WHITE PAPER

Regulatory Challenges for the Transition of Public Telephony to the Internet

Wilhelm Wimmreuter, InCharge Systems, Inc. (US owned)

March 8, 2012

Telephony and other services are moving to a fundamentally different infrastructure as the transition proceeds from the public switched telephone network (PSTN) to the Internet. There are many opportunities to make significant progress on major developments such as separation of functions, modular design, and other desirable features of sustainable solutions. This progress also means that the impacts of some shortcomings of current competitive PSTN services will decline – another benefit of the transition.

However, because PSTN services are essentially being "emulated" over the Internet infrastructure, other aspects of these services will be changed in ways that could affect the public good. In particular, trust-related issues such as authentication and validation, along with their business implications, present significant challenges. This paper explores these issues, including the opportunity that industry and the FCC now have to address them, and suggests approaches to sustainable solutions that can benefit all the stakeholders in this transition.

Introduction

Current FCC activities on the transition of telephony services to the Internet discuss challenges like service functions, trust, identities, new ways to interwork and changes in responsibilities. Important statements have been made with the Truth in Caller ID Act of 2009[1], the FCC report pursuant to the Caller ID Act of 2009[2], and other proceedings such as the recent FCC workshop "The Public Switched Telephone Network in Transition."[3]

These activities include regulations for the public good that remain technology neutral while trying to provide for a smooth migration of public telephony to the Internet. However, there are also some problematic situations that might best be resolvable if we consider them in the context of the evolution of both networks.

At the same time that attention is being paid to PSTN-related issues like Phantom Traffic or Intercarrier Compensation, there is momentum to incorporate the open architecture of the Internet. However, progress in both areas is affected in a variety of ways because of the two

[1] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e). [3]

[2] Caller Identification Information in Successor or Replacement Technologies, Submitted Pursuant to Public Law No. 111-331, with comments on the transition. [4]

[3] "The Public Switched Telephone Network in Transition," FCC workshop, December 14, 2011. [5]

following areas: (1) separation and network-independent use of functions, entities, and identities, e.g. transport, quality of service (QoS), services, and phone numbers, and (2) trust relations between users, services, and service providers.

Current regulation and operational practices have mandated the use of standards and delegations based on mutual trust and Service Level Agreements (SLAs). While this was sufficient for many years, challenges like accurate billing/arbitrage, phantom traffic, and maliciously spoofed caller identification are becoming increasingly problematic. In consequence, it has become economically viable to "tweak" things like routing or call origin because doing so could increase revenues or reduce the utilization of one's own resources.

In contrast, Internet services – other than access – cannot rely on closed design and operations. The Internet is inherently based on "Trust by Authentication" instead of "Trust by Wire". In consequence, every service provider had to build its own schema for user authentication. This raises issues that are far beyond the scope of this document, but the key point is this: the current practice of IP-telephony is practically a centralized approach that often seeks to emulate PSTN paradigms on the Internet. Such emulation of the PSTN on the net seems to undermine the effectiveness of standards such as: (1) Session Initiation Protocol (SIP)[4], (2) Electronic Number Mapping (ENUM)[5], and (3) Transport Layer Security (TLS)[6], among others. The overall benefit of these standards, in this case to simply operate and interconnect PSTN and IP-based telephony in support of public phone service on the Internet, is greatly diminished

In its current state, this pragmatic approach provides VoIP with full end-to-end control over functions, transport, and entities. However, the design as implemented, (e.g., with SIP Trunks or Proxy Authentication), requires establishing and maintaining mutual trust between operators. There are generally barriers to function and service sharing unless prior arrangements on interworking exist, based, for example, on mutual trust and SLAs.

There have been attempts to deal with these issues, and the FCC workshop "The Public Switched Telephone Network in Transition" noted above helped provide some important insights.

In that workshop, a Session Delivery Network (SDN) was discussed by Acme Packet as a way to solve security and interconnect issues. In an important response to this, Henning Schulzrinne mentioned that SDNs in the proposed sense could only succeed if a proper "separation of functions" takes place. This point credits the more modular approach of the Internet, in which functions like transport, services, QoS, authentication, and authorization security could then be leveraged for the good of future network operations.

