IPclip—An Innovative Mechanism to Reestablish Trust-by-Wire in Packet-switched IP Networks

Peter Danielis, Stephan Kubisch, Harald Widiger,
Jens Schulz, Dirk Timmermann
University of Rostock
Institute of Applied Microelectronics and Computer Engineering
18051 Rostock, Germany
Tel./Fax: +49 381 498-7272 / -1187251
Email: {peter.danielis;dirk.timmermann}@uni-rostock.de
Web: http://www.imd.uni-rostock.de/networking

Thomas Bahls, Daniel Duchow
Nokia Siemens Networks GmbH & Co. KG
Broadband Access Division
17489 Greifswald, Germany
Tel./Fax: +49 3834 555-642 / -602
Email: {thomas.bahls;daniel.duchow}@nsn.com

I. Introduction

During the last decades, the Internet has steadily developed into a mass medium. On the one hand, newfangled services replace traditional ones. Naturally, these are thereby expected to offer at least the same features as their classical pendants, e.g., when VoIP replaces traditional fixed line telephone networks. On the other hand, the requirements on network infrastructures and services have changed. A reason for that is the lack of so-called Trust-by-Wire (TBW) in packet-switched IP networks. With TBW, we describe a direct interrelationship between some flavor of user-ID, e.g., a network address, login name, or phone number, and the physical line or geographic location of that user. In other words, TBW stands for unambiguousness and trustworthiness in telecommunication networks. In traditional telephone networks, a phone number directly coheres with a physical line. This direct relationship is not given in modern packet-switched IP networks. An IP address does not identify a physical line! To solve this problem, a new mechanism has been developed, which guarantees TBW in packet-switched IP networks—called Internet Protocol-Calling Line Identification Presentation (IPclip). Already in the access network, unambiguous and trustworthy location information (LI) is added on the IP level. IPclip is thus one step towards increasing security and reliability in IP-based infrastructures.

This paper gives an overview about our current research activities on this project. The abstract is organized as follows: Section II presents the IPclip mechanism in general. In Section III, we introduce various use cases for IPclip. The paper concludes in Section IV.

II. The IPclip Mechanism in General

The name IPclip is derived from the CLIP function of Integrated Services Digital Networks (ISDN). Originally, CLIP is used as an optional feature in ISDN telephone networks. With CLIP, the number of the caller is transmitted to the callee allowing precise identification of the caller. In case of IP, a user's IP address *cannot* be considered as equivalent to a phone number, because IP addresses do not uniquely reference physical lines. Furthermore, IP addresses *do not* provide LI in any case whereas phone numbers *do have* a well-defined origin. Therefore, IPclip reuses selected, principle aspects of the ISDN CLIP function in IP-based packet-switched networks to facilitate enhanced and new services.

With the IPclip mechanism, a customer and his actual geographic location are identified using a tuple, which consists of the current IP address and further information. While the IP address might identify a user, his position must be part of the additional data. Approved geographic standards, which are well-known in the field of geographic information systems such as the Global Positioning System, are used for the IPclip LI.

To provide such LI on a global scale, IPclip inserts it as IP option into every IP packet. IP spans the whole Internet and provides end-to-end connectivity. Structure and size of IP options are standardized. Thus, by using IP options, IPclip is a standard-compliant solution to convey up to 40 bytes of extra information. Thereby, network devices can either process this IP option or ignore it. But in any case, devices must be capable of parsing the complete IP header for reasons of interoperability.

IPclip is located on the linecards of an access node, which is a trustworthy network element of an access network in contrast to customer premises equipments. For detailed information on IPclip's functionality, the interested reader is referred to [1].

III. IPclip's Use Cases

A. VoIP Emergency Calls

In contrast to the best current practices for VoIP emergency calls (ECs), which mainly base on additional push/pull approaches, data base lookups, and manual updates of LI (see [1]), the TBW framework approaches the problem from a different perspective. IPclip carries out the insertion of LI. Thereby, the user is not requested to constantly update his LI or to insert it himself although he still *can* do it. IPclip options can be added into every IP packet or only into selected packets, e.g., into every SIP packet. Thus, trustworthy and accurate LI is always available to localize emergency callers. This brings out an improvement for users of mobile IP phone services compared to the best current practice. The IPclip mechanism is furthermore compatible to current standardization approaches (see [1]) and provides supplementary information.

B. An Anti-Phishing Framework Using IPclip

Anti-phishing techniques try to analyze and filter contents, addresses, and the behaviour of, e.g., suspicious websites or dubious e-mails. Unfortunately, useful information for analysis and recognition of potential threats can be manipulated by phishers. Thus, current anti-phishing techniques are not preventive but solely reactive. Furthermore, current countermeasures mostly represent some flavor of *inband traffic control* and phishers can take counter-countermeasures to annihilate anti-phishing efforts.

