SOURCE IDENTITY (ORIGIN AUTHENTICATION)

Henning Schulzrinne

August 2013

draft-peterson-secure-origin-ps-01
+ mailing list discussion

Overview

- Phone numbers will be with us for 10++ years
- Their lack of validation is the main cause of phone-related criminality and nuisance
- Related to domain name validation, but significant differences
  - each country code has one (regulatory) root
- Validate that originator of call is authorized to use **From** number
- Earlier attempts have failed
- The problem is well-scoped
  - competing ideas are generally compatible
- Known unknowns

Two modes of caller ID spoofing

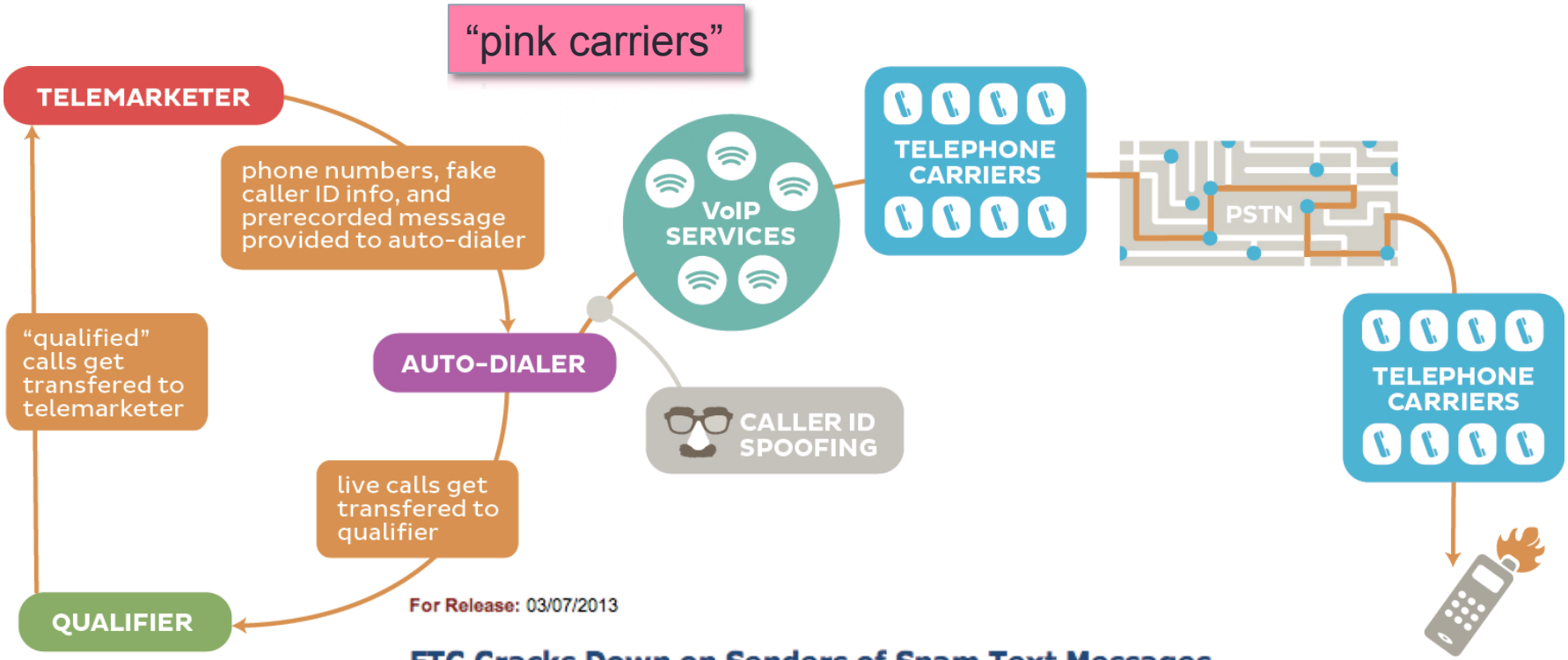
Impersonation

- spoof *target number*
  - personal or 800 number
- Helpful for
  - vishing
  - stolen credit card validation
  - retrieving voicemail messages
  - SWATting
  - disconnect utilities
  - unwanted pizza deliveries
  - retrieving display name (CNAM)

