An Introduction to CIV

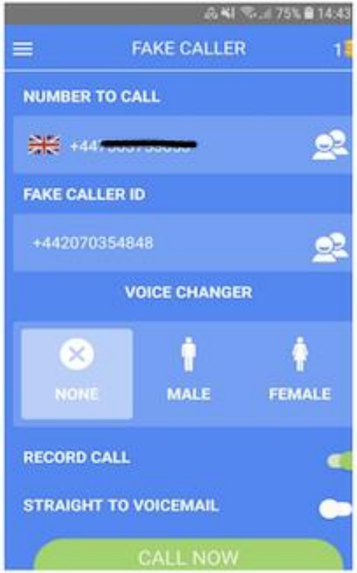
Feng Hao

University of Warwick, UK

SIPNOC 2024

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



FAKE CALLER

NUMBER TO CALL

+44[redacted]

FAKE CALLER ID

+442070354848

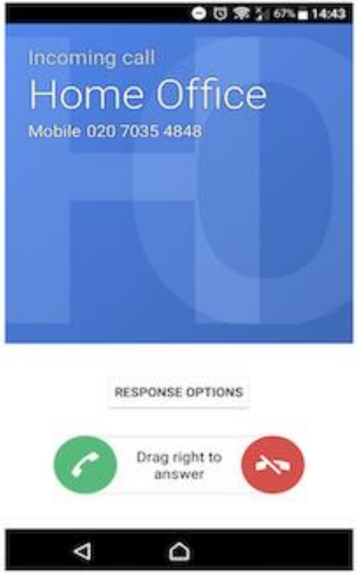
VOICE CHANGER

NONE MALE FEMALE

RECORD CALL

STRAIGHT TO VOICEMAIL

CALL NOW



Incoming call

Home Office

Mobile 020 7035 4848

RESPONSE OPTIONS

Drag right to answer

Spoofing is not necessarily an attack

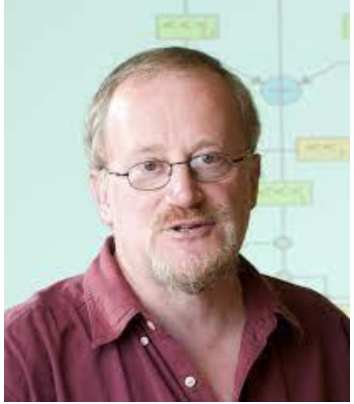
- Caller ID is like the return address on an envelope
- Sometimes you write a different return address for good reasons
- Legitimate cases of number spoofing
  - Using your mobile number as the VoIP caller ID
  - Using a toll-free number for customers to call back
- Illegitimate cases of number spoofing
  - Pretending to be immigration/tax authority
  - Pretending to be in the local area (neighborhood spoofing)
- How to distinguish the two?
  - We distinguish them based on the “possession of the number”

Two categories of solutions

1. Top-down
   - Based on a trusted third party
   - STIR/SHAKEN
2. Bottom-up
   - Does not require a trusted third party
   - Caller-ID Verification (CIV)

Trusted third party

“A trusted third party is a third party who can break your security policy.”



- Professor Ross Anderson (Cambridge)

STIR/SHAKEN

- An industry-driven standard, developed by IETF
- Add a digital signature to every call
- Need a public key infrastructure (trusted certificate authorities)
- FCC mandate on the adoption of STIR/SHAKEN in the US in June 2021

Key problems with STIR/SHAKEN

1. Authentication mismatch
2. Trusted third party
3. Works with IP networks only

Problem 1: authentication mismatch

- The FCC defines STIR/SHAKEN “an industry-standard caller ID authentication technology” – a source of confusion
- What does the “authentication” mean?
- Recall authentication factors: 1) secret knowledge; 2) token; 3) biometrics
- In STIR/SHAKEN, authentication is based on 1) secret knowledge of a signing key, but only the carrier has the key
- Therefore, SIT/SHAKEN is a “carrier authentication technology”
- But that solves a different problem

How about caller ID authentication?