Instead, IPclip provides trustable information and triggers on the IP level, which are out of the scammers' reach. The LI provided by IPclip is a piece of information that cannot be circumvented or manipulated. As described in [2], the trustable LI is used as a supplementary and trustworthy trigger to identify potential phishing threats. Besides, using a set of LI allows for tracing the threat's origin. From an ISP's or network carrier's point of view, this is some kind of *outband traffic control* as discussed in [3].

C. IPclip as Anti-Spam Mechanism

Typical anti-spam mechanisms try to analyze the content, source & sender information or reputation, and the behaviour of e-mail traffic to derive triggers for e-mail classification and tracing. But all information that is available for analysis is to a very large degree within manipulation-reach of spammers. Hence, typical anti-spam efforts can just react and have to take e-mail traffic as it is. Instead, IPclip provides a trustworthy trigger on the IP level, which is *not* within reach of the spammers. As explained in Section II, the main IPclip system itself is implemented on the linecards and belongs to a network carrier's management domain. The LI added by IPclip cannot be manipulated by spammers and can thus be considered as trustable.

As detailed in [4], using LI as user-defined entry in the e-mail header and guaranteeing its trustability, e-mails—including spam—can primarily be traced. In some cases, the acceptance can immediately be declined. Furthermore, IPclip provides another trigger for existing anti-spam mechanism and can be used in honeynets for analysis of IP traffic.

D. Using IPclip for Peer-To-Peer Networks

IPclip is not limited to the scenario of adding LI to identify users by their geographic location. The IP option inserted by IPclip can take any value to support other applications.

In Peer-to-Peer (P2P) networks, the mismatch between logical P2P overlay and underlying physical network becomes a serious obstacle for the development of P2P systems. For increasing physical proximity in unstructured P2P networks to mitigate the mismatching problem, the IPclip option shall contain the initial TTL value of outgoing IP packets. Then, at the packet's destination, hop count can be calculated as the difference between the copied TTL value and the TTL value of the IP header. The hop count value serves as an additional trigger for P2P applications to classify peers according to their physical distance to each other.

In constrast to current approaches (see [5]), we do not intervene with the *construction* of unstructured P2P networks. Instead, we use IPclip to provide a trigger (the hop count) in every packet to be able to select proximate peers in randomly built, unstructured P2P networks. Thereby, no modification of the construction algorithm is necessary and no traffic overhead is created to determine the distance between peers.

IV. Conclusion

We gave an overview about IPclip, which is a new mechanism to guarantee TBW in packet-switched IPv4 networks. It is now feasible to identify a physical line in IP-based packet-switched networks by using trustworthy LI. We described IPclip's application for VoIP ECs, for countering phishing threats, in an anti-spam scenario, and for increasing physical proximity in unstructured P2P networks. The entire mechanism is implemented in hardware for non-blocking operation at wire speed. We developed a hardware prototype for the IPclip system using an FPGA development board [6].

Ongoing and future work covers research on the feasibility and technical aspects of our approach in IPv6 networks since IPv6 will dominate the prospective Internet.

Acknowledgment

We would like to thank the Broadband Access Division of Nokia Siemens Networks in Greifswald, Germany for their inspiration and continued support in this project. This work is partly granted by Nokia Siemens Networks as well as the 4th Priority Research Program on Information- and Communication Technologies, Mecklenburg-Vorpommern, Germany.

References

[1] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow, "Trust-by-Wire in Packet-switched IP Networks: Calling Line Identification Presentation for IP." Genf, Switzerland: 1st ITU-T Kaleidoscope Conference: Innovations in Next Generation Networks - Future Network and Services, May 2008, accepted.

[2] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, D. Timmermann, D. Duchow, and T. Bahls, "Countering Phishing Threats with Trust-by-Wire in Packet-switched IP Networks – A Conceptual Framework," in *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS), 4th International Workshop on Security in Systems and Networks (SSN)*, Miami, FL, USA, April 2008, accepted.

[3] M. Parameswaran, X. Zhao, A. B. Whinston, and F. Fang, "Reengineering the Internet for Better Security," *IEEE Computer*, vol. 40, no. 1, pp. 40–44, January 2007.

[4] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, T. Bahls, D. Duchow, and D. Timmermann, "Hallmarking E-Mails with Distinct, Geographic Location Information in Packet-switched IP Networks." Cambridge, Massachusetts, USA: MIT Spam Conference 2008, March 2008, submitted.

[5] P. Danielis, S. Kubisch, H. Widiger, J. Schulz, D. Duchow, T. Bahls, and D. Timmermann, "A Conceptual Framework for Increasing Physical Proximity in Unstructured Peer-To-Peer Networks." Princeton, NJ, USA: IEEE Sarnoff Symposium 2008, April 28 - 30 2008, accepted.

[6] P. Danielis, S. Kubisch, H. Widiger, J. Schulz, D. Duchow, T. Bahls, D. Timmermann, and C. Lange, "Trust-by-Wire in Packet-switched IP Networks: Calling Line Identification Presentation for IP," in *Design, Automation and Test in Europe Conference and Exhibition (DATE'08), University Booth Hardware Demonstration*, Munich, Germany, March 2008, accepted.