Anonymization

- pick more-or-less *random number*
  - including unassigned numbers
- Helpful for
  - robocalling
  - intercarrier compensation fraud
  - TDOS

Robocalling



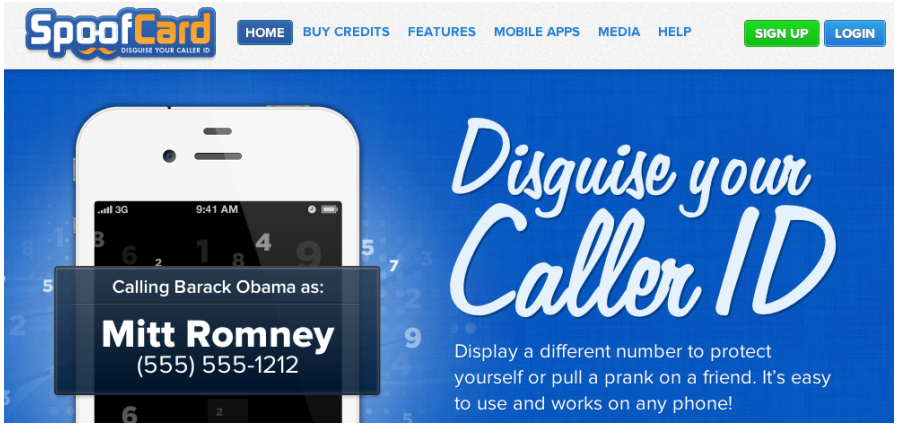
For Release: 03/07/2013

FTC Cracks Down on Senders of Spam Text Messages Promoting "Free" Gift Cards

Defendants Were Responsible for More than 180 Million Spam Text Messages

Caller ID spoofing

- Easily available on (SIP) trunks
- US Caller ID Act of 2009: *Prohibit 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.*
- Also: FCC phantom traffic rules



Legitimate caller ID spoofing

- Doctor's office
  - call from personal physician cell phone should show doctor's office number
- Call center
  - airline outbound contract call center should show airline main number, not call center
- Multiple devices, one number
  - provide single call-back number (e.g., Google Voice) from all devices

anonymity is distinct problem (caller ID suppression)

Requirements

- **E.164** number source authenticity
  - E.164 taken loosely (N11, P-ANI, non-reachable numbers, …)
  - assume that numbers can be canonicalized for signing
    - seems to work for VM, CDRs, SS7 translation, …
- Complete solution (but not necessarily one mechanism)
  - number assignment to validation
  - validate caller ID
  - later?: extended caller information
- Functionality
  - must work without human intervention at caller or callee
  - minimal changes to SIP
  - must survive SBCs
  - must allow *partial authorized & revocable* delegation
    - doctor's office
    - third-party call center for airline
  - must allow number portability among carriers (that sign)

Requirements

- Privacy
  - e.g., third parties cannot discover what numbers the callee has dialed recently
- Efficiency
  - will need a mode that causes minimal expansion of SIP headers (= suitable for UDP)
  - e.g., caching of certs or public keys
- Simplicity
  - minimize overall complexity
  - incremental deployment

Not in scope

- Validate other identifiers (e.g., sip:alice@example.com)
  - might or might not translate (assignment hierarchy)
- Validate textual caller ID (“CNAM”)
  - anybody can call themselves “CARD HOLDER SVC”
- Cross-national
  - calls from +234 codes are not a major problem (right now)
- Content (media) protection or integrity
  - → SRTP
- Most man-in-the-middle signaling attacks
  - e.g., evil proxy retargets call to grandma into selling Medicare supplements
  - content (media) protection or integrity

P-Asserted-Identity (RFC 3325)

```
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000
```

