Privacy Preserving Context Transfer in All-IP Networks

Giorgos Karopoulos, Georgios Kambourakis, and Stefanos Gritzalis

Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, GR-83200 Samos, Greece
{gkar,gkamb,sgritz}@aegean.gr

Abstract. In an all-IP environment, the concept of context transfer is used to provide seamless secure handovers between different administrative domains. However, the utilization of context transfer arises some privacy issues concerning the location and movement of users roaming between domains. In this paper we elaborate on these privacy issues and propose an alternative context transfer protocol that protects user's location privacy as well. In addition, assuming that the context carries a user identity in the form of a Network Access Identifier (NAI), we show how the employment of temporary NAIs can further increase the privacy of our scheme.

Keywords: Privacy, Context Transfer, NAI, all-IP networks, secure handover.

1 Introduction

Today, the uninterrupted continuation of the received services during handover between networks with different access technologies still remains an open issue. In order to have fast, secure handovers in such an all-IP terrain new methods were recently proposed, like OIRPMSA [1], MPA [2] and Context Transfer [3]. As discussed in [4], while these methods do succeed in minimizing the disruption caused by security related delays, it seems that little has been done to protect the end users privacy as well.

Whereas a lot of work has been done in privacy and location privacy in general, the authors are not aware of any previous work preserving location privacy in methods offering fast secure handovers in all-IP based networks. In this work we focus on the Context Transfer solution. We discuss and highlight the privacy issues arising from the employment of the Context Transfer Protocol (CTP) [3] and propose a solution towards solving these problems. We further extent our solution based on the observation that the NAI [5] is a suitable type of identity for networks that span across multiple administration domains. Since this applies to our case we use temporary NAIs as context's identity in order to increase the level of user's privacy. The result of our work is that the decision for user's identity and location disclosure is no longer left to the good will and intensions of the visiting networks and the user is not forced to trust the foreign domains but only his home domain with which he has signed a contract. The rest of this paper is structured as follows. In Section 2, some privacy issues are pointed out from the current functioning of the CTP. Section 3 presents the

V. Gorodetsky, I. Kotenko, and V.A. Skormin (Eds.): MMM-ACNS 2007, CCIS 1, pp. 390–395, 2007.

proposed solution to these privacy issues based on two concepts: Mobile Node (MN) submitted context and frequent NAI change. Section 4 provides a discussion about prerequisites and deployment issues for our protocol. Last section offers concluding thoughts and future directions for this work.

2 The Problem: Privacy Issues in Context Transfer Protocol

The way the CTP operates, as defined in the RFC 4067, arises some privacy issues. These issues concern primarily the end user and more specifically his location and movement between different administrative domains. The first observation has to do with the inner workings of the protocol itself. Every time a handover occurs, the previous Access Router (pAR) uses the CTP to send various context data blocks to the new Access Router (nAR). That is, for every handover the pAR and the nAR know where the user came from and where he is going. When these two ARs belong to the same administrative domain it goes without saying that the domain is aware of the movement of the MN inside its own network. However, when the two ARs belong to different administrative domains there is no reason for the pAR to know which the nAR is and the opposite. To sum up, with the use of the CTP for seamless handovers, every administrative domain is aware of the previous and the next administrative domain of the MN, without excluding itself. This means that every domain can track a part of the user's movement. Continuing from the last conclusion, the user's movement can be completely tracked, given that some administrative domains collude. Note, that this does not imply that all administrative domains in the path of the user movement are required to collude for such an attack, but every second domain in that path.

Another aspect of the location privacy problem when the CTP is in place is the type of the identifier used by the user/MN during the protocol negotiation to authenticate to the new administrative domain. The utilization of a static identifier like the MAC address of the MN or a globally used username of the user simplifies the work of a malicious passive observer. An obvious choice for all-IP networks that belong to different administrative domains is the use of a NAI. However, if the administrative domains collude, they can track the whole movement of the user only by the observation of the use of this static NAI. Furthermore, even when administrative domains do not collude there can be a location privacy breach, since every single domain can recognize an old user that returns to it. It is thus, more than obvious, that systems' logistic files can be anytime processed to disclose information about the whole history of movements of a specific user.

