Globally Identifiable Number (GIN) Registration

Adam Roach

`draft-ietf-martini-gin-07`

MARTINI / Interim VI

September 27th, 2010

Changes Since -05

- Myriad editorial changes from nits reviews during WGLC
- Added normative text around level of support required for GRUUs, reg-event, outbound, path, and service route
- Selected one behavior for malformed “bnc” URIs
- Update from security review
- Several GRUU clarifications
- Several reg-event clarifications
- Updated requirements in appendix A to match RFC 5947

Ticket #51

A registrar that receives a Contact URI with both a "bnc" parameter and a user portion MUST either discard the user portion and process the request as if the parameter were not present or return a 400 (Bad Request) error in response (unless some other error code is more appropriate).

A registrar that receives a Contact URI with both a "bnc" parameter and a user portion return a 400 (Bad Request) error in response (unless some other error code is more appropriate).

MUST *(Whoops)*

When a SIP-PBX registers with an SSP using a "bnc" contact, that contact MUST NOT include a "user" parameter. An SSP registrar that receives a Contact URI with both a "bnc" parameter and a "user" parameter MUST either discard the "user" parameter and process the request as if the parameter were not present or return a 400 (Bad Request) error in response (unless some other error code is more appropriate).

When a SIP-PBX registers with an SSP using a contact containing a "bnc" parameter, that contact MUST NOT include a "user" parameter. An SSP registrar that receives a Contact URI with both a "bnc" parameter and a "user" parameter MUST return a 400 (Bad Request) error in response (unless some other error code is more appropriate).

Mailing List Discussion

- “At the IETF 78 MARTINI WG meeting, during the discussion of Ticket 57 (relating to temporary GRUUs), a suggestion was made that public GRUUs be mandatory to implement for SSPs.”
- “A number of the "against" postings suggested SHOULD so a separate discussion may be needed to iron that out.”

```
7.1.1.  Public GRUUs

   In order to provide support for advanced services, the SSP SHOULD
   implement the public GRUU mechanism described in this section.
   Reasons for not doing so would include situations in which the
   relatively low implementation complexity of public GRUUs would
   dissuade service providers who would otherwise deploy the mechanism
   described in this document from doing so.
```

Ticket #57

7.1.2. Temporary GRUUs

In order to provide support for privacy, the SSP SHOULD implement the temporary GRUU mechanism described in this section. Reasons for not doing so would include systems with an alternative privacy mechanism which maintains the integrity of public GRUUs (i.e., if public GRUUs are anonymized then the anonymizer function would need to be capable of providing as the anonymized URI a globally routable URI that routes back only to the target identified by the original public GRUU).

Ticket #56
(Proposal #1 from Maastricht)

7.1.2.1. Generation of temp-gruu-cookie by the SSP

An SSP that supports temporary GRUUs MUST include a "temp-gruu-cookie" parameter on all "bnc" Contact header fields in a 200-class REGISTER response. This "temp-gruu-cookie" MUST have the following properties:

1. It can be used by the SSP to uniquely identify the registration to which it corresponds.
2. It cannot be modified by the recipient to hijack calls intended for another SIP-PBX.
3. It cannot be replayed at a later date to hijack calls intended for another SIP-PBX.
4. It is encoded using base64. This allows the SIP-PBX to decode it into as compact a form as possible for use in its calculations.
5. It is of a fixed length. This allows for extraction of it once the SIP-PBX has concatenated a distinguisher onto it.

7.1.2.1. Generation of temp-gruu-cookie by the SSP

An SSP that supports temporary GRUUs MUST include a "temp-gruu-cookie" parameter on all Contact header fields containing a "bnc" parameter in a 200-class REGISTER response. This "temp-gruu-cookie" MUST have the following properties:

1. It can be used by the SSP to uniquely identify the registration to which it corresponds.
2. It is encoded using base64. This allows the SIP-PBX to decode it into as compact a form as possible for use in its calculations.
3. It is of a fixed length. This allows for extraction of it once the SIP-PBX has concatenated a distinguisher onto it.
4. The temp-gruu-cookie MUST NOT be forgeable by any party. In other words, the SSP needs to be able to examine the cookie and validate that it was generated by the SSP.
5. The temp-gruu-cookie MUST be invariant during the course of a registration, including any refreshes to that registration. This property is important, as it allows the SIP-PBX to examine the temp-gruu-cookie to determine whether the temp-gruus it has issued to its UAs are still valid.

Ticket #61, Part 2b

Ticket #61, Parts 1 and 2b

7.1.2.2. Generation of temp-gruu by the SIP-PBX

According to RFC5627 [17] section 3.2, every registration refresh generates a new temp-gruu that is valid for as long as the contact remains registered. This property is both critical for the privacy properties of temp-gruu and is expected by UAs that implement the temp-gruu procedures. Nothing in this document should be construed as changing this fundamental temp-gruu property in any way. SIP-PBXes that implement temporary GRUUs MUST generate a new temp-gruu according to the procedures in this section for every registration refresh.

