Security and Privacy issues towards ENUM protocol[1]

G. Kambourakis, D. Geneiatakis, S. Gritzalis, T. Dagiuklas, C. Lambrinoudakis
Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean, GR-83200 Samos, Greece
Tel: +30-22730-82247, Fax: +30-22730-82009, Email:{gkamb, dgen, sgritz, ntan, clam}@aegean.gr

Abstract – Public ENUM is used until now in trials and some "test-bed" or "production" VoIP environments with small volume. Very lately, another application of the ENUM protocol has emerged namely the "Carrier ENUM", becoming popular among VoIP and mobile providers. In this context, a new competitive to public and carrier ENUM, peer-to-peer approach promotes itself, stating to be more reliable and secure, called DUNDi. Although considerable arguing has been generated among various ENUM forums and standardization fora on ENUM implementations, until now, several issues remain obscured and unresolved. In this paper we address security and privacy issues raised by all the aforementioned solutions, presenting implementation details, general concerns, future trends, and possible solutions.

Keywords – ENUM; VoIP; DNS; Security; Privacy

I. INTRODUCTION

ENUM is a protocol developed within the Internet Engineering Task Force (IETF) [1], whereby the Domain Name System (DNS) can be used for identifying available services connected to one's E.164 ordinary number (the number that are currently used by PSTN operators). Through ENUM based transformation process of E.164 numbers into DNS names and the use of existing DNS infrastructure and services like delegation through Nameserver (NS) records, and using Naming Authority Pointer (NAPTR) records [2], one can seek what services are available for a specific E.164 number (domain name) in a decentralized fashion.

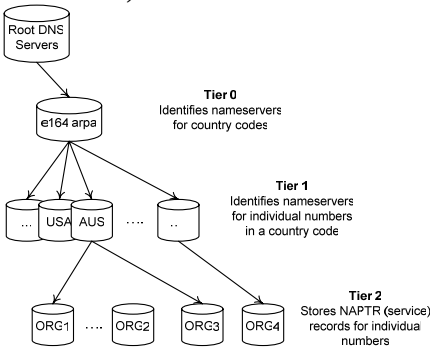

Fig. 1. The ENUM Golden Tree approach

Work on the ENUM implementation to date has been based on a strictly tiered architecture depicted in figure 1. The proposed architecture namely "The Golden Tree" favored by traditional telcos, Internet Service Providers (ISPs) and the IETF seems to finally overwhelm the so called multi-root approach, which is based on multiple DNS trees, favored by the emerging IP telephony operators. The Tier 0 registry is authoritative for the domain e.164.arpa that contains NS records delegating domains corresponding to country codes (e.g. 1.e164.arpa). The Tier 1 registry maintains NS records that in turn delegate domains associated with individual e.164 numbers in a given country code (e.g. Austria). A Tier 1 registry in these instances holds NS records that point to the Tier 2 that contains the actual NAPTR records for a given e.164 number. The NAPTR records contain information for specific communication services associated with any registered number.

ENUM is already supported by many VoIP subsystems (e.g. SIP Proxies such as SER and SNOM 4S, VoIP gateways such as Asterisk and Cisco, and SIP phones). The main focus of attention on ENUM application has been concentrated on voice communications based on Session Initiation Protocol (SIP) [3], H.323 and the general issue of convergence of the IP-based and PSTN networks. Though public ENUM was long expected to be controlled by the end-users, latest IETF and industry activity promotes carrier ENUM or infrastructure ENUM, which means that VoIP service providers will exchange information among themselves about ENUM registered numbers, avoiding fees collected by Public Switched Telephone Network (PSTN) providers for bridging calls among VoIP companies. It will be important to implement ENUM so that the level of security and privacy available in the regular phone system is not compromised. It must be also recognized that the potential use of ENUM as a key enabler in the convergence between IP-based networks and traditional PSTN, might result in additional complexity in commercial relationships and in regulation of the telecommunications sector. Under these circumstances, ENUM introduces several implementation issues that have to be confronted. Among them there are quite a few security and privacy concerns that have to go a long way before they are completely solved. This paper tries to analyze current trends in ENUM trial implementations worldwide, from a security point of view, identifying potential threats for the end-users and the system itself. Moreover, we address how the overall ENUM system's security is influenced by DNS security examining possible solutions. As a final point, we also discuss carrier ENUM issues against public ENUM and briefly compare ENUM system security with the very lately emerged Peer-to-Peer (P2P) based analogous system namely Distributed Universal Number Discovery (DUNDi) protocol [4].

