Universität Stuttgart

INSTITUT FÜR
KOMMUNIKATIONSNETZE
UND RECHNERSYSTEME
Prof. Dr.-Ing. Dr. h. c. mult. P. J. Kühn

Linking VIDs by Mobile IP-Based Communication

Christian Hauser
Institute of Communication Networks and Computer Engineering
University of Stuttgart
hauser@ikr.uni-stuttgart.de

February 23, 2005

Outline

Introduction

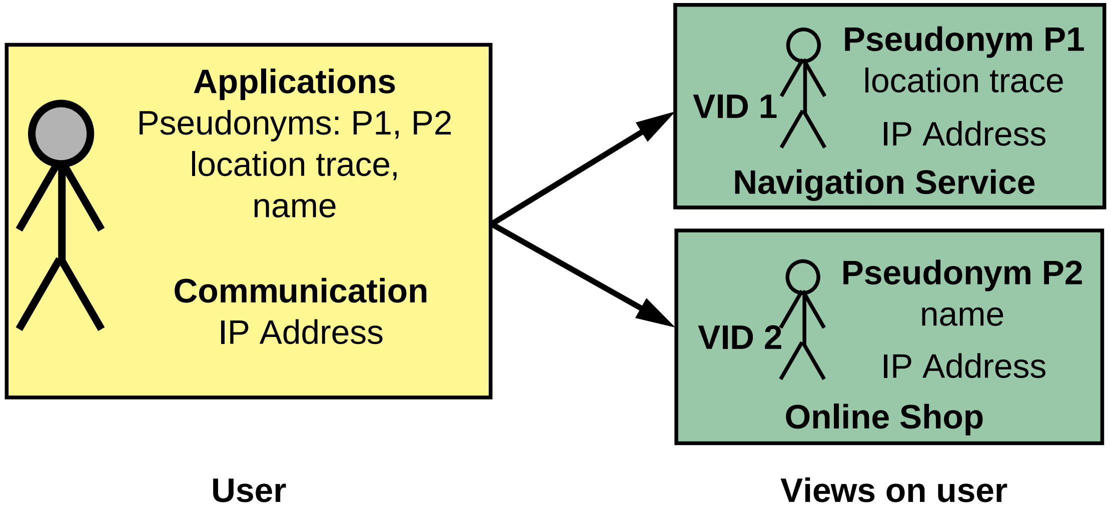
Threat analysis

System idea

Evaluation approach

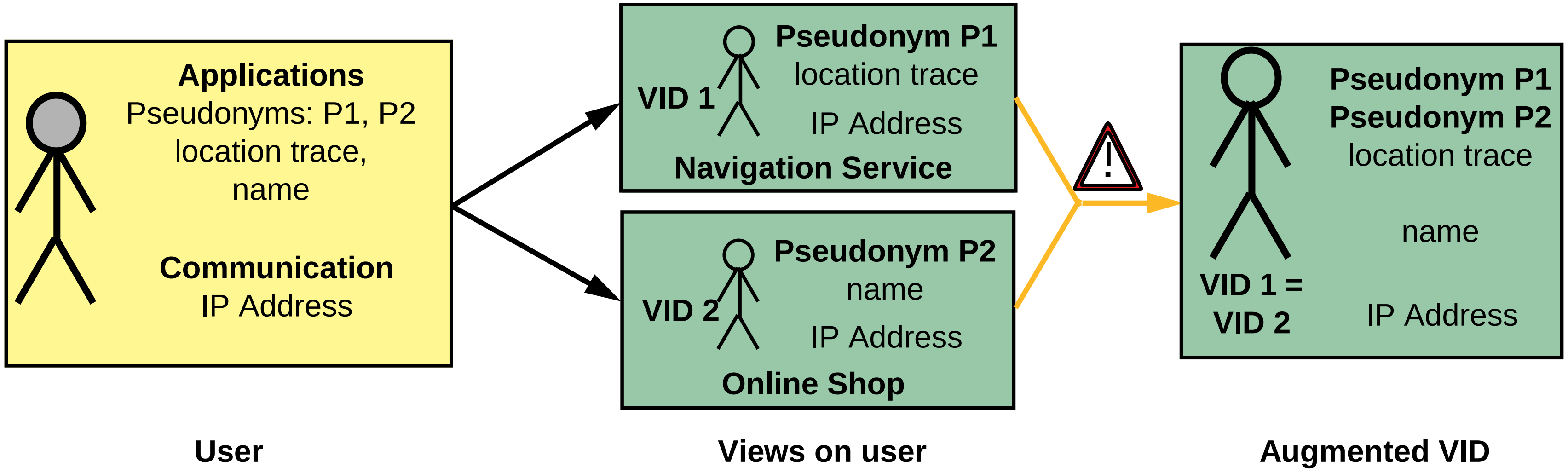
Conclusion and future work

Introduction



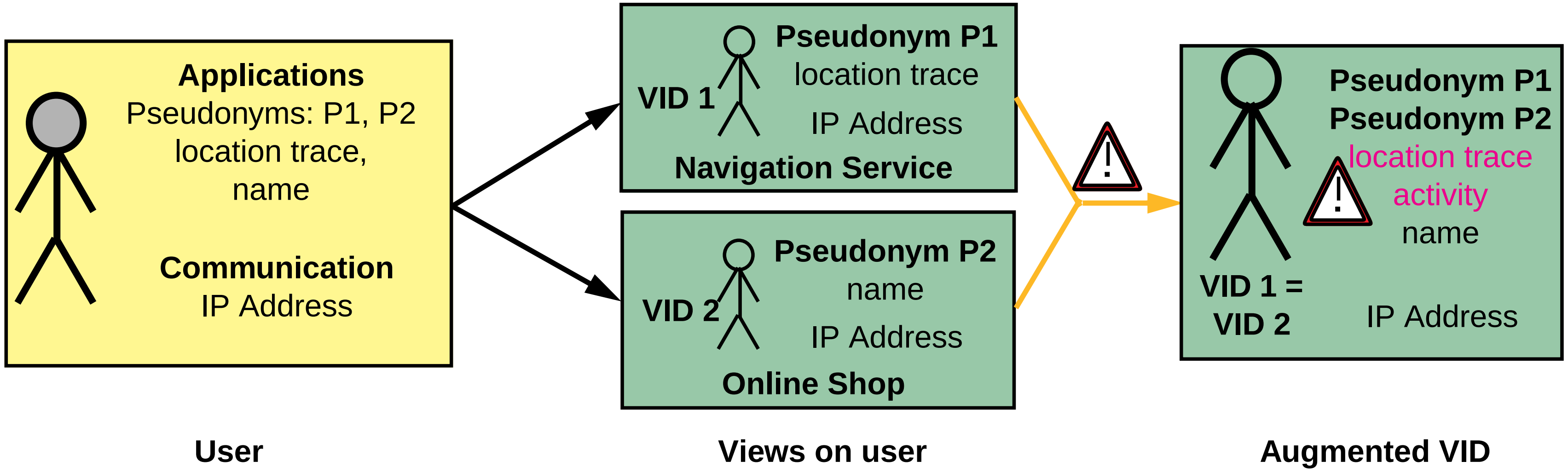
- **Privacy approach**
  - usage of multiple (virtual) identities, VIDs
  - tune amount of disclosed data in context of each identity separately

