IPTEL WG
Internet-Draft
Intended status: Standards Track
Expires: July 21, 2007

V. Gurbani
Bell Laboratories, Alcatel-Lucent
C. Jennings
Cisco Systems
January 17, 2007

Representing trunk groups in tel/sip Uniform Resource Identifiers (URIs)

draft-ietf-iptel-trunk-group-10.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a standardized mechanism to convey trunk group parameters in sip and tel Uniform Resource Identifiers (URIs). An extension to the tel URI is defined for this purpose.

Table of Contents

1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

2. Definitions

Call routing in the Public Switched Telephone Network (PSTN) is accomplished by routing calls over specific circuits (commonly referred to as "trunks") between Time Division Multiplexed (TDM) circuit switches. In switches, a group of trunks that connect to the same target switch or network is called a "trunk group." Consequently, trunk groups have labels, which are used as the main indication for the previous and next TDM switch participating in routing the call.

Formally, we define a trunk and trunk group and related terminology as follows (definition of "trunk" and "trunk group" is from [5]).

> Trunk: In a network, a communication path connecting two switching systems used in the establishment of an end-to-end connection. In selected applications, it may have both its terminations in the same switching system.
>
> Trunk Group: A set of trunks, traffic engineered as a unit, for the establishment of connections within or between switching systems in which all of the paths are interchangeable. A single trunk group can be shared across multiple switches for redundancy purposes.
>
> Digital Signal 0 (DS0): Digital Signal X is a term for a series of standard digital transmission rates based on DS0, a transmission rate of 64kbps (the bandwidth normally used for one telephone voice channel). The European E-carrier system of transmission also operates using the DS series as a base multiple.

Since the introduction of ubiquitous digital trunking, which resulted in the allocation of DS0s between end offices in minimum groups of 24 (in North America), it has become common to refer to bundles of DS0s as a trunk. Strictly speaking, however, a trunk is a single DS0 between two PSTN end offices - however, for the purposes of this document, the PSTN interface of a gateway acts effectively as an end office (i.e. if the gateway interfaces with Signaling System 7 (SS7), it has its own SS7 point code, and so on). A trunk group, then, is a bundle of DS0s (that need not be numerically contiguous in an SS7 Trunk Circuit Identification Code numbering scheme) which are grouped

under a common administrative policy for routing.

A Session Initiation Protocol (SIP) [3] to PSTN gateway may have trunks that are connected to different carriers. It is entirely reasonable for a SIP proxy to choose -- based on factors not enumerated in this document -- which carrier a call is sent to when it proxies a session setup request to the gateway. Since multiple carriers can transport a call to a particular phone number, the phone number itself is not sufficient to identify the carrier at the gateway. An additional piece of information in the form of a trunk group can be used to further pare down the choices at the gateway. As used in this document, trunks are necessarily tied to gateways, and a proxy that uses trunk groups during routing the request to a particular gateway knows and controls which gateway the call is going to be routed to, and knows what trunking resources are present on that gateway.

As another example, consider the case where an IP network is being used as a transit network between two PSTN networks. Here, a SIP proxy can apply the originating trunk group to its routing logic to ensure that the same ingress and egress carrier is chosen.

How the proxy picked a particular trunk group is outside the scope of this document ([6] provides one such way); however, once trunk group has been decided upon, this document provides a standardized means to represent it in the signaling messages.

3. Problem statement

Currently, there isn't any standardized manner of transporting trunk groups between Internet signaling entities. This leads to ambiguity on at least two fronts:

1. Positional ambiguity: A SIP proxy that wants to send a call to an egress Voice over IP (VoIP) gateway may insert the trunk group as a parameter in the user portion of the Request-URI (R-URI), or it may insert it as a parameter to the R-URI itself. This ambiguity persists in the reverse direction as well, that is, when an ingress VoIP gateway wants to send a incoming call notification to its default outbound proxy.
2. Semantic ambiguity: The lack of any standardized grammar to represent trunk groups leads to the unfortunate choice of ad hoc names and values.

VoIP routing entities in the Internet, such as SIP proxies, may be interested in using trunk groups for normal operations. To that extent, any standards-driven requirements will enable proxies from

one vendor to interoperate with gateways from yet another vendor. Absent such guidelines, interoperability will suffer as a proxy vendor must conform to the expectations of a gateway as to where it expects trunk group parameters to be present (and vice versa).

