

Anonymous and untraceable communications: Location privacy in mobile internetworking.

Alberto Escudero Pascual
Laboratory of Telecommunication Systems
Department of Microelectronics and Information Technology
Royal Institute of Technology
Kista - Sweden

May 16, 2001

Abstract

Data protection and privacy is rapidly becoming one of the most important issues on the Internet today. Larger number of Internet sites are collecting personal information from users through forms, cookies, online registrations, or surveys than ever before. New commercial services are springing up that can exploit the ability of mobile communication service providers to determine the geographic location of their users. The new wireless technologies offer mobility; at the same time they offer *location information* that is being used to provide new *location-aware services*.

This licentiate thesis concerns our experience building a new innovative network environment at the IT-University (Royal Institute of Technology). It explains how we present the new security challenges that a wireless network raises together with how we confront and investigate a new form of problem this type of network presents, namely location privacy.

The focus of this work has been on trying to provide unlinkability between the location of wireless users and their activities in the Internet. The thesis includes a protocol extension to a pseudonymous IP network architecture developed by the Canadian company Zero Knowledge Systems Inc. called the Freedom System. The proposed extension to Freedom System permits a mobile client to seamlessly roam among IP subnetworks and media types whilst being untraceable. By untraceable in the context of this thesis we mean the capability of a mobile node to conceal *the relation between location and personal identifiable information* from third parties whilst the user is on the move.

This thesis is composed of four published papers where the main results are presented.

Acknowledgements

First I would like to thanks to my advisors, Prof Björn Pehrson and Prof. Gerald Q. "Chip" Maguire Jr., working with them has been basically: "Great fun!"

To my Lab and student colleagues to cope with my non documented paranoia and unvaluable whiteboard discussions.

To my friends around the world who suprisely always gave me *root* access to their machines to check their security problems.

Gracias especiales a mis siempre vigilantes miembros de Nodo50, with whom i have shared the responsability of building a free space in the Net.

A mis padres, quienes descubrieron la 'Interne' cuando me marche a Suecia y me dieron la oportunidad de aprender ingles cuando los demas jugaban con pistolas.

Lastly I would like to show my deepest gratitude to 'you' anonymous reader... turn round, look to the camera, smile :-)

Contents

1	List of papers	7
2	Introduction	9
3	Related work and thesis background	11
4	Summary of original work	13
5	Conclusions and future work	15
6	Published papers	18

1 List of papers

This licentiate thesis is based on the following papers, which will be referred to by their letters:

- A Alberto Escudero Pascual
Wireless Internet Access: "From the peruvian Amazonia to the Swedish Silicon Valley"
1st International. Conference of Community Networking (CNGLOBAL2000), November 2000, Barcelona, Spain.

- B Alberto Escudero, Björn Pehrson, Enrico Pelletta, Jon-Olov Vatn and Pawel Wiatr
Wireless access in the Kista - IT University: "Integrating MobileIPv4 in a IEEE 802.11b based environment"
11th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN2001), March 2001, Boulder,CO USA.

- C Alberto Escudero
Kista - IT University Wireless Network: "Privacy in mobile internet-working?"
Internet Society Conference (INET2001), Ref: Uses Summit ID U22. June 2001, Stockholm, Sweden

- D Alberto Escudero, Martin Hedenfalk and Per Heselius
Location Privacy in Mobile Internetworking: "Protocol extensions to Freedom Network"
Internet Society Conference (INET2001), Ref: Technical Summit ID T06. June 2001, Stockholm, Sweden.

2 Introduction

There are several important issues regarding security in any kind of communications. These include message integrity, authentication, and confidentiality. Integrity means that the message is transmitted without alteration, authentication means that the sending/receiving user is the one they claim to be, and confidentiality means that no other one than the intended party, is able to read the transmitted message.

All these attributes try and focus on the message itself and make sure that a third person eavesdropping the channel can not read and/or modify the message. Our main interest is to go one step further and try to make sure that a third person *Charlie* eavesdropping the channel can not easily determine which party is talking to whom, illustratively our focus is on the **arrow** [Fig. 1] and to be able to conceal the fact that *Alice* is communicating to *Bob* from *Charlie*.

