

Secure Origin Fallback Mechanism

`draft-rescorla-callerid-fallback`
(to be submitted)

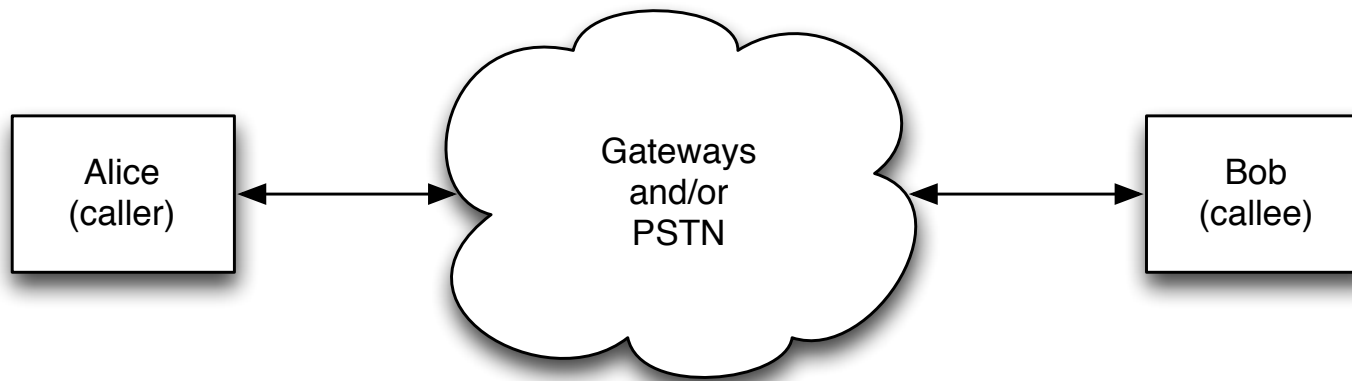
Eric Rescorla
`ekr@rtfm.com`

Not-so-secret workshop
May 31, 2013

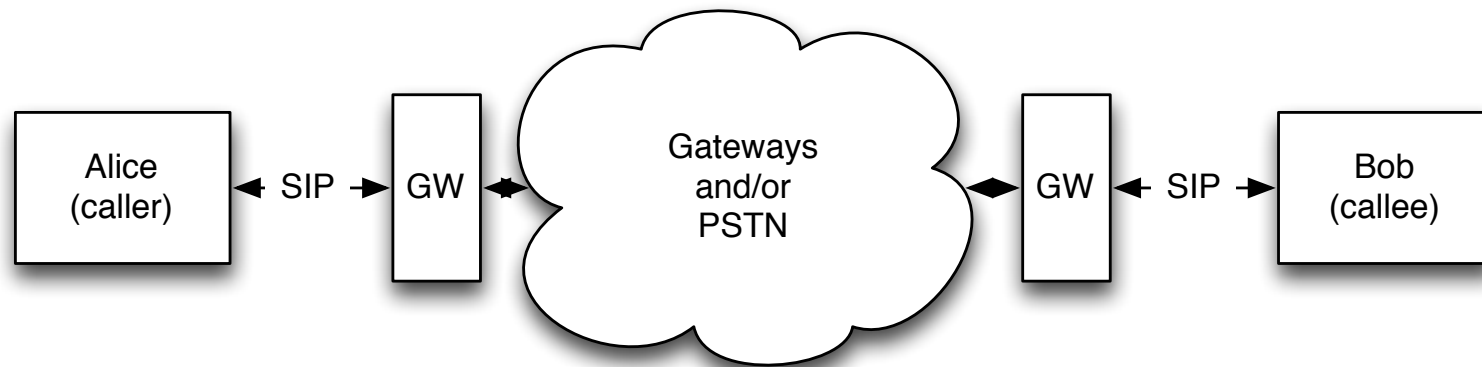
Overview

- RFC 4474 can provide secure origin information
- But SBCs and/or gateways break 4474
 - Change headers
 - Recreate call entirely
- Need to provide source authentication that can survive this
- Basic idea: “Call Detail Service” that validates existence of a call