The aim of this specification is to outline how to structure and represent the trunk group parameters as an extension to the tel URI [4] in a standardized manner.

4. Requirements and rationale

This section captures the motivations for the design decisions for the specification of a trunk group. These motivations are captured as a set of requirements that are used to guide the eventual trunk group specification contained in this document.

4.1. sip URI or tel URI?

REQ 1: Trunk group parameters must be defined as an extension to the tel URI [4].

The trunk group parameters can be carried in either the sip URI or the tel URI. Since trunk groups are intimately associated with the PSTN, it seems reasonable to define them as extensions to the tel URI (any SIP request that goes to a gateway could reasonably be expected to have a tel URI, in whole or in part, in its R-URI anyway). Furthermore, using the tel URI also allows this format to be reused by non-SIP VoIP protocols (which could include anything from MGCP or Megaco to H.323, if the proper information elements are created).

Finally, once the trunk group is defined for a tel URI, the normative procedures of Section 19.1.6 of [3] can be used to derive an equivalent sip URI from a tel URI, complete with the trunk group parameters.

4.2. Trunk group namespace: global or local?

REQ 2: Inter-domain trunk group name collisions must be prevented.

Under normal operations, trunk groups are pertinent only within an administrative domain (i.e. local scope). However, given that inadvertent cross-domain trunk group name collisions may occur, it is desirable to prevent these. The judicious use of namespaces is a solution to this problem. Thus, it seems appropriate to scope the trunk group through a namespace.

At first glance, it would appear that the use of the tel URI's "phone-context" parameter provides a satisfactory means of imposing a namespace on a trunk group. The "phone-context" parameter identifies the scope of validity of a local telephone number. And therein lies the problem. Semantically, a "phone-context" tel URI parameter is applicable only to a local telephone number and not a global one (i.e., one preceded by a '+'). Trunk groups, on the other hand, may appear in local or global telephone numbers. Thus, what is needed is a new parameter with equivalent functionality of the "phone-context" parameter of the tel URI, but one that is equally applicable to local and global telephone numbers.

4.3. Originating trunk group and terminating trunk group

REQ 3: Originating trunk group and destination trunk group must be able to appear separately and concurrently in a SIP message.

SIP routing entities can make informed routing decisions based on either the originating or the terminating trunk groups. Thus a requirement that both of these trunk groups need to be carried in SIP requests.

4.4. Intermediary processing of trunk groups

REQ 4: SIP network intermediaries (proxy servers and redirect servers) should be able to add the destination trunk group attribute to SIP sessions as a route is selected for a call.

5. Trunk group identifier: ABNF and examples

The Augmented Backus Naur Form [2] syntax for a trunk group identifier is given below and extends the "par" production rule of the tel URI defined in [4]:

```
par = parameter / extension / isdn-subaddress / trunk-group /
      trunk-context

trunk-group = ";tgrp=" trunk-group-label
trunk-context = ";trunk-context=" descriptor

trunk-group-label = 1*( unreserved / escaped /
                        trunk-group-unreserved )
trunk-group-unreserved = "/" / "&" / "+" / "$"
```

```
      descriptor is defined in [4].
      unreserved is defined in [3] and [4].
      escaped is defined in [3].

    par = parameter / extension / isdn-subaddress / trunk-group /
          trunk-context

    trunk-group = ";tgrp=" trunk-group-label
    trunk-context = ";trunk-context=" descriptor

    trunk-group-label = 1*( unreserved / escaped /
                            trunk-group-unreserved )
    trunk-group-unreserved = "/" / "&" / "+" / "$"
```

Trunk groups are identified by two parameters: "tgrp" and "trunk-context"; both of these parameters MUST be present in a tel URI to identify a trunk group. Collectively, these two parameters are called "trunk group parameters" in this specification.

All implementations conforming to this specification MUST generate both of these parameters when using trunk groups. If an implementation receives a tel URI with only one of the "tgrp" or "trunk-context" parameter, it MUST act as if there were not any trunk group parameters present at all in that URI. Whether or not to further process such an URI is up to the discretion of the implementation, however, if a decision is made to process it, the implementation MUST act as if there were not any trunk group parameters present in the URI.