If *Alice* and *Bob* communicate using an IP computer network, their point contact in "net space" is represented by their IP addresses: IP_A and IP_B . When *Alice* wants to send an IP datagram to *Bob*, the source address of *Alice* (IP_A) and the destination address of *Bob* (IP_B) are included in the packet within the message. If *Charlie* is located somewhere along the route where the datagram travels, *Charlie* will be able to determine when the parties are communicating by reading the source and destination addresses of all the packets passing by.

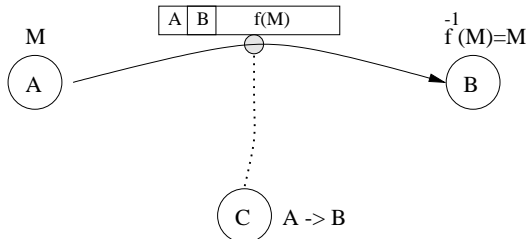


Figure 1: Charlie knows that Alice is talking to Bob.

MobileIP_{v4} [4] allows users to move between different networks while maintaining the same IP address. This is done by associating a care-of-address with the mobile node when it is away from home. All traffic to the mobile node is intercepted in the home network by a home agent that tunnels the data to the care-of-address.

If *Alice* is talking to *Bob* and *Bob* changes his point of attachment, *Bob's* home agent will take care of *Alice* messages by sending them in an encapsulated message to *Bob's* care of address. In wireless networks, where users move between different networks and media types, the fact that our eavesdropper *Charlie* can obtain the consecutive care of addresses of *Bob* [Fig. 2] implies that *Bob's* movements can be easily tracked [5][6].

The efforts of the Internet Engineering Task Force in terms of location privacy are concentrated in making sure that neither *Alice* nor *Bob* can obtain the care of address of their correspondent party.

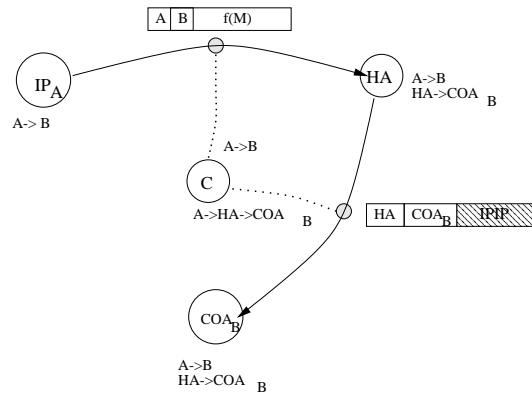


Figure 2: Charlie knows that Bob has moved to COA_B .

Our vision is to take IETF’s work one step further by extending the definition of *location privacy* and we want to ensure that:

- The correspondent node should have no knowledge about which foreign network the mobile node is connected to.
- The home network should have no knowledge about which foreign network the mobile node is currently connected to.
- Similarly, the foreign or “roaming” network should have no knowledge about the mobile node’s home network.
- An eavesdropper or man-in-the-middle should not be able to tell who the communicating parties are.

That means, that *Alice* should have no knowledge about where *Bob* is roaming and vice versa. *Bob’s* home network should have no knowledge about which foreign network *Bob* is attached to. The foreign network where *Bob* is connected to should have no knowledge about *Bob’s* home network and *Charlie* should not be able to tell that *Alice* is talking to *Bob*. In conclusion: *Bob’s* activities should not be linkable with his location and mobility.

3 Related work and thesis background

The only previous work that we found published in our area was done by Fasbender A, Kesdogan D. and Kubitz O.[1] in March 1996. Their paper presented a possible extension of the proposed *MobileIP_{v4}* and route optimization protocols, the Non-Disclosure Method (NDM). NDM is based on the idea of mixes, which has been suggested by Chaum [2] for hiding the originator addresses of electronic mails. Unfortunately no further work was developed by the authors in this direction and the paper left open issues, for example: key management or topology discovery.

In January 2000, during the preparation of the Licentiate Proposal for this thesis and after some time testing AX.25 wireless links in Amazonia [PAPER A], the author approached “The Onion Routing research project” [3], they were building an Internet-based system that strongly resists traffic analysis, eavesdropping, and other attacks both by outsiders and insiders (Onion Routers themselves). Unfortunately the project is not active anymore and the USA’s export restrictions did not help in trying to get architecture design information from the group.

