Intarea Working Group
Internet-Draft
Intended status: Informational
Expires: April 12, 2015

R. Romansky, Ed.
Tech. Univ. of Sofia.
B. Khasnabish
ZTE (TX) Inc.

October 9, 2014

PSTNization of the Internet
draft-rdsx1-intarea-pstnize-internet-00.txt

Abstract

This draft discusses the features and functions that the Internet must support in order to be as robust and trustworthy as the public switched telephone network (PSTN, http://en.wikipedia.org/wiki/Public_switched_telephone_network). In general the PSTN-like features and functions include verifiable addressing and numbering, higher privacy and security, increased reliability (no more than around five minutes of unplanned outage over one year time period), survivability and resiliency, desirable level of scalability, alarms, correlation, and diagnosis capability, and local/international level of accountability. Incorporation of these (or similar) features are expected to harden the Internet.

The topics related to Internet hardening were discussed during IETF88 technical plenary (http://www.ietf.org/proceedings/88/technical-plenary.html) in Vancouver, BC, Canada in Nov. 2013. A follow-up joint W3C/IAB workshop on strengthening the Internet against pervasive monitoring (STRINT, https://www.w3.org/2014/strint) was held before IETF89 meeting in London, UK. During the IETF90 Technical Plenary Session (http://www.ietf.org/proceedings/90/minutes/minutes-90-iab-techplenary) on Monday, 21 July 2014 in Toronto, Canada the Technical Topic discussion focused on Network topology and geography. The presentations revealed that for business relationship and/or policy reasons, local traffic routinely cross national borders for so called 'efficient' routing, thereby facilitating monitoring, copying, and surveillance of traffic from users' sessions by both authorized and unauthorized entities. All of the technical presentations are available at the website of IETF90 proceedings(http://www.ietf.org/proceedings/90/slides/slides-90-iab-techplenary-9.pdf).

In this draft, we discuss the requirements for PSTNization of Internet interfaces, protocols, services, and management and configuration capabilities.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Internet, as defined in [RFC2026] along with the World Wide Web [W3C, http://www.w3.org/] can provide data, text, voice, video, etc. services seamlessly to almost everywhere in the World. Work groups like RTCWeb (in IETF, http://datatracker.ietf.org/wg/rtcweb/) and WebRTC (in W3C) have been enhancing the protocols and interfaces in order to enrich Web-based audio, video, collaboration, and gaming services. However, a number of Entities have been utilizing privacy-invading Internet innovations (PIIs) in the name of societal and economic advancements. Some of these Entities (e.g., the Internet.org) are partnering with local Communities and Non-Profit organizations in order to improve bandwidth, connectivity, and reachability to all of the inhabitants of the World through wired and wireless (mobile) devices. Consequently, it is becoming increasingly important to consider bringing back PSTN-like features and functions including privacy and security, resiliency, and accountability.

Benefits: The are many benefits of PSTNizing the Internet. The major ones would be bringing back trust, and confidence in the Internet along with improving user experience and satisfaction.

1.1. Scope

The scope of this document is discussion on incorporating PSTN features and functions in the Internet.

Ongoing discussions on supporting high-quality [I-D.khasnabish-dispatch-qoe-management] real-time services over the Internet can be especially found in the following IETF and IRTF Websites: RTCWeb [http://datatracker.ietf.org/wg/rtcweb/] NEA [http://datatracker.ietf.org/wg/nea/], DISPATCH [http://datatracker.ietf.org/wg/dispatch/] OAUTH [http://datatracker.ietf.org/wg/oauth/],and SDN-RG [http://irtf.org/sdnrg].

1.2. Abbreviations

. . . .

7. Privacy and Security Considerations

In order to improve the flexibility and scalability of the Internet, the current trend is to utilize virtualization, as discussed in [I-D.junsheng-opsawg-virtual-resource-management], and separation of control and transport (and forwarding), as discussed in e.g., [RFC3654] and [RFC3746]. It is expected that both capital and operational expenditures will be significantly reduced because of using virtualization of resources like CPU, memory, storage, links,

nodes, and value-added service devices like firewall, deep packet inspector, deep stats inspector, etc.