Basic Setting



Alternate Setting



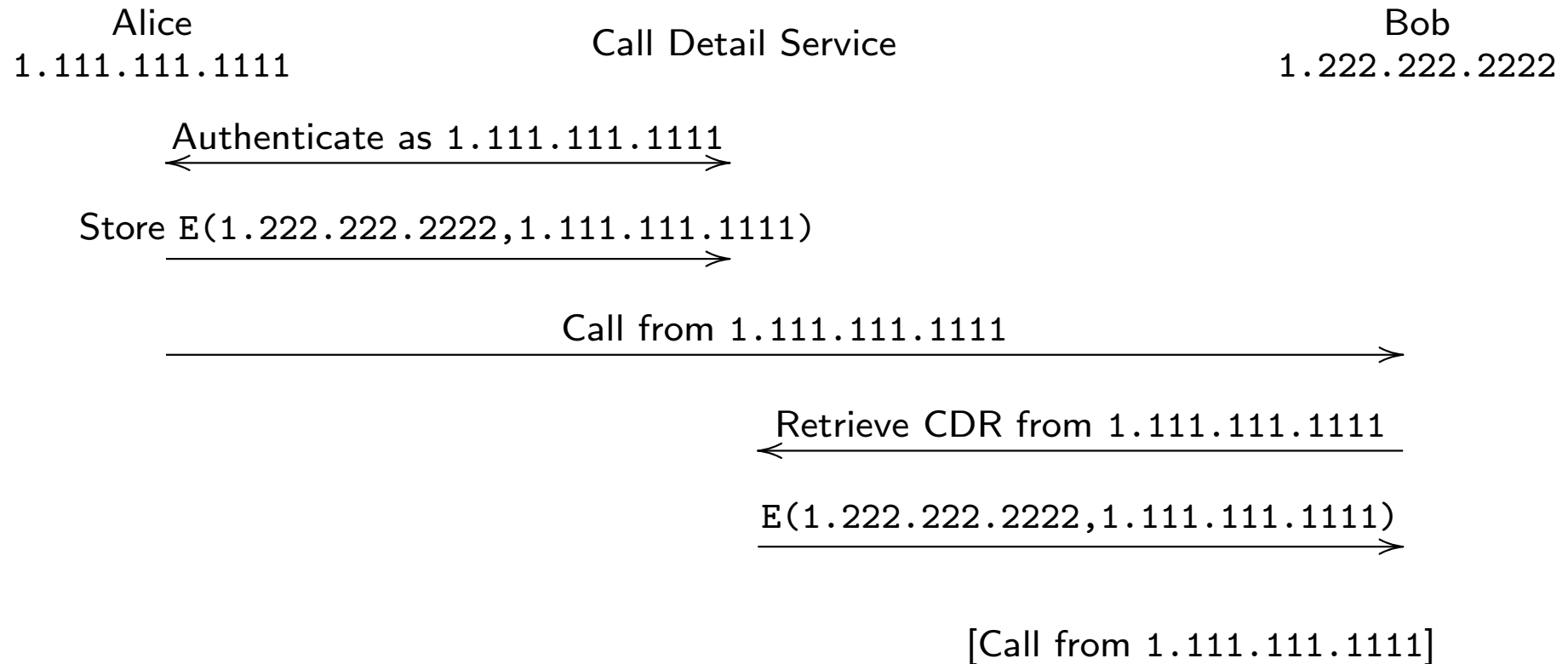
Assumptions (see Jon's talk)

- Endpoints are programmable
 - User has a smartphone, softphone, etc.
 - User has a dumb phone but is serviced by a programmable gateway
- Very restricted channel between endpoints
 - Effectively just a PSTN call
 - Caller cannot reliably control caller-id information (CIN field)
- Each E.164 is associated with cryptographic credentials
 - Usable for encryption, authentication, etc.

