From Understanding Telephone Scams to Implementing Authenticated Caller ID Transmission

Huahong Tu (Raymond)

A Dissertation Presented in Partial Fulfillment of the Requirement for the Degree Doctor of Philosophy

CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

ASU Ira A. Fulton Schools of Engineering
Arizona State University

sefcom
security engineering for future computing

Committee Introduction

Adam Doupé, PhD, (Co-Chair)

Gail-Joon Ahn, PhD, (Co-Chair)

Ziming Zhao, PhD

Dijiang Huang, PhD

Yanchao Zhang, PhD

Overview

Problem: Telephone spam and scams

Cause: Impersonation and caller ID spoofing

Method: A novel architecture and method to authenticate the caller ID

Result: A security indicator, that can help to prevent users from becoming a victim of telephone spam and scams.

The Problem Statement

Understanding Why Telephone Scams Work

Identifying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

Implementing Prototype With Evaluations

Conclusion

The Problem Statement

Despite various efforts to curb the growth of unwanted calls—the FTC received record numbers of telephone spam, scam, and fraud complaints in the recent years.

Why existing solutions do not work effectively?

What is the root cause of the problem?

What kind of solution should be developed?

Americans lost $8.6 billion to phone fraud in last year, survey suggests

Herb Weisbaum
TODAY

Aug. 27, 2014 at 10:25 AM

Survey: 11% of adults lost money to a phone scam last year

Millennials were one of the most victimized groups

01/26/2016 | ConsumerAffairs | Scams

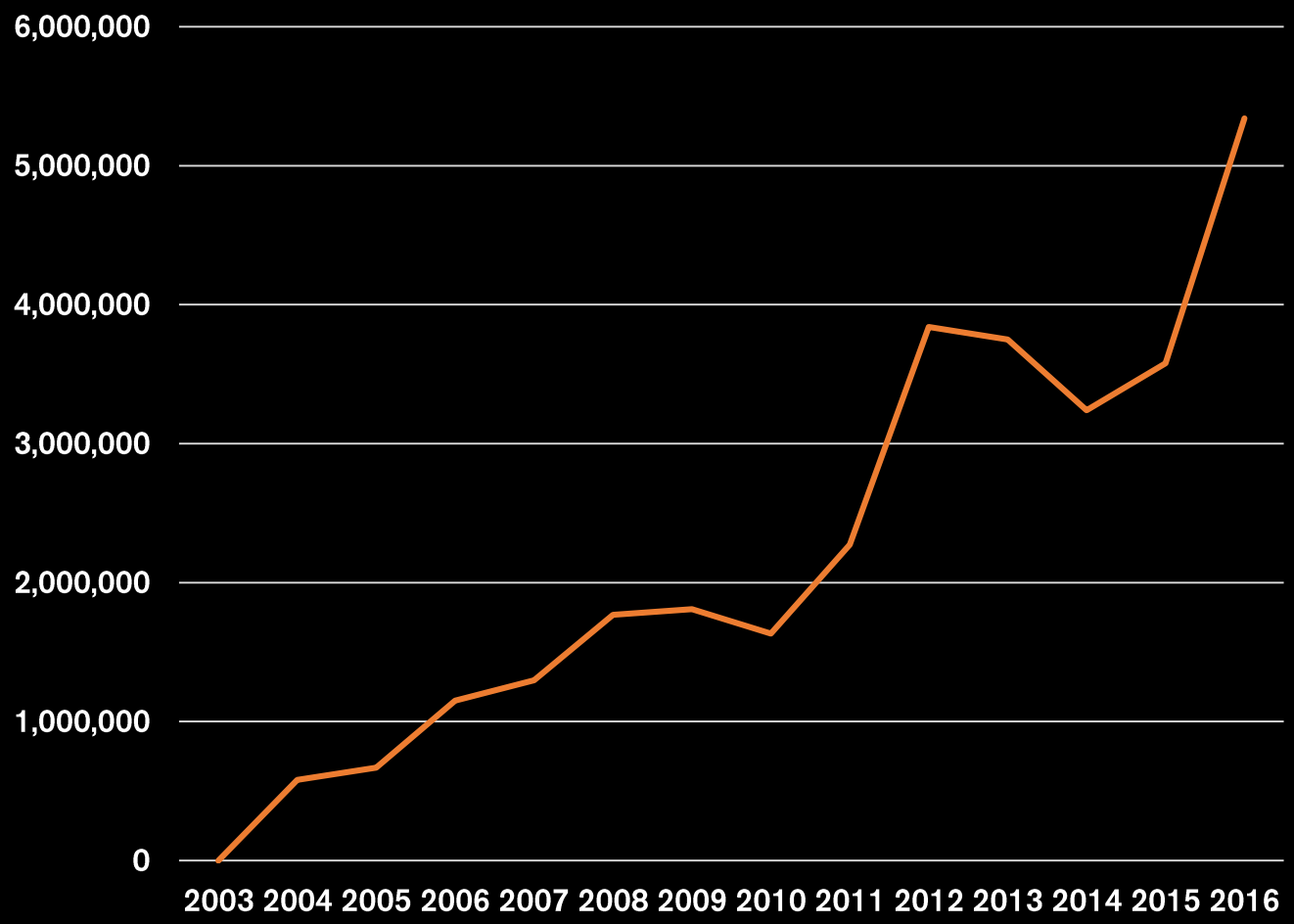
The New York Times | http://nyti.ms/ZBKHRz

TECHNOLOGY

Phone Hackers Dial and Redial to Steal Billions

By NICOLE PERLROTH OCT. 19, 2014

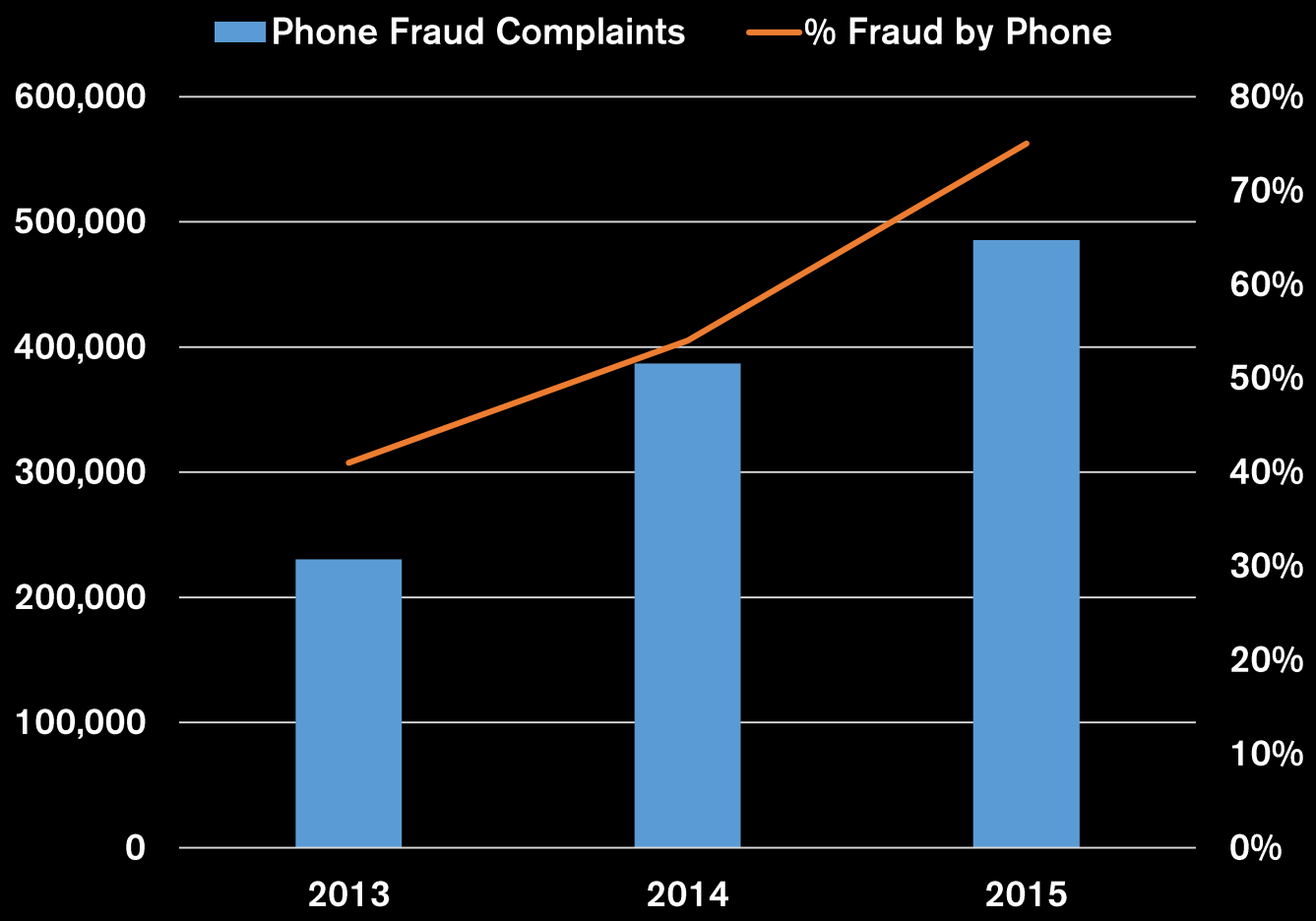
National Do-Not-Call Registry Complaints

