3261: e.g., 200 OK, 180 Ringing, 181 Call Is Being Forwarded, 182 Queued, 183 Session Progress, 301 Moved Permanently, 480 Temporarily Unavailable, 481 Call/Transaction Does Not Exist, 486 Busy Here, 487 Request Terminated, ・・・
PEM	RFC5009: sendrecv, sendonly, recvonly, inactive
URN-Alert	RFC7462: normal (default), call-waiting, forward, recall:callback, recall:hold, recall:transfer, ・・・
VoLTE FSM	TS24.229, TS24.628, TS24.615: e.g., carrying early-media value or alert-info in 180/183, call terminated by network when busy ・・・

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

2. Two-phases verification strategy

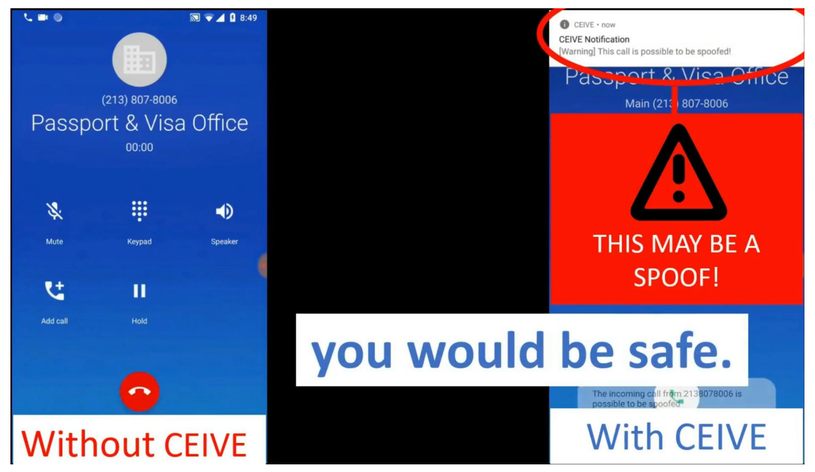


What CEIVE achieves

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**
  - ✓ 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.

PURDUE UNIVERSITY Discovery Park

CERIAS