The rest of this paper is structured as follows: Next Section provides an introductory to ENUM technology discussing protocol's details. Section III analyses ENUM implementation

[1] *This work was conducted with the support of the EC under the 2005 project COOP-005892 - SNOCER*

issues focusing on security and privacy concerns with possible solutions, while Section IV sets up the scene for carrier ENUM comparing it with its public version. Section V discusses the alternative to ENUM, P2P driven, DUNDi system comparing them from a security point of view. Last Section concludes the paper and gives pointers to future work.

II. BACKGROUND

A. The ENUM protocol

ENUM defines a method to convert an ordinary telephone number, such as +61-0-12345678, into a format that can be used on the Internet alias addressing information (such as, for example, VoIP or e-mail addresses). To accommodate a different convention used in the Internet domain names, the ENUM protocol takes a complete E.164 address (including the country code), and then removes all non-digit symbols from the address. Next, the digit string is reversed and a "." (dot) is placed between each pair of digits. The (domain) string .e164.arpa is then appended to make a complete DNS query string. Using this process, the above ordinary telephone number is transformed into the DNS query: 8.7.6.5.4.3.2.1.0.1.6.e164.arpa. The Internet addressing information of an ENUM number is stored within the DNS, providing instructions on how to reach a device associated with a particular ENUM number. More than one piece of contact information can be stored in the DNS record that is associated with a particular ENUM number.

The Uniform Resource Identifier (URI) resource records used by ENUM are Naming Authority Pointers (NAPTR) records [2]. NAPTR records follow the general structure of DNS records and can contain numerous information (Class, Type, Order, Preference, Service, etc). Among them two interchangeably used fields have a special meaning: A regular expression to allow the client to rephrase the original request into a DNS format; A Replacement field, if employed, contains the domain name to be used in the next DNS query.

Summarizing, the intended operation of ENUM is to first take the E.164 number and convert it to a query in the e164.arpa domain. The resulting set of services is specified by the returned collection of NAPTR records. The user agent selects a service that matches the service characteristics of the original request and takes the corresponding URI for further resolution by the DNS. The elements of this URI are further decomposed (as per any rewrite rules) in the NAPTR record. DNS queries are generated depending on the sequence of preferred NAPTR rewrite operations. The ultimate result of this sequence of DNS queries is the specification of a protocol, an associated port address, and the IP address for a preferred server to provide the service.

B. An example of ENUM usage in SIP

Let's say Bob's Internet telephone services are mapped to the E.164 address +61-0-12345678. When Alice tries to call Bob, the telephone network routes the call request towards the Internet gateway that is the nominated service agent for this E.164 number. The Internet gateway setups the call with Bob's number and the resultant DNS string FQDN 8.7.6.5.4.3.2.1.0.1.6.e164.arpa. This name is then passed as a query to the DNS, to retrieve all associated NAPTR DNS resource records. Bob has specified that he prefers to receive calls using SIP addressed at the server sip.servbob.gr by placing the following in the DNS:

$ORIGIN 8.7.6.5.4.3.2.1.0.1.6.e164.arpa.
IN NAPTR 100 10 “u” “sip+E2U” “!^.*$!sip:bob@sip.servbob.gr!”
IN NAPTR 101 10 “u” “mailto+E2U” “!^.*$!mailto:bob@mail.servbob.gr!”
IN NAPTR 102 10 “u” “http+E2U” “!^.*$!http://www.webhostbob.gr!”
IN NAPTR 103 10 “u” “tel+E2U” “!^.*$!tel:+61-4 12341234!”