Similarly, if the registration that a SIP-PBX has with its SSP expires or is terminated, then the temp-gruu cookie it maintains with the SSP will change. This change will invalidate all the temp-gruus the SIP-PBX has issued to its UAs. If the SIP-PBX tracks this information (e.g., to include <temp-gruu> elements in registration event bodies, as described in RFC 5628 [9]), it can determine that previously issued temp-gruus are invalid by observing a change in the temp-gruu-cookie provided to it by the SSP.

Ticket #60 (Sections 7.2 and 7.3)

7.2. Registration Event Package

Neither the SSP nor the SIP-PBX is required to support the Registration event package defined by RFC 3680 [12]. However, if they do support the Registration event package, they MUST conform to the behavior described in this section.

7.3. Client-Initiated (Outbound) Connections

RFC 5626 [16] defines a mechanism that allows UAs to establish long-lived TCP connections or UDP associations with a proxy in a way that allows bidirectional traffic between the proxy and the UA. This behavior is particularly important in the presence of NATs, and whenever TLS security is required. Neither the SSP nor the SIP-PBX is required to support client-initiated connections.

Ticket #60 (Section 7.4)

may be different from each other. Support for non-adjacent contact registration is required in all SSPs and SIP-PBXes implementing the multiple-AOR-registration protocol described in this document.

At registration time, any proxies between the user agent and the registrar may add themselves to the Path. By doing so, they request that any requests destined to the user agent as a result of the associated registration include them as part of the Route towards the User Agent. Although the Path mechanism does deliver the final Path value to the registering UA, UAs typically ignore the value of the Path.

To provide similar functionality in the opposite direction -- that is, to establish a route for requests sent by a registering UA -- RFC 3608 [11] defines a means by which a UA can be informed of a route that is to be used by the UA to route all outbound requests associated with the AOR used in the registration. This information is scoped to the AOR within the UA, and is not specific to the Contact (or Contacts) in the REGISTER request. Support of service route discovery is optional in SSPs and SIP-PBXes.

Ticket #55 and Ticket #61, Part 2a

In particular, the "bnc" parameter is forbidden from appearing in the body of a reg-event notify unless the subscriber has indicated knowledge of the semantics of the "bnc" parameter. The means for indicating this support are out of scope of this document.

Because the SSP does not necessarily know which GRUUs have been issued by the SIP-PBX to its associated UAs, these records will not generally the contain <temp-gruu> or <pub-gruu> elements defined in RFC 5628 [9]. This information can be learned, if necessary, by subscribing to the individual AOR registration state, as described in Section 7.2.2.

Ticket #59, Issue 3

MARTINI WG
Internet-Draft
Updates: 3680 (if approved)

If the Request-URI in a SUBSCRIBE request for the registration event package indicates a contact that is registered by more than one SIP-PBX, then the SSP proxy will fork the SUBSCRIBE request to all the applicable SIP-PBXes. Similarly, if the Request-URI corresponds to a contact that is both implicitly registered by a SIP-PBX and explicitly registered directly with the SSP proxy, then the SSP proxy will semantically fork the SUBSCRIBE request to the applicable SIP-PBX or SIP-PBXes and to the SSP registrar function (which will respond with registration data corresponding to the explicit registrations at the SSP). The forking in both of these cases can be avoided if the SSP has and can maintain a copy of up-to-date information from the PBXes.

Section 4.9 of RFC 3680 [12] indicates that "a subscriber MUST NOT create multiple dialogs as a result of a single [registration event] subscription request." Consequently, subscribers who are not aware of the extension described by this document will accept only one dialog in response to such requests. In the case described in the preceding paragraph, this behavior will result in such client receiving accurate but incomplete information about the registration state of an AOR. As an explicit change to the normative behavior of RFC 3680, this document stipulates that subscribers to the registration event package MAY create multiple dialogs as the result of a single subscription request. This will allow subscribers to create a complete view of an AOR's registration state.

Ticket #59, Issue 1

> If the SIP-PBX is not registered with the SSP when a registration event subscription for a contact that would be implicitly registered if the SIP-PBX were registered, the the SSP SHOULD accept the subscription and indicate that the user is not currently registered. Once the associated SIP-PBX is registered, the SSP SHOULD use the subscription migration mechanism defined in RFC 3265 [6] to migrate the subscription to the SIP-PBX.

Ticket #61, part 3

> A SIP-PBX that supports both GRUU procedures and the registration event packages SHOULD implement the extension defined in RFC 5628 [9].

Ticket #56
(Proposal #2 from Maastricht)

> Further, the use of RSA decryption when processing GRUUs received from arbitrary parties can be exploited by DoS attackers to amplify the impact of an attack: because of the presence of a cryptographic operation in the processing of such messages, the CPU load may be marginally higher when the attacker uses (valid or invalid) temporary GRUUs in the messages employed by such an attack. Normal DoS mitigation techniques, such as rate-limiting processing of received messages, should help to reduce the impact of this issue as well.