Introduction



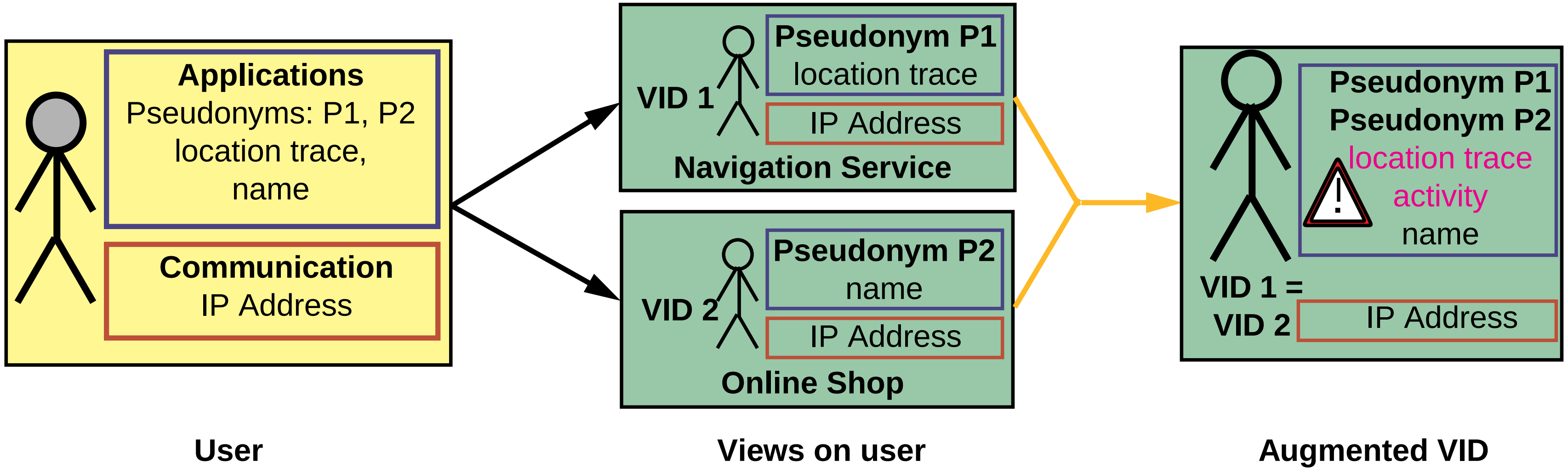
- **Privacy approach**
  - usage of multiple (virtual) identities, VIDs
  - tune amount of disclosed data in context of each identity separately
- **Pitfall: Augmentation of a VID**
  - Two possibilities: Linking of several VIDs

Introduction



- **Privacy approach**
  - usage of multiple (virtual) identities, VIDs
  - tune amount of disclosed data in context of each identity separately
- **Pitfall: Augmentation of a VID**
  - Two possibilities: Linking of several VIDs and inference of data

Introduction



- **Privacy approach**
  - usage of multiple (virtual) identities, VIDs
  - tune amount of disclosed data in context of each identity separately
- **Pitfall: Augmentation of a VID**
  - Two possibilities: Linking of several VIDs and inference of data
    - application data
    - data of communcation system
  - Two possible attackers: Communication partners and communication system provider

Differences to Daidalos

- **No trusted operator**
- **Virtually everybody can be a mobility provider**
  - Mobile IP Home Agent can be provided by everybody
  - huge amount of IPv6 addresses
    - ➥ not impossible to get some IP addresses which can be sold as home addresses

➥ **Two consequences**

- Mobile IP providers are not trusted
  - ➥ complexity increases
- huge amount of providers available
  - ➥ distribution of trust
  - but: it cannot be 100% known whether two providers are in fact one

- **Goals**
  - evaluate how far you can come without trust
  - evaluate how much trust you need

➥ **Don’t worry: What we hear here is out of the scope of Daidalos!**

Threat Analysis I

- **Packet based communication: Two basic pieces of information**
  - identifier: indicates which device is addressed
    - can be chosen arbitrarily (thus without containing any sensitive information)
    - is known to communication system and communication partner
  - locator: indicates where packet must be delivered to
    - inherently contains location in terms of network topology which can be mapped to sensitive geographical location in IP
    - must be known to communication system
    - does not have to be known to communication partners
- **Classical IP**
  - both pieces of information collapse into the IP address
- **Mobile IP**
  - home address is a kind of identifier
  - care-of address is a kind of locator
  - but: home address is locator to user's home and care-of address is known to communication partners in case of route optimization

Threat Analysis II

	Threats in fixed scenario	Additional threats in mobile scenario
Linking of VIDs	**LinkF:** Identical data in context of VIDs *Example:* Identical identifier, identical locator	**LinkM(1):** Identical behavior of VIDs observed by identical patterns of data or events *Example:* Change from identical old locator to identical new locator
		LinkM(2): Identical behavior of VIDs observed by similar patterns of data or events *Example:* Simultaneous locator changes with unknown locators
Inference of personal information	**InfFI:** Inference from the identifier *Example:* home of VID	No additional inference from the identifier
	InfFL: Inference from a single locator *Example:* Location of the user at communication time	**InfML(1):** Inference from several locators *Example:* Location trace of a user over a period of time
		InfML(2): Inference from user behavior by locator changes *Example:* Inference of activity by rate of locator changes