In November 2000, after some months building the Kista - IT University wireless network [PAPER B], and after a controversial Ny Teknik’s press article [5] about the surveillance possibilities of our wireless monitor system “*Big Brother*” [PAPER C], the author contacted Zero Knowledge Inc. in order to explore the possibilities of extending their pseudonymous IP network [7] to support wireless mobility.

A final result of this work is a set of protocol extensions to the Freedom System architecture [PAPER D]. The proposed extension to Freedom System permits a mobile client to seamlessly roam among IP subnetworks and media types while remaining *untraceable* and *pseudonymous*. The extensions were presented on the 7th of June 2001 during the 11th Annual Internet Society Conference in Stockholm, Sweden.

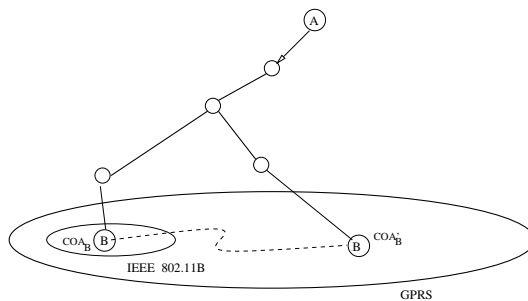


Figure 3: Unlinkability between home and foreign networks in Freedom System.

4 Summary of original work

The objective of this section is to present a short description of the appended publications forming this licentiate thesis.

Paper A

Alberto Escudero

Wireless Internet Access:

"From the Peruvian Amazonia to the Swedish Silicon Valley".

1st Intl Conference of Community Networking (CNGLOBAL2000), November 2000, Barcelona, Spain.

The paper presents two initiatives to provide Internet Access using wireless technologies. The first one provides broadband wireless access for the students of the new IT University programme in the so called Swedish Silicon Valley in Kista (Stockholm) using *TCP/IP* over *IEEE 802.11b* protocol. A second initiative, EHAS,¹ is using low cost technologies to provide e-mail access to isolated medical personnel in the Peruvian Amazonia using *TCP/IP* over *AX.25* protocol.

The author of the this thesis has been involved in the design and implementation of open source solutions for both *EHAS* (1997-1999) and the Kista -IT University wireless networks (2000). As a result of these projects, it is possible to send an e-mail from a health establishment of Shucushyacu in the Amazonia to the restaurant of the Royal Institute of Technology in Kista.

Paper B

Alberto Escudero, Björn Pehrson, Enrico Pelletta, Jon-Olov Vatn and Pawel Wiatr

Wireless access in the Kista - IT University:

"Integrating MobileIPv4 in a IEEE 802.11b based environment"

11th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN2001), March 2001, Boulder,CO USA. ²

This paper gives a detailed description of the new wireless environment available at KTH IT-University as of winter 2001. The paper focuses on design and functional issues and introduces the network in a top-down approach, that is, describing the functional blocks and the details of the implementation.

The paper explains how we have managed to integrate *MobileIPv4* services in a conventional *IEEE 802.11* distribution system providing high levels of security with low maintenance.

Concrete contributions of the author include: the integration of a firewalled network with *MobileIPv4*, the creation of the first linux distribution with native support for wireless mobility '*Flying Linux*' and the design and deployment of a location monitor system for wireless lan users '*Big Brother*'.

¹EHAS stands for Enlace Hispanamericano de Salud. Hispano-American Health Link <http://www.ahas.org>)

²Paper B is the result of a joint effort of the coauthors during the Kista IT University project.

Paper C

Alberto Escudero

Kista - IT University Wireless Network: "Privacy in mobile internetworking?"

Internet Society Conference (INET2001), June 2001, Stockholm, Sweden

This paper was written in order to create social awareness about the need of deployment of legal and technical means so that the user can have control over the dissemination of his or her location information.

The user's location information should be considered as personal identifiable information and stored confidentially. Furthermore, technical means should be investigated to allow to the wireless user to choose whether or not they want to make available to third parties to their location information together with their activities in Internet.