- RFC 3325 assumptions:
  - originating end systems cannot alter SIP headers (or intermediate entities can be trusted to remove PAI headers)
  - trusted chain of providers

RFC 4474 (SIP Identity)

```
INVITE sip:bob@biloxi.example.org SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.example.org>
From: Alice <sip:alice@atlanta.example.com>;tag=1928
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.example.com>
Identity: "KVhPKbfU/pryhVn9Yc6U="
Identity-Info: <https://atlanta.example.com/atl.cer>;alg=rsa-sha1
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
...
```

SBC may change domains

changed by SBC

Problems with RFC 4474

- see rosenberg-sip-rfc4474-concerns
- Cannot identify assignee of telephone number
- Intermediate entity re-signs request
- B2BUAs re-originate call request
  - replace everything except method, **From** & **To** (if lucky)

draft-jennings-vipr-overview

VIPR concerns

- Uses PSTN for reachability validation
  - “own” number → proof of previous PSTN call (start/stop time, …)
- First call via PSTN
  - doesn’t deal with robocalls
  - “A domain can only call a specific number over SIP, if it had previously called that exact same number over the PSTN.”
- Single, worldwide P2P network
  - deployment challenging
- Allows impersonator to find out who called specific number

Changes in environment

Old (pre-2000)	new
Small number of carriers serving customers with fixed number pools (residential, inbound)	• carriers that provide services to non-carriers (e.g., Google Voice, VRS) • voice service providers (via APIs)
Carriers either larger or rural → trusted	“Pink” carriers (robocalls = lots of minutes)
Carriers with deep engineering skills	Telecom engineers fired or retired
Call routing determined by physical transport (MF or SS7)	logical routing via SIP proxies
Domestic calls stay within the country	call from NJ to NY may visit Berlin
#’s only for certificated carriers (~ 1000)	interconnected VoIP providers (trial)
1000 block assignment	individual numbers?
Geographic assignment (LATA, area code)	no direct relationship to geography (800#, mobile, VoIP, M2M, …)

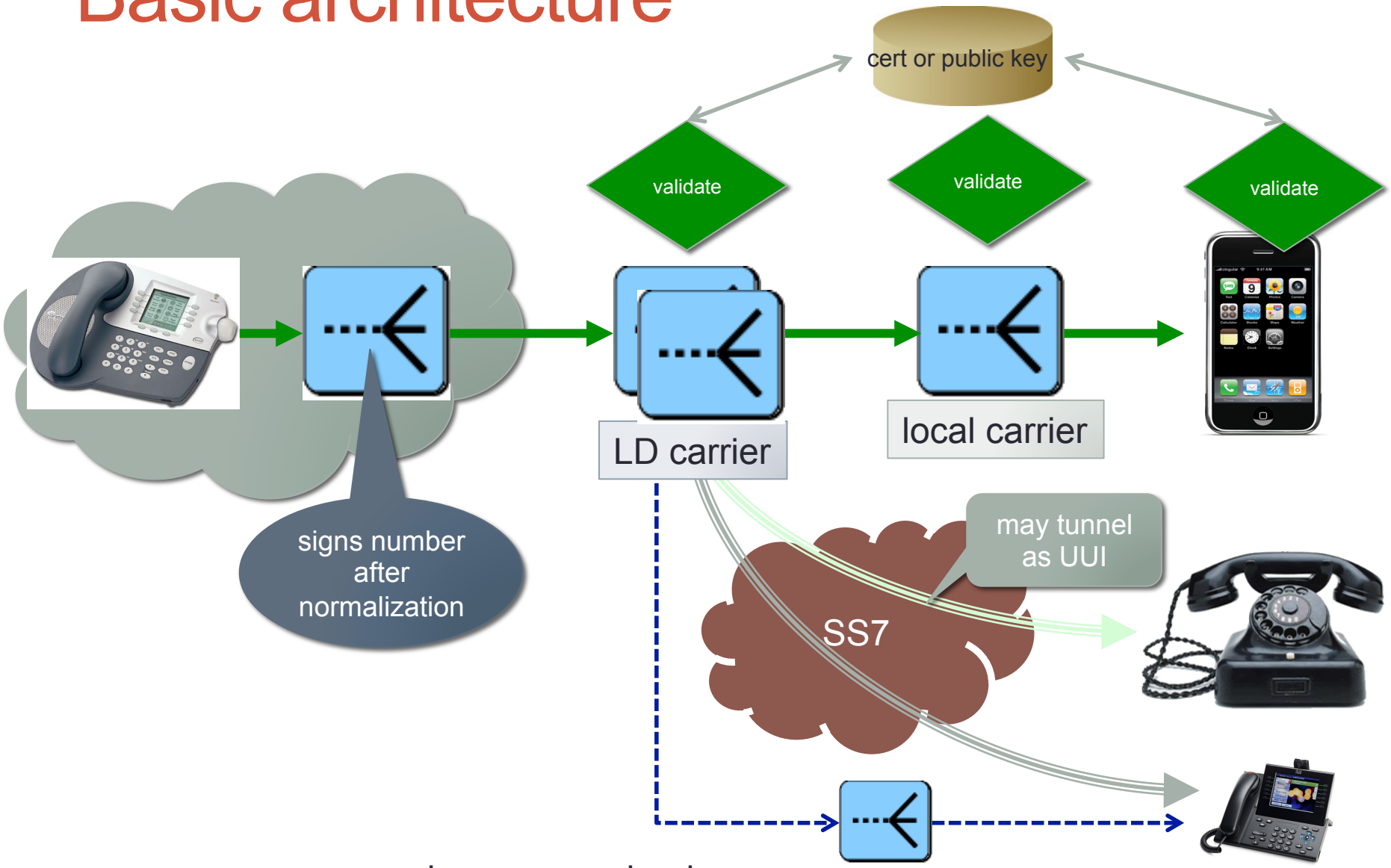
What makes solutions harder than in 2002?

