Mobility Management Meets Privacy – the Failure of Existing Proposals and a New, Future-Proof Approach

Christian Hauser

Institute of Communication Networks and Computer Engineering, University of Stuttgart
Pfaffenwaldring 47
D-70569 Stuttgart, GERMANY

hauser@ikr.uni-stuttgart.de

ABSTRACT

Protection of user privacy will gain increasing importance in future mobile systems. To meet the users' privacy needs the approach to reveal different amounts of personal data under several different pseudonyms is promising. This approach can still be undermined with application knowledge as well as with information originating from the communication process itself. Here, mobility management plays a central role as it reflects the user's behavior. Thus, the approach of multiple pseudonyms can only be successful if the communication system is designed for it. In this paper, the respective threats resulting from IP-based mobility management are analyzed. As existing proposals do not protect against these threats, a new approach to mobility management protecting multiple pseudonyms is outlined.

Categories and Subject Descriptors

C.2.m [Computer-Communication Networks]: Miscellaneous; H.3.4 [Information Storage and Retrieval]: Systems and Software---Distributed systems

General Terms

Security

Keywords

Mobility Management, Privacy, Multiple Identities, Mobile IP

1. INTRODUCTION

A prevalent trend in communication systems is an open philosophy as adopted in the Internet. Considering recent developments in networking, e.g., the wide spreading of IEEE 802.11 networks and the huge amount of addresses available in IPv6, virtually everybody can act as a communication service provider by either offering a network for roaming users or by providing a Mobile IP Home Agent and Home Addresses for mobile users. Similar to the number of free E-mail providers today, a large number of mobility management providers for IP-based communication can be assumed in the future. As the users will not always know these providers and they are not always large well-established companies, this situation can lead to varying or even diminishing trust of users in providers.

The trend in the access network infrastructure goes towards an integration of different technologies with IP as a common communication platform and mobility management being handled on network layer by Mobile IPv6. Research already studies so-called all-IP approaches with mobility management being done on IP layer only, e.g., [5]. This approach will be considered in this paper to analyze the resulting threats. An exact justification of these trends is out of the scope of this paper. Details can be found, e.g., in [4] and [5].

Following these arguments, new protection mechanisms have to be adopted. Service and network providers must be considered as potential attackers. A promising approach to achieve this protection is to use multiple pseudonyms. Thereby, a user is able to separately tune the personal information revealed in the context of each pseudonym.

Communication partners do not only see data the user explicitly releases on application level, e.g., the name. They also see additional information which is evolving in the context of the communication process itself, e.g., the currently used IP address. To emphasize this difference, the term virtual identity (VID) is used throughout this paper. A VID comprises the complete view a certain entity has on a user. The crucial threat when using multiple VIDs is that an attacker can infer additional information, thus augmenting its view on the user. This can happen by linking several VIDs of a user or by inferring sensitive information about a VID which the user intended to conceal. A solution for protecting VIDs which focusses on application layer only is insufficient. It cannot prevent attacks based on information resulting from the communication layer.

The rest of the paper is structured as follows. First, the threats emerging by IP-based mobility in the context of multiple VIDs are presented in section 2. In section 3, the protection given by existing proposals is shortly discussed. Section 4 proposes a new approach protecting multiple VIDs. Finally, section 5 concludes and gives an outlook to future work.

2. IP-BASED MOBILITY IN THE CONTEXT OF MULTIPLE VIDS

In the following threat analysis it is generally assumed that a user has a single device which has a single interface with one IP address. This is a simplification compared to real-life, in which a user can have several devices with several interfaces. This simplification allows a clearer description of the problems without affecting the principle considerations and results. Moreover, it is assumed that IP addresses are globally routable and do not refer to the device, e.g., they do not have the link layer address encoded as may be done in IPv6.

In packet-based communication there are two basic pieces of information necessary: First, each device connected to the network needs an identifier for addressing which is unique in the addressing domain. Each packet carries this identifier.

MobiWac '04, October 1, 2004, Philadelphia, Pennsylvania, USA.
ACM 1-58113-920-904/0010.

Second, each packet has a locator attached which indicates the location to where it has to be delivered, i.e., the topological location of the destination device. In this paper, the terminology *identifier* and *locator* is adopted from the respective IETF discussions, e.g., in [6].

In contrast to the identifier, the device's locator is sensitive regarding privacy. In IP the topological location can be mapped to the geographical location with a certain accuracy. Furthermore, the locator is identifying the user's access network. Concerning fixed IP-based communication, one specific property is that the IP address serves as both, identifier and locator. There exist approaches in the IETF to alleviate this problem, e.g., [6]. Nevertheless, these approaches are neither standardized yet, nor can be anticipated to replace or enhance IP in a conceivable timeframe.