While this separation of functions and shared use is state of the art on the Internet, a typical PSTN network has far fewer instances of sharing, such as transport, overflow routing, or shared base stations. This then leads to the introduction of tight coupling of border gateways and transport systems, instead of more modular use and independent control of transport, functions, or services themselves.

[4] IETF RFC 3261, "SIP: Session Initiation Protocol." [8]

[5] IETF RFC 6116, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)." [11]

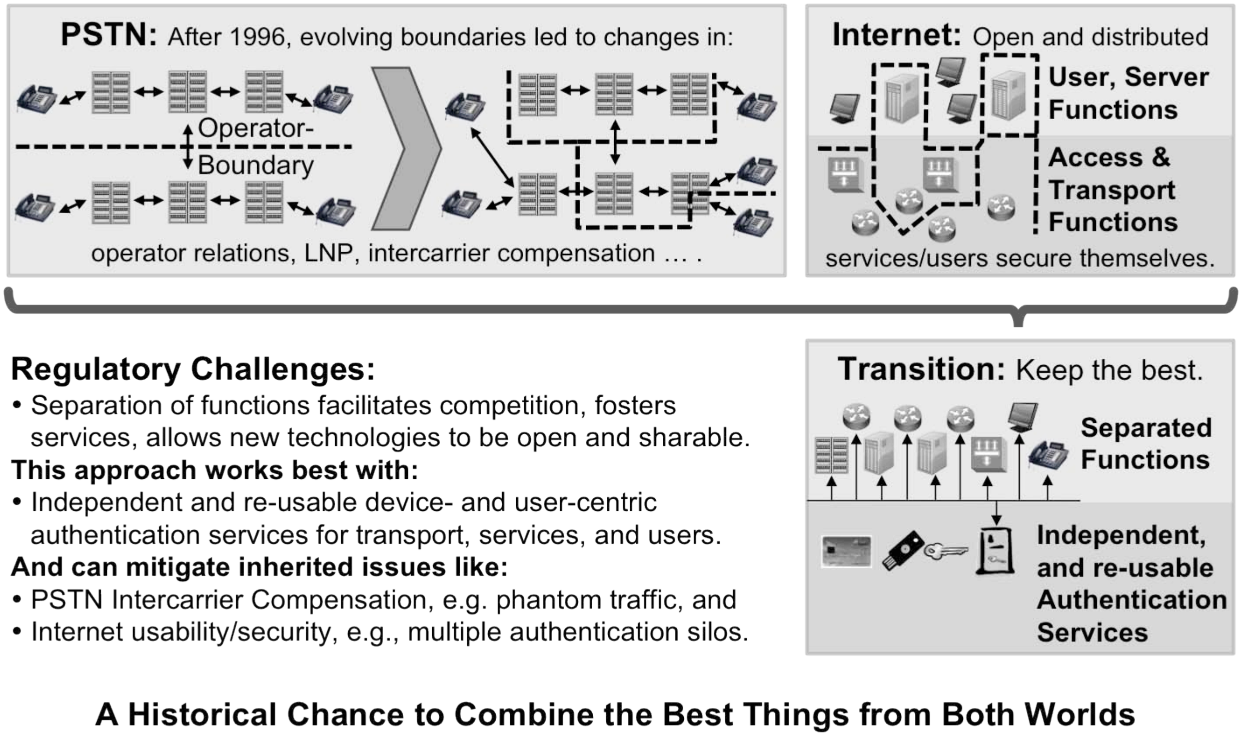
[6] RFC 5246, "The Transport Layer Security (TLS) Protocol." [10]

Therefore, it seems evident that sustainable solutions entail the following:

1. **Separation/decomposition of:**
   - Functions (transport, QoS, services).
   - Identities (phone numbers).
   - Modular design to separate transport and services.
2. **Trust implications caused by separation of functions:**
   - Authentication credentials should be accepted by all entities in real-time.
   - Validation should be possible for all entities participating in a session.
3. **Business implications of separation of functions:**
   - New business cases arise for additional uses of telephone numbers.
   - Intercarrier compensation regime may change, e.g. for phantom traffic detection, etc.