- Mostly E.164 numbers, not domain-based SIP URIs
- Failure of public ENUM → no central database
- B2BUA deployment
  - → SDP rewritten for most calls
- Stickiness of infrastructure
  - SS7 will be with us, unchanged, for decade+
- Lots of non-SIP interconnection
  - for both technical and non-technical reasons
  - note: regulators typically encourage VoIP interconnection

Changes: opportunities

- Mobile, programmable devices
  - IP connectivity
  - allows (some) end system validation
- IP-enabled PBX & SIP trunking
- PKI developments, e.g., DANE

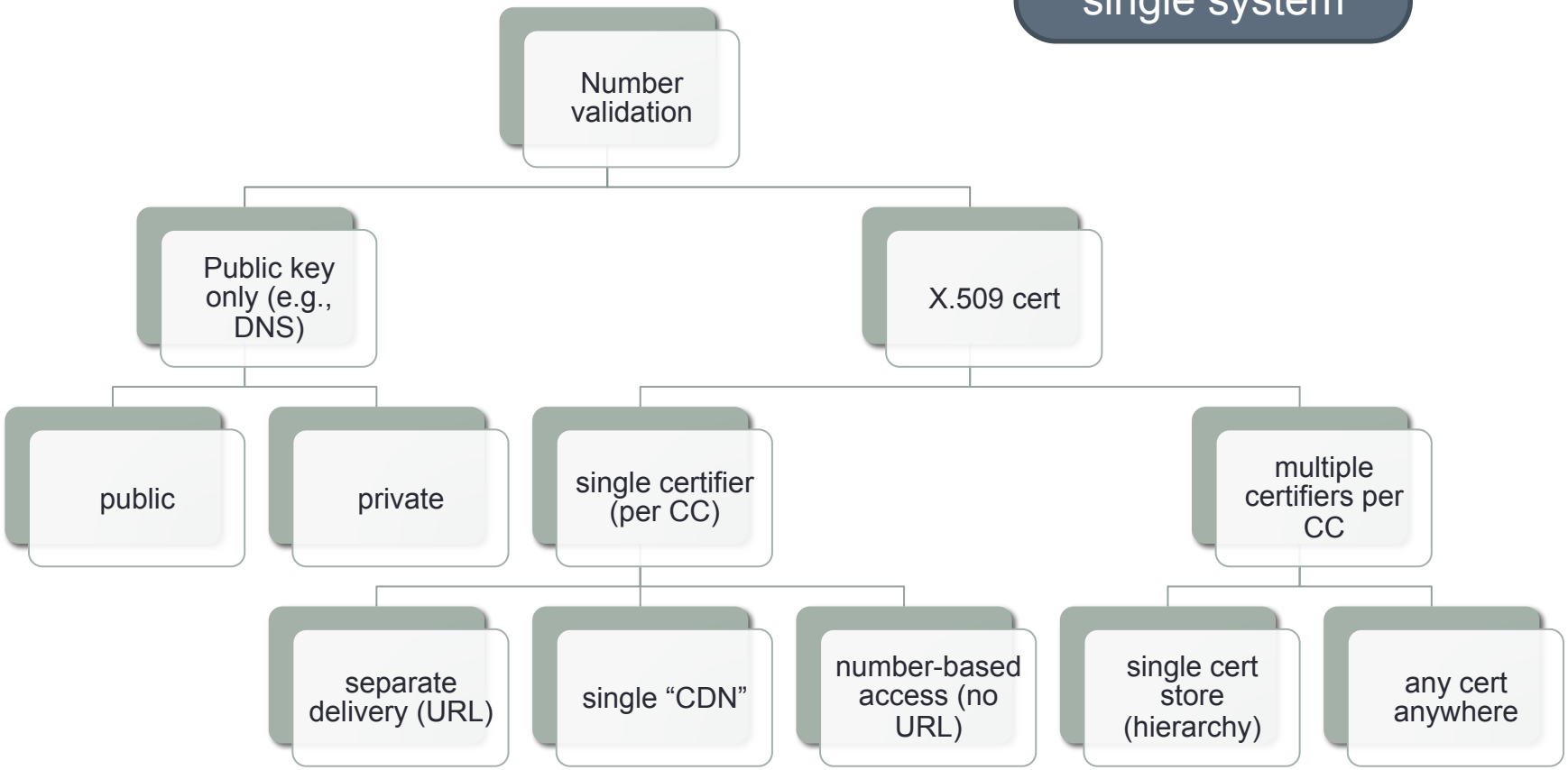
Basic architecture



rendezvous mechanism

Options

almost all of these could interoperate in single system



Certificate models

- *Integrated* with assignment
  - assignment of number includes certificate: “public key X is authorized to use number N”
  - issued by number assignment authority, possibly with delegation chain
    - allocation entity → carrier → end user
- *separate* proof of ownership
  - similar to web domain validation
  - e.g., Google voice validation by automated call back
    - “Enter the number you heard”
  - SIP OPTIONS message response?