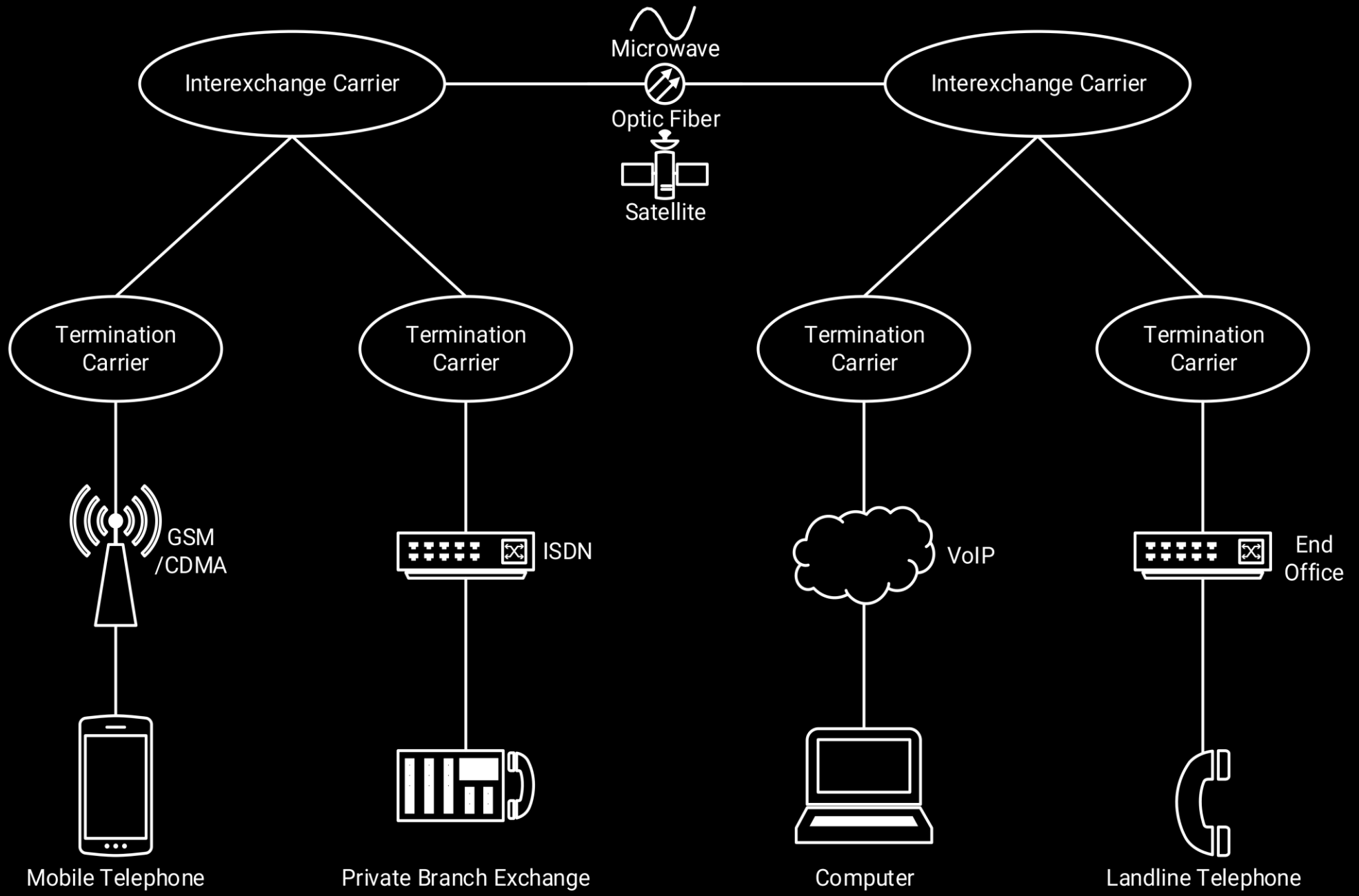


NATIONAL
DO NOT CALL
REGISTRY

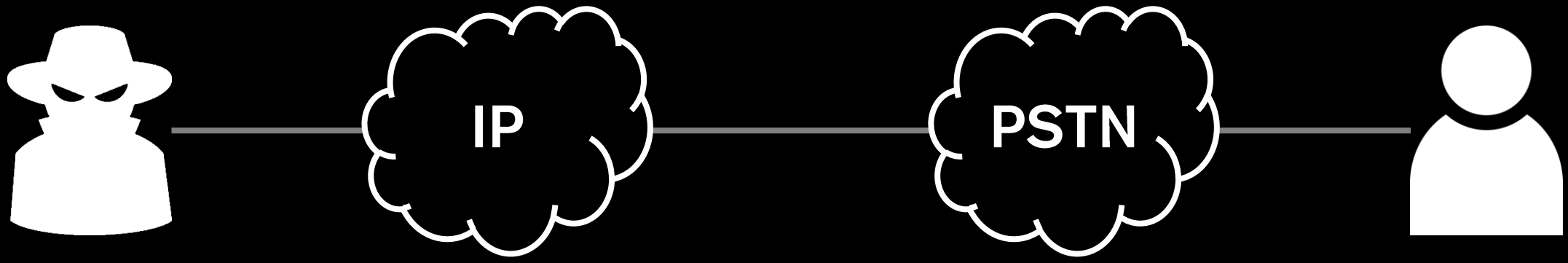
5,340,234
complaints
in 2016

FTC Phone Fraud Complaints

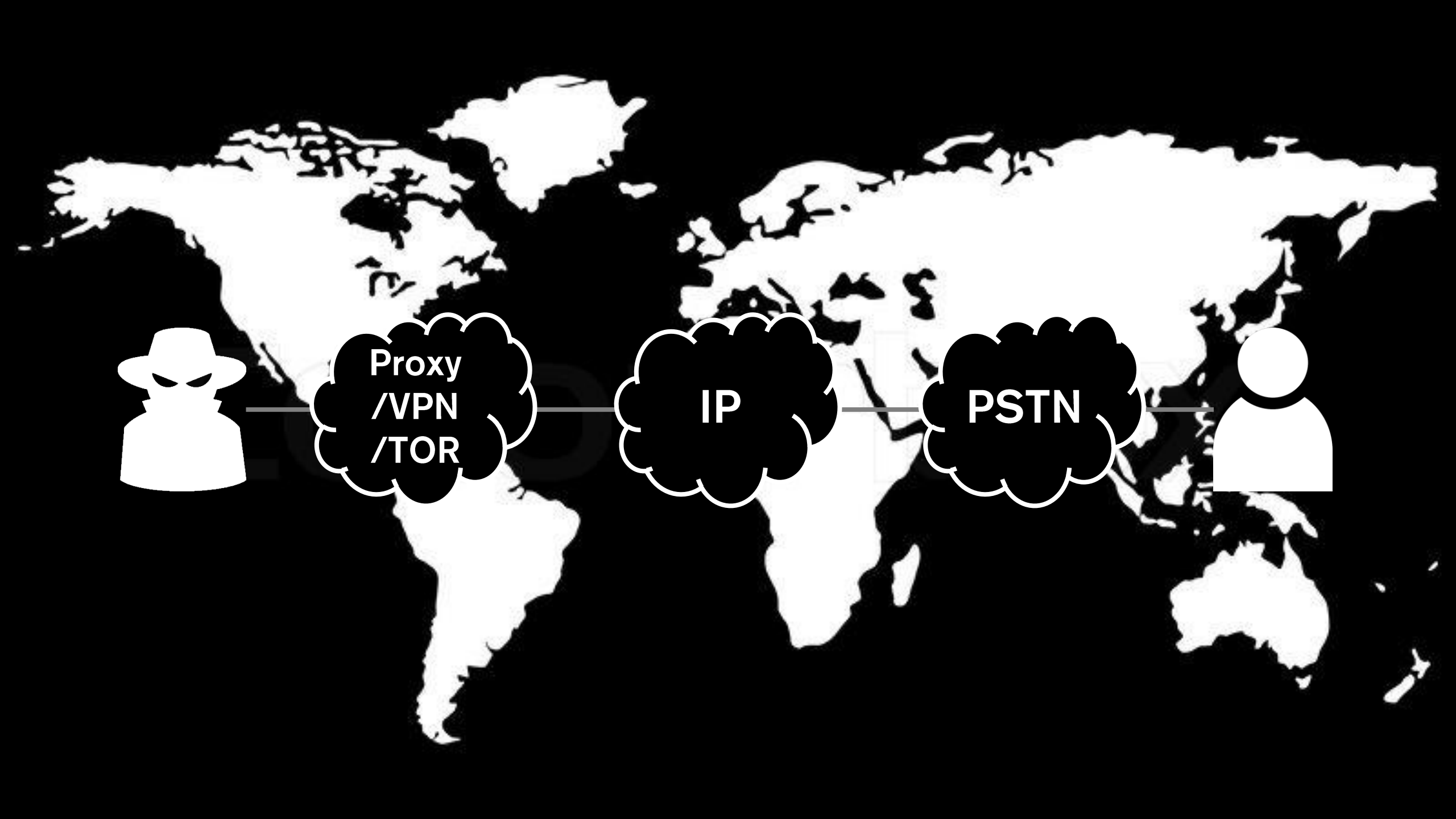



Microwave
Interexchange Carrier
Interexchange Carrier
Optic Fiber
Satellite
Termination Carrier
Termination Carrier
Termination Carrier
Termination Carrier
GSM /CDMA
ISDN
VoIP
End Office
Mobile Telephone
Private Branch Exchange
Computer
Landline Telephone


PSTN


IP
PSTN


Proxy
/VPN
/TOR
IP
PSTN


Proxy
/VPN
/TOR
IP
PSTN


Call Loop


One Call Now
A Send Word Now Company


call-em-all


VoiceShot
Your Do It Yourself Online Call Center


slybroadcast
Voice Messaging
for Business


VOICENT
CONNECT.ENGAGE.SUCCEED


CallFire


dialogtech

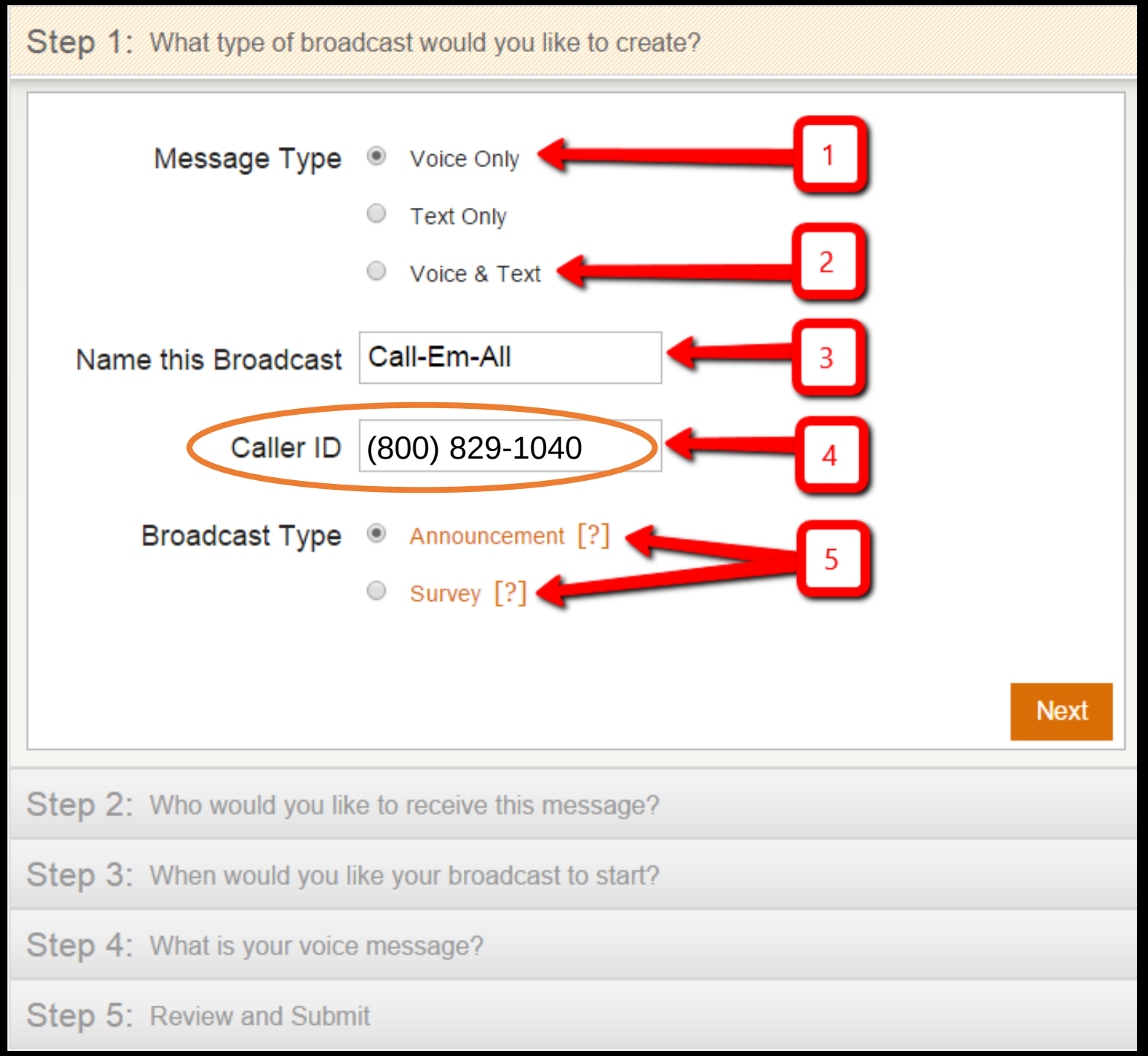

VoiceBlaze
Your Voice Broadcasting Headquarters.


TCMS


SimplyCast
Multi-Channel Marketing Solved!

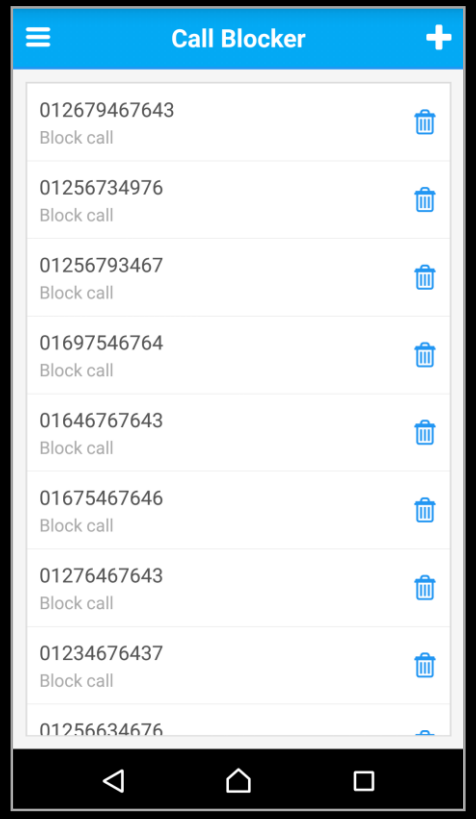
Type	Price	Unit
US Local Number	$0.3500	Per Month
Toll Free DID	$0.7500	Per Month
Call Inbound	$0.0055	Per Minute
Call Outbound	$0.0100	Per Minute
Call Toll Free Inbound	$0.0195	Per Minute
Call Toll Free Outbound	$0.0100	Per Minute
SIP Call Inbound	$0.0025	Per Minute
SIP Call Outbound	$0.0100	Per Minute
SMS Inbound	$0.0000	Per Message
SMS Outbound	$0.0050	Per Message
SMS Short Code Outbound	$0.0100	Per Message

Data source: Bandwidth Voice & Messaging API Platform


Step 1: What type of broadcast would you like to create?
Message Type
Voice Only
Text Only
Voice & Text
1
2
Name this Broadcast
Call-Em-All
3
Caller ID
(800) 829-1040
4
Broadcast Type
Announcement [?]
Survey [?]
5
Next
Step 2: Who would you like to receive this message?
Step 3: When would you like your broadcast to start?
Step 4: What is your voice message?
Step 5: Review and Submit


(800) 829-1040
IRS - Washington, DC

Existing Solutions



Rely on gathering offending caller IDs

Do not work effectively if the caller ID has been spoofed

Caller ID Spoofing

Make caller identification difficult

Defeat call blockers

Prevent feedback

Further impersonation scams

Hack into accounts

Conduct pranks

Frame caller ID owners

Avoid law enforcement

THE ORANGE COUNTY REGISTER

OC Watchdog

Fed up with rising robocalls, millions say 'Do Not Call' list doesn't work and want relief

Oct. 3, 2016 | *Updated Oct. 5, 2016 7:13 a.m.*

The Problem Statement

Understanding Why Telephone Scams Work

Identifying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

Implementing Prototype With Evaluations

Conclusion

Why Is It Important to Understand Telephone Scams?

75% of reported frauds are communicated over the phone.

Little research has been done to study why people fall for telephone scams.

Learning why telephone scams work can help us design more effective solutions.

How to Conduct a Study?

1. Collect scam samples
2. Identify attributes
3. Design experiments
4. Standardize experiment procedure
5. Disseminate phone calls
6. Collect and tabulate results
7. Select analysis criteria and present analysis results
8. Provide evaluations and recommendations

Attributes Identified

Area Code: e.g. 202, 480, 800

Caller Name: name associated with the caller ID

Voice Production: e.g. human or synthesized

Gender: e.g. male or female

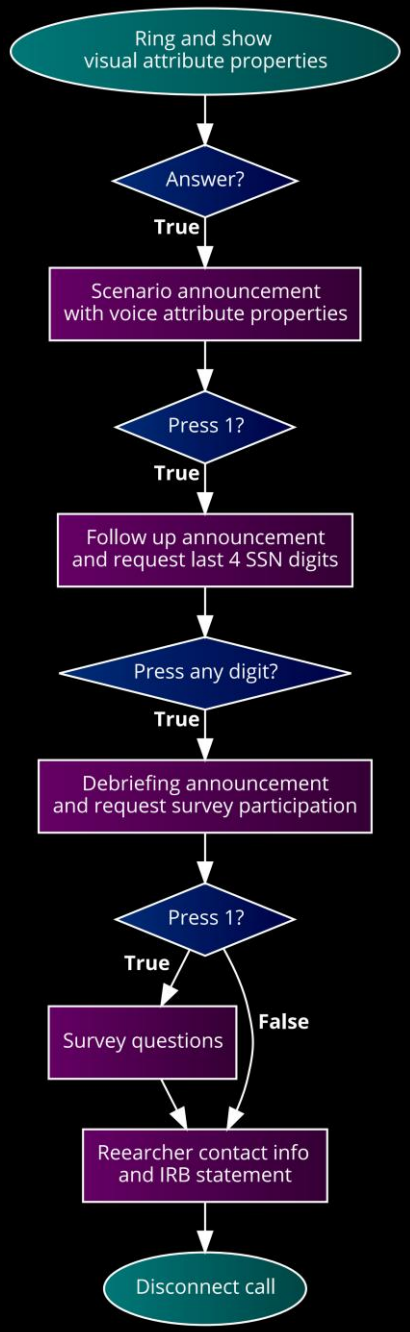
Accent: e.g. American or Indian

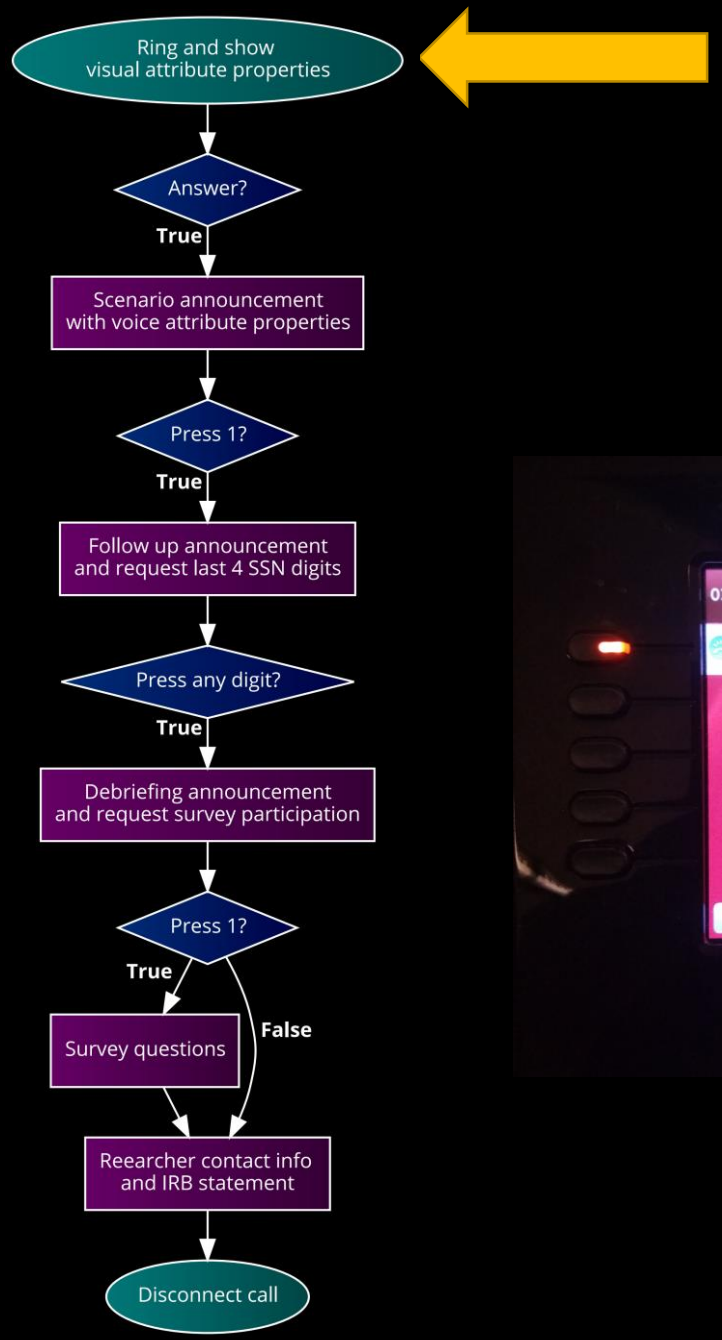
Entity: who to impersonate, e.g. IRS or HR

