IETF ENUM WG
Internet Draft
Document:
draft-shockey-enum-privacy-security-00.txt
Expires: March 2003

Richard Shockey
NeuStar,Inc

October 2002

Privacy and Security Considerations in ENUM

Status of this Memo

Copyright Notice

Abstract

Many individuals and groups have expressed concerns about the privacy and security of personal information to be established in implementations of RFC 2916. This document discusses some of the technical as well as security and privacy considerations national implementations of ENUM should consider.

This is a work in progress. Input from security and privacy experts is welcome.

draft-shockey-enum-privacy-security-00.txt October 2002

Discussion of this document is welcomed on the IETF ENUM mailing list.

General Discussion:enum@ietf.org
To Subscribe: enum-request@ietf.org
In Body: subscribe
Archive: ftp://ftp.ietf.org/ietf-mail-archive/enum/

Conventions used in this document

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 [2].

Table of Contents

1) Introduction

Readers of this Internet Draft are expected to have a working knowledge of

principals embodied in [RFC2916bis].

Many individuals groups have expressed concerns about the privacy and data security implications of ENUM as it moves forward toward global deployment. In that context there are several different views

of what ENUM is, what it does, and how a global ENUM system may affect personal privacy and the security of data contained in the global ENUM system.

It is important to note that ENUM is first and foremost the DNS. Specifically ENUM is a system that translates E.164 phone numbers [ITU-T] into Fully Qualified Domain Names that can be queried to return a specific set of data (URIÆs)in the form of NAPTR records [RFC 3403]. The global and distributed nature of the DNS means delegation and control can occur at any point within the ENUM defined FQDN. Many entities, service providers, enterprises and indeed some consumers could, control their own DNS servers for ENUM registered domain names.

There are two forms of data required for the ENUM system to work. First is the actual data to be entered into the global ENUM DNS system, the NAPTR records, that can be accessed by any IP end point any where in the world, without restriction and second, the data that will be required to maintain appropriate authentication, valid registration, administrative and technical contact for DNS servers. Issues involving domain name registration are well known to the privacy and security communities and have continually surfaced in context with the Domain Name Registration industry and ICANN approved registry-registrar business practices.

The agreements between the IAB and the ITU over the management and control of the e164.arpa namespace [RFC 3026] for those portions of the E.164 global numbering plan clearly articulates that the administration, management and control of the zones and administrative portions of the E.164 plan are nation-state issues governed by appropriate national laws and regulations, many of which have yet to be determined.

2) THE RATIONALE FOR ENUM

Before a discussion of privacy and security issues can be applied to

various parts of the global ENUM system it is essential to note why the IETF technical community developed ENUM, what applications it was designed to serve and the implications of those applications for privacy and security issues.

Since Telephone Numbers are the global naming and addressing scheme for Public Switched Telephony, ENUM was designed to map phone numbers with the Internet DNS and its naming and addressing conventions (IP numbers and Domain Names). Principally ENUM enables the use of phone numbers as identifiers of services defined as URIÆs on the Internet as well as facilitate the interconnection of systems that rely on telephone numbers with those that use URIÆs to route transactions.

It is well known that businesses and consumers are very comfortable with using telephone numbers for PSTN communications. The E.164 numbering plan is a well organized and internationally recognized system of naming and addressing that is essential to the proper functioning of the PSTN. Phone Numbers have the additional advantage of being easily understood, are a useful input mechanism on billions of terminal devices (telephones) that do not have QWERTY like keyboards and, significantly, are linguistically neutral, unlike domain names.

Though it is clear that ENUM can and will be used for service routing of applications other than voice, the principal focus of attention on ENUM application development has, naturally, been voice communications based on SIP [RFC 3261] and ITU developed H.323, and the general concept of convergence in IP and PSTN networks.

3) THREE VIEWS OF ENUM

Even within the technical community there are different views of what ENUM is and what it is designed to accomplish.

3.1 NUMBER TRANSLATION DATABASE

One view sees ENUM in the DNS as essentially a benign number translation database that exposes on the minimal subset of data necessary to establish a connection between two endpoints. This is

the model we essentially have in the DNS now. DNS translates the URI concept such as http://www.foobar.org to an IP number necessary for a client to find a server running HTTP. No other intervention by the DNS is necessary.

This is also the function of the DNS in E-mail where the DNS is used to locate an MX record for a SMTP server within a domain. No policy or personal information is exposed in the DNS beyond a server name.

This concept is roughly analogous to the concept of a Service Control Point within the architecture of the PSTN that provide routing data to a circuit switch based on the numeric input of a phone number.