The "trunk-context" parameter imposes a namespace on the trunk group by specifying a global number or any number of its leading digits (e.g., +33), or a domain name. Syntactically, it is modeled after the "phone-context" parameter of the tel URI [4], except that unlike the "phone-context" parameter, the "trunk-context" parameter can appear in either a local or global tel URI.

Semantically, the "trunk-context" parameter establishes a scope of the trunk group specified in the "tgrp" parameter, i.e., whether it is valid at a single gateway, a set of gateways, or an entire domain managed by a service provider. The "trunk-context" can contain four discrete value types:

1. The value in the "trunk-context" literally identifies a host (a gateway), in which case the trunk groups are scoped to the specific host.
2. The value in the "trunk-context" is a subdomain (e.g., "north.example.com"), which identifies a subset of the gateways in a domain across which the trunk groups are shared.

3. The value in the "trunk-context" is a service provider domain (e.g., "example.com"), which identifies all gateways in the specific domain.
4. The value in the "trunk-context" is a global number or any number of its leading digits; this is useful for provider-wide scoping and does not lend itself very well to specifying trunk groups across a gateway or a set of gateways.

For equivalency purposes, two URIs containing trunk group parameters are equivalent according to the base comparison rules of the URIs. The base comparison rules of a tel URI are specified in Section 4 of [4], and the base comparison rules of a sip URI are specified in Section 19.1.4 of [3].

Examples:

1. Trunk group in a local number, with a phone-context parameter (the line breaks added for readability):

```
tel:5550100;phone-context=+1-630;tgrp=TG-1;
  trunk-context=example.com

Transforming this tel URI to a sip URI yields:
sip:5550100;phone-context=+1-630;tgrp=TG-1;
  trunk-context=example.com@isp.example.net;user=phone
```

2. Trunk group in a global number, with a domain name trunk-context:

```
tel:+16305550100;tgrp=TG-1;trunk-context=example.com

Transforming this tel URI to a sip URI yields:
sip:+16305550100;tgrp=TG-1;
  trunk-context=example.com@isp.example.net;user=phone
```

3. Trunk group in a global number, with a number prefix trunk-context:

```
tel:+16305550100;tgrp=TG-1;trunk-context=+1-630

Transforming this tel URI to a sip URI yields:
sip:+16305550100;tgrp=TG-1;
  trunk-context=+1-630@isp.example.net;user=phone
```

6. Normative behavior of SIP entities using trunk groups

The terminating (or egress) trunk group parameters MUST be specified in the R-URI. This is an indication from a SIP entity to the next

downstream entity that a specific terminating (or egress) trunk group should be used.

> This is consistent with using the R-URI as a routing element; SIP routing entities may use the trunk group parameter in the R-URI to make intelligent routing decisions. Furthermore, this also satisfies REQ 4, since a SIP network intermediary can modify the R-URI to include the trunk group parameters.

Conversely, the appearance of the trunk group parameters in the Contact header URI signifies the trunk group over which the call arrived on, i.e., the originating (or ingress) trunk group. Thus, the originating (or ingress) trunk group MUST appear in the Contact header of a SIP request.

The behavior described in this section effectively addresses REQ 3.

6.1. User Agent Client behavior

A User Agent Client (UAC) initiating a call that uses trunk groups and supports this specification MUST include the trunk group parameters in the Contact header URI (a Contact URI MUST be a sip or sips URI, thus, what appears in the Contact header is a SIP translation of the tel URI, complete with the trunk group parameters). The trunk group parameters in the Contact header represents the originating trunk group. As a consequence of the processing rules for the Contact header defined in RFC 3261 [3], subsequent requests in the dialog towards this user agent will contain this Contact URI in the R-URI. Note that the user part of this URI, which contains the trunk group parameters, will be copied as a consequence of this processing.

> Arguably, the originating trunk group can be part of the From URI. However, semantically, the URI in a From header is an abstract identifier which represents the resource thus identified on a long-term basis. The presence of a trunk group, on the other hand, signifies a binding that is valid for the duration of the session only; a trunk group has no significance once the session is over. Thus, the Contact URI is the best place to impart this information since it has exactly those semantics.