However, the use of virtualization may also make the network resources more vulnerable to abuse and spoofing. For example, the security considerations for virtualized resources in data-center environment can be found in [I-D.karavettil-vdcs-security-framework].

7.1. Privacy and Personal Data Protection (PDP) in Digital World

The initiatives for improving of the Information Society (IS) define new requirements to the contemporary information technologies (IT) to decide important problems of globalization including field as distributed information servicing, remote access to distributed environments, sharing and using different public and own resources, cloud and mobile cloud computing, social computing, e-learning, etc. All these opportunities of contemporary network world expect creation of personal profiles and uploading personal information that could be accessed by other users, not always in a correct way [Lam]. This requires necessity for modernization of data protection rules and digital privacy for all participants in the digital world.

It is possible to ask the question "What are the components of the digital world built on the base of the network space?" Traditional component of course is the web-environment that proposes large collection of contents, specific and traditional and specialized information resources, tools for virtual reality [Garber], etc. that could help users obtain some knowledge based on interactive communications.

This collection of means and tools could be extended by opportunities of cloud environments and data centres (using remote resources as a services) [Chen], social media and Web 2.0 (tools that permit collaboration and sharing of information and knowledge between large set of users) [Kinast], distributed environments for online/distance learning (using and sharing learning content and organize the collaboration on the base of specific interests) [Yong], Massive Open Online Courses (MOOCs) that many educational institutions apply; the tendency is that MOOCs will change the higher education in the coming years [Meyer].

Creation and supporting users' profiles in the network space permit different personal information to be accessed by other users of the global network. This could be made very undesirable problems for users and to disturb their privacy. In this reason the Personal Data Protection (PDP) should be important obligation of the distributed services providers. Some problems of digital privacy in the network world and challenges of cloud servicing for the personal data

protection are discussed in [Romansky-1] and [Romansky-2]. A brief summary of the challenges of digital world for privacy and PDP is presented below.

7.2. Digital World and Digital Privacy

It is well-known that privacy is an important fundamental human right uniting personal data processing, personal communications via post and Internet, processing personal profiles in social media, forums and other distributed environments. The new situation in the digital world changes the traditional understanding of the privacy as "the right to be alone" and introduces the new vision of "the right to be forgotten." In this reason, giving different information resources and distributed information services by Internet requires creation of knowledge in the society for principles, methods and technological means and tool for adequate data processing.

The digital world permits accessing and using components as web-sites, distributed resources, content, libraries, forums, social media, cloud services, etc. Most people (individuals and employees) use Internet to extend their knowledge, social contacts and relationships. Social network, forums and blogs permits to contact with different users. Fact is that more employers visit social forums to select possible employees for their companies. In this case the users are not only passive participants, but they could realize different forms of direct communications, uploading information and make access to published information of other users.

Identical problems with data protection policy exist in the fields of network communications, distance learning, cloud services and other opportunities of the digital world. This requires a serious risk analysis of activities by using web applications and network environments. For example, the using of cloud services permits to increase the processing and storage power without additional investments for a company. This form of remote data processing uses virtual machines and disks (storage) via Internet. The problem is that the cloud collects more and more personal data of individuals and information about institutions. All these activities in the digital world require developing an adequate information security policy and improving personal data protection legislation.

Extended discussion about main principles and rules for data protection organization, securing privacy in the network world and summarized some important challenges of cloud servicing for the personal data protection are discussed in [Romansky-1] and [Romansky-2].

7.3. Mine Principles of Personal Data Protection

The Data Protection Policy must be regarded in the context of IT Security Policy as a part of Security Policy as shown in Figure-1.