3.2 CALLED PARTY CONTROL OF ENUM ENABLED COMMUNICAITONS

An emerging view of ENUM is that it enables an advanced form of called party control of communications since it is presumed that the communications servers at the edge of network are under the administrative or operational control of the called party. Called party control of those servers permits policy in some form to be directly applied to inbound communications irrespective of the wishes of the calling party.

This view is particularly relevant in the case of SIP based communication [PETERSON et.al.]. The classic SIP model is based on the use of proxies between end point client/user agents that can then negotiate information about each other in order to establish a session. The calling party has no need to discover the capabilities of the called parties end point since those are established during the signaling portion of a SIP session using Session Description Protocol.

The called parties proxy can also be used to enforce policy about sessions including how, when and from whom to establish sessions. The presumption of this model is that only the minimum information about an endpoint is necessary to expose in the global DNS, since the proxies perform all other forms of session negotiation and policy enforcement.

Consequently it is not necessary to expose in the DNS whether a particular SIP endpoint supports voice, instant messaging, video or fax or whether that endpoint operates on a wire line or wireless connection.

3.3.1 THE USE OF REAL AND OR ALIAS NAMES IN A SIP ADDRESS-OF-RECORD.

Because SIP can negotiate the session creation between end points, it is not necessary expose in the global DNS specific personal identification elements, such as a personal name, to establish a successful end-to-end SIP connection.

Information, such as a personal name, is exposed only because an end user chooses to do so by configuration of their entries into the DNS.

For example, a classic example of a ENUM response with a SIP URI using a personal name might be as follows:

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"      "!^.*$!sip:patrik.faltstrom@foobar.se!"
```

One alternative method of achieving the same result with out exposing a real name is to configure the called parties ENUM DNS entries to use other forms of names as aliases. In the following example, the identification of the SIP endpoint is configured using the generic format "sip:e164number@userdomain.foo"

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"      "!^.*$!sip:4689761234@foobar.se!"
```

OR

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"      "!^.*$!sip:anon5613@foobar.se!"
```

Where the user name "anon5616" is randomly selected.

Notice that the ENUM query only returns information that a SIP proxy for the user "4689761234" or "anon5616" exists within the domain

foobar.se. No personal information is exposed in the global DNS other than the domain to which a SIP proxy exists and a form of user name.

From the perspective of the called parties SIP proxy, if properly configured, there is no functional difference between
sip:patrik.faltstrom@foobar.se or
sip:4689761234@foobar.se or
sip:anon5651@foobar.se.

All three could accurately describe a unique SIP client or user agent and transactions could be routed equally among all three names.

These examples illustrate an alternate view of what is necessary to establish a connection between two parties using ENUM and SIP. This concept of can easily be applied to many applications which can be ENUM enabled.

An individual may choose give out a form of personal SIP URI using their personal on their business card, but there is no practical reason this must be entered into the global DNS.

Current discussion in the IETF ENUM WG have explored the concept of indirect resolution to all forms of communications, not just SIP, through the use of presence servers or a concept called a Service resolution service. Once again the called party who is registering their phone number in the global ENUM system would then have control of how he or she could be contacted by any method.

The concept of a Service Resolution Service has not been defined in the IETF, however it is within the realm of technical possibility.

TBD Examples

3.3 CALLING PARTY CONTROL OF COMMUNICATIONS

One other view of ENUM wishes to give the calling party the maximum control and options over how they wish to contact someone else. The preference here is for the maximum amount of information exposed in the DNS to permit the calling party the choice of contact

methodology to the called party.

Not only are all potential communications endpoints exposed in the global DNS but verbose hints to the nature and capabilities of those endpoints are described in the NAPTR enumservice field.[BRADNER]

The ENUM DNS query returns all the available URIÆs listed, however the in these examples the called party has chosen to display other attributes about those services such as voice:home, sip:im , voice:mobile,mailto, etc.

A client application or service parses the NAPTR records and displays the various options and the calling party then selects the most appropriate option based on their preference and not that of the called party.

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip:voice:home"    "!^.*$!sip:patrik.faltstrom@foob

IN NAPTR 100 10 "u" "E2U+sip:voice:mobile"  " !^.*$!sip:faltstrom@carrier.se

IN NAPTR 100 10 "u" "E2U+mailto"             "!^.*$!mailto:faltstrom@dorame.

IN NAPTR 100 10 "u" "E2U+sip:im"           "!^.*$!sip:patrik@hugesoftwareco.

IN NAPTR 100 10 "u" "E2U+sip:fax"           "!^.*$!sip:patrik@fasolaredo.se!
```

3.4 OBSERVATIONS ON CALLED PARTY VS CALLING PARTY CONTROL

It would be unreasonable and inappropriate to conclude that either view of ENUM enabled communications is right or wrong. There are clearly circumstances where consumers or businesses, for various reasons, might prefer each option.