In this case, the first line of the DNS entry uses an order value of 100 (lower preference so it is picked first) and a weight of 10. The "u" flag indicates that the rule is terminal and that the specified URI is to be used. The service field specifies that the SIP protocol is to be used, in conjunction with the E.164 to URI (E2U) resolution service [3]. The operation of the regular expression produces the URI of the form sip:bob@sip.servbob.gr. For this call request, the gateway picks the sip+E2U service and performs the associated regular expression transformation using the original E.164 number and the regular expression. This produces a SIP URI. The gateway then reuses DNS to resolve the domain part of the URI, servbob.gr, into an IP address using a DNS “A” record. The gateway then opens up a session using UDP/TCP port 5060 on the SIP server to complete the call setup, requesting a voice session with the user Bob on this server. The whole procedure is depicted in Figure 2.

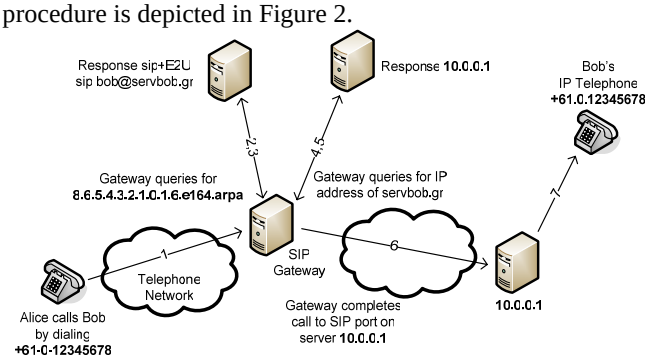

Fig. 2. ENUM and SIP call

If, on the other hand, Bob is not answering, Alice can choose to send him a short message delivered to Bob as an email. In this case the gateway would utilize this mailto: URI and use the domain part of the URI as a MX (Mail Exchanger) DNS query. The DNS responses are a list of mail server names and the associated preferences. Subsequently, the gateway selects the most preferred server and resolves this name to an IP address by a further query to the DNS for an “A” address record. The gateway can complete the original text message delivery request by opening a TCP session on port 25 of the mail server and sending the message as mail addressed to user bob@mail.servbob.gr.

III. ENUM IMPLEMENTATION APPROACHES AND SECURITY

A. General Security Architecture in ENUM

Figure 3 gives an overview of the general ENUM security architecture, its components and interactions, as advocated throughout the most trial implementations until now. More specifically, the ENUM registrant, that is, the assignee of an

E.164 number who has chosen to subscribe to ENUM, interacts with various entities to provide ENUM records corresponding to his telephone number. The registrant must request registration through an accredited registrar, who authenticate the registrant and validates his number assignment. The registrar provisions NS records into Tier 1 registry pointing to the registrant's designated Tier 2 provider. Depending on the registrant's selection, the registrant, the registrar or even the Application Service Provider (ASP) can populate Tier 2 registry with new NAPTR records.

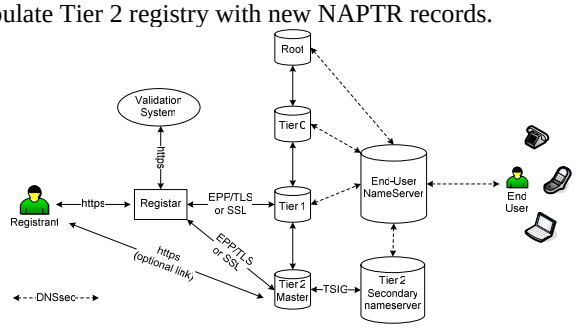

Fig. 3. ENUM general security architecture

The security mechanisms include secure http (https) for registrant's provision to the registrar and for registrar communication with the validation system in place. Moreover, Extensible Provisioning Protocol (EPP) in conjunction with Transport Layer Security (TLS) protocol can be used for securing registrar's communications with Tiers 1 and 2. The registrant may also interact via https directly with his Tier 2 provider e.g. to modify the corresponding ENUM account. Viewing the figure from right to left, end users' DNS queries and the associated responses are secured by the DNSsec protocol, while the Transaction Signatures (TSIG) mechanism [12] is employed to secure communications between Tier 1 and between Tier 2 nameservers.