After a sound analysis, which can be found in the extended version of this paper [3] the threats to VIDs in fixed and mobile IP-based communication as shown in the following list are evolving. There are two main threats: Linking of different VIDs of one user (1. and 2.) and inference of personal information (3. and 4.). The threats are named by abbreviations. The first part indicates whether it is a link threat (Link) or an inference threat (Inf). The second one indicates whether it is a threat also appearing in the fixed scenario (F) or only in the mobile scenario (M). Inference threats have a third letter indicating whether the sensitive information is inferred from the locator (L) or from the identifier (I).

1. Linking of VIDs, threats in *fixed* scenario

- *LinkF:* identical data in context of VIDs
  Example: identical identifier, identical locator

2. Linking of VIDs, additional threats in *mobile* scenario

- *LinkM(1):* identical behavior of VIDs observed by identical patterns of identical 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 non-readable locators

3. Inference of information, threats in *fixed* scenario

- *InfFI:* inference from the identifier
  Example: home network of the VID if the identifier is a Mobile IP Home Address
- *InfFL:* inference from a single locator
  Example: location of the user using a VID at time of communication

4. Inference of information, additional threats in *mobile* scenario

- *InfML(1):* inference from several locators
  Example: location trace of a user using a VID over a period of time
- *InfML(2):* inference from behavior by locator changes
  Example: inference of activity by rate of locator changes

Generally, it is possible that an attacker gains a precise knowledge as well as an imprecise knowledge about a VID. A precise inference is possible, if obvious data is visible to the attacker. Often, this knowledge cannot be inferred precisely but only imprecisely with a certain probability. Then, the attacker only has a suspicion. Together with knowledge outside the communication system it is often possible to gain certainty. It is also possible to substantiate a suspicion by observing several states of the system.

3. ANALYSIS OF EXISTING PROPOSALS

Existing proposals for mobility management and privacy-aware communication are evaluated with respect to the threats of Section 2. Aspects not being related to these threats, e.g., performance issues, are beyond the scope of this paper. Protection is evaluated against communication partners as well as the mobility management system as potential attackers.

The argumentative analysis shows, that none of the existing proposals offers sufficient protection when used with multiple VIDs. Most of the proposals offer a certain level of protection against correspondent nodes as attackers but practically no protection against the mobility management system as potential attacker. This is because the mobility management system is assumed to be fully trusted. As motivated above, this assumption should be loosened in the future. Moreover, the threat of substantiating an imprecise suspicion is mostly not considered in current proposals. The full evaluation is presented in the extended version of this paper [3].

The shortcomings of protection can be explained by the fact that many evaluated proposals originally aim at different objectives than those of this paper, e.g., unobservability of communication. They all fulfill well their primary purpose for which they were invented. Here, it is analyzed how they could be used to protect against the specific threats in a mobile scenario with multiple VIDs per user, which is a new emerging scenario that was not yet considered in the design of those proposals. Moreover, several systems are not specifically proposed for mobile communication. Those systems are combined with Mobile IP for the evaluation.

4. NEW APPROACH FOR PRIVACY-PRESERVING MOBILE COMMUNICATION

In this section, an outlook to a new conceptual approach based on [2] is given. Figure 1, shows the basic scenario.

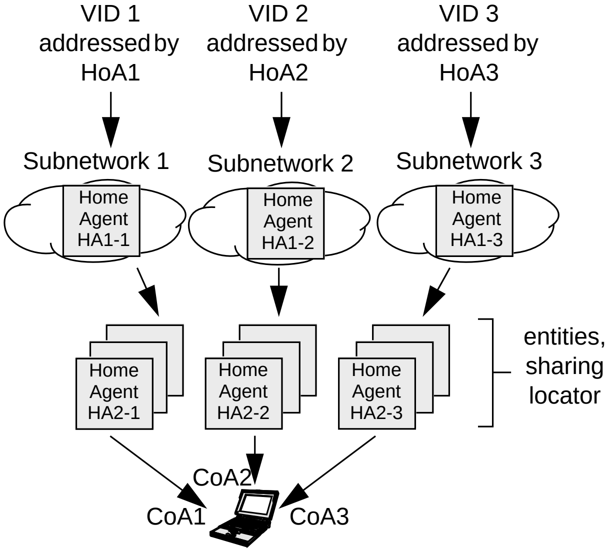

Figure 1. Architectural overview

A common vulnerability of existing proposals is inference of sensitive information from the identifier (InfFI). In this new approach, the identifier, which resembles a Mobile IP Home Address (HoA) is not from the user's home network, but from an arbitrary subnetwork of the Internet, thus not containing any sensitive information about the user. In order to protect against LinkF regarding Correspondent Nodes, the identifiers of different VIDs are chosen from different subnetworks each having a Home Agent (HA1-x) running. Thus, the user's fixed presence is no longer related to the real, physical home and the user has several different fixed presences.