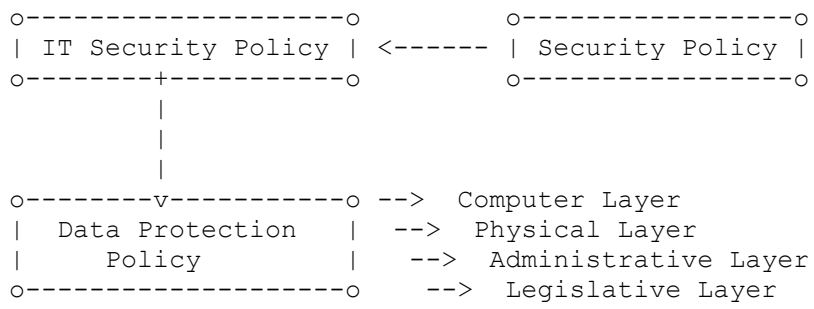

Figure 1: Data Protection Policy in the Frame of Security Policy

Security Policy should be regarded as set of means and methodologies for preventing incidents, detecting attacks and restoring the system after successful attack. It includes rules, procedures and tools used on hierarchical layers (network, software, hardware, physical and administrative). Data Protection Policy should be discussed in the frame of IT Security Policy and harmonization of data protection with information security rules from the security core (computer layer) to the external layers (administrative and legislative) is needed. The computer layer presents embedded instruments for protection of personal data structures (hardware, software, cryptographic, biometric). The physical layer consists of technical instruments, means and tools for unauthorized access blocking, separation of LAN segments, recognition of legitimate users, etc. The next two layers unite organizational rules, instructions and procedures for administrative control and legislative and normative documents.

European understanding for "personal data" is the information that permits to identify a person directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. A popular definition in USA is connected to the rights and obligations of the individuals and institutions about collection, using, keeping and disclosing personal information. In this reason any operation or set of operations with personal data (using automatic or not-automatic means) is called "processing of personal data." The main participants in this process are "data subject" (the owner of personal data), "data controller" (determines

the purpose and the means of processing and it is responsible for all procedures with personal data), "data processor" (real processing of personal data on the base of agreement with the data controller), "receiver of personal data" (the giving of personal data could be on the base of lawful reason only).

Life cycle of personal data processing is proposed in Figure-2 and describes the traditional processing of personal data by a sequence of phases beginning from giving of personal data by individual and finishing with personal data destroying (by the data controller) after the goal realization. The purpose of the phases is listed below.

- The COLLECTION of personal data must be made based on a legitimate reason only and with the consent of the individual;
- The PRESERVATION of collected data should be realized in the registers based on preliminary defined goal and criteria;
- The UTILIZATION must be made by legitimate persons on the base of principles of information security; authentication by using username, password, digital certificate, personal identification number, and biometric means; authorization on the base of developed digital right management system; accountability using personalization of the access to the data structures and registration of user activities;
- ACTUALIZATION, that is the personal data must be correct, full and actual; integrity and content management;
- The TRANSFER to other country and the giving to other person must be realized on the base of strong rules only;
- ARCHIVING could be made if it is required by law but for a limited period of time only;
- DELETION of personal data must be made after realization of the goal.