B. New Privacy and Security considerations arising out of ENUM

There are two different conceptions of how ENUM might be implemented: the first approach allows the calling party to control how the call will be connected, while the second approach places the control with the called party. These two models are depicted in figures 4 and 5 respectively. Both approaches are not mutually exclusive but they do have important differences from the perspective of privacy (see, [8]). In the "calling party control" approach, the person initiating the call always receives all possible contact methods assigned to the corresponding called party and can choose which to use. Consequently, as further discussed, the calling party may retain all of the information and use it for other purposes. On the contrary, using the "called party control" approach only a single method of contact is placed in the DNS record. That contact method points out to a SIP proxy server. That server – based on predefined rules set by the called party – would decide what contact method(s) should be returned to the callee. In the context of a SIP proxy server that rules can be implemented using scripts that determine how a call has to be processed and the contact methods that will be returned to the calling party. For example, a rule can define that: "My colleagues and my family can receive my office VoIP and email addresses at any time". Rules can be defined, amended, maintained or even deleted by the corresponding users through an appropriate (e.g. https) Web based interface.

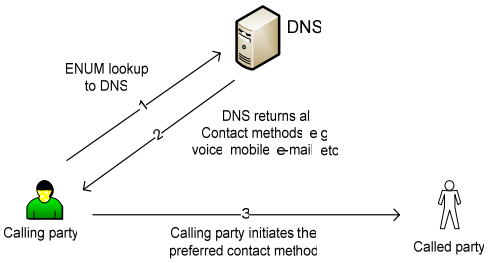

Fig. 4. The" calling party control" approach

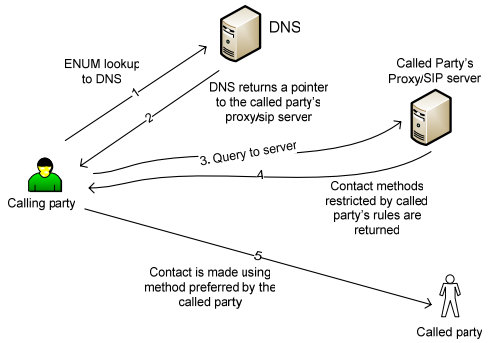

Fig 5. The" called party control" approach

Further threats may arise from particular implementations of ENUM that suffer from poor supervision of controls. This includes new opportunities for "passing off" or "identity theft", where an entity represents itself as someone or something that it is not. This gives the opportunity to malevolent users to achieve a commercial advantage, to disclose sensitive personal information or to use it for various illegal purposes. For instance, one's phone calls and e-mails can get routed to the attacker, analyzed and finally forwarded back to him/her. In the context of ENUM, passing off could occur when an entity provisions another user's E.164 numbers in the DNS by having their own details inserted in the NAPTR records corresponding to another person's or company's number. Passing off weakens the trust that individuals and organizations should have in transactions that rely on ENUM services.

Furthermore, in a particular connection attempt, the callee should be asked to confirm opening a Web page (e.g. http+EU2, see Section II.B) or starting an anonymous ftp session. Using either a Web or Ftp service, defined in [9], is not so secure, so the calling party must apply the same caution when entering personal data as he would do if using a client application started with any other method. For example, the application using ENUM services can alarm the user by displaying a prompt on whether the communication is secured. The same applies for downloading or evaluating web content as this can involve execution of embedded or linked malicious content. Consequently, the automatically "download or evaluate feature" on the client application must be disabled. It is also possible that some ENUM services can be addressed

for applications that require some sort of security protection, but do not provide the necessary mechanisms themselves. For instance, storage of confidential information for supporting e.g. alarm systems or service passcodes can be implemented by defining an appropriate underpinning ENUM system. In this case, an external confidentiality service is required. Another issue rises from the new opportunities that deceitful service providers have, to insert themselves in the path for calls to a given E.164 number, without the actual permission of the called party. This hijacking of incoming calls situation may occur when an Internet Telephony Service Provider (ITSP) arranges for end user's E.164 numbers to be serviced in the DNS/ENUM system in such a way that calls to those numbers are redirected via its network. Consequently, the service provider unlawfully collects transit profits contradicting end user's decision regarding the ITSP to service its incoming calls.