Scenario: motivation to divulge SSN, e.g. tax or payroll issue

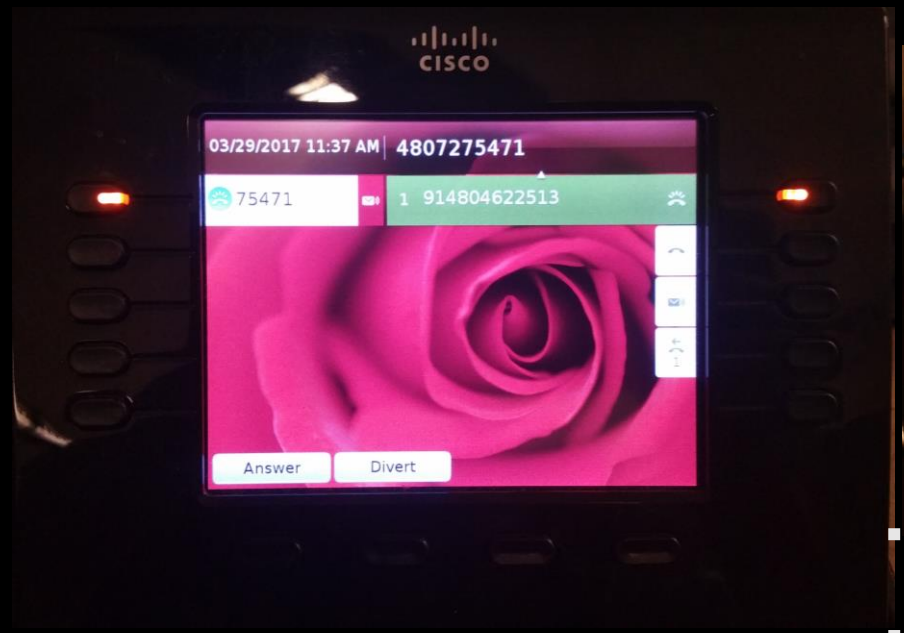
Experiment Groups

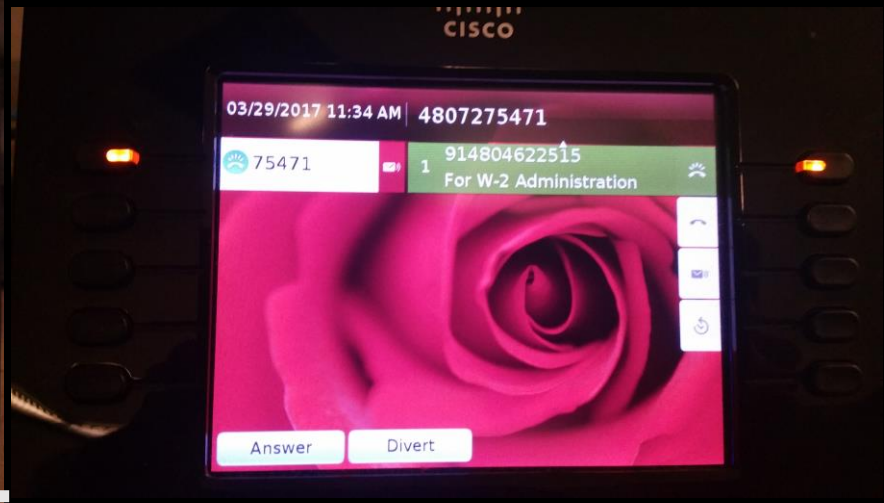
No.	Caller ID	Area Code Location	Caller Name	Voice Production	Gender	Accent	Entity	Scenario
E1	202-869-4555	Washington, DC	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E2	800-614-1339	Toll-free	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E3	480-939-5666	University Location	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E4	202-869-2440	Washington, DC	N/A	Synthesizer	Female	American	IRS	Tax Lawsuit
E5	202-869-2442	Washington, DC	N/A	Synthesizer	Male	American	IRS	Unclaimed Tax Return
E6	202-849-5707	Washington, DC	N/A	Human	Male	American	IRS	Tax Lawsuit
E7	202-869-4024	Washington, DC	N/A	Human	Male	Indian	IRS	Tax Lawsuit
E8	480-462-2513	University Location	N/A	Synthesizer	Male	American	EDU	Payroll Withheld
E9	480-462-2515	University Location	W-2 Administration	Synthesizer	Male	American	EDU	Payroll Withheld
E10	480-462-2517	University Location	N/A	Synthesizer	Male	American	EDU	Bonus Issued

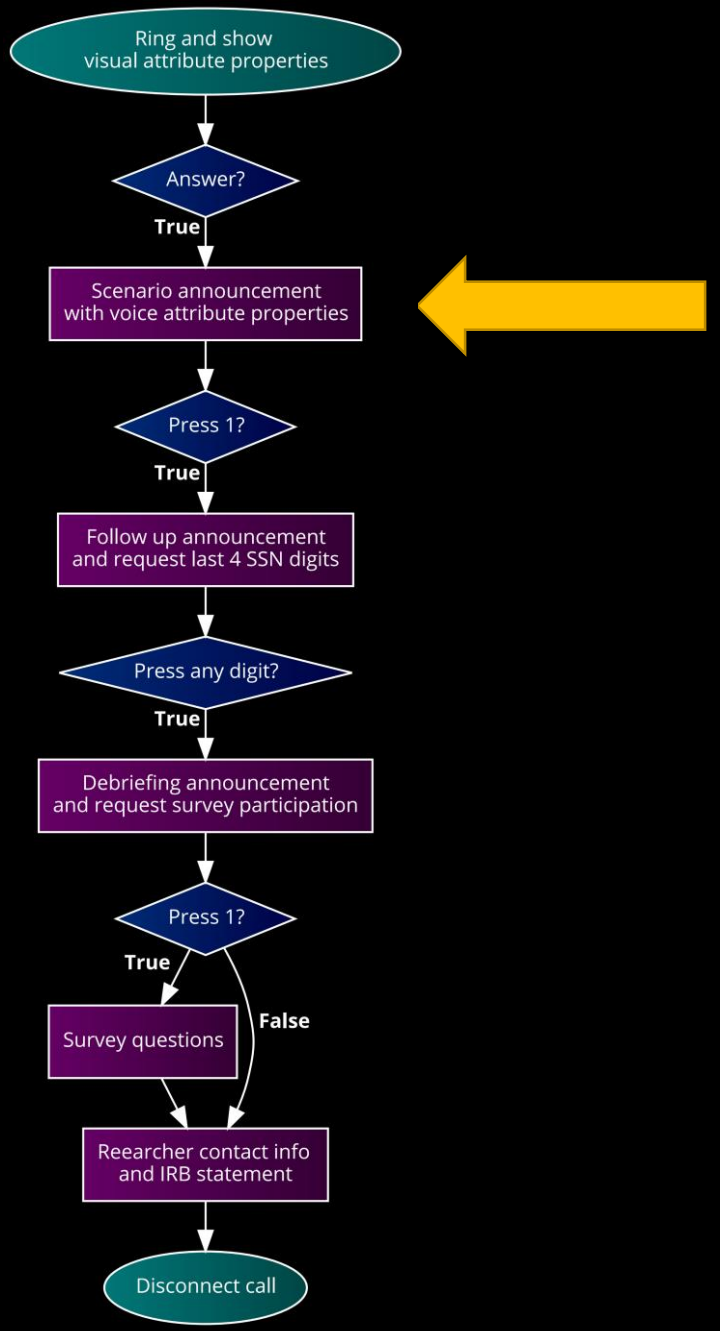

Ring and show visual attribute properties
Answer?
True
Scenario announcement with voice attribute properties
Press 1?
True
Follow up announcement and request last 4 SSN digits
Press any digit?
True
Debriefing announcement and request survey participation
Press 1?
True
False
Survey questions
Reearcher contact info and IRB statement
Disconnect call



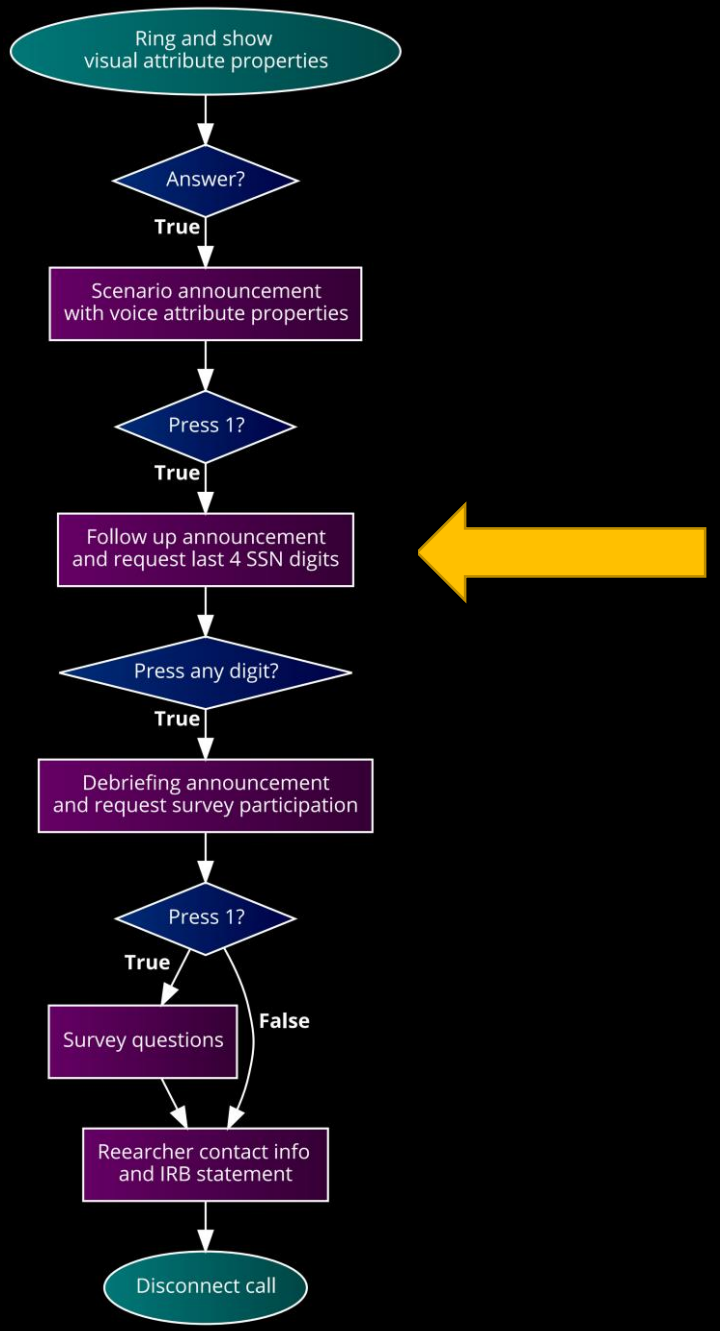
Ring and show visual attribute properties