If the UAC is aware of the routing topology, it MAY insert the destination trunk group parameters in the R-URI of the request. However, in most deployments, the UAC will use the services of a proxy to further route the request, and it will be up to the proxy to insert such parameters in the R-URI (see Section 6.3)

6.2. User Agent Server behavior

To the processing User Agent Server (UAS) associated with a gateway, the trunk group parameters in the R-URI implies that it should use the named trunk group for the outbound call. If a UAS supports trunk groups, but finds that all the trunk circuit identification codes for that particular trunk group are occupied, it MAY send a 603 Decline final response.

If a UAS supports trunk groups but is not configured with the particular trunk group identified in the R-URI, it SHOULD NOT use any other trunk group other than the one specified in the parameters. In such a case, it MAY reject the request with a 404 final response; or if it makes a decision to process the request in any case, it MUST disregard the values in the "trunk-context" and the "tgrp" parameters.

If the receiver of a SIP request is not authoritatively responsible for the value specified in the "trunk-context", it MUST treat the value in the "tgrp" parameter as if it was not there. Whether or not to process the request further is up to the discretion of the processing entity; the request MAY be rejected with a 404 final response. Alternatively, if a decision is made to process the request further, the processing entity MUST disregard the values in the "trunk-context" and the "tgrp" parameters since it is not authoritatively responsible for the value specified in "trunk-context".

6.3. Proxy behavior

A proxy server receiving a request that contains the trunk group parameter in the Contact header SHOULD NOT change these parameters as the request traverses through it. Doing so may have adverse consequences, since the UAC that populated the parameters did so on some authoritative knowledge that the proxy may not be privy to. Instead, the proxy SHOULD pass the trunk group parameters in the Contact header unchanged to the client transaction that the proxy creates to send the request downstream.

A proxy that is aware of the routing topology and supports this specification, MAY insert destination trunk group parameters in the R-URI if none are present (see Section 7.1 and Section 7.2 for an example). However, if destination trunk group parameters are already present in the R-URI, the proxy SHOULD NOT change them unless it has further authoritative information about the routing topology than the upstream client did when it originally inserted the trunk group parameters in the R-URI.

Depending on the specific situation, it is perfectly reasonable for a proxy not to insert the destination trunk group parameters in the R-URI. Consider, for instance, a proxy that understands the originating trunk group parameters and, in accordance with local policy, uses these to route the request to an alternative destination than a PSTN gateway.

7. Example call flows

7.1. Reference architecture

Consider Figure 1, which depicts a SIP proxy in a routing relationship with three gateways in its domain, GW1, GW2, and GW3. Requests arrive at the SIP proxy through GW1. Gateways GW2 and GW3 are used as egress gateways from the domain. GW2 has two trunk groups configured, TG2-1 and TG2-2. GW3 also has two trunk groups configured, TG3-1 and TG2-2 (TG2-2 is shared between gateways GW2 and GW3).