Both of the aforementioned risks designate the need for urgent and adequate mechanisms to guarantee that the request to provision a number in the DNS is authentic and is originated from the rightful assignee of the E.164 number. Similar problems may arise in cases of amendment or withdrawal of a number. In this case, the involved parties are confronted with the challenge to ensure that the procedure meet the requirements that ensure the consistency between ENUM domain names and E.164 numbers and on the other hand not imposing a heavy administrative task to perform. The regulated monopoly of the golden tree approach could sometime in the future lead to the creation of multiple competitive ENUM DNS zones, deployed in different Top Level Domains (TLDs). However, this fact can originate some additional problems as well as opportunities (e.g. additional level of competition that could be assisted). This means that we need to establish flexible mechanisms and controls that can ensure the consistency and adequate protection of data. On the contrary, multiple databases make it more difficult to crash the entire system (see also Section V).

Associated with the previous scenario is the potential creation of ENUM type services within what is known as "alternative roots". Alternative roots are domain trees, which are not under the jurisdiction of Internet Corporation for Assigned Names and Numbers/Internet Assigned Numbers Authority (ICANN/IANA). Such implementations are considered a serious threat to the universal resolvability of the DNS, because a given name has to be resolvable only in a particular root. It is also possible that control of the domain that hosts ENUM or the location of DNS servers upon which the ENUM service depends, by authorities in a single country or region could provide that country or region with excess influence over the operations of converged Internet telephony networks.

Aside from the discussed ENUM model (registrant – registrar, etc), the issue of who is getting to populate and administer the e164.arpa domain with all these URIs, continues to give arguing and is directly related with the actual ownership of these ENUM DNS zones. Someone could say that this task is a primary responsibility of the existing telephone service providers, because after all, these entities operate the E.164 address space in each country. It could also be said that this is a responsibility of ITSPs, or maybe the end subscribers can populate the DNS with their own entries, based on a collection of services that may be sourced from a set of providers. Though, we could see ITSPs claiming access to a country's E.164 number plant, in order to provide various forms of ENUM services. Given that each element of an ENUM service collection can use URIs that refer to different ISP services, it is possible that one ENUM record can be updated by URIs referring to numerous different service providers. However, this multi-agent or synergetic access model to such infrastructure resource records can be shown as a totally novel concept to many regulatory and operating realms, where a single operator manages the entire associated infrastructure elements that are needed to deliver a service.

ENUM promotes a single telephone number as being a reference not only for a person's Internet phone service, but also for the provisioning of value-added services such as instant messaging, e-mail, Web page, Ftp, and any other service that is associated with him. One identifier is all that would be required to reach an individual, using a service protocol and the preferable service provider. On a personal level, the direct implication of such a use is that no more personal cards filled with phone numbers, fax numbers, mobile numbers, e-mail addresses, Web addresses, etc are needed. But one person's ease of use is often another's opportunity to exploit. In addition to the commercial opportunity in operating ENUM registries, ENUM can be seen as jeopardy of personal privacy on the Internet. As used by ENUM, DNS is a global, distributed database. Thus, any information stored there is visible to anyone anonymously. For instance, it could be used to track individuals within the Internet. So, it is considerably questionable what information will be available via the WHOIS-database (e.g. see the debate in the Australian ENUM forum – www.acma.gov.au).