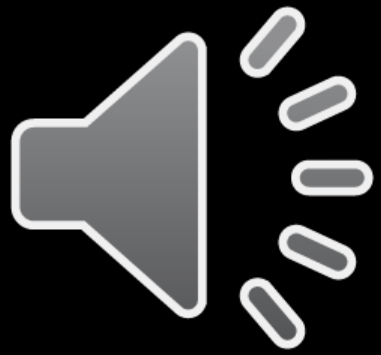


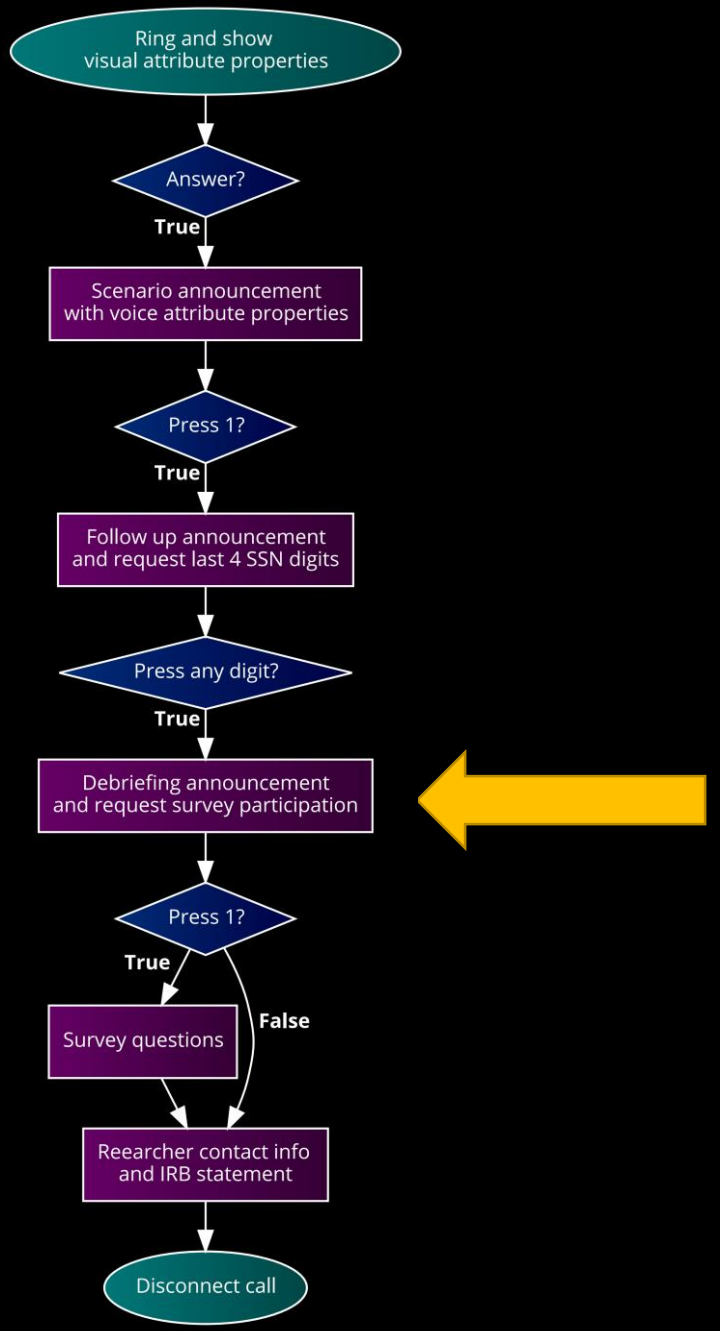


Scenario announcement with voice attribute properties

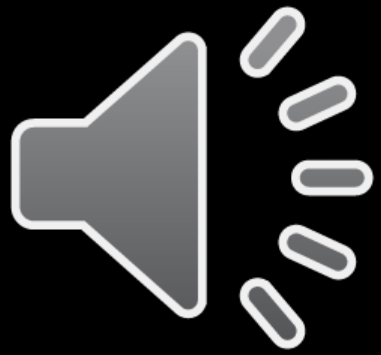


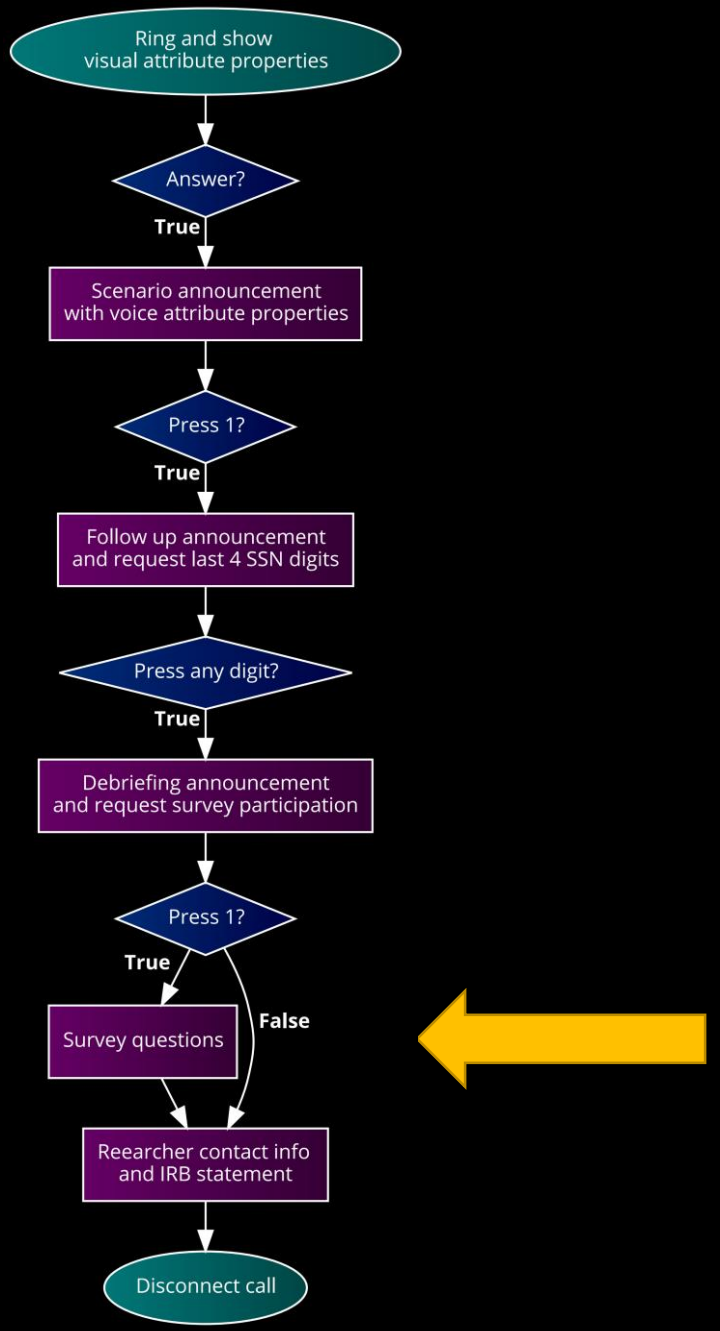
Follow up announcement and request last 4 SSN digits





Debriefing announcement and request survey participation





Survey questions

Dissemination

3,000 work phones

10 experiments simultaneously

1 work week

10am–5pm

Return calls directed to start of each experiment's procedure

Collected Results

No.	Continued		Entered SSN		Convinced		Recordings		Unconvinced		Recordings	
E1	12	4.00%	6	2.00%	0	0.00%	0	0.00%	4	1.33%	2	0.67%
E2	19	6.33%	15	5.00%	3	1.00%	0	0.00%	3	1.00%	3	1.00%
E3	13	4.33%	8	2.67%	1	0.33%	1	0.33%	2	0.67%	1	0.33%
E4	23	7.67%	13	4.33%	2	0.67%	0	0.00%	3	1.00%	2	0.67%
E5	9	3.00%	2	0.67%	1	0.33%	0	0.00%	1	0.33%	1	0.33%
E6	9	3.00%	8	2.67%	2	0.67%	2	0.67%	2	0.67%	1	0.33%
E7	13	4.33%	9	3.00%	3	1.00%	1	0.33%	5	1.67%	4	1.33%
E8	53	17.67%	30	10.00%	8	2.67%	3	1.00%	9	3.00%	8	2.67%
E9	60	20.00%	35	11.67%	7	2.33%	3	1.00%	4	1.33%	3	1.00%
E10	45	15.00%	22	7.33%	8	2.67%	7	2.33%	4	1.33%	2	0.67%
Total	256	8.53%	148	4.93%	35	1.17%	17	0.57%	37	1.23%	27	0.90%

Analysis Criteria

No.	Entered SSN	Unconvinced	Possibly Tricked	
E9	35	4	31	10.33%
E8	30	9	21	7.00%
E10	22	4	18	6.00%
E2	15	3	12	4.00%
E4	13	3	10	3.33%
E3	8	2	6	2.00%
E6	8	2	6	2.00%
E7	9	6	3	1.00%
E1	6	4	2	0.67%
E5	2	1	1	0.33%
Total	148	37	111	3.70%

Analysis Results

Hypothesis	Group A	Possibly Tricked	Group B	Possibly Tricked	p-value	Significant ($p < 0.05$)	Cohen's d	Effect Size	Conclusive
Can manipulating the area code have a significant effect on the attack success of a telephone scam?	E1	2/300	E2	12/300	0.0033	Yes	0.222	Small & somewhat educationally significant	**Somewhat**
Can manipulating the type of voice production have a significant effect on the attack success of a telephone scam?	E1	2/300	E6	6/300	0.0769	No	0.117	Very small & not educationally significant	No
Can manipulating the voice gender have a significant effect on the attack success of a telephone scam?	E1	2/300	E4	10/300	0.00955	Yes	0.192	Small & not educationally significant	**Hardly**
Can manipulating the voice accent have a significant effect on the attack success of a telephone scam?	E7	3/300	E6	6/300	0.157	No	0.082	Very small & not educationally significant	No
Can spoofing a known caller name have a significant effect on the attack success of a telephone scam?	E8	21/300	E9	31/300	0.073	No	0.119	Very small & not educationally significant	No
Can impersonating an internal entity have a significant effect on the attack success of a telephone scam?	E1 + E5	3/600	E8 + E9	39/600	4.97E-09	Yes	0.331	Small & educationally significant	**Yes**
Can manipulating the type of motivation have a significant effect on the attack success of a telephone scam?	E5 + E10	19/600	E1 + E8	23/600	0.265	No	0.036	Very small & not educationally significant	No

Key Findings and Recommendations

Impersonating an internal entity had the most significant effect to the attack success.

The key is to target and prevent impersonation.

Vigilance is an important reason for not falling for impersonation scam, based on our survey feedback.

Caller ID authentication and security indicators can provide early warnings to instill vigilance.

The Problem Statement

Understanding Why Telephone Scams Work

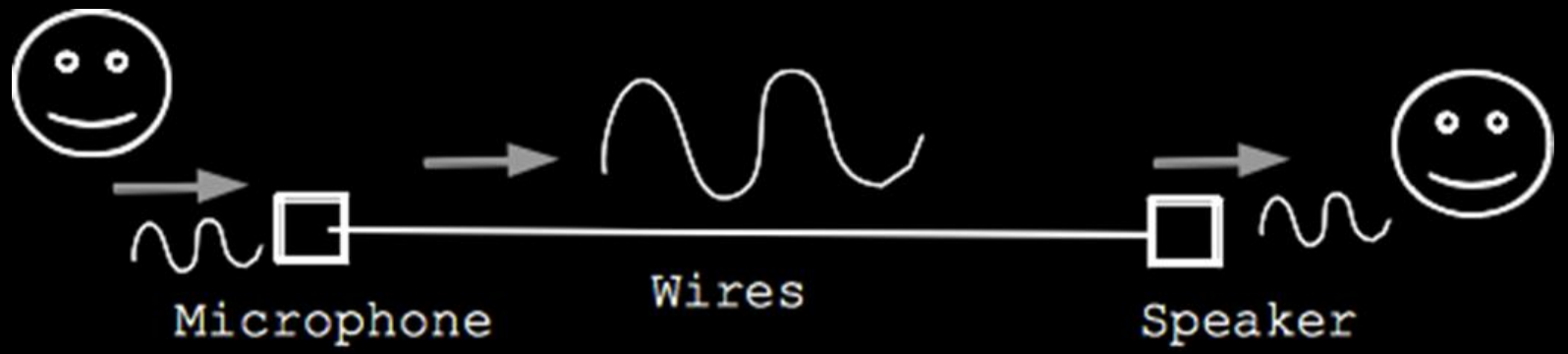
Identifying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

Implementing Prototypes With Evaluations

Conclusion

Key Challenges


Microphone
Wires
Speaker


UNDERSTANDING ONLINE STAR RATINGS:
[HAS ONLY ONE REVIEW]
EXCELLENT
CRAP

		References	Usability						Deployability						Robustness					
			No-Disturbance-to-Recipient	*Scalable-for-Recipient*	*Effortless-for-Caller*	*Negligible-Delays*	*Permissive-for-VoIP-Callers*	*Permissive-for-Unknown-Callers*	*Negligible-Changes-to-Infrastructure*	*Negligible-Changes-to-Call-Setups*	*No-Third-Party-Involvement*	*Low-Maintenance*	*Low-Resource-Requirement*	*Negligible-Cost-per-Call*	*Effective-Against-Dynamic-Caller-ID-Spoofing*	*Effective-Against-Targeted-Caller-ID-Spoofing*	*Effective-Against-Unavailable-Caller-ID*	*Effective-Against-Multiple-Identities*	*Effective-Against-Answering-Machine-Detection*	*Effective-Against-Dynamic-Audio-Content*
Call Request Header Analysis	Caller ID Blacklisting	[24], [25]	●	◐	●	●	●	●	●	●	●	◐	●	●	○	○	○	◐	●	●
	Caller ID Whitelisting	[26], [27]	●	●	●	●	●	○	●	●	●	◐	●	●	●	○	○	●	●	●
	Caller Reputation System	[28]–[42], [90]	●	◐	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Caller Behavior Analysis	[29], [32], [33], [35], [39], [41], [43]–[54], [91], [92]	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Device Fingerprinting	[55]	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	◐	◐	●	●
	Caller ID Anomaly Detection	[56], [57]	●	●	●	●	●	●	●	●	◐	◐	●	●	◐	○	◐	○	●	●
	ANI-CPN Matching	[58]	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
	ANI-II Filtering	[58]	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
Voice Interactive Screening	Audio Fingerprinting	[61]–[67]	●	●	◐	○	●	●	●	●	◐	○	○	◐	●	●	●	●	◐	◐
	Speech Content Analysis	[62], [68]	●	●	◐	○	●	●	●	●	◐	◐	○	◐	●	●	●	●	◐	◐
	Acoustic Pattern Analysis	[71]–[74]	●	●	◐	○	●	●	●	●	◐	◐	◐	◐	●	●	●	●	◐	◐
	CAPTCHA/Turing Test	[75]–[77]	●	●	○	○	●	●	●	●	●	◐	◐	◐	●	●	●	●	●	●
Caller Compliance	Do Not Call Registry	[22]	◐	◐	◐	●	●	●	●	●	○	◐	◐	●	○	○	○	◐	●	●
	Graylisting	[74], [79]	●	●	◐	○	●	◐	●	◐	●	●	●	○	●	●	●	●	●	●
	Consent-based Communication	[80]–[82]	○	○	◐	○	●	◐	●	◐	●	●	●	◐	●	◐	●	●	●	●
	Call Back Verification	[83], [84]	◐	◐	◐	○	◐	◐	●	●	●	●	●	○	●	●	●	●	●	●
	Weakly Secret Information	[85]	●	◐	◐	◐	●	○	◐	◐	●	◐	●	●	●	●	●	●	●	●
	Payment at Risk	[38]	●	○	◐	●	●	○	○	○	○	○	○	○	●	●	●	●	●	●
	Proof of Work	[86], [93]–[95]	●	●	●	●	●	○	◐	○	●	●	◐	●	●	●	●	●	●	●
	Proof of Identity	[83], [87]–[89]	●	●	●	●	●	○	◐	○	◐	●	◐	●	●	●	●	●	●	●

●= satisfy the criteria ◐= may satisfy the criteria ○= does not satisfy the criteria

	Usability	Deployability	Robustness
Call Request Header Analysis	★★★	★★★	★
Voice Interactive Screening	★	★★	★★
Caller Compliance	★★	★★	★★★

Analysis of Combined Techniques

	[96], [97]	[98]	[99]	[100]	[101]	[102]	[103]	[104]	[105]	[106]
Phased Decisions	✓	✓	✓	✓						✓
Weighted Scoring	✓	✓			✓	✓	✓	✓		
Conditional Procedures								✓	✓	✓
Caller ID Blacklisting	✓	✓	✓	✓	✓	✓	✓		✓	✓
Caller ID Whitelisting	✓	✓		✓	✓	✓	✓		✓	
Caller Reputation System	✓		✓	✓	✓	✓			✓	✓
Caller Behavior Analysis	✓	✓	✓		✓	✓	✓		✓	✓
Device Fingerprinting										✓
Caller ID Anomaly Detection										
ANI-CPN Matching										
ANI-II Filtering										
Audio Fingerprinting				✓						
Speech Content Analysis	✓									✓
Acoustic Pattern Analysis	✓									
CAPTCHA/Turing Test	✓	✓	✓	✓		✓		✓		✓
Do Not Call Registry										
Graylisting	✓					✓	✓			✓
Consent-based Communication	✓		✓							✓
Call Back Verification										
Weakly Secret Information	✓									
Payment at Risk										
Proof of Work	✓							✓		
Proof of Identity			✓	✓					✓	

Key Findings and Recommendations

Combining techniques create synergy however it can add more complexity and delay.

