Caller ID Verification in SIP

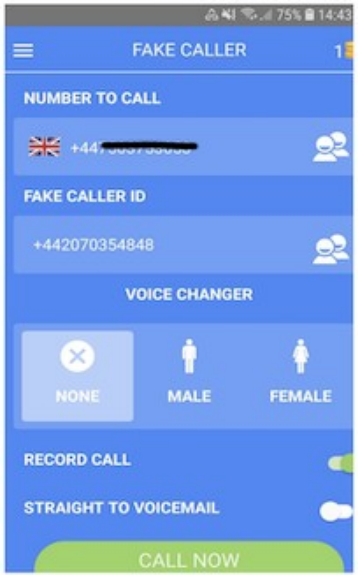
Feng Hao

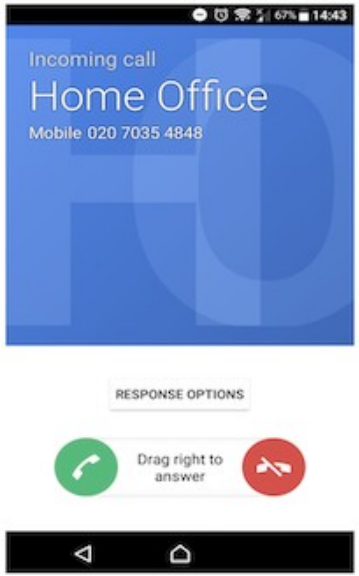
University of Warwick, UK

IETF 122 STIR WG, 2025

Caller ID spoofing

- Modify the caller ID to a different number
- In the old days, only the carriers can do this and there were only few carriers
- With VoIP, modification is trivial
- Fraudsters are abusing it as part of a social engineering attack





STIR/SHAKEN

- Digitally sign every call (caller ID included in the signed content)
- Mandated in US since 2021
- Do we need another solution?

Do we need another solution?

- In SHAKEN, any signed content is automatically accepted as “genuine”
- The security of a digital signature critically relies on key management
- If the carrier’s private key is lost, the attacker can impersonate any caller ID (or any RCD) to any telephone user in the country.
- SHAKEN does not authenticate the caller ID in real time.
- We currently don’t have a solution on this.

An overview of Caller ID Verification (CIV)

- Alice calls Bob: INVITE request with a “**civ**” tag in Purpose
- Bob holds the call and makes a verification call with “**civ-veri-call**” value
  - Like a flash call
  - Embed 4 random digits as a challenge in the caller ID
- In response, Alice sends the same digits to Bob through DTMF

https://datatracker.ietf.org/doc/draft-hao-civ/ for more details.

Comments on -00

1. Reflection DoS attack
   - [OK] Terminating carrier can easily block them based on comparing “civ-veri-call” and state.
2. Enterprise/Call center
   - Multiple outbound servers, inbound servers without matching relation
   - [OK] Use a few bits in session ID to encode the outbound server
3. Call forwarding to multiple numbers simultaneously
   - [OK] Revise to allow the originating carrier to receive multiple challenges and match them to the call based on session ID. Only one call can be connected.
4. Conditional forwarding shows unverified caller ID
   - [OK] Same as above. We will verify caller ID before testing forwarding conditions

Conclusion

- CIV provides an option to do real-time validation of caller ID when needed
- The trade-off is a single round-trip time (1-RTT)
- Need to keep this latency negligible, so it is unnoticeable to the caller

Recall HTTP/HTTPS

- HTTPS provides a secure comm option over HTTP
- At the cost of extra round trips (2 in TLS 1.2 and 1 in TLS 1.3)
- The latency difference between HTTP and HTTPS has become negligible