On a more immediate level of concern, it opens up the opportunity for spammers to use a variety of new ways to drive you to complete despair e.g. by sending you junk faxes, emails, SMS or the chance to DoS/DDoS attackers to completely isolate you from the rest of the world. Many users try to counter fight spamming by having one "master" email address and use other supplementary email accounts when e.g. they post to an email-list. Of course, this is not so easy with E.164 numbers to arrange. Moreover, due to the globally accessible published data, each subscriber must be explicitly informed when his/her data are published in ENUM. Other regional regulations may require that the subscriber can at any time request his/her data to be removed and that consent for its publication is confirmed at regular intervals. Note, that spam calls are expected to be a major issue in VoIP in the years to come [10]. Moreover, this information could be used to determine the identity of the person associated with a randomly entered E.164 number, for example, by looking at the name in their email address, or at any other entry in their NAPTR record that gives a clue to their name. This possible misuse of ENUM service may by used to promote identity theft or to give the opportunity to various organizations to build lists of identities to use for the propagation of spam communications across a wide range of different communication services and all this without any indication that this has been done and by whom. As already mentioned

earlier, ENUM can be vulnerable to multi-service DoS attacks. For instance, anyone mounting a flood attack on the DNS NAPTR records can prevent the legitimate users to retrieve any communication addresses from the corresponding NAPTR records. This happens as it is impossible for anyone querying the NAPTR record to get any response to his query, thus completely disabling the subscriber's incoming communications. However, where the E.164 number associated with the NAPTR record is also provisioned in a PSTN network, it may still be possible to reach the victim of such a DoS attack using the E.164 number in the PSTN network. As a result, the regulatory and social implications of ENUM are expected to be more difficult to solve than those of technical issues. Deploying ENUM on an opt-in basis seems to be the most popular and "safe" solution. But, yet, this cannot be considered as a foolproof tactic. The telephone has also launched on an opt-in basis, but gradually has become indispensable.

C. Common security threats and requirements in DNS

Tier 1 registries, Shared Registration System (SRS) and NS data are susceptible to a wide range of security threats and attacks including data tampering, cache poisoning, Denial of Service (DoS) and Distributed Denial of Service (DDoS), etc. In addition, because Tier 1 registries will store proprietary data records from various competing registrars, security mechanisms must include robust user authentication procedures. Consequently, each EPP session has to be authenticated and encrypted using TLS. This can be accomplished using an X.509 server certificate, issued by a trusted authority, to authenticate the network, and an ENUM registrar password in conjunction with IP range checking (subnet filtering) to authenticate the registrar. However, apart from EPP inbred vulnerabilities when used over TCP [5], this is not enough to prevent e.g. password guessing, brute force or man-in-the-middle attacks. Mutual registrar – Tier 1 authentication using public certificates would be a great solution, but this requires an accredited Public Key Infrastructure (PKI) (VeriSign?) to generate and distribute public key certificates to accredited registrars beforehand. Systems must also be firewall protected in hardware, and apply IP filtering rule sets to reject incoming packets from unknown sources.

DNS security mechanisms directly affect ENUM, so attacking the underlying DNS infrastructure is one way of attacking the ENUM service itself. The most important DNS threats that undermine smooth ENUM operation can be categorized as following: Packet interception, ID Guessing and Query Prediction, cache poisoning and Name Chaining attacks, IP Address Spoofing, betrayal by Trusted Servers, using DNS Servers for Bandwidth Consumption DoS Attacks, etc. Some other sort of DNS threats like Authenticated Denial of Domain Names and Wildcards are reported in [6]. While it certainly would be possible to sign DNS/ENUM messages using a channel security mechanism such as TSIG (based on the symmetric model that does not scale very well) or IPsec, or even encrypt them using IPsec, this would not be a very good solution for interception attacks. This approach would impose a fairly high processing cost per DNS message, as well as a very high cost associated with establishing and maintaining bilateral trust relationships between all the parties that might be involved in resolving any particular query. E.g., for heavily used names servers (root zone), this cost would almost certainly be prohibitively high. Moreover, the underlying trust model would only provide a hop-by-hop fashioned integrity check on DNS/ENUM messages.