Usability is the most important thing to consider.

Call Request Header Analysis is the best overall solution, its only downside is vulnerability to caller ID spoofing.

The key to solving the telephone spam problem is to develop effective prevention of caller ID spoofing.

The Problem Statement

Understanding Why Telephone Scams Work

Surveying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

Implementing Prototypes With Evaluations

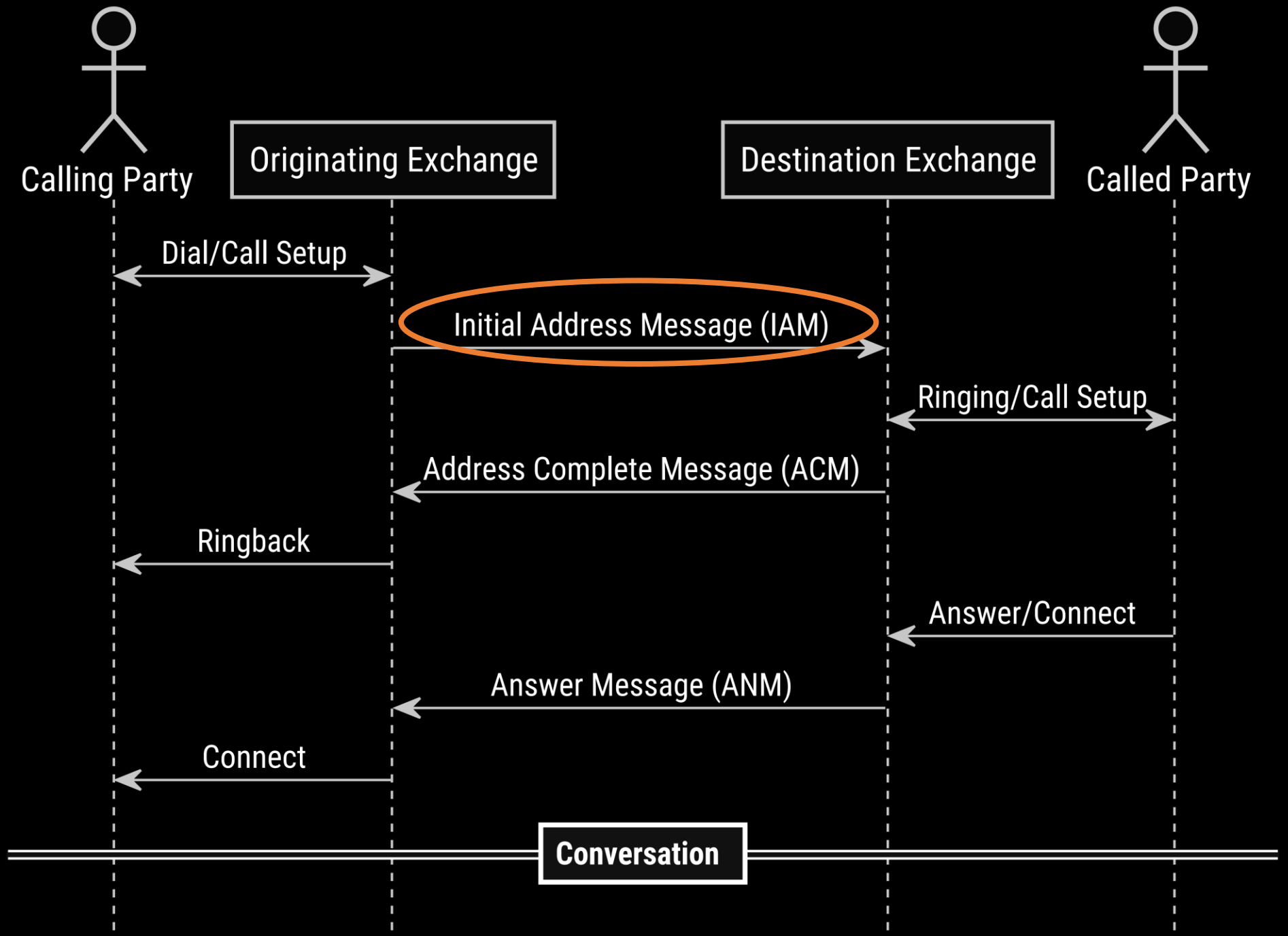
Conclusion

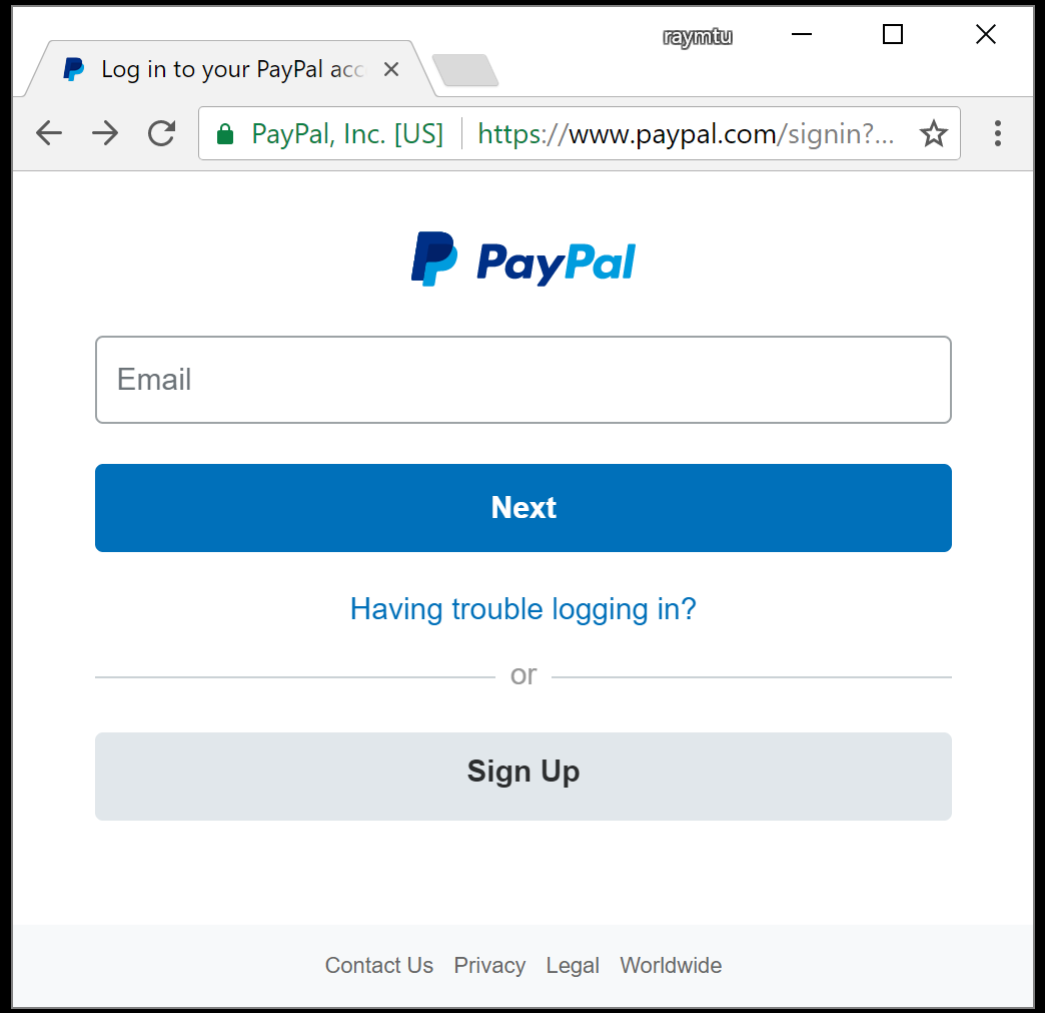
STAGE 3 DESCRIPTION FOR NUMBER IDENTIFICATION SUPPLEMENTARY SERVICES USING SIGNALLING SYSTEM No. 7

The format of the calling party number parameter field is shown in Figure 11.

	8	7	6	5	4	3	2	1
1	O/E	Nature of address indicator						
2	NI	Numbering plan indicator			Address presentation restricted indicator		Screening indicator	
3	2nd address signal				1st address signal			
:								
:								
m	Filler (if necessary)				*n*th address signal			

Figure 11/Q.763 – Calling party number parameter field

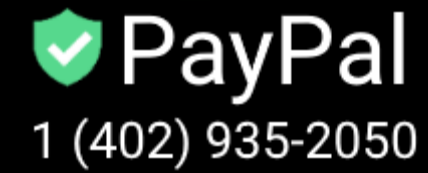

Calling Party
Originating Exchange
Destination Exchange
Called Party
Dial/Call Setup
Initial Address Message (IAM)
Ringing/Call Setup
Address Complete Message (ACM)
Ringback
Answer/Connect
Answer Message (ANM)
Connect
Conversation


raymtu
Log in to your PayPal acc
PayPal, Inc. [US] | https://www.paypal.com/signin?...
PayPal
Email
Next
Having trouble logging in?
or
Sign Up
Contact Us Privacy Legal Worldwide