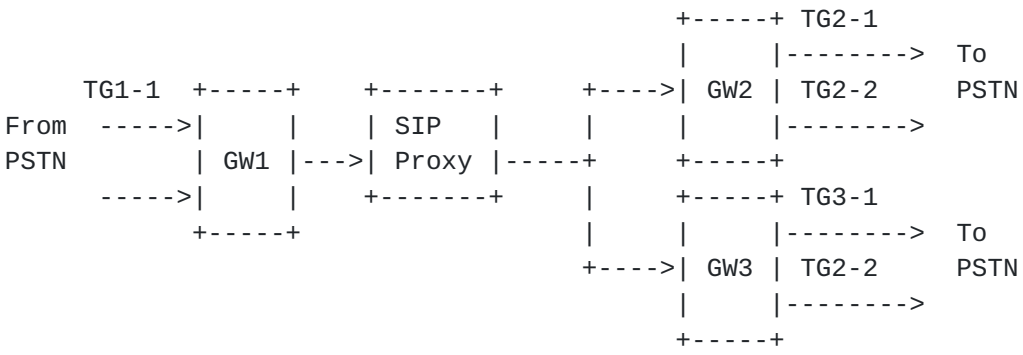


Figure 1: Reference architecture

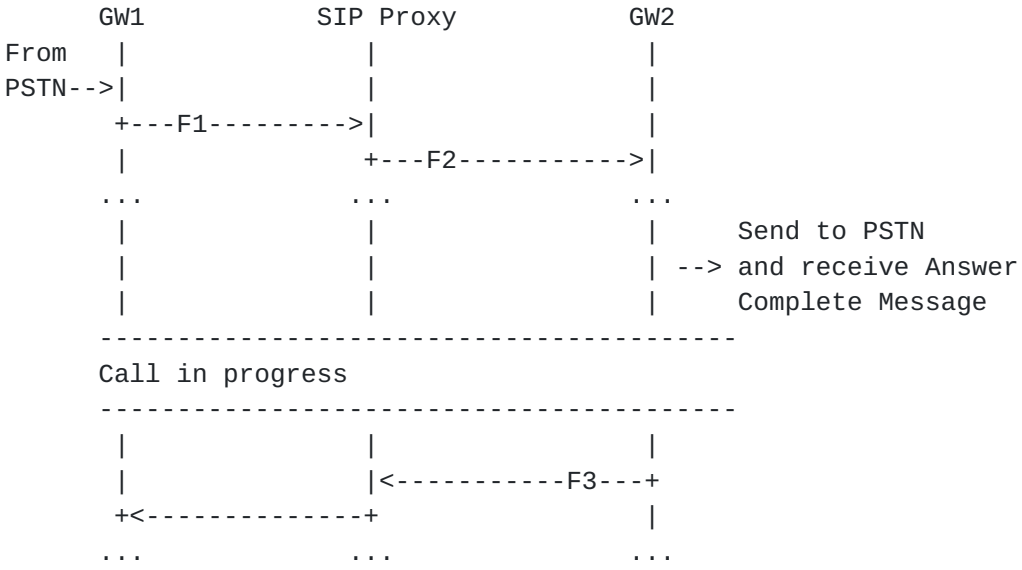
GW1 in Figure 1 is always cognizant of any requests that arrive over trunk group TG1-1. If it wishes to propagate the ingress trunk group to the proxy, it must arrange for the trunk group to appear in the Contact header of the SIP request destined to the proxy. The proxy will, in turn, propagate the ingress trunk group in the Contact header further downstream.

The proxy uses GW2 and GW3 as egress gateways to the PSTN. It is assumed that the proxy has access to a routing table for GW2 and GW3 which includes the appropriate trunk groups to use when sending a call to the PSTN (exactly how this table is constructed is out of scope for this specification; [6] is one way to do so, a manually created and maintained routing table is another). When the proxy sends a request to either of the egress gateways, and the gateway

routing table is so configured that a trunk group is required by the gateway, the proxy must arrange for the trunk group to appear in the SIP R-URI of the request destined to that gateway.

7.2. Basic Call Flow

This example uses the reference architecture of Figure 1. Gateways GW1, GW2, GW3 and the SIP proxy are assumed to be owned by a service provider whose domain is example.com.



In the call flow below, certain headers and messages have been omitted for brevity. In F1, GW1 receives a call setup request from the PSTN over a certain trunk group. GW1 arranges for this trunk group to appear in in the Contact header of the request destined to the SIP proxy.

```
F1:
INVITE sip:+16305550100@example.com;user=phone SIP/2.0
...
Contact: <sip:0100;phone-context=example.com;tgrp=TG1-1;
   trunk-context=example.com@gw1.example.com;user=phone>
...
```

In F2, the SIP proxy translates the R-URI and adds a destination trunk group to the R-URI. The request is then sent to GW2.

```
F2:
INVITE sip:+16305550100;tgrp=TG2-1;
  trunk-context=example.com@gw2.example.com;user=phone SIP/2.0
...
Record-Route: <sip:proxy.example.com;lr>
Contact: <sip:0100;phone-context=example.com;tgrp=TG1-1;
   trunk-context=example.com@gw1.example.com;user=phone>
...
```

Once the call is established, either end can tear the call down. For illustrative purposes, F3 depicts GW2 tearing the call down. Note that the Contact from F1, including the trunk group parameters, is now the R-URI of the request. When GW1 gets this request, it can associate the call with the appropriate trunk group to deallocate resources.

```
F3:
BYE sip:0100;phone-context=example.com;tgrp=TG1-1;
  trunk-context=example.com@gw1.example.com;user=phone SIP/2.0
Route: <sip:proxy.example.com;lr>
...
```