Related Work - Conceptually Four Classes

Threat	Mobile IP and similar systems		Systems providing sender anonymity		Hierarchical systems		Systems protecting against Home Agent (scen. 1 / scen. 2)	
	Corr. Nodes	System	Corr. Nodes	System	Corr. Nodes	System	Corr. Nodes	System
LinkF	–[a]	–[b]	–[a]/+[c]	–[b]	–[a]	–[d]	–[a]	–[a,e] / –[a]
LinkM(1)	+	+	+	+	+	+	+	+/+
LinkM(2)	+	–	+	–	+	–	+	–[f] / +
InfFI	–	–	–	–	–	–	–	–[g] / –[g]
InfFL	+	–	+	–	+	–	+	–[f] / –[f]
InfML(1)	+	–	+	–	+	–	+	–[f] / –[f]
InfML(2)	+	–	+	–	+	–	+	–[f] / –[f]

a. Depends on size of potential user group of home network

b. Depends on size of potential user group of foreign network

c. Protection regarding previously contacted Correspondent Nodes can be achieved. In Hordes this is possible for all Correspondent Nodes.

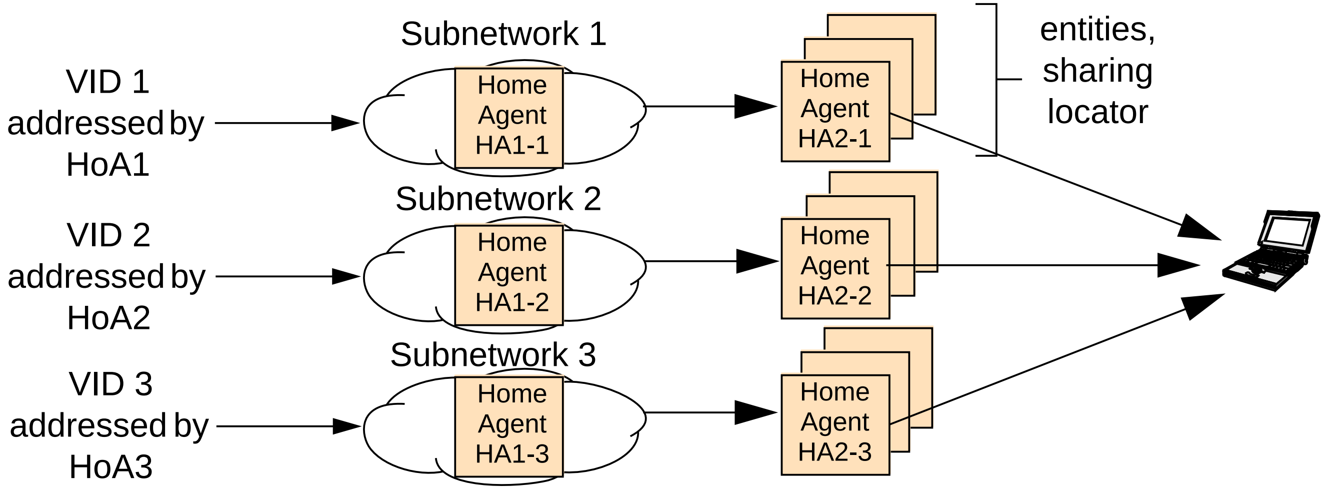
d. Depends on size of intersection of potential user groups of respective entity and of next level entity

e. Depends on size of intersection of potential user groups of respective entity and of next entity in chain