- Carriers include a claim (attestation) about the authenticity of the caller ID
- **Key problem** - how to distinguish legitimate and illegitimate spoofing?
  - This needs a “common numbering database” (Ofcom)
  - But this database doesn’t exist; creating one is infeasible
- STIR/SHAKEN solution is to use A, B, C levels to a label a “claim” but this doesn’t solve the key problem

	Carrier attests the caller is authentic	Carrier attests the caller can use the caller ID
Full (A)	Yes	Yes
Partial (B)	Yes	Not sure
Gateway (C)	Not sure	Not sure

Problem 2: Trusted third party

- Several USA telcos were appointed by FCC as CAs
- All other telcos must pay them fees for certificates (based on % of revenues)
- The FCC is the effectively the root of the trust
- This cannot scale up
- Other countries will not want to trust and pay these CAs

Problem 3: Works with only IP networks

- Need to transmit not only a digital signature, but also a chain of certificates
- Typically, this is 1 to 2 kilobytes data
- Traditional networks don’t support this due to much limited bandwidth

UK Ofcom consultation (2023 - 2024)

- Should the UK adopt STIR/SHAKEN?
- A public consultation by Ofcom
  - Started in June 2023
  - Concluded in February 2024
- In Ofcom final assessment report
  - **“We should not proceed with CLI authentication [STIR/SHAKEN] at this time”**
- This begs the question: what are the alternatives to STIR/SHAKEN?

An alternative to STIR/SHAKEN

- Caller ID Verification (CIV)
  - Authenticates the caller ID (not the carrier)
  - Does not require any trusted third party
  - Works with IP and non-IP networks
- Based on a peer-reviewed paper (research funded by EPSRC)
  - Wang, Delavar, Azad, Nabizadeh, Smith, Hao, "Spoofing Against Spoofing: Towards Caller ID Verification In Heterogeneous Telecommunication Systems," *ACM Transactions on Privacy and Security*, 2023 https://arxiv.org/abs/2306.06198
  - Not patented; free to use

UKRI

Engineering and
Physical Sciences
Research Council

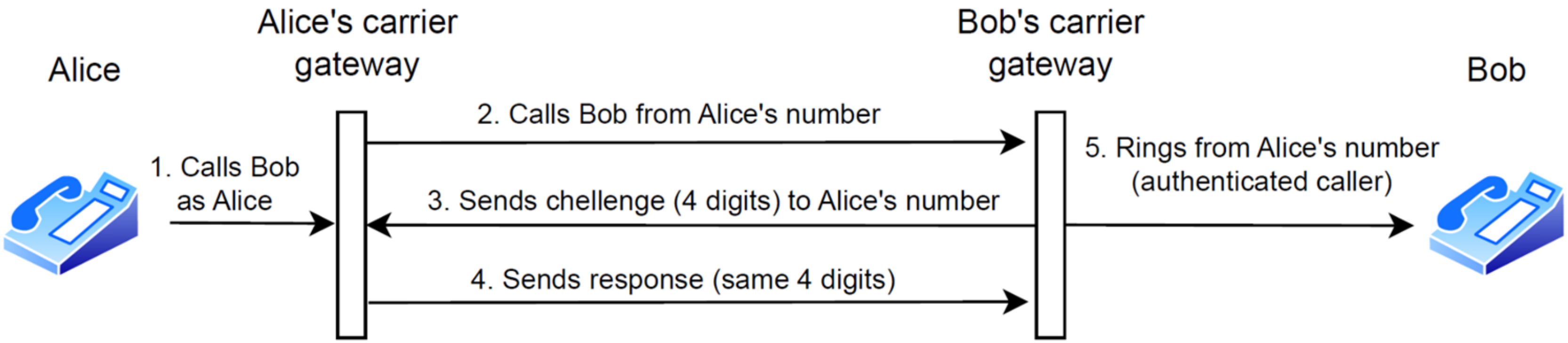
High-level intuition of CIV

- When receiving a suspicious call, one solution of verifying the caller ID is to call back the number and see if you talk to the same caller.
- CIV follows a similar idea, but it automates the verification process through a challenge-response protocol