On the contrary, DNSsec (based on the asymmetric model), when used properly (and become mature), does provide end-to-end data integrity check but on the other hand does not provide any protection against modification of the DNS message header. Moreover, it significantly increases the size of DNS response packets making, among others, the servers that implement DNSsec more efficient as DoS amplifiers [7]. Besides that, DNSsec answer validation, loads the resolver with extra overhead (signature validation, issue further queries, etc), increasing the overall time to get an answer back to the DNS/ENUM client. For instance, this situation directly affects SIP signalling performance as it is very likely to cause both DNS timeouts and re-queries, serving as well as a valuable tool for DoS and DDoS attackers [7]. Furthermore, in case of root public key leakage, key rollover is really a hard problem to deal with. To the best of our knowledge, there is still a long way to go until adequately specifying how the root keys are replaced or they are configured from the first place. A final point to consider is that even with DNSsec some classes of attacks e.g. betrayal by trusted servers are not easy to overcome.

IV. CARRIER OR PRIVATE ENUM

In parallel with public ENUM advent, carriers found that the same protocol can be useful for interconnecting their VoIP islands. That is because ENUM lets carriers interconnect VoIP networks directly and avoid access fees for transmitting calls over PSTN. Some carriers, like VeriSign (MSO-IP connect) and Stealth Communications, are already run their own ENUM registries. Carrier ENUM has been also embraced in the United States by mobile operators that use it to look up Local Number Portability (LNP) information in other carriers' databases. The protocol has been proved also useful for transmitting Multimedia Messaging Service (MMS) messages from one mobile network to another. For example, when a user downloads a ringtone, it is sent to the destination Multimedia Messaging Service Center (MMSC), which in turn requires a mailto: destination address ultimately discovered by ENUM. However, such uses of ENUM far evade from the original purpose of the protocol. It is also true, that the confusion over the development of carrier ENUM might proved a significant delaying factor for the development of the Golden Tree. Moreover, very recently, an IETF draft proposal [11] has been posted putting both public ENUM and carrier ENUM within the same DNS tree. The authors argue that Tier 1 should include two NAPTR records containing separate service parameters for each number in place. The first would point to the end-user's Tier 2 records and the other to carrier's Tier 2. Of course, this approach contradicts the original ENUM architecture. Moreover, from a security point of view, existing considerations as stated above still apply. In

addition, a carrier ENUM could undermine end-users privacy as it can be possible for others to identify "ex-directory" or unpublished numbers based on their ENUM registration.

From the providers point of view there are some additional security issues. Although may be desirable for any provider to peer with others, to do so he has to (somehow) publish his E.164 numbers (e.g. SIP Address of Records or IP addresses) and probably also publish information on how his SIP servers, ingress gateways, session borders controllers and other sensitive network entities can be contacted. But, can one trust all the other providers/contenders? In ENUM/DNS settings the data are hosted within each provider's Tier 2 or can be uploaded to a Tier 1 hosting the NAPTRs disclosing the SIP URIs. However, SIP URIs will reveal which numbers the provider hosts and this can be potentially harmful. Therefore it would be great if the data can be somehow anonymized. Towards this direction there is already a commercial solution connecting VoIP islands namely XConnect network (xconnect.com). XConnect secure network does not return the URI, only the IP address.

V. ALTERNATIVES TO ENUM

As we already showed ENUM provides a strictly hierarchical method for locating services associated with a given E.164 number. Generally, ENUM presents several implementation deficiencies, including: Lack of built-in access for separate services (e.g. SIP security services); Requires one entity in charge of the root ENUM domain and separate authorities for each delegation (imposing charges, taxes, etc); A complete list of all numbers that a provider terminates must be available to the entity managing the ENUM database; Security and privacy are not adequately protected, within an enterprise; ENUM requires effort to provide a foolproof solution against server (e.g. Tier 2) failures; Does not provide information regarding the preferences of a subscriber with respect to unsolicited calling (this can be however avoided in the called party control" approach). A new, alternative to ENUM approach, namely Distributed Universal Number Discovery (DUNDi) [4], has very lately emerged based on P2P philosophy. In the DUNDi model, there is no central repository. On the contrary, nodes e.g. enterprise communication servers, participate in a system of trust, in which each node must has a trust relationship with at least one other or more nodes. When a client wants to resolve a number or extension, it queries its neighbors. Those nodes in turn will query the directly to them connected nodes and so on. The responses, if any, are collated, cached at each intermediate node, and forwarded back to the requesting client. Exchanged messages are binary encoded and authenticated using the AES and RSA algorithms correspondingly. When implemented to large scale DUNDi is supposed to offer a common E.164 web of trust. Moreover, an acceptable use policy called General Peering Agreement (GPA) signed by all participants prevents VoIP spam calls.

