What is caller-ID spoofing?

Caller deliberately falsifies their caller-ID to disguise their identify.
Why worry about caller-ID spoofing?

Average of $700 each in 2017, for a total loss of $332 million

DA: One victim in SF ‘Chinese Embassy Scam’ lost $3 million in con job

People have reported losing thousands to Chinese-language phone scams, but what can be done?

Halton police’s non-emergency telephone number ‘spoofed’
Caller-ID spoofing is a growing problem

Nearly 50% Of U.S. Mobile Traffic Will Be Scam Calls By 2019

% OF SPOOFED CALLS IN THE US

FIRST ORION
TRANSPARENCY IN COMMUNICATION
Why is caller-ID spoofing still feasible?

Evolved Packet Core (EPC)
Subscriber Identifiers: IMSI, MSISDN

IP-Multimedia Subsystem (IMS)
Subscriber Identifiers: SIP (TO, FROM)
Lack of runtime authentication

Lack of *Runtime Authentication* in VoLTE calls can lead to caller-ID spoofing
Existing solutions

Network
- Passive Validation

Endpoint
- Callback
- Verification

Active User Authentication (CHAP, TLS)

Provider
- Network
- Network

(1) Call-Setup
(2) Validate
(3) Validate
(4) Validate
(5) Validate
Comparison of runtime caller-ID validation solutions

Telecom regulatory bodies such as the FCC in US now require network operators to provide caller-ID authentication.

- Robust Passive Validation Solution
  - Network: NASCENT
  - Active User Authentication (CHAP, TLS)

Lower overheads
Easier to deploy

Deployment Complexity

End points
- Third Party Certificate
- Callback Verification
Network Assisted Caller-ID Validation with NASCENT

Detect

Analyze

Deploy
Why is caller-ID spoofing still feasible?

Can we leverage EPC authentication to support runtime caller-ID validation?
Leverage EPC authentication to perform runtime caller-ID validation
Leverage EPC authentication to perform runtime caller-ID validation.

1. INVITE (Caller-ID)
2. INVITE
3. INVITE

(1) The PGW is not SIP aware.
(2) Subscriber preferences are configured at IMS level.

FROM: Alice, TO: Bob

MSISDN = Caller-ID

Validate Caller-ID

EPC INVITE

Alice Calling

FROM: Alice, TO: Bob
Challenges in the real world (1)

Leverage EPC authentication to perform runtime caller-ID validation

FROM: Alice, TO: Bob

1. INVITE (Caller-ID)
   FROM: Alice, TO: Bob

2. INVITE
   EPC
   INVITE
   PGW

3. Verify (Caller-ID)
   Existing Procedure
   NASCENT Extension

4. Verify Response

5. INVITE
   IMS
   Alice Calling
   FROM: Alice, TO: Bob

1a. Create Mapping
   Caller-ID
   MSISDN

3a. Fetch Mapping
   Key Value Store (Local/Remote)

SIP message processing is done at IMS
Challenges in the real world (2)

1. **INVITE** (Caller-ID)

   - EPC
   - INVITE

2. **INVITE**

   - PGW
   - IMS

   - No direct connection exists between the PGW and IMS
     - PGW and IMS interface via the Policy Control and Charging Function (PCRF)

3. **Verify (Caller-ID)**

4. **Verify Response**

(2) IMS Access control procedure is performed after the Callee is Notified.

- **Gx Interface**
- **Rx Interface**

1. **INVITE** (Caller-ID)

2. **INVITE**

3. **183 (IN-PROGRESS)**

   - 2a. INVITE

5. **Re-Auth Request**

6. **Re-Auth Response**

7. **AA Response**

4. **AA Request**
NASCENT: Trade-offs in the real world

<table>
<thead>
<tr>
<th>Spoofed Call Notification</th>
<th>Overhead</th>
<th>Backward Compatibly</th>
<th>New Interfaces?</th>
<th>NASCENT Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Notification</td>
<td>Low</td>
<td>Yes</td>
<td>No</td>
<td>NASCENT-Rx-Gx</td>
</tr>
</tbody>
</table>

IMS Access control procedure is performed before the Callee is notified.
NASCENT vs Existing runtime caller-ID validation

NASCENT is a network supported Passive Validation solution that leverages Trusted EPC Identifiers to detect caller-ID spoofing.

Active User Authentication (CHAP, TLS)

Network

Passive Validation

Network

Endpoin

Third Party Certificate

Callback Verification
Experimental Evaluation
Experimental evaluation goals

- What is the performance overhead of *NASCENT*?
  - Resource overhead (CPU)
  - Latency incurred by users
- How does *NASCENT* compare with other Active User Authentication solutions (CHAP)?
Evaluation results (Traditional Deployment)

PERCENTAGE OF SUCCESSFUL CALLS AT 0% SPOOFED CALLS

Baseline
Active-Validation (CHAP)
NASCENT-Rx-Gx

NASCENT has significantly lower resource overhead
Evaluation results (Traditional Deployment)

AVERAGE LATENCY AT 0% SPOOFED CALLS

- Baseline
- Active-Validation (CHAP)
- NASCENT-Rx-Gx

Up to 70% lower latency incurred compared to CHAP
Experimental evaluation goals

- How does the Service Deployment Model impact the performance?

**Traditional**

- PCRF
- PGW
- IMS
- SIP Server
- REST

**NFV**

- PCRF
- PGW
- IMS
- SIP Server
- REST

Physical machines
Evaluation results (NFV Deployment)

- Lower overheads due resource sharing between EPC and IMS
Much more in the paper..

• **NASCENT** variants and trade-offs
  • Backward compatibility vs performance overhead

• Selective validation of caller-ID
  • **NASCENT** has negligible overhead if 5% of calls are validated

• Will **NASCENT** work in 5G?
Conclusions

• Caller-ID spoofing is an important and challenging problem
  • Existing solutions have high infrastructure and performance overheads

• NASCENT proposes a cross validation based solution to detect Caller-ID spoofing
  • Leverage existing EPC authentication
  • Multiple variants to balance trade-offs

• NASCENT outperforms existing solutions
Questions?
Backup
Experimental setup

VNF  | Functionality                                   | Components          | Software
---   | -----------------------------------------------|---------------------|-------
IMS CSCF | SIP Call setup + Caller-ID validation          | SIP Server + REST   |       
PCEF   | Tunnel SIP Traffic + Diameter Gx + Caller-ID Mapping management | REST, Diameter       |       
PCRF   | Diameter Gx + Rx Interface Support            | Diameter            |       
Load Generator | Generate SIP traffic                         | SIPp                |       

Load Generator

SIPp

PCEF

REST

PCRF

IMS CSCF

SIP Server

REST

Docker

Docker open implementation
Evaluation Results (Traditional Deployment)

CPU UTILIZATION WITH 0% SPOOFED CALLS

- Baseline
- Active-Validation(CHAP)
- NASCENT-Rx-Gx
Why is Caller-ID spoofing possible in 4G?

Packet Delivery + Call Addressing

2G

Evolved Packet Core (EPC)
Subscriber Identifiers: IMSI, MSISDN

FROM: Alice, TO: Bob
GTP
INVITE

4G

IP-Multimedia Subsystem (IMS)
Subscriber Identifiers: SIP (TO, FROM, etc)

FROM: Alice, TO: Bob
INVITE

Invoking Call Addressing