A challenge-response protocol

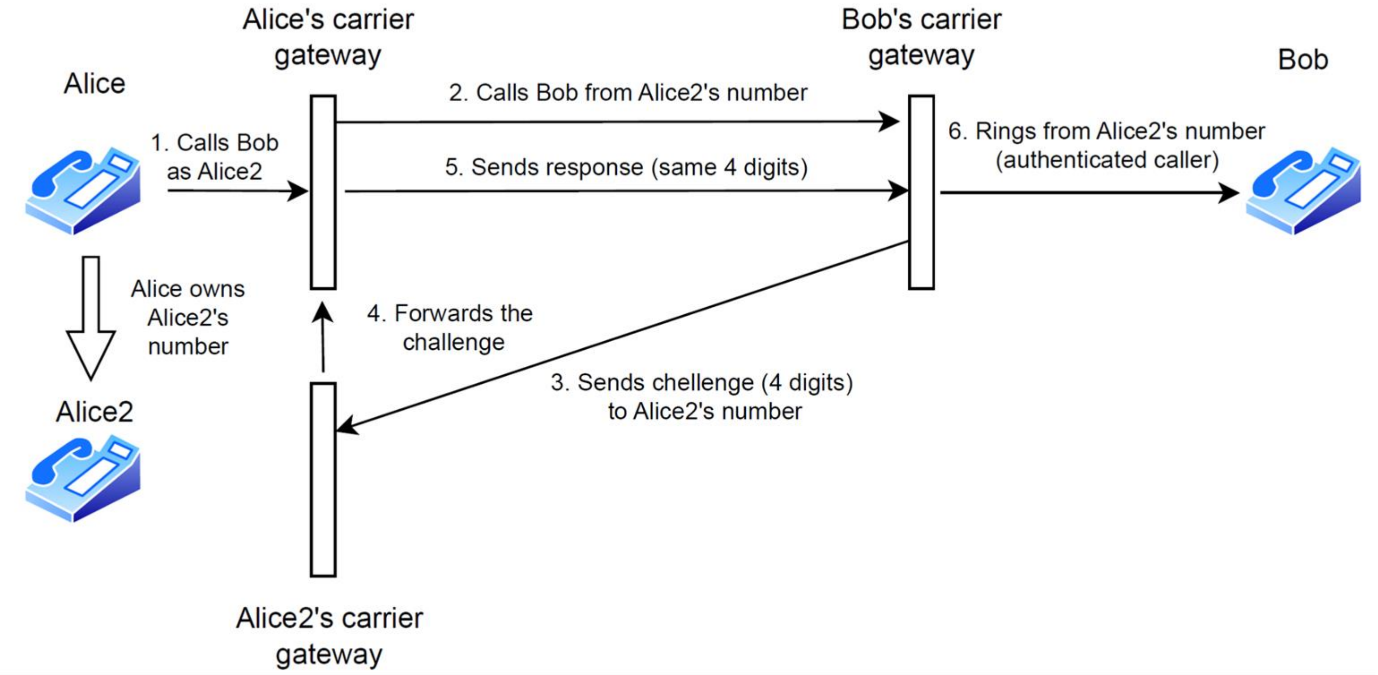
- Alice calls Bob: INVITE request with an indication of support for CIV
- Bob holds the call and makes a verification call to the caller ID: sending 4 random digits as a challenge by embedding the digits as part of the caller ID
    - Like a flash call
    - Require number spoofing, which is available to all carriers
- In response, Alice sends the same digits to Bob through DTMF
    - DTMF is universally supported by IP and non-IP networks

Case 1: legitimate caller uses an unmodified number


Alice
Alice's carrier gateway
Bob's carrier gateway
Bob
1. Calls Bob as Alice
2. Calls Bob from Alice's number
3. Sends chellenge (4 digits) to Alice's number
4. Sends response (same 4 digits)
5. Rings from Alice's number (authenticated caller)