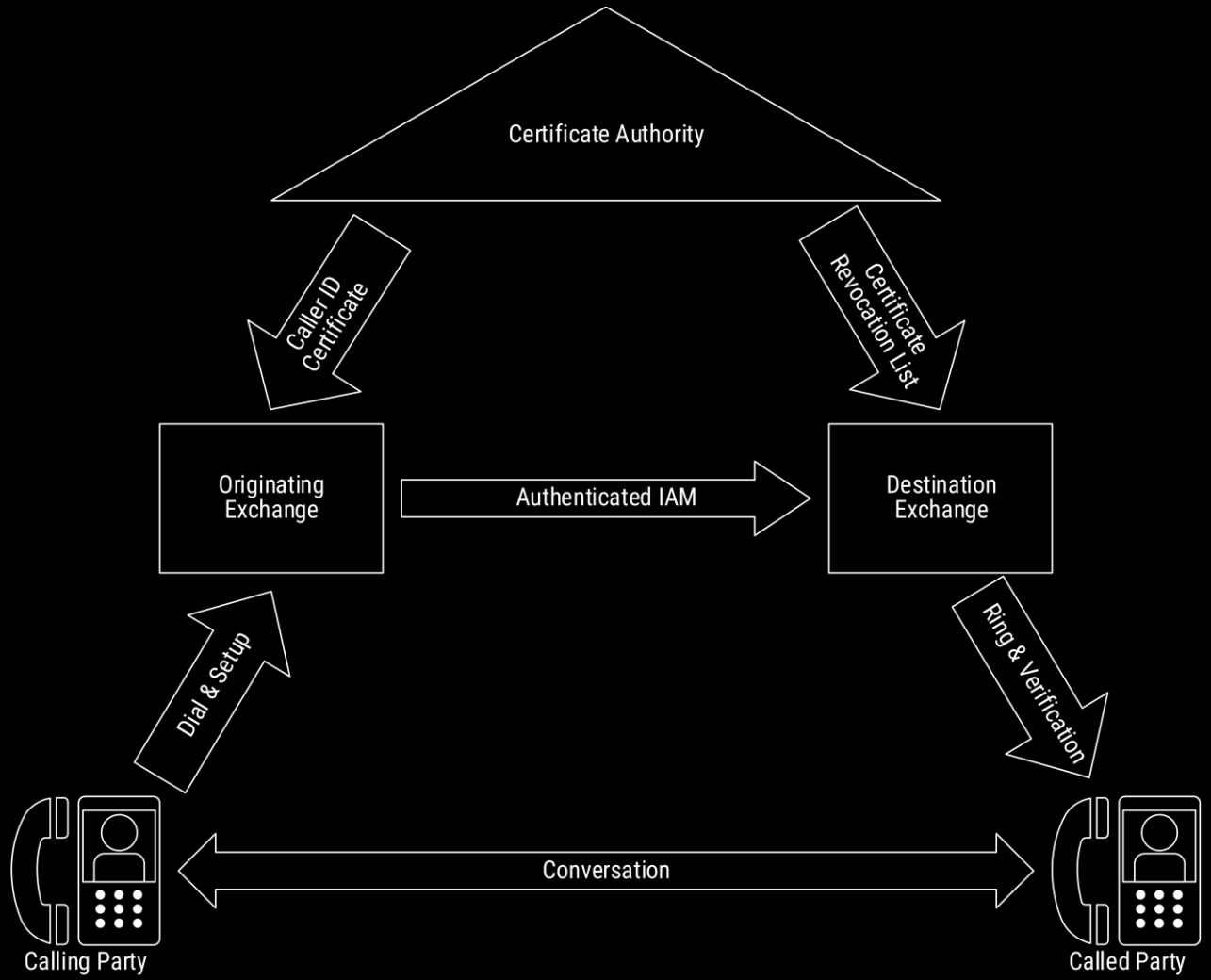
Solution: Security Indicators


10:57
PayPal
1 (402) 935-2050
INCOMING CALL

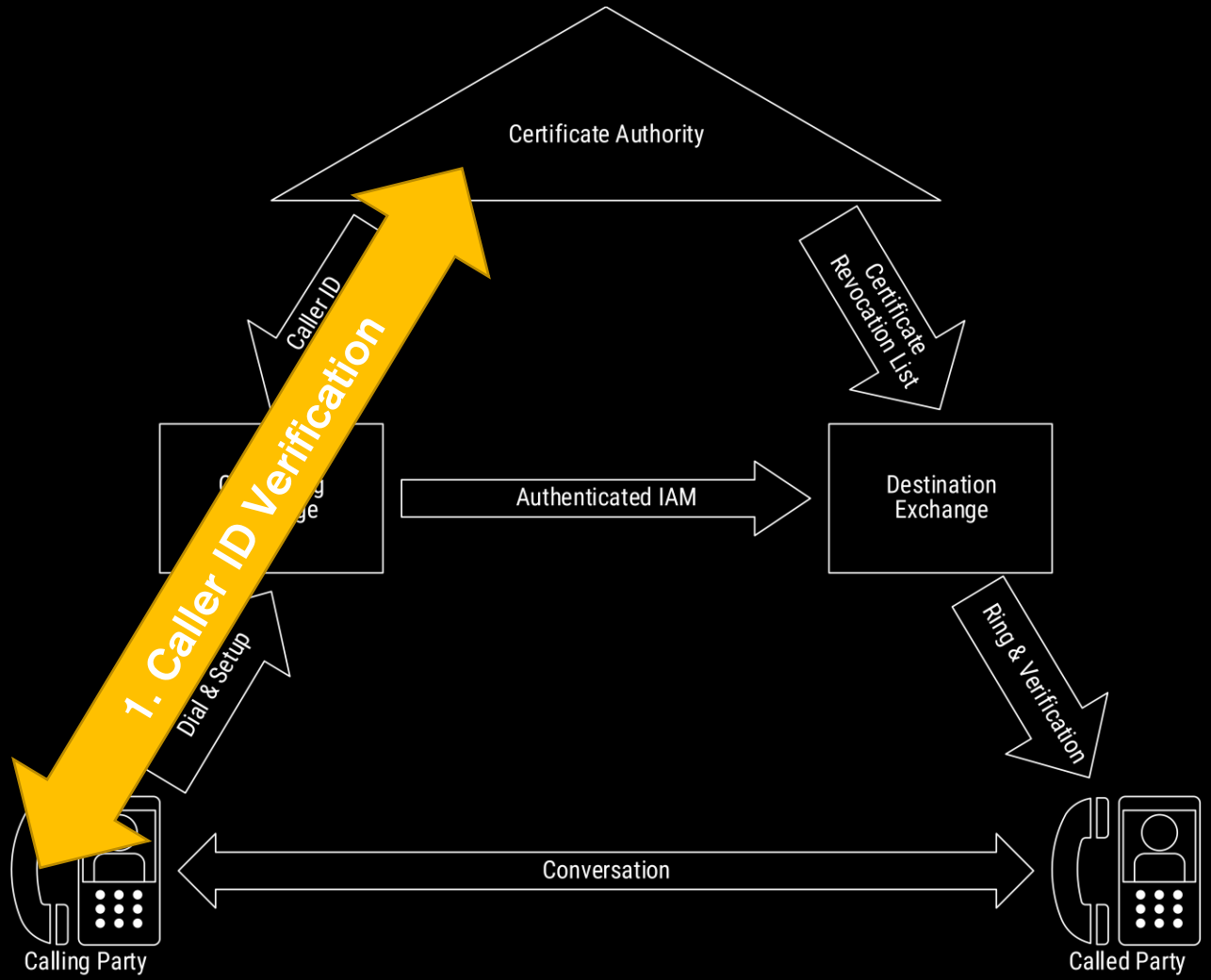
Solution: Security Indicators



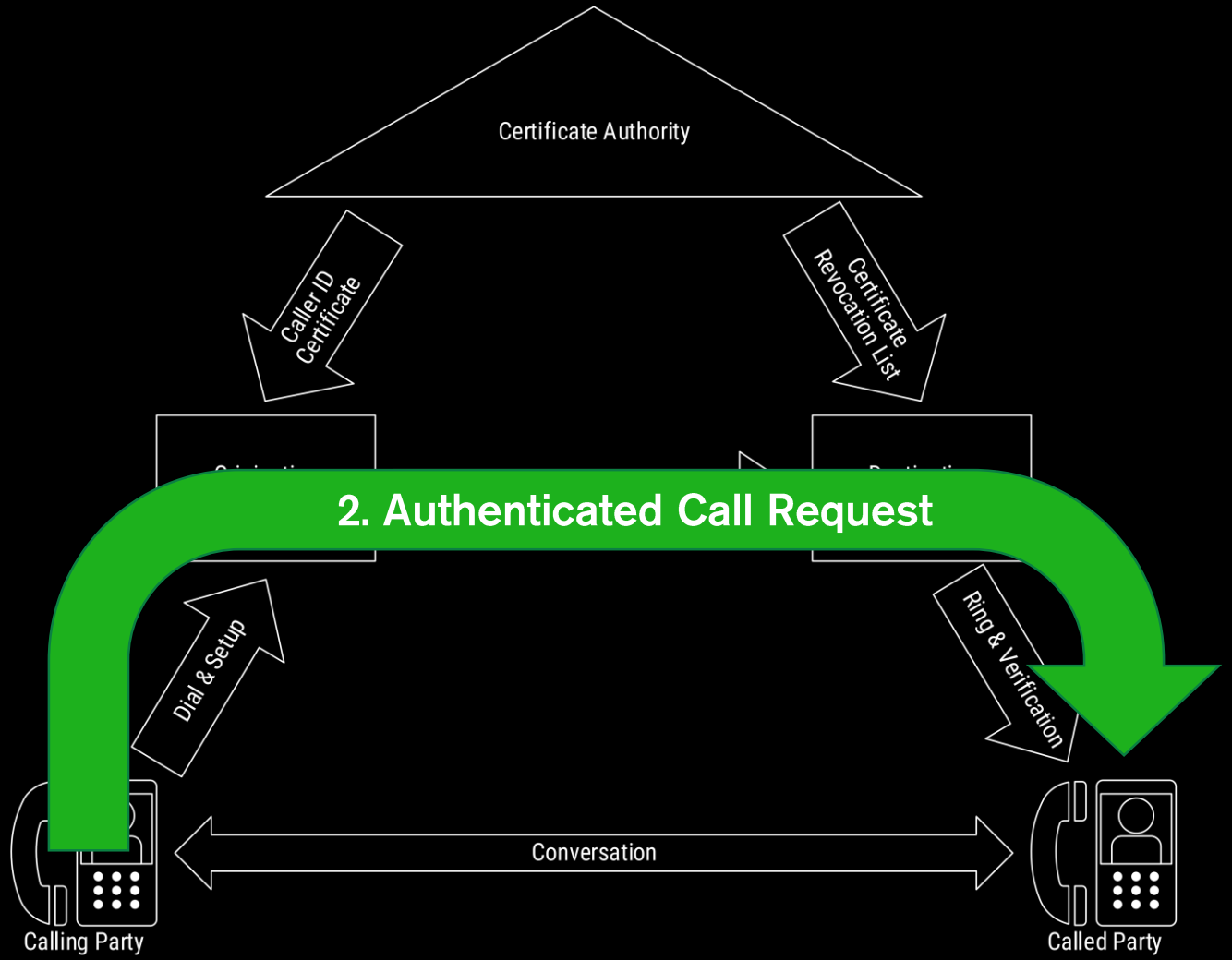
Architecture



Caller ID Verification



Authenticated Call Request



Key Benefits of the Proposed Scheme

- Usability
  - Immediate cue of a verified caller
  - Promotes vigilance for identity verification
- Robustness
  - Provides a foundation for spam defenses
  - Provides assurance for communication over the phone
- Deployability

The Problem Statement

Understanding Why Telephone Scams Work

Identifying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

Implementing Prototype With Evaluations

Conclusion

How to Implement a Prototype?

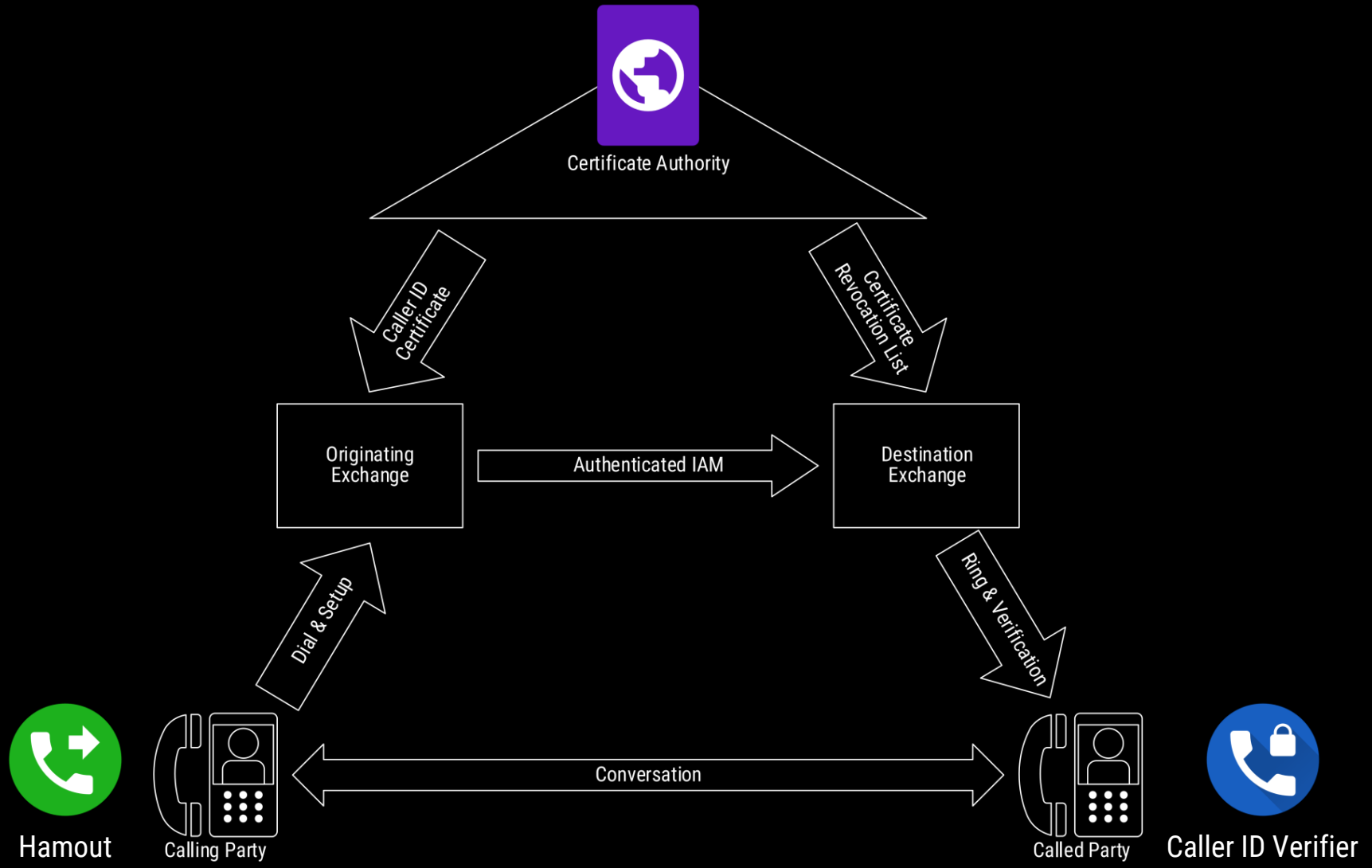
Core PSTN infrastructure is proprietary and modification is too expensive.

Using out-of-band channel transmission requires no infrastructure modification.

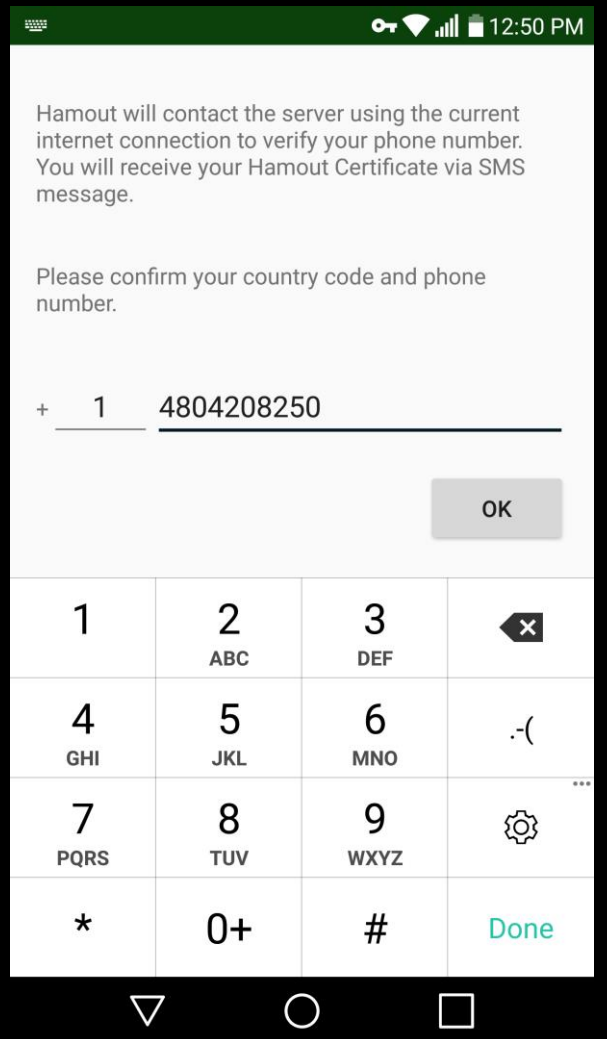
Vast majority of telephone users today are Android phone users.

Implement Android prototype that relies on out-of-band SMS transmission.

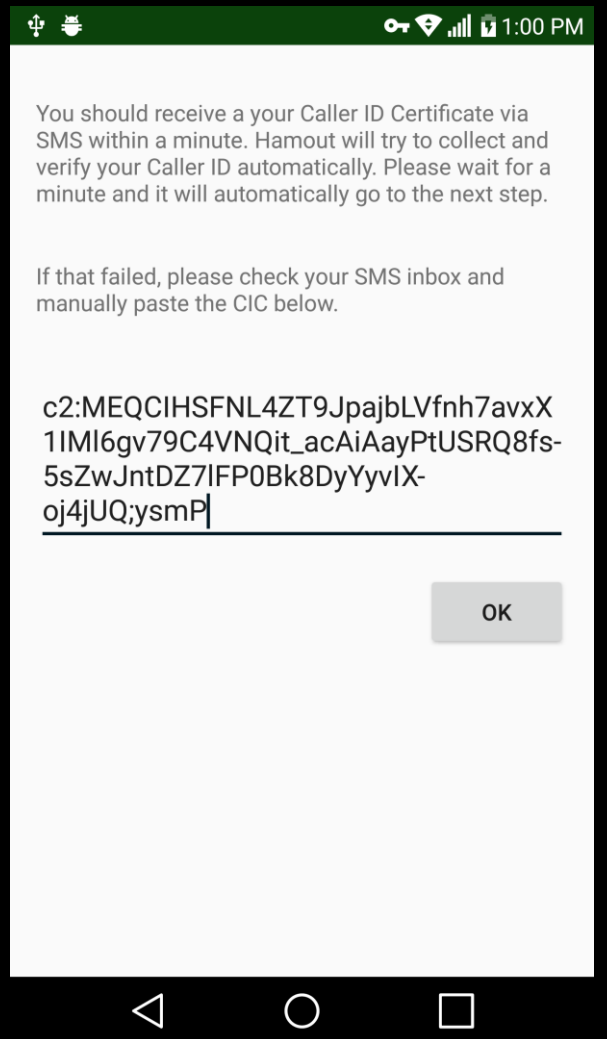
Prototype Implementations



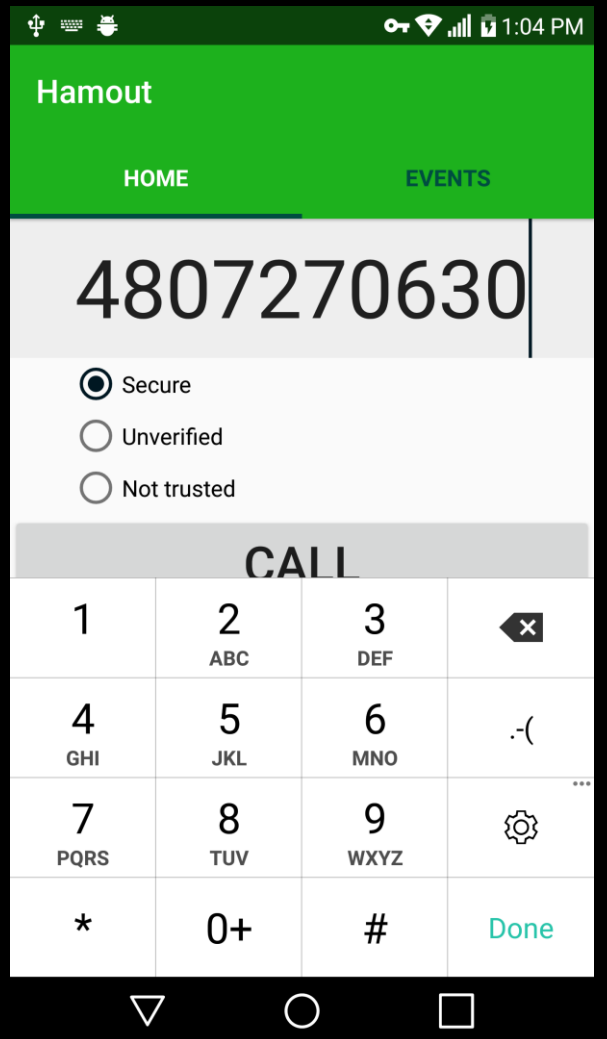
Hamout


12:50 PM
Hamout will contact the server using the current internet connection to verify your phone number. You will receive your Hamout Certificate via SMS message.
Please confirm your country code and phone number.
+ 1 4804208250
OK
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
.-(
7 PQRS
8 TUV
9 WXYZ
*
0+
#
Done