Careful regulation and wise policies for the above items could help with a range of requirements, and could also provide for the re-use of authentication credentials and functions beyond current public telephony services. For example, assume that the use of an acceptable enforceable marker is in place, consisting of a signed request introduced by a principal coupled with the ability of relying parties to perform validations anywhere along the call path. Then, mutual agreements or separate rules such as "do not modify message headers" would not be needed.

The concepts of this view of the PSTN Transition are illustrated in Figure 1 below.


PSTN: After 1996, evolving boundaries led to changes in:
Operator-
Boundary
operator relations, LNP, intercarrier compensation … .
Internet: Open and distributed
User, Server
Functions
Access &
Transport
Functions
services/users secure themselves.
Transition: Keep the best.
Separated
Functions
Independent,
and re-usable
Authentication
Services
A Historical Chance to Combine the Best Things from Both Worlds

Regulatory Challenges:

- Separation of functions facilitates competition, fosters services, allows new technologies to be open and sharable.

This approach works best with:

- Independent and re-usable device- and user-centric authentication services for transport, services, and users.

And can mitigate inherited issues like:

- PSTN Intercarrier Compensation, e.g. phantom traffic, and
- Internet usability/security, e.g., multiple authentication silos.

Figure 1: The Big Move - PSTN in Transition

It is important to note that the concepts shown in Figure 1 shouldn't be seen in isolation. They are highly interdependent, and therefore desired synergies to support public progress towards sustainable and technology neutral regulatory frameworks will need to be considered.

Problem Statement

Broadly speaking, the paradigm of closed, single-purpose telephony networking with well defined and mutually trusted interfaces is the foundation of current PSTN services, technology, and regulation. By contrast, Internet telephony does not, indeed cannot, rely on these centralized considerations because its services run on top of a multi-purpose transport network with modularized services that operate in a network independent fashion.

As a result, there are forces that pull, if not drive, ongoing trends in several different directions. These forces are:

1. **Separation and modularization to utilize the power of the Internet:**

   - Centralized network, transport, and service binding, as in the PSTN, cannot fully utilize the modularized end-to-end approach of the Internet, and
   - Separation of functions is needed in order to utilize this end-to-end approach.

   Requiring a separation of functions seems to be the clear solution of choice, but it changes some fundamental things. In particular, it breaks the assumption of implicit inheritance of trust and authorization that PSTN network operations rely upon. Consequently, the transition to the Internet impacts how trust and authentication capabilities work.

2. **Transition of trust and authentication for the Internet:**

   - The PSTN relies on "Trust by Wire," as it inherits trust from the initial access line assignment, protecting transport rather than services or users.
   - The Internet relies on "Trust by Authentication". It cannot utilize "Trust by Wire" because the architecture of the Internet does not incorporate the PSTN's access line binding or protected transport to service binding.

   In this setting, relying entities – services, transport, or terminating users – cannot rely upon preceding entities for accurate and trustworthy authentication because there is no protected binding between transport and services/functions.

3. **IP telephony issues inherited from the existing PSTN:**

   - As one example, phantom traffic is an issue inherited from the PSTN.
   - As another example, termination fee fraud can be said to be a commercial consequence of deregulation.

4. **Deployment practices used to mitigate PSTN inherited issues:**

   Operators deploy various architectures and employ a number of techniques to deal with these PSTN-related issues.

   - As an example, transport is protected, instead of protecting users and services by using TLS, VPNs or even dedicated wires.
   - As another example, IP-PSTN gateways are authenticated, instead of authenticating IP Users (SIP-Trunking is a sort of PSTN emulation).

Current practice emulates the combination of transport and functions of PSTN networks and therefore inhibits the power of modularization that can be utilized on the Internet.

In addition, some existing PSTN commercial practices, such as examples mentioned above, may appear to be related to the two issues of separation and trust. However, as progress is made on these issues, it is very likely that such practices could be mitigated, if not solved, as a result. The reasoning is clear: positive outcomes from sustainable solutions for separation and trust could enable any relying party to independently validate originating identities. This could have a number of far-reaching benefits.