It is assumed, that different subnetworks are operated by independent parties to distribute the sensitive information among them. Note, that a large number of providers is realistic in a system with an open philosophy.

Several proposed systems are prone to linking attacks by the mobility management system's entities. In order to eliminate these threats in the proposed approach, separate contexts are retained for each VID throughout the packet's path to the Mobile Node. The packets of each VID are forwarded to a different Home Agent on the second level (HA2-x). In order to protect against inference of sensitive information by knowledge about the HA2-x, these agents are also arbitrarily distributed in the network. Moreover, by having two entities in a row, it is achieved that no entity knows both, the identifier and the locator.

The separation of VID contexts duplicates the sensitive knowledge of the locator. Thus, protection of the locator becomes even more important than in simpler systems with only one entity knowing it.

Different care-of addresses (CoA) can be used for different VIDs. Thus, protection against LinkM(1) considering the mobility management as potential attacker is assured. Moreover, the locator is invisibly distributed across several parties. Only if it is needed, i.e., in case of a packet arriving for the respective VID, the locator is recombined. Technically, this can be achieved by secret sharing techniques [1], in which the sensitive information is split into several pieces which are all necessary to recombine the information but which do not contain any sensitive information when being observed alone. Thus, protection against LinkM(2), InfFL, InfML(1) and InfML(2) can be perfectly achieved during silent phases of a VID which often is the majority of the time.

To improve protection against the dynamic threats LinkM(2), InfML(1) and InfML(2) during communication times, the entity which is recombining and observing the locator (HA2-x) is changed frequently. Thereby, it is firstly not possible to gain a long trace of locators from which sensitive information can be inferred and secondly it is not possible to substantiate an imprecise suspicion about two VIDs assumed to be linked.

As compared to existing proposals the number of necessary entities can be decreased to a more acceptable number. This is possible by the invisible storage of the sensitive locator which allows an entity of the mobility management system to serve several VIDs of a user simultaneously as long as only one of them is communicating. Even if they communicate simultaneously, they can be linked only imprecisely–as different CoAs are used for different VIDs–and a fraudulent HA2-x cannot substantiate this link by several observations as the VIDs change their serving entities. The probability of this case to happen depends on the concrete usage scenario in the same way as the preciseness of the observed link depends on the anonymity set of the concrete scenario, i.e., how many different users can potentially have the observed similar CoAs. This allows the user to choose a trade-off between the number of necessary entities–which have to be paid in a real scenario–and the level of protection.

5. CONCLUSION AND FUTURE WORK

In this paper, the threats to VIDs caused by mobile IP-based communication were presented. It turned out that these are basically the threat of links between several VIDs of one user and inference of personal information of the user behind a VID. It was pointed out, that dynamics of mobile communication adds largely to the complexity of the challenge of solving future privacy needs.

With the weak points of existing proposals in mind, an outlook to a new approach protecting VIDs in mobile communication was given at the end. It allows the user a large freedom in controlling the trade-off between performance, scalability and privacy. As privacy protection always is a trade-off with performance, the exact quantification of this will be a future working area. Therefore, a detailed performance analysis has started. Moreover, the approach is going to be detailed and specified.

6. ACKNOWLEDGEMENTS

The author would like to thank Christoph Gauger for invaluable discussions. This work was partly funded by the German Research Foundation (DFG) through the Center of Excellence (SFB) 627.

7. REFERENCES

[1] Schneier, B. Applied Cryptography - Protocols, Algorithms, and Source Code in C (2nd edition). 2. Edition, John Wiley & Sons, Inc., 1996, ISBN: 0-471-12845-7.

[2] Hauser, C. A New Approach for Privacy-Preserving Communication by Combining Virtual Identities with Mobility Management. European Symposium on Research in Computer Security (ESORICS 2002) – Poster Session, Zurich, 2002.

[3] Hauser, C. Mobility Management Meets Privacy – the Failure of Existing Proposals and a New, Future-Proof Approach (Extended Version). Technical Report 49, Institute of Communication Networks and Computer Engineering, University of Stuttgart, August 2004, www.ikr.uni-stuttgart.de/~hauser/IB49.pdf.

[4] Hohl, F., Kubach, U., Leonhardi, A., Rothermel, K., Schwehm, M. Next Century Challenges: Nexus - An Open Global Infrastructure for Spatial-Aware Applications. In Proceedings of ACM MobiCom '99, pp. 249-255, Seattle, USA, August 1999.

[5] The DAIDALOS Project–Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services. http://www.ist-daidalos.org.

[6] www.ietf.org/html.charters/hip-charter.html.