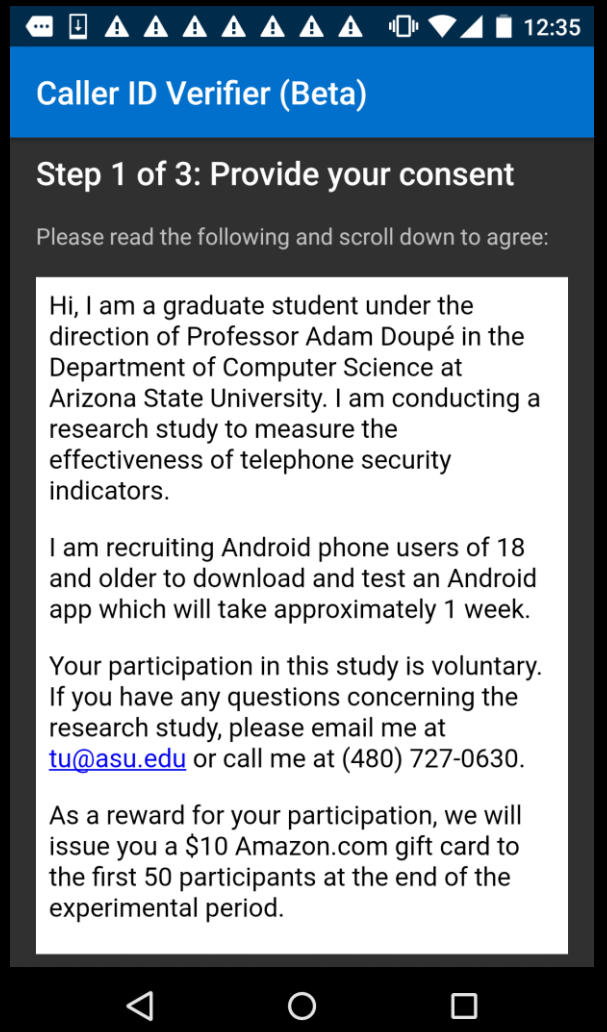
Hamout


1:00 PM
You should receive a your Caller ID Certificate via SMS within a minute. Hamout will try to collect and verify your Caller ID automatically. Please wait for a minute and it will automatically go to the next step.
If that failed, please check your SMS inbox and manually paste the CIC below.
c2:MEQCIHSFNL4ZT9JpajbLVfnh7avxX1IMl6gv79C4VNQit_acAiAayPtUSRQ8fs-5sZwJntDZ7lFP0Bk8DyYyvIX-oj4jUQ;ysmP
OK

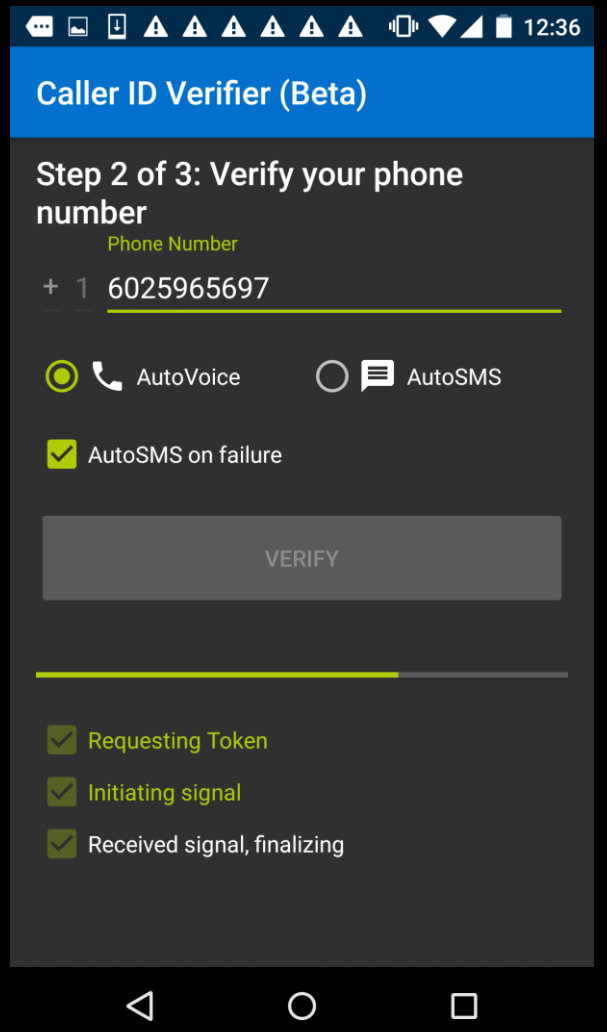
Hamout


1:04 PM
Hamout
HOME
EVENTS
4807270630
Secure
Unverified
Not trusted
CALL
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
.-(
7 PQRS
8 TUV
9 WXYZ
*
0+
#
Done