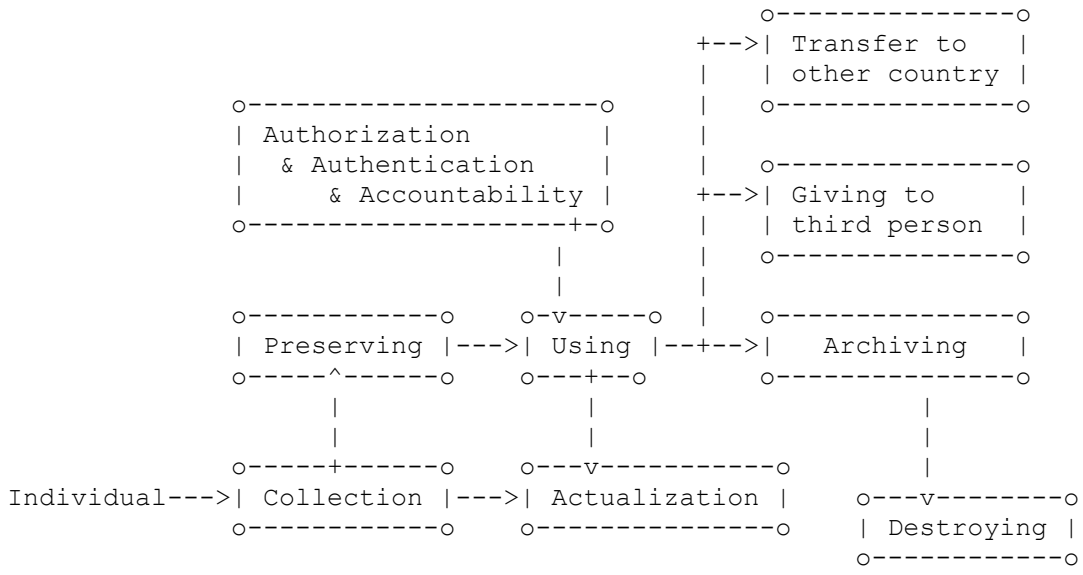

Figure 2: Life Cycle of Personal Data Processing

7.4. Problems of Digital World for Privacy and Personal Data Protection

The contemporary network world causes different problems for digital privacy. For example the privacy in social media concerns with protection of users' information and securing the users' rights. The media must try to prevent different incidents with users' data as unauthorized access, viruses, illegal transfer to third party, etc. Analogous problems could be detected and at cloud services also because the cloud customers need to be assured that providers implement adequate security policy for data protection. Challenges of cloud for PDP discussed in [Romansky-2] are common for all network world. Typical problem for cloud environments is multi-tenancy that could be risk category because it permits possible access to personal data of network user by another unauthorized user. A short summary of common challenges for the privacy in the digital world is presented below.

- Clear IDENTIFICATION of the roles of the participants in PDP processes ("Data Controller," "Data Processor" and "Data Subject")and to determine the responsibility for data protection procedures (rules, measures, data subject rights, etc.). According to the definitions of Directive 95/46/EC the data controller determines purposes and means of the processing of personal data. The problem in network world is that the functions of customer, vendor and provider and the relation between them

could be defined for concrete case only. The service providers have no legal obligation to protect personal data if they are not defined as controllers or processors. This characterization will permit to ignore the data protection obligations at the cases of personal data outsourced or transferred to a third party for processing.

- Data subject's RIGHTS. This is an integrated problem because the individuals have different rights during the personal data processing. One of the main problems during the registration is that there is a risk for user's privacy (more personal data could be required for registration and identification). For example, some social networking sites collect extended personal information in the page known as a "profile"(names, birth date, address, phone number, social life, gender, country, hobbies, relationships, etc.). These pieces of data personalize the users in major level and the individuals must know the purpose of these data and reason for processing. Another problem with the data subject's rights is the impossibility to revise, access, block or delete their personal data. In other hand, the providers have a full access to the customer's data. Data controller must guarantee that each user could define restriction for the own profile accessing. This will prevent unauthorized access and incorrect dissemination of personal information. This action could be realized by making the profile private from the user by selection of these who can visit the page and access to be after authentication.

- International data TRANSFER - according to Directive 95/46/EC personal data could be transferred to third countries if the level of personal data protection is adequate to those in the EU countries. The data transfer between different service providers (social media) or data centers (clouds) located anywhere in the word is typical procedure. Each personal information that is uploaded to cloud, social media, networking site, etc. must be protected according to the Directive 95/46/EC and users (data owners) must be informed for all transfers.

