Trust-by-Wire in Packet-Switched IPv6 Networks:
Tools and FPGA Prototype for the IPclip System

Peter Danielis, Stephan Kubisch, Harald Widiger,
Jens Rohrbeck, Vladyslav Altman, Jan Skodzik, 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
Broadband Access Division
17489 Greifswald, Germany
Tel./Fax: +49 3834 555-642 / -602
Email: {thomas.bahls;daniel.duchow}@nsn.com

Abstract—This demonstration shows the hardware prototype of the IPclip (IP Calling Line Identification Presentation) mechanism for IPv6 networks. IPclip is a mechanism, which provides Trust-by-Wire in IP-based networks by adding trustworthy location information to IP packets. It is implemented on an FPGA development board and configurable at runtime via a graphical configuration tool. We show IPclip’s basic functionality in a localization scenario using an analysis tool and Google Earth and discuss several application scenarios during the demonstration.

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 Voice over IP (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 the 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 and existing services such as emergency calls (ECs) rely upon it. 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 in real-time during the life of each and every packet—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, which can be used for various applications.

We developed a working FPGA prototype for the IPclip mechanism. As IPv6 will be the dominating protocol in the prospective Internet, we adapted the TBW idea and the IPclip functionality to IPv6 environments.

Section II presents the basic concept of the IPclip mechanism and its use cases. In Section III, we introduce the configuration tool and the analysis tool. Section IV briefly sketches a localization demonstration scenario before the paper concludes.

II. IPCLIP – THE BASIC CONCEPT

Basically, IPclip is a mechanism to insert LI into packets in the upstream data path. To provide such LI on a global scale, IPclip inserts it as IP option in case of IPv4 and as extension header of an IPv6 packet respectively. The whole IPclip architecture also includes functionality for identification, verification and validation of user provided LI. Furthermore, the IPclip system provides the option to remove existing LI from IP packets in the downstream data path to not forward LI to the end-user.

IPclip is currently adapted to IPv6 environments for this demonstration. For detailed information on IPclip’s functionality, the interested reader is referred to [1].

![Access network with IPclip](image-url)

A. General Functionality

Network ingress—also known as access network—is the most reasonable place where LI can be added and verified. Access networks comprise Customer Premises Equipments (CPEs) as well as so-called access nodes (ANs) like IP DSL Access Multiplexers (IP DSLAMs). Usually, ANs consist of multiple line cards (LCs) and an aggregation card. As sketched
in Figure 1, IPclip is located on the AN. From an ISP’s point of view, an AN is a trustworthy network element in contrast to CPEs because it is within an ISP’s management domain. That is why IPclip is implemented on an AN and verification of LI is done here.

With the IPclip mechanism, a customer and his actual geographic location are identified using a tuple, which consists of the current IP address and extra information. While the IP address might identify a user, his position must be part of the additional data. Preferably, a standardized format of LI is used. It can be interpreted for analysis, for classification, for generation of syslog-calls to induce further exceptional actions, or to send help to a person that requires medical assistance in case of VoIP ECs.

B. Use Cases

As proposed in [2], [3], the IPclip mechanism can be used for various use cases such as supporting VoIP ECs, countering phishing threats and in an anti-spam scenario. Due to IPclip’s manifold fields of application, it constitutes a contribution to extending and supporting network-based services offered by consumer electronics.

III. Configuration and Analysis Tool

To configure and update IPclip’s internal parameters (e.g., the own LI of the AN and the size of LI in bytes) dynamically at runtime, we developed a graphical user interface (GUI), which allows for an easy “push-button” configuration of the entire system. The GUI allows for the configuration of global system parameters as well as for configuring ports to be added in addition to LI for a corresponding IP packet.

Additionally, an analysis tool has been developed for the IPclip system. When packets are received, those containing LI are highlighted and trustworthiness of received LI is indicated. Received LI can be pictured on a terrestrial globe using Google Earth (see Figure 2).

IV. The Localization Demonstration Scenario

IPclip is implemented on an Xilinx Virtex4 FX20 FPGA development board (ML-405). The typical, complex environment of IPclip on an AN cannot be rebuilt. Instead, a localization demonstration scenario has been prepared, which provides an insight into the operation modi of the different functional modules in the IPclip system. Thereby, the FPGA board emulates an AN with IPclip.

Localization Demonstration: In this demonstration, a user sends IPv6 packets without and with LI to a target used as a monitor. We analyze outgoing packets with the protocol analyzer Wireshark [4]. A dissector has been developed for Wireshark to parse our used LI format. Packets pass our FPGA prototype on their way to the target. The IPclip mechanism is implemented on this FPGA and configured by means of our developed configuration tool. Packets without LI are enriched with GPS LI using a GPS receiver. In this case, LI is regarded as network provided, trusted. In packets that contain user provided LI, user provided LI is identified and verified by the IPclip prototype. If user provided LI passes verification, it is labeled as user provided, trusted. Otherwise, user provided LI is replaced by GPS LI and packets are labeled as network provided, untrusted. At the packet’s destination, the LI’s trustworthiness is indicated by our analysis tool and LI is pictured with Google Earth (see Figure 2).

Furthermore, in the demonstration, we discuss advantages and disadvantages of IPclip’s application scenarios concerning security and privacy issues.

V. Conclusion

We presented the working prototype of the previously published IPclip mechanism for IPv6 networks. For comfortable system configuration, we also proposed a graphical configuration tool, which is used to configure the IPclip prototype on the FPGA development board at runtime. The second GUI serves as an analyzer to picture received location information on a terrestrial globe and to show whether received location information is trustworthy. Furthermore, we briefly introduced a localization demonstration scenario.

More details are given on the poster and during the demonstration session.

REFERENCES