As mentioned previously, the issues of separation and trust are deeply interwoven, and because they are interdependent, their respective issues cannot be solved in isolation. Sustainable solutions based on this interdependence, solutions that enable any relying party to independently validate originating identities, could have a number of far-reaching benefits.

Technical Approach

There is a broad range of possible implementation scenarios for using Separation of Functions in sustainable solutions. However, a successful technical approach will depend on three critical elements: (a) clear boundaries for splitting functions, so that functions can be used independently; (b) re-usable trust and authentication with enforceable markers, so that any function or relying party can validate its users and authenticate itself; and (c) comprehensive accounting and debugging tools, so that cross-operator session accounting and tracing, in compliance to regulatory requirements, can be practicably supported.

In the transition from the PSTN to the Internet, there are a number of considerations and possible consequences of implementing separated functions.

1. Separate transport and telephony service(s):

The separation of transport and telephony service(s) is well understood for VoIP deployment, although currently there are some issues stemming from the reliance of telephony services on strong bindings to underlying network and transport services.

The advantages of implementing this split include: (1) service independent management and protection of transport networks, and (2) regulatory compliance with respect to competition.

2. Separation of re-usable or sharable functions:

Sharing or reusing functions, as appropriate, is beneficial when implementing value-added or infrastructure services, because these practices can: (1) support re-usability for customers of other operators, (2) save resources by sharing services for any user, and as a result (3) lead to additional revenue and/or savings on resources and costs.

3. Autonomous 3rd party authentication:

This is a key element to implementing a successful and usable separation of functions, because it closes the "authentication gap" between, for example, the requirements of the Truth in Caller ID Act and the deployed authentication silos provided by operators.

Autonomous third party authentication allows the introduction and use of enforceable markers for users, servers, and session owners. These credentials would then be available for use by any of the principal entities involved in a session, e.g., by any party along the "call path." This has the following advantages: (1) re-usable authentication and validation throughout the session, (2) migration of ownership of information to the end user, (3) availability of end-point or user identities (e.g., phone numbers) for other services, (4) simplified session accounting and non-repudiation services, and (5) traceability for regulatory compliance.

It is envisioned that the use of third party authentication would lead to a number of positive uses in a scalable fashion, to include mitigation of current challenges like accurate billing/arbitrage, phantom traffic, and maliciously spoofed Caller ID.

4. Additional uses of phone number identities:

Successfully implementing separation of functions along with trust and authentication could provide new opportunities for services involving the phone number name space. In fact, phone number based identities could be used to facilitate other applications and drive new, innovative services like the Rogers[7] One Number offering. Mobile phone numbers are also being used by some ISPs for their Internet based Unified-Communication (UC) service offerings, and new, accurate, comprehensive E.164 "directories" could provide public service benefits along with commercial potential.

Although further discussion of this topic is beyond the scope of this document, it is useful to note that separation plus trust can lead to workable approaches for implementing and using infrastructures for these applications. Irrespective of how future applications and services may use phone numbers, this technical approach could also help leverage the resource that is the public telephone number space.

Possible side effects could be involved in any of the above considerations. This is very important because dependencies could lead to much more expensive solutions, or might even present significant barrier to interoperability.

As an example, let us consider a successful separation of various telephony functions that, for the purposes of discussion, doesn't include either network and service independent authentication or enforceable markers, e.g., signatures usable for validating identities. But, authentication is still critically necessary. To make authentication work, all of the separated functions relying on authentication would have to implement their own authentication functions at extra cost. In this scenario there would therefore be: (1) additional development effort, (2) increased provisioning and management expenses, (3) broken chains of trust where some or all functions lack the capability to authenticate, and (4) the need of workarounds or network isolation to overcome these deficiencies.

On the other hand, these problems don't exist if the separation of functions is implemented and is based on authentication schemes that allow for: (a) enforceable markers or signatures attached to session requests, and (b) the capability for validating these markers by any of the relying parties involved in the session.