- Data DELETION. If any user wants to delete data in his/her profile he/she must be sure that these data will be really deleted. In some cases, data could be transferred to other service provider and a copy of data could be stored in different place(s). This will be a problem of privacy for the individual. Another case is when the information that was deleted or removed by the user is passed to third party before deletion. Data protection legislation gives strong rules for deletion of personal data in the traditional cases, but for the social media this is not clearly determined.

- SHARED information - all objects in the network society (sites, social media, clouds) could be accessible from different places of the world and the sharing of information will cause Internet-related security problems (loss of data, destroying the integrity, problems with accountability, hackers' attacks, etc.). For example, each user of social media uploads information that will be shared between a set of users and it could be disseminated to different locations. In this case the data subject does not know what policy and measures are used for counteraction to eventual attacks. This problem is very important if data are sensitive (medical status, for example).

- TECHNICAL and ORGANIZATIONAL measures for data protection - an important obligation for the data controllers is to implement appropriate measures for information security. These measures should be a counteraction to all forms of destruction or loss of personal data, to an unauthorized access (during the personal data processing or transmission via communication links), and to all illegal forms of processing. The service providers should guarantee an effective protection of data integrity and data availability in cloud environment, but it is known that more data security measures will reduce the performance of the information processing. In this reason, the providers must choose the most appropriate security measures.

7.5. Last Regulations in Privacy and PDP

Modernization of data protection rules on European level has been made in the last years. An example is the document "Proposed Regulation" of the European Commission in January 2012 that proposes new rules to strengthen online data protection rights. The reason for these draft amendments is the fact "that rapid technological development and globalization have profoundly changed the world and brought new challenges to the protection of personal data" [Knijpenga]. This document discuses the paradigm "right to be forgotten" as shown in Article 17, and the data subject rights to data portability as discussed in Article 18, transfer between different electronic processing systems.

The European Parliament has determined on 12 March 2014 that architecture and fundamental principles of the data protection reform for improving user protection and security in Cyber-space [Fischer]. The conclusion is that the further development and exploitation of Cyber-space could not be realized without an adequate and strong protection of the rights of individual users [EC]. The following FOUR pillars have been determined.

- Pillar-1: "One continents one law" - a requirement about the regulation and sanctions in private and public sectors.

- Pillar-2: "Strong regulation of European digital industry" - a requirement for the non-European companies, when offering services to European consumers, to apply the European rules and level of data protection.

- Pillar-3: "The right to be forgotten / The right to be erased" - this is the right of an individual to remove own personal data from the system if she/he no longer want to use the online services or there is no legitimate reason for keeping it in this online system. This regulation will permit the individuals to control own online identify and to require the personal profile to be removed from the system (including social media platforms).

- Pillar-4: A "One-stop-shop" for businesses and citizens - a regulation for the personal data processing by controller or processor established in more that one country of European Union.The new principles of regulation must extend the PDP frame determined by the previously directives, and to propose adequate solutions for all problems of PDP in social environments.

The new principles of regulation must extend the PDP frame determined by the previously directives, and to propose adequate solutions for all problems of PDP in the digital world.

In other hand, the users should undertake personal measures to protect own information. The best practice say "protect yourself" by using modern Internet security solutions (anti-virus programs, firewalls, tools for browser protection, reputation-checking tools, etc.). These tools must be regularly updated. An important side of the protection is using effective policy for authentication - the password should be a mix of letters and numbers, and change them often. It is not correct to use the same password at the access to different network resources. The visiting network resources must be deliberated and the reputation and safety rating of websites before using must be analyzed. Finally, the main principle of users must be "guard your personal data." Users must publish limited personal and financial information in the Internet, for example, social media, Internet cafes, websites, libraries, forums, etc.

8. IANA Considerations

. . . .

10. References

10.1. Normative References

[Chen] Chen, D., H. Zhao, "Data security and privacy protection issues in cloud computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), vol.1, pp.647-651 , March 2012.