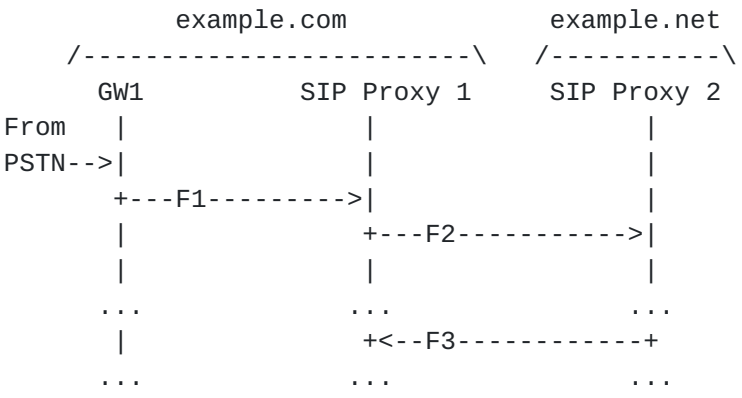
It is worth documenting the behavior when an incoming call from the PSTN is received at a gateway without a calling party number. Consider Figure 1, and assume that GW1 gets a call request from the PSTN without a calling party number. This is not an uncommon case, and may happen for a variety of reasons, including privacy and interworking between different signaling protocols before the request reached GW1. Under normal circumstances (i.e., instances where the calling party number is present in signaling), GW1 would derive a sip URI to insert into the Contact header. This sip URI will contain, as its user portion, the calling party number from from the incoming SS7 signaling information. The trunk group parameters then becomes part of the user portion as discussed previously.

If a gateway receives an incoming call where the calling party number is not available, it MUST create a tel URI containing a token that is generated locally and has local significance to the gateway. Details of generating such a token are implementation dependent; potential candidates include the gateway line number or port number where the call was accepted. This tel URI is subsequently converted to a sip URI to be inserted in the Contact header of the SIP request going downstream from the gateway.

The tel scheme does not allow for an empty URI; thus the global-number or local-number production rule of the tel URI [4] cannot contain an empty string. Consequently, the behavior in the above paragraph is mandated for cases where the incoming SS7 signaling message does not contain a calling party number.

7.3. Inter-domain Call Flow

This example demonstrates the advantage of namespaces in trunk groups. In the example flow below, GW1 and SIP Proxy 1 belong to the example.com domain and SIP Proxy 2 belongs to another domain, example.net. A call arrives at GW1 (F1) and is routed to the example.net domain. In the call flow below, certain headers and messages have been omitted for brevity.




```
F1:
INVITE sip:+16305550100@example.com;user=phone SIP/2.0
...
Contact: <sip:0100;phone-context=example.com;tgrp=TG1-1;
   trunk-context=example.com@gw1.example.com;user=phone>
...
```

In F2, the SIP proxy executes its routing logic and re-targets the R-URI to refer to a resource in example.net domain.

```
F2:
INVITE sip:+16305550100@example.net;user=phone SIP/2.0
...
Record-Route: <sip:proxy.example.com;lr>
Contact: <sip:0100;phone-context=example.com;tgrp=TG1-1;
   trunk-context=example.com@gw1.example.com;user=phone>
...
```

In F3, the example.net domain sends a request in the backwards

direction. The example.net domain does not interpret the trunk group parameters in the Contact header since they do not belong to that domain. The Contact header, including the trunk group parameters, is simply used as the R-URI in a subsequent request going towards the example.com domain.

```
F3:
BYE sip:0100;phone-context=example.com;tgrp=TG1-1;
   trunk-context=example.com@gw1.example.com;user=phone
Route: <sip:proxy.example.com;lr>
...
```

8. Security considerations

The trunk group parameters are carried in R-URIs and Contact headers; it is simply a modifier of an address, and any existing trust relationship between the originator of a request and an intermediary (or final recipient) that processes the request is not affected by such a modifier.

Maliciously modifying a trunk group of a R-URI in transit may cause the receiving entity, say a gateway, to prefer one trunk over another; thus leading to attacks that use resources not privy to the call. For example, an attacker who knows the name of a toll-free trunk on a gateway may modify the trunk group in the R-URI to effectively receive free service, or he may modify the trunk group in a R-URI to affect the flow of traffic across trunks. Similarly, modifying the trunk group in a Contact header may cause the routing intermediary to erroneously associate a call with a different source than it would normally be associated with.