However, until now, DUNDi is supported only by Asterisk boxes (www.asterisk.org). For this reason it has to be considered vendor limited in contrast to ENUM, which is already widely supported. Further, DUNDi could have potential issues with scaling, as adding more and more nodes to the network, can cause increasingly long wait times to discover routes. On the other hand, as ENUM is DNS based, it will not suffer from scalability issues. For a security point of view, DUNDi is an explicit trust system. Consequently, any trusted box has the ability to inject bogus routes. For these reasons, DUNDi must be considered, in terms of efficiency, as yet unproven in the large scale, useful for VoIP providers and enterprises wanting to facilitate a way to distribute their dialing plan. To put it another way, it can considered as a replacement or orthogonal to carrier ENUM.

VI. CONCLUSIONS AND FUTURE WORK

ENUM is one of the latest advances in telephony world. However, despite the several trial implementations until now, several issues and potentialities e.g. ENUM-enabled number ranges for nomadic users, remain unclarified and cloudy. Among them, security and privacy concerns continue to bear arguing. Meanwhile, VoIP providers discovered a new application for the ENUM protocol, namely carrier ENUM, which creates new opportunities, but also brings out new undiscovered areas and challenges. In this context, opposing to the Golden Tree approach another competitive P2P based protocol has emerged to support the identification of available services connected to one's E.164 number. Nevertheless, along with the materialization of the demand for such services (especially for public ENUM), all the above protocol implementations have to be carefully addressed both from performance effectiveness and security robustness and in conjunction with predominant VoIP signaling protocols like SIP and H.323. Currently, we are planning to deploy ENUM and DUNDi protocols in a properly designed test-bed environment using the SIP protocol in order to extensively evaluate some of these issues, particularly focusing on security.

REFERENCES

[1] Faltstrom, P., Mealling, M., The E.164 to Uniform Resource Identifiers Dynamic Delegation Discovery System Application, RFC 3761, 2004

[2] Mealling, M. & Daniel, R., The Naming Authority Pointer (NAPTR) DNS Resource Record, IETF RFC 2915, 2000

[3] Rosenberg J., et al. "Session Initiation Protocol", IETF RFC 3261, 2002

[4] Spencer, M., "Distributed Universal Number Discovery (DUNDi)", Internet-Draft, 2004

[5] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport Over TCP, IETF RFC 3734, 2004

[6] Atkins, D. & Austein, R., "Threat Analysis of the Domain Name System (DNS)", IETF RFC 3833, 2004

[7] Geneiatakis D., Kambourakis G., Dagiuklas T., Lambrinoudakis C. and Gritzalis S., "SIP Security Mechanisms: A state-of-the-art review", in the proc. of the 5th Int. Network Conference, pp. 147-155, Greece, 2005

[8] Shockey, R. & Morris, J., "Privacy and Security Considerations in ENUM", IETF Internet Draft, 2003, <draft-shockey-enum-privacy-security-00.txt>, http://www.cdt.org/standards/draft-ietf-enum-privacy-security-01.txt.

[9] Brandner, R., Conroy, L. & Stastny, R., IANA Registration fro Enumservice 'web' and 'ft', IETF RFC 4002, 2005

[10] Rebahi, Y. & Sisalem, D., SIP service providers and the Spam problem, Proc. of the 2nd Workshop on Securing VoIP, Washington, 2005

[11] Pfautz, P., Lind, S. & Creighton, T., "IANA Carrier/User enumservice Registration", Internet-Draft, 2005

[12] Vixie, P. et al., Secret Key Transaction Authentication for DNS (TSIG), IETF RFC 2845, May 2000