[7] Rogers One Number, "Unleash the true power of your wireless number." [14]

An example of this would be a PKI-based system as described in RFC 4474[8], used for SIP-specific signature implementation. The underlying concept is that authentication credentials can be used to prove the authenticity of the session and the requesting party.

While migrating control and management of information to the end-user, one must consider possible costs and resources, conflicting requirements and dependencies, implementation alternatives and consequences, and then weigh all of these against potential gains. There are non-technical as well as technical aspects that will need to be assessed.

In summary, we believe that a smooth migration, function by function, is possible once the basic functions such as service-independent authentication and the separation of transport and service are in place. We believe it could be of material benefit in the transition from PSTN to Internet.

We also believe that additional uses for phone number identifiers could lead to innovative commercial services and would also provide more opportunities for authorities to enhance public service offerings. See, for example, this look at the future of numbering resources.[9] ([12])

Utility to FCC Regulations

Fraud and misuse in the PSTN and Internet-based telephony networks require the FCC and public service operators to introduce and execute new regulatory mandates. Such requirements apply during the period of transition as well as for the phone systems of the future. This requires a regulatory framework that allows for evolving and new technologies while protecting consumer rights, ensuring competitive service offerings, and promoting fair and reliable network operations.

The additional challenge that faces regulation both during the transition and the future stems from fundamental differences between the PSTN and the Internet, because these systems of networks are based on different paradigms for design, control, security, authentication and identities. Therefore, regulation impacts, and is impacted by these areas. Some issues to be considered are described in Table 1 below.

[8] RFC 4474, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP).” [9]

[9] T. McGarry, “Telephone Numbers Are for People, Not Machines,” NeuStar Blog entry. [12]

Area	PSTN	Internet	Regulatory impact & comments
Design	Centralized	Distributed	**Minimal:** Mostly technical. Interoperability presents some challenges.
Control	Centralized	End-to-End	**High:** Multiple service silos, authentication, customer lock-in, transport and service dependencies – PSTN emulation.
Security	Trust by Wire	Trust by Authentication	**High:** Service- and end- entities must handle their own security on the Internet. Reliability increases since large single points of attack and failure will become highly distributed.
Authentication	Centralized: Phone numbers, Wires and PINS	Multiple methods: Username/Password, PKI, and other tokens	**High:** Look beyond centralization and multiple passwords. Service operators could utilize user centric approaches with user choice to help avoid multiple authentications now seen on the Internet.
Identities / Identifiers	Phone numbers, operator IDs	User names, Domain names and others	**Medium:** The PSTN binds phone numbers to services. Internet services are identity agnostic. Consider how phone numbers could be used for additional services to create new business cases and opportunities for services benefiting the public.
Privacy	Closed, with Unlisted numbers, Traffic profiles, Legal intercept	Fairly open, with VPNs, encryption	**High:** The PSTN is based on trust in operators and legal authorities. The Internet requires trust in multiple service providers and legal authorities. Many Internet operators do profiling and collect data. Privacy needs protections while exceptions for legal needs are supported.

Table 1: Major areas of Regulatory Impact for the Transition

The brief overview above includes areas for progressing regulatory action where we believe it is useful and important to look at issues from the perspective of what is in the public interest. We believe the public good will be served when aspects such as usability and re-use are considered. We would hope to avoid or lessen such things as the need for multiple passwords, the prevalence of customer lock-in, or the lack of competition.

We believe that regulation has a potential role to play to help fulfill requirements and goals like those stated in the Truth in Caller ID Act[10] or the Strategy for Trusted Identities in Cyberspace.[11]

We also believe that additional uses of phone number identities can have both commercial and public service benefits, where this is facilitated by the combination of separation and trust discussed in this paper.

[10] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e). [3]

[11] National Strategy for Trusted Identities in Cyberspace (NSTIC). [7]

Recommendations

The previous sections described how two key areas - (1) separation of functions and (2) trust and authentication - underlie the transition from the PSTN to the Internet. Technical approaches that take these into account could be very important, and active regulation could play a significant role in facilitating a smooth and manageable transition. The following recommendations include further studies and areas for possible regulation that could help with this transition and could serve the public good.