Although this specification imparts more information to the R-URI and the Contact header in the form of trunk groups, the class of attacks and possible protection mechanism are the same as that specified for baseline SIP systems [3]. The Security Session Initiation Protocol Secure (SIPS) scheme and the resulting Transport Layer Security (TLS) mechanism SHOULD be used to provide integrity protection, thereby mitigating these attacks.

A question naturally arises on how does the receiver determine whether the sender is authorized to use the resources represented by the trunk group parameters? There are two cases to consider: intra-domain signaling exchange as discussed in Section 7.2, and inter-domain signaling exchange as discussed in Section 7.3.

In the intra-domain case, a proxy reciving trunk group parameters from an upstream user agent (typically a gateway) should only accept

them using the SIPS URI scheme, and furthermore, it should use HTTP Digest to challenge and properly authorize the sender. A user agent (or a gateway) receiving the trunk group parameters from a proxy will not be able to challenge the proxy using HTTP Digest, but it should examine the X.509 certificate of the proxy to determine whether the proxy is authorized to insert the resources represented by the trunk group parameters into the signaling flow.

In the inter-domain case, a receiving proxy may depend on the identity stored in the X.509 certificate of the sending proxy to make a determination whether the sender is authorized to insert the resources represented by the trunk group parameters in the signaling message.

Because of these considerations, the trunk group parameters are only applicable within a set of network nodes among which there is mutual trust. If a node receives a call signaling request from an upstream node that it does not trust, it SHOULD remove the trunk group parameters.

The privacy information revealed with a trunk group does not generally advertise much information about a particular (human) user. It does, however, convey two pieces of potentially private information which may be considered sensitive by carriers. First, it may reveal how a carrier may be performing least-cost routing and peering; and secondly, it does introduce an additional means for network topology and information of a carrier. It is up to the discretionary judgment of the carrier if it wants to include the trunk group parameters and reveal potentially sensitive information on its network topology. If confidentiality is desired, TLS SHOULD be used to protect this information while in transit.

9. IANA considerations

This specification does not require any IANA considerations.

The tel URI parameters introduced in this document are registered with IANA through the tel URI parameter registry document [7].

10. Acknowledgments

The authors would like to acknowledge the efforts of the participants of the SIPPING and IPTEL working group, especially Jeroen van Bemmel, Bryan Byerly, John Hearty, Alan Johnston, Shan Lu, Rohan Mahy, Jon Peterson, Mike Pierce, Adam Roach, Brian Rosen, Jonathan Rosenberg, Dave Oran, Takuya Sawada, Tom Taylor, and Al Varney.

Jon Peterson was also instrumental in the original formulation of this work.

Alex Mayrhofer brought up the issue of lexicographic ordering of tel URI parameters when it is converted to a sip or sips URI.

Ted Hardie, Sam Hartman, and Russ Housley took pains to ensure that the text around URI comparisons and security considerations was as unambiguous as possible.

11. References

11.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[4] Schulzrinne, H., "The tel URI for Telephone Calls", RFC 3966, December 2004.

11.2. Informative References

[5] "Bellcore Notes on the Network", Telcordia SR2275, Dec 1997, <http://www.telcordia.com>.

[6] Bangalore, M., Kumar, R., Rosenberg, J., Salama, H., and D. Shah, "A Telephony Gateway REgistration Protocol (TGREP)", draft-ietf-iptel-tgrep-08.txt (work in progress), January 2007.

[7] Jennings, C. and V. Gurbani, "The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry", draft-ietf-iptel-tel-reg-04.txt (work in progress), December 2006.

Authors' Addresses

Vijay K. Gurbani
Bell Laboratories, Alcatel-Lucent
2701 Lucent Lane
Rm 9F-546
Lisle, IL 60532
USA

Phone: +1 630 224 0216
Email: vkg@alcatel-lucent.com

Cullen Jennings
Cisco Systems
170 West Tasman Drive
Mailstop SJC-21/3
San Jose, CA 95134
USA

Phone: +1 408 421 9990
Email: fluffy@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).