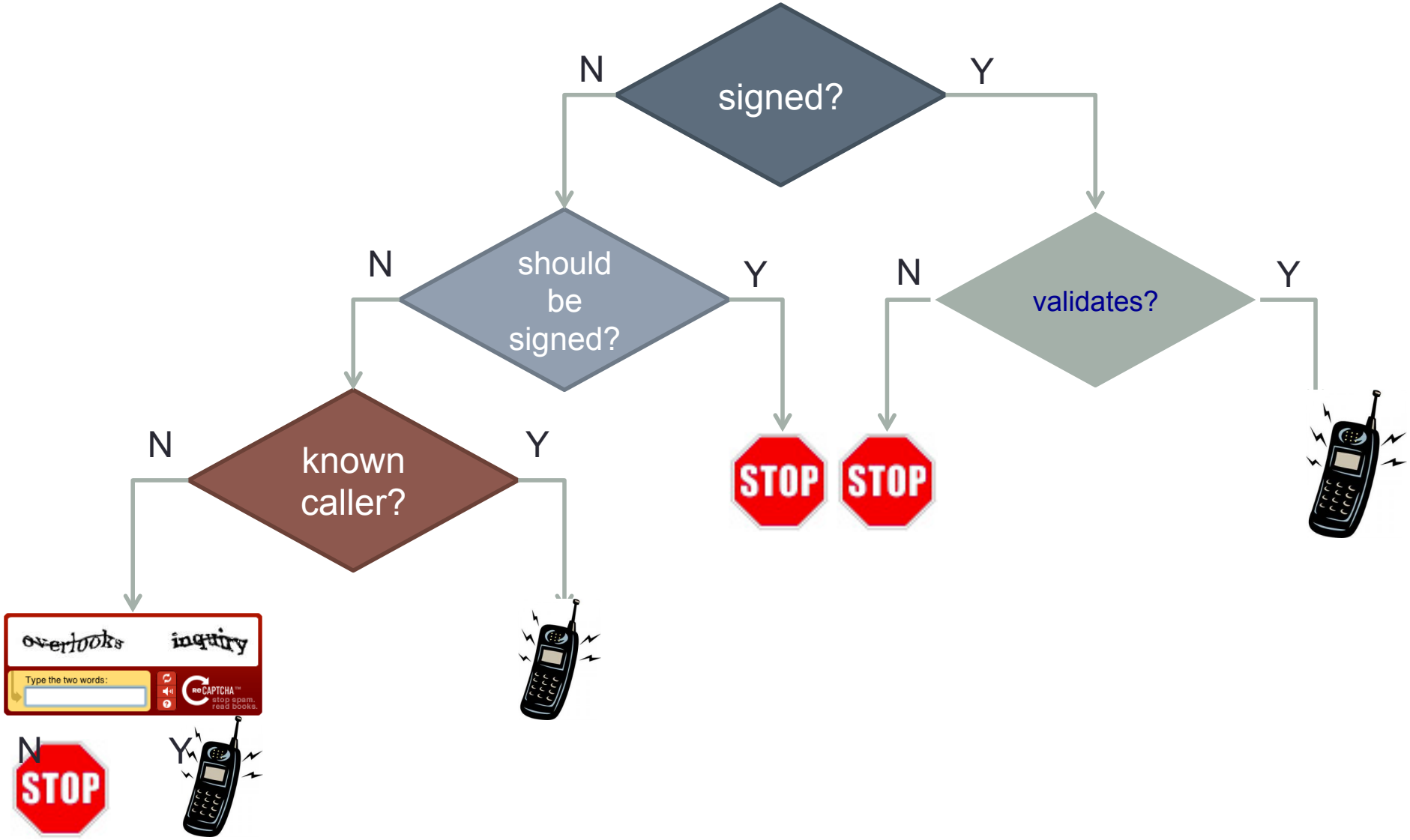
Delegation options

1. Official holder of number block interacts with registry
   - “My customer TheDoctorIsOut can use 212-555-1234 out of my number block”
   - requires database interaction
2. X.509 certificate delegation chain
   - reveals relationship of carriers and customers

Known unknowns

- Who will **sign** first, by choice or mandate?
  - large carriers (“get rid of robocall complaints”)
  - legitimate outbound call centers (“I want my snow day alert to be received”)
  - high-value users (“I want to prevent identity theft”)
  - smartphone end users
- Who will **validate** first?
  - carriers concerned about intercarrier compensation fraud
  - carriers sick of customer complaint calls
  - new entrants looking for differentiator (“switch and no more robocalls!”)

Incremental deployment



Conclusion

- Number spoofing is root of (almost) all phone evil
- Number spoofing may accelerate decay of PSTN
- Centralized number assignment makes problem tractable
- Solution approaches based on different assumptions
  - who is willing to do what & when?
- All in for one approach or multiple solutions?
  - reduce risk by multiple approaches?
  - cost to central entities vs. cost to signers & validators
  - or increase confusion, cost and non-adoption?