International Working Group
on Data Protection
in Telecommunications

675.33.13 6 September 2006

Working Paper on Privacy and Security in Internet Telephony (VoIP)

40th meeting, 5-6 September 2006, Berlin

The provision of telephone services over the Internet (internet telephony or "voice over IP" - VoIP) is on the increase. Already now services based on DSL or other broadband connectivity are available that allow for a complete replacement of fixed telephone lines. Providers of "traditional" telephone services have also begun to deliver services using the VoIP protocol. At the same time mobile equipment becomes available allowing for placing phone calls over the Internet also in a mobile environment. This development is only at its beginning, and further changes of the telephony landscape are likely to occur in the near future.

The introduction of VoIP services to the mass market comes with risks for security and privacy of its users that need to be tackled appropriately at an early stage.

The introduction of VoIP poses challenges to the existing national and regional regulatory regimes. For example, providers of VoIP services may not be obliged by national laws to provide for telecommunications secrecy, which is a basic right laid down in many national constitutions as well as in supranational regulatory instruments.

Many national regulatory regimes also contain provisions restricting the processing of traffic data, normally bound to billing needs. VoIP services may instead process more personal data than necessary for billing purposes (e.g. call records for incoming calls) without user being aware of or being able to restrict such processing.

The challenges the introduction of internet telephony will pose for the secrecy of telecommunications should not be underestimated[1]: VoIP telephones are technically speaking computers connected to the Internet. As such they are targets for attacks of any kind common on the Internet today. The different protocols (e.g. the widely used SIP protocol) also implement certain privacy-related functions in different ways. For example, calling line identification restriction may not be available for calls between VoIP telephones.

The content of messages in VoIP services is routed over a network of - in comparison with the fixed telephone network - relatively insecure nodes, making them vulnerable to potential attacks by a potentially large number of other users. It is therefore essential to encrypt signalling messages as well as the content of the communication. As encrypted messages may also be recorded and then be decoded at a later stage, a sufficiently secure encryption method is required.

Security may also be at risk when VoIP technology is applied within a company or a body of the public administration as a replacement for conventional PABX systems. Security aspects must be considered when VoIP technology is introduced.

[1] A study commissioned in 2005 by the German Federal Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik - BSI) concluded that VoIP systems inherit the security risks from the IP world, while keeping most of those from the telco world; cf. http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf on page 134 (German only).

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Telecommunications secrecy has been in the focus of the Working Group since it was founded[2]. The principle of inviolability of telephone conversations is guaranteed in the constitutional documents of many countries. As with any processing of personal data, appropriate measures must be taken on the networks and servers used for delivering VoIP services to guarantee for availability, confidentiality, integrity and authenticity of the data transmitted[3].

In the light of the above, the Working Group makes the following recommendations:

Regulators are called upon to ensure in the applicable regulatory frameworks as well as when negotiating international agreements that VoIP service providers are obliged to ensure the same level of security and privacy as providers of traditional fixed and mobile telephone services as a minimum[4].

VoIP providers and manufacturers of respective hard- and/or software are called upon to

1. inform their customers about privacy and security risks of VoIP services[5] and possible remedies[6],

2. take appropriate technical and organisational measures to provide for a secure and privacy-friendly use of VoIP services,

3. offer interoperable end-to-end encryption facilities as a standard feature of their service at no additional costs,

4. make sure that security and privacy features of their products are activated by default,

5. strive to swiftly eliminate any security or privacy flaws of the protocols and the hard- and/or software in use[7],

6. use open standards and inform their customers and the general public about the protocols and/or products in use,

7. restrict the amount of personal data stored and processed by default (e.g. traffic data) to what is necessary for the provision and billing (as applicable) of the service, unless additional storing and/processing of data is explicitly mandated by law.

8. offer privacy-relevant features at least in the same manner as in the fixed telephone network (e.g. suppression of the presentation of the calling number at the called party)[8],

---

[2] Cf. e.g. the report of the Working Group on Telecommunication and Media on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners 14th Conference, 29. October 1992, Sydney <http://www.datenschutz-berlin.de/attachments/134/fernm_en.pdf>

[3] Cf. Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements - Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000) <http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf>

[4] VoIP privacy standards should not be tied to a baseline of telephone privacy expectations. Although privacy features in traditional telephone services can serve as an imperfect example of desirable features, VoIP systems should be developed with consideration of what features would best protect privacy, regardless of whether they have been implemented in the traditional phone network.

[5] Inter alia, a VoIP provider should notify any user whose personal information has been lost, stolen, or accessed by an unauthorized party while in that service provider's possession.

[6] In the case of VoIP over WLAN services this should include information on risks and remedies for WLAN technology, cf. Working Paper on potential privacy risks associated with wireless networks.
Main Recommendations (14-15 April 2004, Buenos Aires); <http://www.datenschutz-berlin.de/attachments/197/1_en.pdf>

[7] This may include extensions or changes of the protocols in use (e.g. the SIP protocol) to allow for user control over the protocol information transmitted and/or displayed on the equipment of the called and the calling party.

[8] Cf. footnote 4 above

9. not to collect a user's availability and physical location information except to provide emergency services or, if collected in an anonymous form, to improve service quality. Such information should be stored no longer than those purposes require, and it should be accessible only for those purposes. This information should not be displayed to other customers, including any other party or parties to any communication, unless the data subject affirmatively and explicitly chooses to do so. A user should be able to choose which other users (if any) can see her availability and location information. Availability and physical location information should not be sold or used for targeted advertising without the user's explicit consent.

10. maintain the possibility to use telecommunications networks via public access points in an anonymous way.