A variety of businesses and enterprises my wish to expose and individually describe the maximum number of contact points in the global DNS order to facilitate communications by calling parties by the most convenient means available.

Consumers may prefer information about them to be masked or aliases

in the DNS, in order to benefit from advanced IP communications, such as SIP, while preserving personal preferences and privacy.

What is important is ENUM and the global ENUM system is flexible enough to permit either concept. The choice is directly a function of called parties registering their E.164 resources in the global ENUM system and configuring their NAPTR resources appropriately to their wishes.

4) WHAT OTHER INFORMATION IS NECESSARY FOR ENUM REGISTRATION?

Various national ENUM groups have emerged with the task of developing policies and procedures for administrating the ENUM system within their various jurisdictions. Many of these forums have described a multi-tier model for ENUM registration and provisioning that will require some forms of personal data to be collected and stored as well as technical contact data on who is the responsible party for the management of the authoritive name servers that hold and manage ENUM records.

Many concepts and principals have been borrowed from domain name registration where there are three distinct parties to the transaction, Registrant, Registrar and Registry.

Various jurisdictions have different laws and regulations regarding data acquisition and the protection of data acquired from consumers (registrants). (See 5 and 6)

Unlike the ICANN administered domain name industry, the global ENUM system has no requirement for a central WHOIS registry of registrants. Information on whom or what entity is in administrative control of a phone number is widely available as a part of normal telephone service subscription.

What is different about the ENUM system is that it depends on the security and stability of DNS servers to function properly. It is necessary and prudent that this technical contact data for these servers be widely available to network administrators so that they can be contacted in the event there is a technical problem with aspects of the DNS under their management and control. Consequently

it is suggested that national ENUM implementations SHOULD implement a form of WHOIS for the technical contact data appropriate to the registration of a E.164 number.

5) PRIVACY AND DATA PROTECTION CONSIDERATIONS IN THE NORTH AMERICAN CONTEXT

TBD

6) PRIVACY and DATA PROTECTIONS CONSIDERATIONS IN THE EUROPEAN COMMUNITY CONTEXT

TBD

7) SECURITY CONSIDERATIONS IN ENUM

7.1 SECURITY OF THE DNS

The security issues surrounding the DNS are well understood. This has enormous implications for emerging national ENUM administrations. In particular a DNS request can be subject to man-in-the-middle attacks where the response from the DNS may be altered in transit. This has serious implications for the accuracy and authentication of responses from the DNS to ENUM formatted queries by applications.

The IETF has developed DNSSEC [ARENDS] to authenticate that the responses from the DNS are indeed from the zone from which they have been requested, however DNSSEC is still in early testing and deployment and has not been deployed in a large scale environment such as generic or country code Top Level Domain.[RFC 3130]

Consequently it is premature for emerging national ENUM administrations to consider mandating DNSSEC for those Country

Code zones and administrative number ranges under their control until such time as there is sufficient operational experience with DNSSEC.

7.2 SECURITY OF ENUM PROVISIONING INFRASTRUCTURE.

TBD

8) References

1. [RFC2916bis] Faltstrom, P.& Mealling,M. ôThe E.164 to URI DDDS Applicationsö,draft-ietf-enum-rfc2916bis-01.txt, (work in progress), May 2002

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

3. [ITU-T], "The International Public Telecommunication Number Plan", Recommendation E.164, May 1997.

4. [RFC3026] Blaine, R. öLiaison to IETF/ISOC on ENUMö RFC 3026,January 2001

5. [RFC 3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The URI Resolution Application", RFC 3403 October 2002.

6. [PETERSON] Peterson, J. etal, ôUsing ENUM for SIP Applicationsö, draft-ietf-sipping-e164.02.txt, (work in progress), October 2002

7. [BRANDER] Brandner, R. et.al."Categorical enumservices", draft-brandner-enum-categorical-enumservices-00.txt, (work in progress, June 2002

8. [DNSEXT] Arends, R.,ôDNS Security Introduction and Requirementsö, draft-ietf-dnsext-dnssec-intro-03.txt, (work in progress) October 2002

9. [RFC 3130] Lewis, E. ôNotes from the State-Of-The-Technology: DNSSECö RFC 3130, June 2001

9) Acknowledgments

The original suggestion for this document came from Allison Mankin and Scott Bradner.

10) Author's Addresses

Richard Shockey
NeuStar, Inc
46000 Center Oak Plaza
Sterling, VA 20166
Phone: +1 571 434 5651
Email: richard.shockey@neustar.biz

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.