Credentials

- This assumes that each phone number is associated with credentials
- Requirements
 - Bind an E.164 number to key(s)
 - Suitable for both encryption and authentication
 - Possible to quickly retrieve the credentials for any number
- Example: a public key certificate with the E.164 number as subject

Call Flow



Caller Behavior

- Look up callee's credentials (may be cached)
- Sign and encrypt CDR for callee*
- Contact the CDS
 - Authenticate as the caller
 - Store encrypted CDR
- Initiate call to callee

*Special formats needed; must not contain recipient's identity in the clear.

CDS Behavior

- Only store credentials from authorized callers
 - This prevents spamming the CDS
- Provide CDR to any responder
- What if no CDR exists?
 - Generate a random CDR(s)
 - This helps mask the calling rate
 - * Though not so well for high-rate callers such as call centers

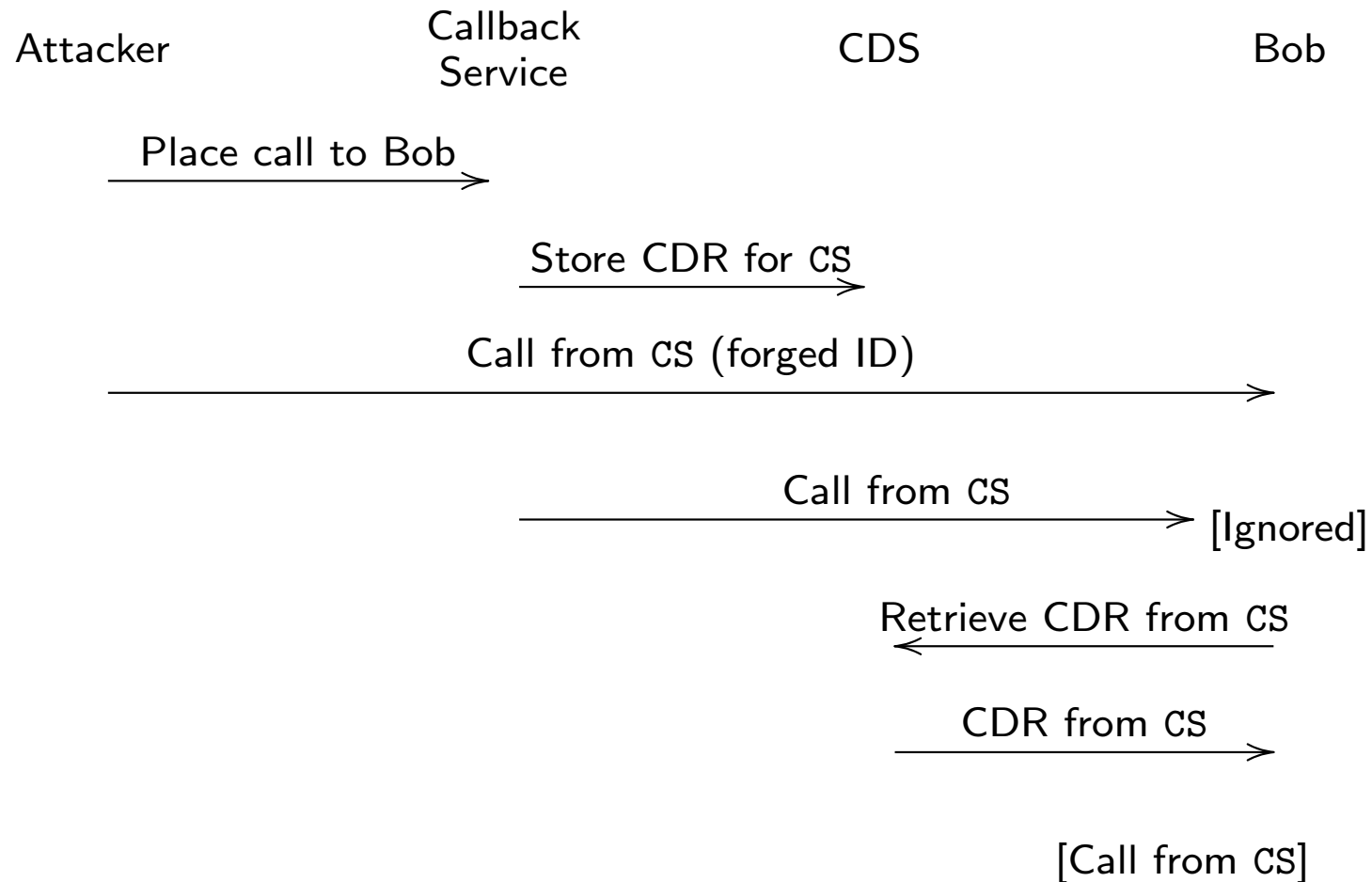
Callee Behavior

- Retrieve encrypted CDR from CDS using claimed caller number
- Decrypt CDR using private key
- Verify CDR signature matches caller's alleged identity
- Check timestamp for relevance (replay prevention)

What are the security guarantees?

- There exists a relatively recent call from caller to callee
 - Assuming credentials not compromised, etc.
- No guarantee that it is *this* call
- This defends against robocalling but not MITM attacks

Substitution Attack



Privacy Properties I: Off-path Attackers

- Cannot determine anything about who is calling who
- Cannot determine how many calls a callee is getting
- Limited information about how many calls a caller is generating
 - By polling caller number
 - Can tell if it is more than the minimum number of fake CDRs the CDS generates

Privacy Properties II: On-path Attackers (to CDS)

- Cannot directly tell who is calling who
 - Assuming communications to CDS are encrypted
- If call volumes are low, can do traffic analysis
 - Alice and Bob both contacted the CDS within a few seconds
- Can measure call volumes for caller and callee
 - Unless they are hidden behind some kind of proxy (Tor, etc.)

Privacy Properties III: CDS

- Anything an on-path attacker can do
- Can directly measure caller's call volume

