Caller ID Spoofing and Call Authentication Technology

MODERATOR:
Kati Daffan, FTC

PANELISTS:
Henning Schulzrinne, FCC
Adam Panagia, AT&T
Patrick Cox, TrustID
Vijay A. Balasubramaniyan, Pindrop Security
Henning Schulzrinne
Chief Technology Officer
Federal Communications Commission
Caller ID Act of 2009: *Prohibits any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.*
Number authentication

From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.net>
Contact: <sip:alice@pc33.example.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE

RFC 3893 (2004)

public-private key pair provided with phone number
Caller identification

- known caller
- previous calls
- sent her emails

- name unimportant
- bank ✔
- credit card office ✔

- name unimportant
- IEEE ✔
- known university ✔

what’s your SSN?

can you recommend student X?
Attribute validation

Attribute Reference ID (ARID)
https://fcc.gov/4163

1. Requests an ARID, selecting attributes to disclose

2. Makes a call with the ARID and part of access code

3. Validates ARID with access code and retrieves selected attributes (e.g., Alice’s role)

Attribute Validation Server (AVS): Issuer
e.g., fcc.gov

{Alice’s username, credentials, user ID, role}

HTTP over TLS
SIP over TLS

Caller: Principal = Alice
Employee of fcc.gov
tel:+12345678

Callee: Relying Party = Bob
Accepts calls from members in *.gov; does not know Alice’s phone number
Adam Panagia

Director
AT&T Network Fraud Investigations
Caller ID Spoofing and Call Authentication Technology

Current legislation prohibits Caller ID spoofing if the intent is to defraud, cause harm, or wrongfully obtain anything of value.

Historically spoofing required an advanced knowledge of telephony equipment and could be quite expensive.

Spoofing is now available to the amateur due to the availability of open source software. The cost and the effort have been drastically reduced; thus decreasing the barrier to entry which has resulted in significant increases in the incidents of malicious large scale spoofing events.

There are currently no available solutions in the Public Switched Telephone Network that completely “eliminate” this risk.
“CALLER ID SPOOFING”

The practice of sending false or misleading information, so as to deceive the receiving party and/or hide the caller’s true identity and/or call origination.
Mass Calling Generator with "Spoofing" capability

Robo Call Flow

Provider A

Provider B

Provider C

AT&T

End Users

PSTN

VoIP

PSTN

VoIP

PSTN
Terminating Call Distribution Call Flow

Mass Calling Generator with “Spoofing” capability

VoIP Provider

Provider 1

Provider 2

Provider 3

Provider C

Provider D

Provider E

Provider F

Provider G

Local Service Provider

Provider A

Provider B
Patrick Cox
CEO
TrustID
Who is TRUSTID and why are they represented at the FTC Robocall Summit?

TRUSTID technology enables businesses to **Serve Customers, Not Criminals**

- TRUSTID credentials Caller ID and ANI, so that companies will know with certainty
  - who is *really* calling them before they answer
  - in an undetectable way
  - that stops spoofers from causing mayhem
  - and protects customer and company assets
Why does my Caller ID sometimes show my Bank calling, when they aren’t?

Up to about 2004, Caller ID was mostly trustworthy

- That changed when the Internet and the telephone-network became deeply connected
- Now, anybody in the world with an Internet connection & basic computer skills controls Caller ID
- Threats to telephone-network security now resemble Internet security threats
HOW TRUSTID AUTHENTICATION WORKS

1. A customer calls your call center claiming identity using an unvalidated telephone number (Caller ID or ANI).

2. The caller’s claimed telephone number is transmitted to TRUSTID using secure https—before the call is answered.

3. Employing network-based physical authentication, TRUSTID determines the authenticity of the caller’s telephone number and credentials.

4. Caller’s credentials are returned to the call center within seconds.
TRUSTID’s technology value is in the **green** calls

- Authenticated Callers: Landline, Wireless, Non-PC VoIP
- Non-Authenticated
- Spoofed ANI
- PC VoIP
Can TRUSTID stop spoofing on my home phone too?

- TRUSTID technology requires the line types (i.e. PRI) and PBX equipment that businesses use and will not work for consumers today.
Vijay Balasubramaniyan, PhD
CEO & Co-founder
Pindrop Security
State of Fraud Report

There were 1,296,554 fraud calls from January-June 2012.

That's a 29% increase since 2H of 2011.

Or five fraud calls every minute.
State of Fraud Report

Fraudsters still use VOIP phones the most but cell phone use increased by almost 300% in the last 6 months.

- 46% VOIP
- 14% Cell Phone
- 40% Landline
State of Fraud Report

FRAUD CALLS HAPPEN EVERYWHERE
FREQUENCY OF ATTACK BY STATE PER CAPITA

1 FRAUD CALL PER 3,000 TO 6,000 CITIZENS
1 FRAUD CALL PER 2,000 TO 2,999 CITIZENS
MORE THAN 1 FRAUD CALL PER 999 CITIZENS
The Phone Channel Is Vulnerable

- Caller ID is easily spoofed
- VoIP makes it cheap and easy to call globally
- No metadata transmitted - only data is audio signal

There’s an App for that!
Multi-layered Defense

Known Attackers
- Blacklist

New or Unknown Attackers
- Geography
  - Georgia
- Phone type
- Caller ID

Authentication
Acoustic Fingerprinting

- LOSS
  - Packet loss
  - Robotization
  - Dropped frames

- NOISE
  - Clarity
  - Correlation
  - Signal-to-noise ratio

- SPECTRUM
  - Quantization
  - Frequency taggers
  - Codec artifacts

- VOICE
  - Timbre
  - Range
  - Obfuscation

Call Audio

Acoustic Fingerprint

Risk Score

Phone Type

Geo-location

Known Fraud Caller

RISK SCORE
Protecting the Phone Ecosystem

INPUTS

Enterprise Traffic
- Call centers
- Recorded calls
- Anti-fraud teams

Consumers
- Complaints
- Web
- Phones
- PindropSecurity.com

Attack Data
- Phoneypots
- Spam/phishing

AUTOMATED ANALYSIS

Acoustical Fingerprinting

Reputation Analysis

Active Recon

Carriers

Enterprises

Home/Mobile