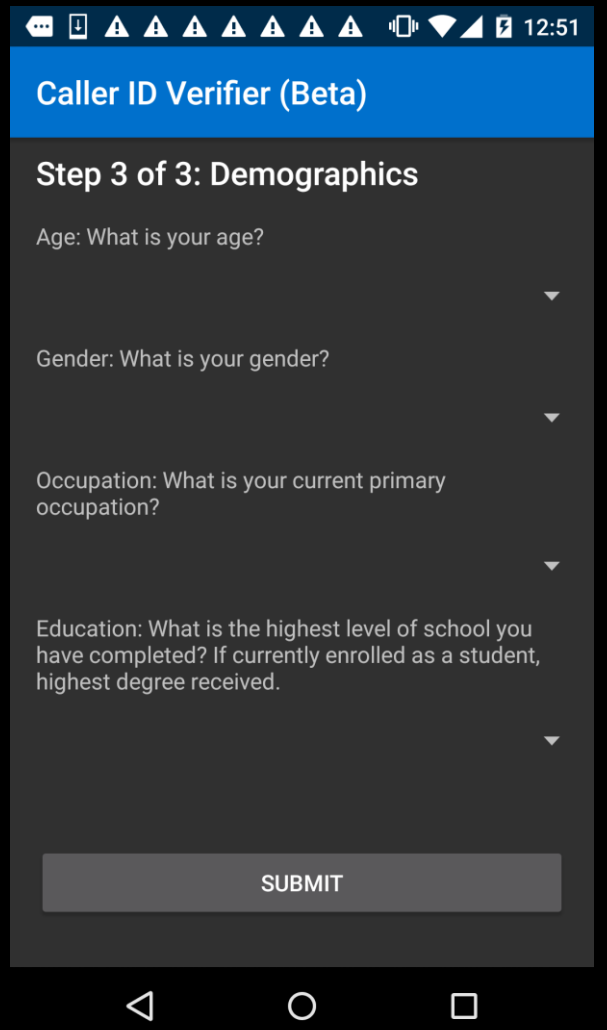
Caller ID Verifier



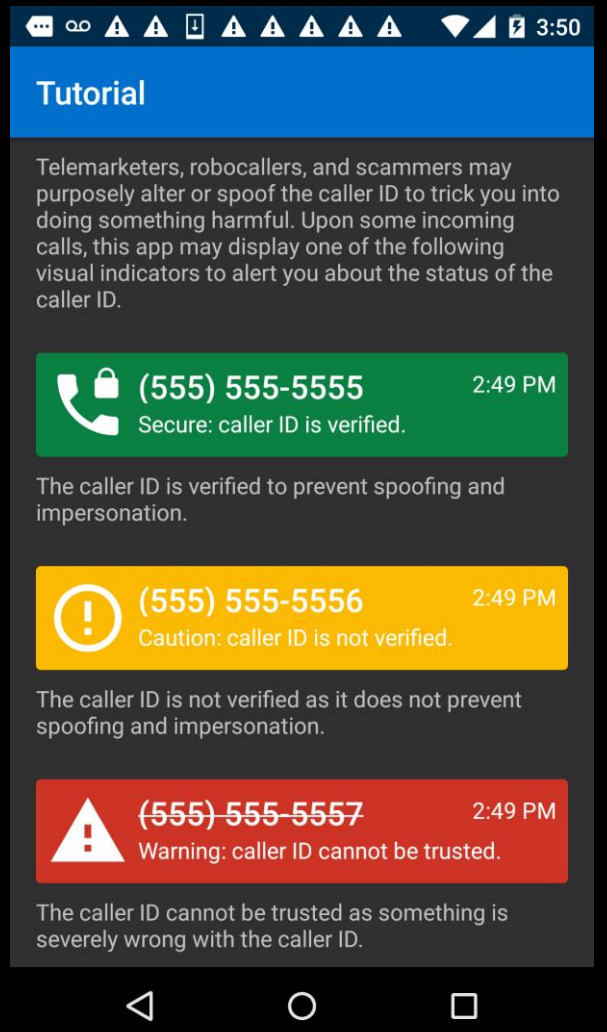
Caller ID Verifier



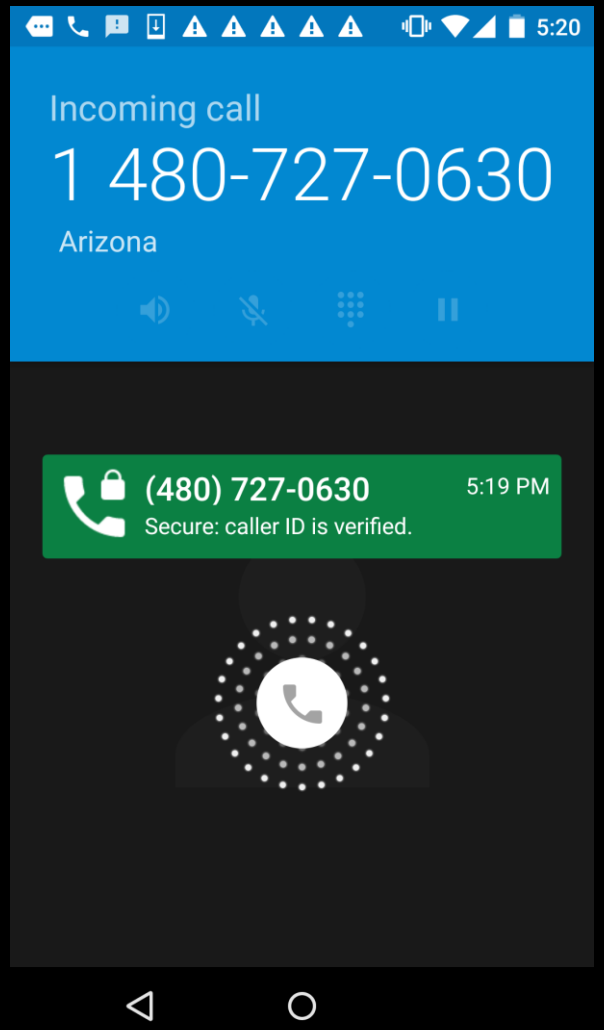
Caller ID Verifier



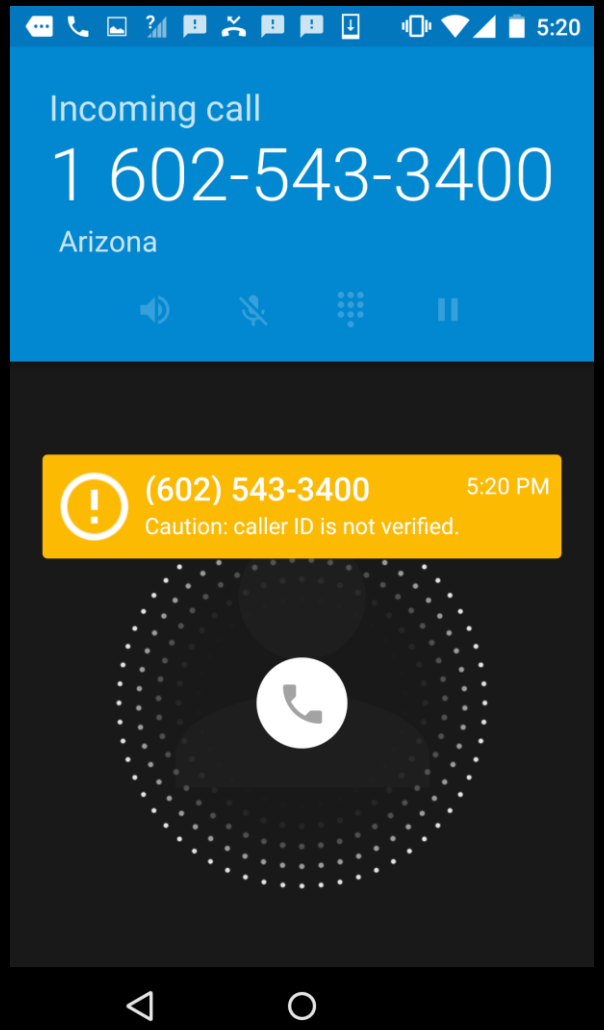
Caller ID Verifier



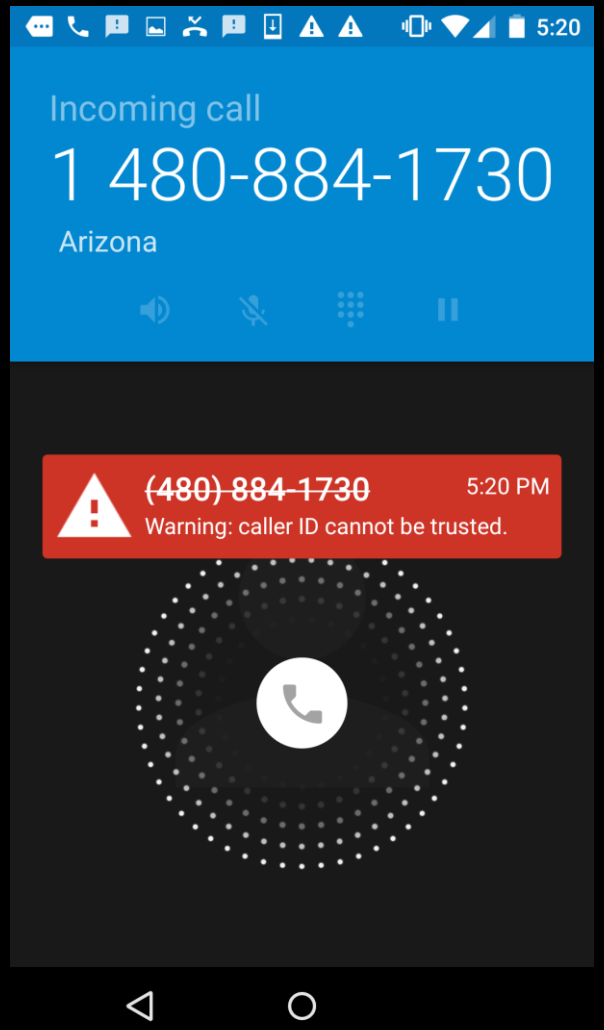
Caller ID Verifier



Caller ID Verifier



Caller ID Verifier



Analysis Objectives

Measure performance

Understand user behaviors

Gather feedback

Performance Analysis

Security Provider	AndroidKeyStore 5.0				SpongyCastle 1.52	
Signature Algorithm	SHA256withECDSA		SHA256withRSA		SHA256withECDSA	
ECC Curve	prime192v1	prime256v1	-		prime192v1	prime256v1
Key Size	192 bit	256 bit	1024 bit	3072 bit	192 bit	256 bit
Avg. Key Pair Generation Time	999.724 ms	1002.18 ms	1719.42 ms	23247.54 ms	424.88 ms	608.09 ms
Avg. ACR Sig Generation Time	14.51 ms	20.14 ms	35.85 ms	621.02 ms	402.39 ms	602.54 ms
Avg. ACR Sig Verification Time	7.2 ms	9.55 ms	5.81 ms	6.16 ms	525.16 ms	646.58 ms
ACR Size	71 bytes	87 bytes	143 bytes	399 bytes	71 bytes	87 bytes
ACR + CIC Size	217 bytes	265 bytes	484 bytes	1240 bytes	217 bytes	265 bytes
Median SMS Delivery Time	8579 ms	11480 ms	18610 ms	39762 ms	-	

Key Findings from Performance Analysis

The good:

- Negligible delay with ECDSA
- ACR fits safely in all existing types of call header

The bad:

- SMS delivery = inconsistent network delays

Key Findings from Performance Analysis

- Need to improve ACR delivery speed and consistency
  - MMS (costly)
  - Cloud messaging (depends on WiFi or data speeds)
  - Embed in call header (requires standardization & modification)

Why Conduct a User Study?

Gather both qualitative and quantitative data.

Know the user behavior when they see a security indicator.

Learn about potential use cases of caller ID authentication.

Inspire future improvements and refinements.

Study Design

Group 0

No security indicator

Group 1

Display security indicator only

Group 2

Display security indicator with SMS ACR delivery

Recruitment

Announcement emails

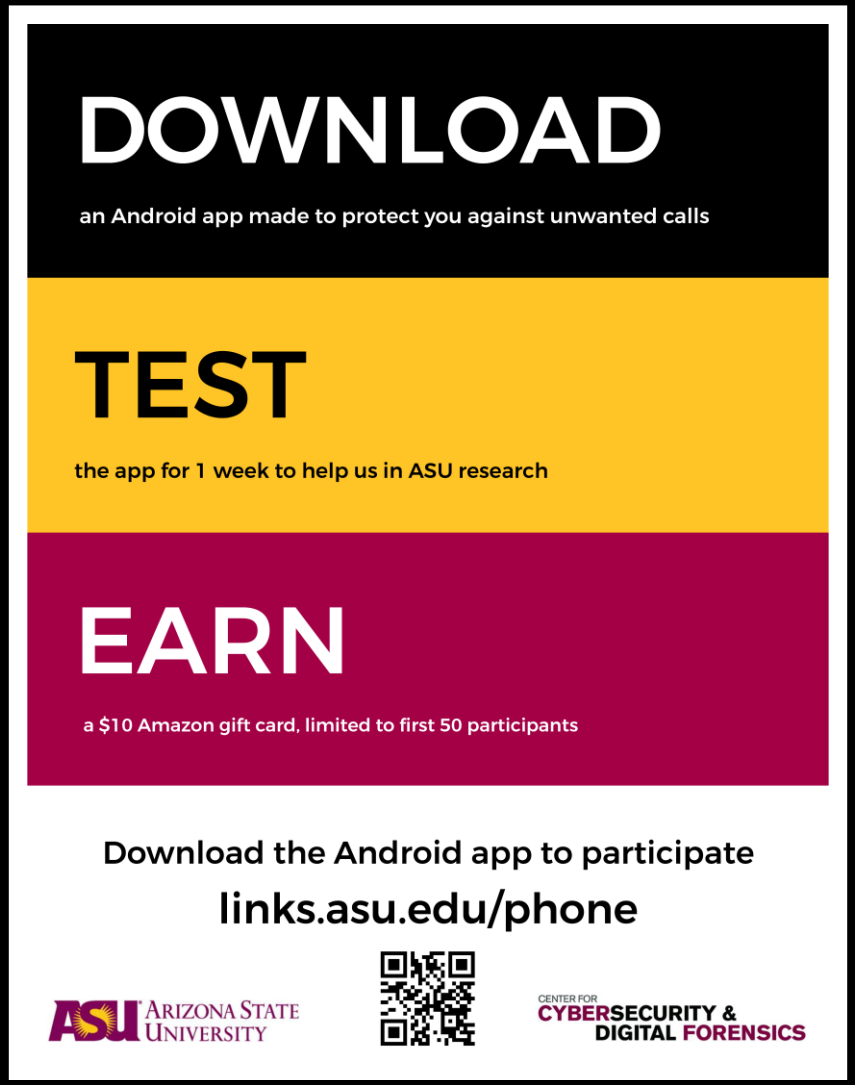
Bulletin boards

Facebook posts

Craigslist ads

Incentive: $10 Amazon gift card

Recruitment Poster



GET IT ON Google Play

Caller ID Verifier (Beta)

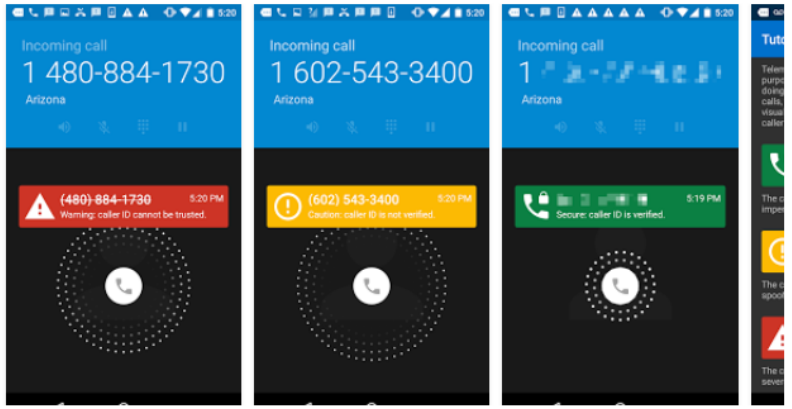
ASU Center for Cybersecurity and Digital Forensics **Communication**

Everyone

Woohoo! You're a beta tester for this app.

You don't have any devices

Add to Wishlist **Install**



Telemarketers, robocallers, and scammers may purposely alter or spoof the caller ID to trick you into doing something harmful. Upon some incoming calls, this app may display an alert inform you about the status of the caller ID. The goal of this app is to provide you with useful visual alerts to help you decide whether to answer or block an incoming call.

WHAT'S NEW

Recruitment Results

70 app installs

57 total participants

19 participants in each group

Experiment Procedure

1 week

56 calls each group

168 total phone calls

Collect recipient data via app

Data Collected

136 data records received from app participants.

- Group 0 - 44 records and 3 comments
- Group 1 - 38 records and 9 comments
- Group 2 - 54 records and 6 comments

Data Collected

Data Collected	Description
Phone number	The verified phone number of the participant.
Gender	Optional response to the demographic question asking the gender of the participant.
Occupation	Optional response to the demographic question asking the occupation of the participant.
Education	Optional response to the demographic question asking the education of the participant.
Incoming call action	The action taken upon an incoming call from us.
Incoming call action delay	The amount of time from the start of incoming call to the action taken.
Incoming call count	The number of incoming calls received from us.
Security Indicator Type	The type of security indicator shown during the incoming call.
Has seen notification	Participant's feedback on whether the he/she saw the security indicator.
Action feedback	Participant's feedback on the action taken upon the incoming call.
Did notification led to action	Participant's feedback on whether the security indicator led to the action taken.
Other comments	Participant's feedback on other comments.

Participant Demographics

Age		Gender		Occupation		Education	
18-35	35	Male	41	Student	49	Bachelor's	19
25-34	17	Female	12	Faculty	1	Master's	7
Unspecified	5	Unspecified	4	Employed	1	Some college credit	7
				Self-Employed	1	High school	6
				Unspecified	5	Doctorate	2
						Associate	2
						Unspecified	14

Key Findings from App Data Collection

App engagement keeps users

- Group 0 participants had twice as high uninstall rate compared to other groups.

Answer rate depends on type of indicator

- Secure > Caution ≥ Warning

Curiosity in the indicator have resulted in higher than expected answer rate

- Warning > No indicator

SMS delivery resulted in some indicators not displayed correctly

- Higher than expected # of Caution indicators in group 2

Interviews

Dig deep into areas of interest not gathered from app data collection

Followed up with some of the app participants

7 participants emailed us

3 participant interviews (one from each group)

Findings Collected from the Interviews

General users do not understand caller ID spoofing

- Focus on accurate prevention of spam and scam calls

Warning indicator should be made more distinctive

- Bigger screen cover, more colorful, animation

Warning indicator should provide a reason

- Telemarketer? Scam? Impersonator?

Findings Collected from the Interviews

Secure indicators are useful for urgent and important calls

- Delivery notice, store pickups, etc.

Provide more information about unknown callers

- Verified name, GPS location, etc.

Provide better app engagement and customization

- More indications, allow disabling for certain caller IDs

The Problem Statement

Understanding Why Telephone Scams Work

Identifying Key Challenges and Existing Countermeasures

Proposing Authenticated Caller ID Transmission

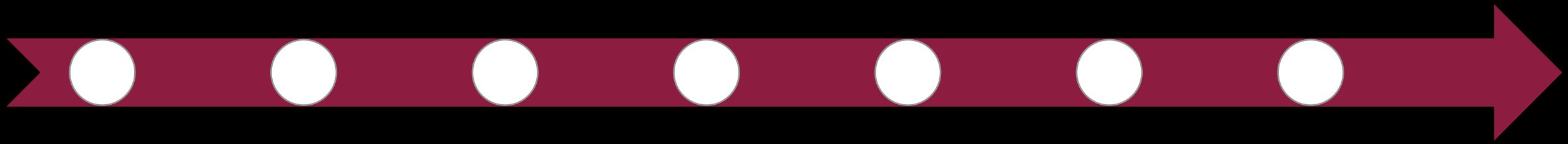
Implementing Prototype With Evaluations

Conclusion

Dissertation Contributions

- ❑ Problem: Telephone spam and scams
  - ✓ Understanding why telephone scams work
- ❑ Cause: Impersonation and caller ID spoofing
  - ✓ Identifying key challenges and existing countermeasures
- ❑ Method: A novel architecture and method to authenticate the caller ID
  - ✓ Proposing authenticated caller ID transmission
- ❑ Result: A security indicator, that can help to prevent users from becoming a victim of telephone spam and scams.
  - ✓ Implementing prototype with evaluations

Timeline



2011
- Started PhD

2012
- Courses

2013
- Courses
- Internship

2014
- Joined SEFCOM
- Started spam survey research

2015
- Started caller authentication research

2016
- USPTO filed
- IEEE-SP published
- ITU-K published

2017
- USPTO non-provisional filed
- IEEE-COMM published
- IEEE-SP submitted
- ITU-T contribution

Media Interactions

Television

- CBS WNCN, Aug 2017
- CBS 5 KPHO and 3TV KTVK, Jun 2017 and Mar 2017

Radio

- 89.3 KPCC (Southern California NPR), Oct 2016

Print

- Ars Technica, Aug 2017
- The Orange County Register, Oct 2016

Professional Talks

“Toward Authenticated Caller ID Transmission” invited talk, at ITU-T Study Group 11, ITU Telecommunication Standardization Sector (ITU-T), Feb 2017

“Everyone hates Robocalls: Why is it so hard to stop?” invited talk, at Open Web Application Security Project (OWASP) Phoenix Chapter, Oct 2016

Standards Contribution

“Propose to initiate a new work item on architecture and signalling requirement of calling identification authentication” joint contribution with China Telecom, at ITU-T Study Group 11, ITU Telecommunication Standardization Sector (ITU-T), Oct 2017

Patent Application

Huahong Tu, Adam Doupé, Gail-Joon Ahn and Ziming Zhao, “Systems and methods for authenticating caller identity and call request header information for outbound telephony communications,” filed for Non-Provisional patent, USPTO application number 62/308,105, Arizona Technology Enterprises (AzTE), Mar 2016

Publications

Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn,
“SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephony Spam,” IEEE Symposium on Security and Privacy (IEEE-SP), IEEE Computer Society, May 2016

Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn,
“Toward Authenticated Caller ID Transmission: The Need for a Standardized Authentication Scheme in Q.731.3 Calling Line Identification Presentation,” ITU Kaleidoscope 2016 (ITU-K), ITU Telecommunication Standardization Sector, Nov 2016 (Best Paper Award)

Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn,
“Toward Standardization of Authenticated Caller ID Transmission,” IEEE Communications Standards Magazine (IEEE-COMM), IEEE Communications Society, Sep 2017

Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn,
“SoK: Don't Fall Victim to Phone Scams: A Study of Why Telephone Phishing Works,” under review in IEEE Symposium on Security and Privacy (IEEE-SP), IEEE Computer Society, 2017

Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn,
“Designing the Caller ID Authentication Security Indicators for the Future Telephone Network,” in progress for submission in an ITU/IEEE/Tech conference, 2017

Thank You!

Questions?