Federated CDSs

- Don't need to have one giant CDS
- Each user can select their own CDS
 - Indicated in their credentials?
 - Or delegated from the master CDS?
- This does not need to be exact
 - Callers can fall back (or be bounced) to master CDS during transitions

What about the Credential Service?

- All callers and callees need to have credentials
- Must be possible for any caller to get callee credentials
 - Quickly
 - Somewhat privately
 - Possible design approaches
 - * Pre-fetch plus pub-sub
 - * Caching servers/proxies (a la DNS)
- Caller can provide the callee with his credentials

How important is credential timeliness?

- Attacker has caller's credentials
 - Can forge calls from attacker
- Attacker has callee's credentials
 - Can poll for calls to callee
 - But probably only for a small number of callers
- Compromise versus reassignment?
 - Can we not reassign during credential validity window?
 - This lets us make validity windows longer
 - Doesn't do anything for compromise
- What is the minimum detection time?

Escalation to VoIP

- Everything here has assumed that calls are carried through PSTN
 - What about VoIP?
 - Provides more features and better security (See Jon's talk)
- CDRs can contain more than just the caller/callee number
 - For instance, a SIP URI
 - * Similar concept to VIPR
- How aggressive should we be about this kind of upgrade?

Why not store under callee's number? (Barnes)

- No need for CDS to verify caller
- Avoids trial decryption stage
- Hard to avoid spamming of CDS
 - Could be mitigated by authenticated proxies?
- Doesn't let callee control privacy properties
 - If caller doesn't use a proxy then CDS can do traffic analysis

Why not...?

- Insert a correlation token in the caller's number
 - Could use it to store CDR
 - Assumed not to be possible
- Store under a hash of the caller's number
 - Better privacy but requires sending more traffic from CDS- \rightarrow callee
- Store under a hash of the caller + callee's number
 - May make privacy situation worse
 - Unless hash is shorter than either number
 - Very weak if either side is known
- Is there a practical Private Information Retrieval (PIR) protocol we can use here?

Questions?