The paper includes references to the controversial *Big Brother System*. The system was initially designed as a networking tool to help us with the positioning of the wireless access points in the *Kista - IT University wireless network*. Big brother is a monitoring system that detects the movements of the wireless users at the Kista IT-University.

Paper D

Alberto Escudero, Martin Hedenfalk and Per Heselius

Location Privacy in Mobile Internetworking: "Protocol extensions to Freedom Network"

Internet Society Conference (INET2001), June 2001, Stockholm, Sweden. ³

The last paper describes a set of protocol extensions to the Freedom System architecture to permit a mobile node to seamlessly roam among IP subnetworks and media types whilst remaining *untraceable* and *pseudonymous*.

The Freedom System is a pseudonymous IP network that provides privacy protection by hiding the user's real IP addresses, email addresses, and other personal identifying information from communication partners and eavesdroppers. These extensions make it possible to support transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings in the same way that *MobileIP_{v4}* does, but with the addition that the home and foreign network are unlinkable.

Our initial ideas were in the direction of integrating *MobileIP_{v4}* into the Freedom System by encapsulating registration and deregistration messages and IPIP/GRE tunnels into Freedom Traffic [1]. Further studies and preliminary results showed that it was more adequate to extend Freedom to provide the same functionalities of *MobileIP_{v4}*. Also to provide the mobile node with the flexibility of rebuilding partial routes hiding the mobility associated with certain pseudonymous.

In this paper we also introduce the possibility of having an *unlocated mobile server* roaming behind the Freedom System. The mobile server is able to accept incoming connections via a home address and port previously registered in one of the Freedom System's wormholes.

³Paper D is the result of a joint effort of the coauthors during the 2g1319/2001 Computer System Design Course.

5 Conclusions and future work

The objective of this thesis was to investigate whether it is possible to give to a mobile user internet communication with: anonymity, untraceability, unobservability, and good performance.

The main conclusion is that my proposed extensions to the Freedom protocols can achieve the above goals and the provide the mobile nodes with functionality similar to *MobileIP_{v4}* whilst allowing them to remaining untraceable and pseudonymous.

The protocol design ensures:

Untraceability: the activities of a mobile user are not linked with their location, giving the user the control over their personal identifiable information on the Internet whilst on the move.

Pseudonymity: the user maintains one or more persistent personae (pseudonyms) that are not linked to the mobile user's physical identity. The pseudonym or *Nym* is defined by a unique email address at Freedom.net and the associated digital signature key.

Unobservability: the link encryption and packet padding applied between node-pairs hide the nature and characteristics of the traffic between them. The existence of Freedom traffic remains observable but not the nature of the traffic itself.

The IT University/KTH-Kista wireless network provided a real life environment in which to investigate and address the most challenging security and privacy problems that arise in a mobile internet.

Since my current work has focused on providing the correct functionality in *IP_{v4}*, my future work will focus on:

1. performance measurements of the Freedom System,
2. handover management of a Freedom client,
3. traffic analysis of Freedom System and
4. how to achieve these same goals in *IP_{v6}*, especially with regard to location privacy.

References

- [1] A. Fasbender, D. Kesdogan and O. Kubitz. Analysis of security and privacy in MobileIP. *4th International Conference of Communications Systems Modeling & Analysis*, Nashville, USA. March 1996
- [2] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of ACM*, v 24, .2, Feb 1981
- [3] M. Reed, P. Syverson and D. Goldschlag. Anonymous Connections and Onion Routing. *Naval Research Laboratory Research Papers*. 1998
- [4] C. Perkins, IP Mobility support, RFC 2002. 1996
- [5] S. Andersson. NyTeknik. "På KTH utvecklas teknik att stoppa övervakning". Nov 2000
http://www.nyteknik.se/pub/pub26_3.asp?art_id=12932
- [6] Aftonbladet Nyheter "KTH-studenter övervakas via trådlöst nätverk Storebror ser dig". Nov 2000
<http://www.aftonbladet.se/nyheter/0011/03/kth.html>
- [7] I. Goldberg, A pseudonymous communications infrastructure for the internet. *PhD Thesis*. Fall 2000

6 Published papers