f. Last entity in chain sees locators and their changes but not identifier

g. First entity sees identifier but not locator

System Approach



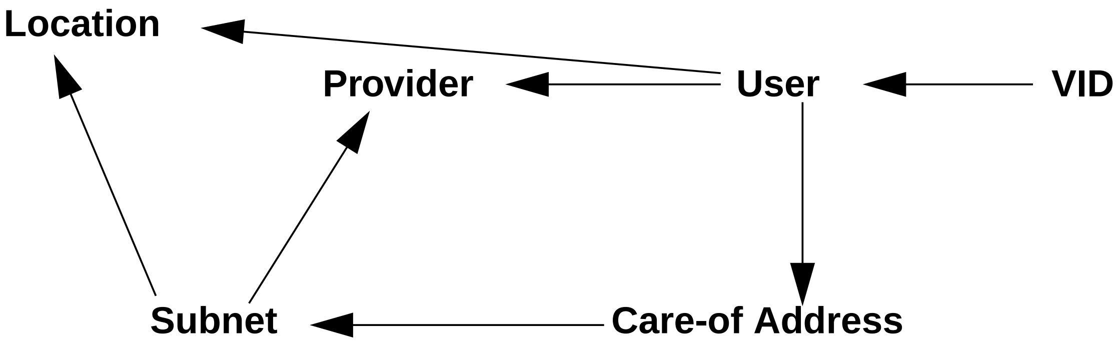
- **Identifiers not from home netw. but from different, arbitrary networks**
  - Each of those networks has a "Home Agent"
- **Different networks supposed to be operated by different parties**
- **Separate contexts for VIDs throughout packet's path**
- **Two agents in a row: no entity knows both, identifier and locator**
- **Locator invisibly stored when not needed**
- **Home Agents HA2-x are changed frequently**
- **User can configure trade-off between performance and privacy**

Future Work: Find Sensible Configurations

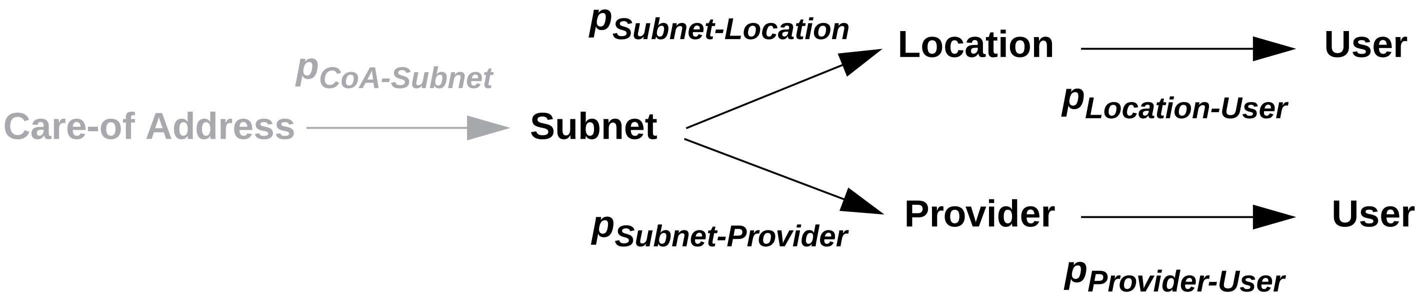
- **Perfect privacy**
  - performance overhead
    - due to spreading of Home Agents
    - due to collection of locator shares
  - scalability: huge amount of servers (and providers)
  - several extensions possible, e.g., to avoid simultaneous share updates
- **Question: Trade-off between performance/scalability and privacy**
  - quantification of performance/scalability costs
  - quantification of privacy benefits
  - providers can collaborate as attackers
  - identification of scenarios
    - trade-off changes according to: number of VIDs, ratio: talkspurt / silence, mobility of user, network and provider scenario (size of "cells" and their provider), ...
- **Approach**
  - event-driven simulation of scenarios
  - framework for quantifying privacy

Evaluation Approach

- **Very simple, static model of sensitive information**



- **Collected observations:**
  VID1 <-> CoA1, VID2 <-> CoA2, CoA1, CoA2 of same subnet


$p_{Subnet\text{-}Location}$
Location
User
$p_{CoA\text{-}Subnet}$
Care-of Address
Subnet
$p_{Location\text{-}User}$
Provider
User
$p_{Subnet\text{-}Provider}$
$p_{Provider\text{-}User}$

- **2 statements about equality of user [attention: (in-)dependence)]**
- **Methodology to be searched**
  - step1: combination of imprecise statements
  - step 2: even probability can be imprecise

Conclusion and Future Work

- **Threat analysis**
  - new threat: linking of VIDs
  - mobility adds significantly to threat
  - ➥ solution must be especially designed for multiple identities and mobility
- **Existing proposals not well prepared**
  - not built for protecting multiple VIDs
  - not built for mobility
  - often only outgoing communication
- **New approach**
  - solves or at least alleviates all identified problems
  - user in control of trade-off: costs vs. privacy
- **Future work**
  - quantification of protection
  - quantification of (performance/scalability) costs
  - ➥ evaluation of sensible configurations