- Further analyze impacts of evolving technology for the transition, e.g., Real-Time-Communications on the web (RTC-Web)[12].
- Further analyze regulatory impacts of the differences between PSTN-based “Trust-by-Wire” systems and the “Trust-by-Authorization” approach used on the Internet.
- Study aspects of potential benefits in leveraging E.164 numbering for future additional uses of phone number identifiers.
- Analyze current regulatory challenges, e.g., phantom traffic, and how they potentially could benefit from this autonomous, modular approach.
- Consider deployment approaches that harmonize the regulatory efforts of both the Internet and the PSTN.

Conclusion

User requirements, experience, and economics are dictating the transition of telephony from the PSTN and dedicated VoIP networks to the Internet. These forces will further drive the migration towards rich Internet applications and network-independent shared use of functions and of authentication. This can be bolstered by careful regulation for the public good that encourages and takes advantage of both the best of the Internet and the best of PSTN.

Acknowledgements

The author gratefully thanks his colleague Andrew Gallant of InCharge Systems Inc. for his support and effort to make this document possible.

Contacts

Administrative Contact

Warren Bent
724 Duane Street
Glen Ellyn, IL. 60137
+1.630.474.9451 (t)

warrenbent@inchargesys.com

Technical Contact

Wilhelm Wimmreuter
Brehmstr. 12
D-81543 Munich
+1.415.639.3754 (t)
+49.151.121.64041 (t)
wilhelm@inchargesys.com

[12] Real-Time Communication in WEB-browsers (Active WG).[15], [16],

References

[1] "Telecommunications Act of 1996," U.S. G.P.O., Public Law No: 104-104, http://transition.fcc.gov/Reports/tcom1996.pdf, and a summary of related documents at http://transition.fcc.gov/telecom.html.

[2] "Telecommunications Act of 1936 (new)," versions updated Communications Act of 1934, as amended by the 1996 Act, http://transition.fcc.gov/Reports/1934new.pdf.

[3] "Truth in Caller ID Act of 2009," Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e), signed by President Obama on Dec. 22, 2010.

[4] FCC, "CALLER IDENTIFICATION INFORMATION IN SUCCESSOR OR REPLACEMENT TECHNOLOGIES," submitted pursuant to Public Law No. 111-331, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.pdf.

[5] FCC, "The Public Switched Telephone Network in Transition," workshop, Dec. 14, 2011, http://www.fcc.gov/events/public-switched-telephone-network-transition-0.

[6] FCC, "Developing an Unified Intercarrier Compensation Regime," Adopted: Feb. 6, 2012, http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0207/DA-12-154A1.pdf.

[7] "National Strategy for Trusted Identities in Cyberspace (NSTIC)," http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[8] IETF, RFC 3261, "SIP: Session Initiation Protocol," http://datatracker.ietf.org/doc/rfc3261.

[9] IETF, RFC 4474, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," http://datatracker.ietf.org/doc/rfc4474.

[10] IETF, RFC 5246, "The Transport Layer Security (TLS) Protocol," http://datatracker.ietf.org/doc/rfc5246.

[11] IETF, RFC 6116, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," http://datatracker.ietf.org/doc/rfc6116.

[12] T. McGarry, "Telephone Numbers Are for People, Not Machines," NeuStar Blog entry at http://www.neustar.biz/blog/author/tmcgarry/, last retrieved on Feb. 7.2012.

[13] David Pogue, New York Times, "One Number to Ring Them All," Mar. 2009 http://www.nytimes.com/2009/03/12/technology/personaltech/12pogue.html.

[14] Rogers One Number, "Unleash the true power of your wireless number," http://www.rogers.com/web/content/wireless_ron.

[15] IETF Working Group, "Real-Time Communication in WEB-browsers (Active WG)," http://tools.ietf.org/wg/rtcweb/.

[16] W3C Work Group, "Real-time Communication Between Browsers," http://dev.w3.org/2011/webrtc/editor/webrtc.html.