[EC] "Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote", European Commission - MEMO, Strasbourg , March 2014,

<http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>.

[Fischer] Fischer, A. E., "Improving User Protection and Security in Cyberspace", Report of Committee on Culture, Science, Education and Media, Council of Europe , March 2014, <http://www.statewatch.org/news/2014/mar/coe-parl- ass-cyberspace-security.pdf>.

[Garber] Garber, L., "The Challenges of Securing the Virtualized Environment", Computer, pp.17-23 , January 2012, <http://www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf>.

[I-D.junsheng-opsawg-virtual-resource-management] Chu, J., Khasnabish, B., Qing, Y., and Y. Meng, "Virtual Resource Management in Cloud", draft-junsheng-opsawg-virtual-resource-management-00 (work in progress), July 2011.

[I-D.karavettil-vdcs-security-framework] Karavettil, S., Khasnabish, B., Ning, S., and W. Dong, "Security Framework for Virtualized Data Center Services", draft-karavettil-vdcs-security-framework-05 (work in progress), December 2012.

[I-D.khasnabish-cloud-reference-framework] Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y., and M. Yu, "Cloud Reference Framework", draft-khasnabish-cloud-reference-framework-07 (work in progress), October 2014.

[I-D.khasnabish-dispatch-qoe-management]
Khasnabish, B., Fernando, G., and L. Ya, "End-point based Multimedia QoE Management", draft-khasnabish-dispatch-qoe-management-02 (work in progress), July 2013.

[Kinast] "Social Media and Data Protection", Kinast and Partner , 2014, <http://www.kinast-partner.com/data-protection-law/social-media-and-data-protection/>.

[Knijpenga]
Knijpenga, A., "The Modernization of European Data Protection Rules.", Deloitte , 2012, <http://www.deloitte.com/assets/Dcom-Switzerland/Local%20Assets/Documents/EN/Audit/RCL/ch_en_the_modernization_of_european_data_protection_rules.pdf>.

[Lam] Lam, S. K., J. Riedl., "Are our online "friend" really friends?", Computer, pp.91-93 , January 2012.

[Meyer] Meyer, J.P., S. Zhu, "Fair and Equitable Measurement of Student Learning in MOOCs", Research and Practice in Assessment, 1 (vol. 8), pp.26-39 , 2013, <http://www.rpajournal.com/dev/wp-content/uploads/2013/05/SF3.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[Romansky-1]
Romansky, R., "Digital Privacy in the Network World", In Proceedings of the International Conference on Information Technologies (InfoTech-2014), St. St. Constantine and Elena, Bulgaria, pp.273-284 , September 2014, <http://infotech-bg.com/proceedings>.

[Romansky-2]
Romansky, R., "Cloud Services: Challenges for Personal Data Protection", International Journal on Information Technologies and Security, No 3, pp.67-80 , September 2012, <http://ijits-bg.com/ijitsarchive>.

[Yong] Yong Chen, Wu He, "Security Risks and Protection in Online Learning: A Survey", The International Review of Research in Open and Distance Learning, 5 (vol. 14), pp.108-127 , December 2013, <http://www.irrodl.org/index.php/irrodl/article/viewFile/1632/2750>.

10.2. Informative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC3654] Khosravi, H. and T. Anderson, "Requirements for Separation of IP Control and Forwarding", RFC 3654, November 2003.

[RFC3746] Yang, L., Dantu, R., Anderson, T., and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", RFC 3746, April 2004.

Authors' Addresses

Radi Romansky (editor)
Tech. Univ. of Sofia.
8 Kliment Ohridski BLVD
Sofia , Bulgaria 1000
Europe

Phone: □2-965-3295
EMail: rrom@tu-sofia.bg

Bhumip Khasnabish
ZTE (TX) Inc.
USA

Phone: 퍍781-752-8003
EMail: vumip1@gmail.com, bhumip.khasnabish@ztetx.com
URI: http://tinyurl.com/bhumip/