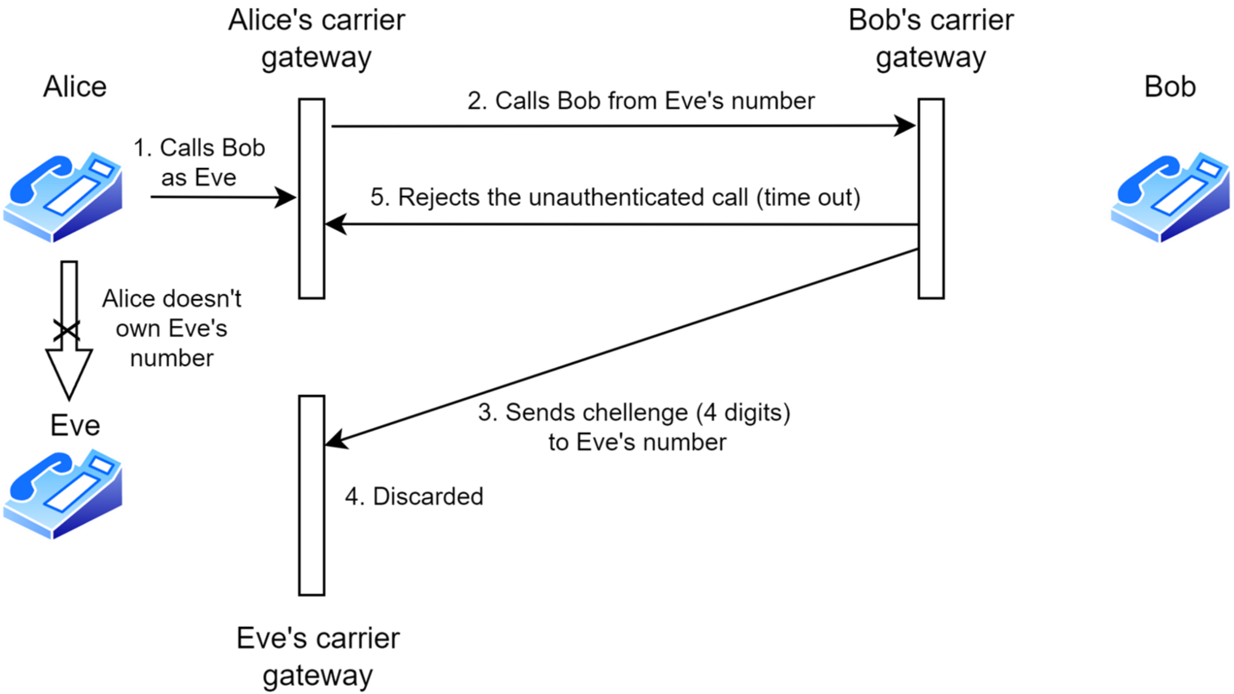
- The call is rejected at the gateway if the caller indicates support for CIV but the challenge-response fails

Case 2: legitimate caller uses a modified number they own


Alice's carrier gateway
Bob's carrier gateway
Bob
Alice
2. Calls Bob from Alice2's number
1. Calls Bob as Alice2
6. Rings from Alice2's number (authenticated caller)
5. Sends response (same 4 digits)
Alice owns Alice2's number
4. Forwards the challenge
3. Sends chellenge (4 digits) to Alice2's number
Alice2
Alice2's carrier gateway

- Alice sets the call-forwarding function since she owns the number
- In case of PBX: need to keep states of outgoing calls and match them with verification calls

Case 3: illegitimate caller uses a modified number they don’t own


Alice's carrier gateway
Bob's carrier gateway
Alice
Bob
2. Calls Bob from Eve's number
1. Calls Bob as Eve
5. Rejects the unauthenticated call (time out)
Alice doesn't own Eve's number
Eve
3. Sends chellenge (4 digits) to Eve's number
4. Discarded
Eve's carrier gateway

- Eve discards the challenge if it finds 1) no outgoing call from Eve; 2) no call-forward configuration
- A real attacker will most likely choose a carrier that doesn’t support CIV (downgrade attack)

Possible downgrade attack

	Originating carrier	Terminating carrier	Presentation to the called user
1	Supports CIV	Supports CIV	Caller ID with explicit “**verified**” status
2	Doesn’t support CIV	Supports CIV	Caller ID with explicit “unverified” status
3	Supports CIV	Doesn’t support CIV	Caller ID with implicit “unverified” status
4	Doesn’t support CIV	Doesn’t support CIV	Caller ID with implicit “unverified” status

- CIV supports active authentication: the caller must cooperate to pass authentication
- Any downgrade attack will lead to the caller ID “unverified”

Comparison

	STIR/SHAKEN	**CIV**
Mechanism	Digital signatures	Challenge-response
Authentication	Carrier	Caller
Distinguish legitimate and illegitimate spoofing	No (left to carriers)	Yes
PKI and trusted third parties	Yes	No
Date transmission	Signature + certificate chains (kb)	4 digits
Telephony networks	SIP-only	All networks
Overhead	Verifying signature (may involve round trips to check status of certificates)	A round-trip to send/receive 4 digits

Supporting CIV in SIP

- Sending the challenge through spoofing is supported by all existing carriers
- Send the response through DTMF is universally supported
- We need a flag to indicate support for CIV in the INVITE request
- We propose an extension to the INVITE header
  - Adding a “civ” tag in the Supported header to indicate support for CIV
  - Adding a “civ-verification-call” value for the Purpose parameters of Call-Info to indicate it’s a verification call (networks just need to route the call without allocating resources)
- An IETF Internet Draft is under submission; comments are welcome.

Contact: feng.hao@warwick.ac.uk