3 The Proposed Solution

The proposed solution protects the location privacy of users roaming between different administrative domains utilising the CTP to receive uninterruptible services during handover. Our solution is twofold and it is proposed that: (a) the context

should be submitted by the MN, and (b) there should be a frequent NAI change. The basic idea behind our scheme is that the user's sensitive information should only be known to the user himself and his home domain and no-one else, including the visiting domains. This is very important since the user has agreed and signed only one subscription contract; with his home domain.

3.1 Mobile Node Submitted Context

As it is stated in RFC 4067, the context is transferred between layer-3 entities from the old network domain to the new network domain. This way, a part of the MN user's route can be tracked. As already stated this is the case of a single domain tracking the movement of the user; if domains collude, then the full movement of the user can be tracked simply by using the information revealed by the CTP. One possible solution to avoid such problems is to have the MN submitting its own context to the network it is moving to. The complete abstract protocol steps are as follows: *Step 1* - The MN establishes a secure session with the AR of the new domain. This secure session must have the following properties: (a) it must be encrypted and (b) the AR must be authenticated to the MN. *Step 2* - The MN sends the context over the previously established protected channel. *Step 3* - The AR authenticates the MN and re-establishes the services based on the context. It is also assumed that the current domain has established some kind of trust relationships beforehand with the home domain. This way the authentication is processed locally based on an authentication token located in the context, which is digitally signed by the home domain.

The above procedure is the equivalent of a PEAP [6] or an EAP-TTLS [7] authentication and key establishment method using the context as user authentication means. The first phase of the PEAP or EAP-TTLS method is followed as is, e.g. a secure session is established with the use of the digital certificate of the AR. In the second stage the authentication of the user is taking place with the utilization of the credentials contained in the context. The key establishment phase could also be benefited by the context transfer since the context can contain security parameters i.e. cryptographic keys, supported suites, tokens, etc. The proposed method can be used in either a reactive or proactive scenario. In cases where a high QoS must be preserved, the aforementioned procedure could be executed proactively, that is before the MN actually moves to the new administrative domain. This situation is comparable to the pre-authentication procedure exercised in IEEE 802.11 or 802.16 networks. An example of a context transmitted by the MN is shown in Fig. 1. When the MN moves towards P3 the handover procedure starts. The MN establishes a secure channel with the nAR and through this channel transfers the context. As it can be easily noticed, the ARs do not play any role in the context transfer procedure and there is no communication between them. Also, they are not aware of each other in any way. One potential drawback of our method is the possible degradation of service during the handover process; however, this is left to be proved in a future work. The factors that lead to this are the use of asymmetric cryptography and the increased number of messages during the whole procedure.

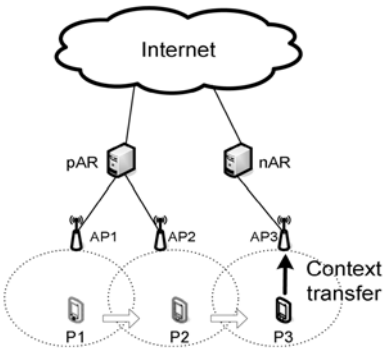

Fig. 1. MN submitted context

3.2 Frequent NAI Change

In this heterogeneous environment one way to identify the users is the use of NAI. Of course, the NAI can also be utilised in conjunction with the CTP. When the NAI concept is employed in the proposed way (MN submits the context) then the current domain or some colluding domains still can track the location of the user simply by observing the transmission of NAIs. More specifically, the current domain can always be aware when a single user was present in its network or when a user returns to it. When the domains collude things get worse since they can observe the exact route of a single user. The solution is based on the use of temporary NAIs and the frequent change of them. Thus: (a) The home domain is the only one that has the correspondence between the true identity of the user and the NAI assigned to him, (b) when a context is created for the user, it contains a temporary NAI. This temporary NAI uses as user_id a random unused string, which the home domain connects with the true identity of the user, and as domain_id the assigned domain_id. Each temporary user_id is used once for every single domain by one user at a time. When the user handovers to another domain (either new or previously visited) he must use a different user_id. The reuse of a temporary user_id by another user is not forbidden since the home domain is also aware of the date and time each user is using it. Therefore, the only sensitive information about the user that is revealed to foreign domains is the home domain of the user, and (c) after the completion of the handover of the MN to a new domain, the MN is using a secure channel (like a TTLS session) to contact its home domain and obtain a new temporary NAI. This way, when the user returns to a previous visited domain, the domain cannot recognize him.

Even if the correspondence between the true identity of the user and his NAI or any temporary NAI is revealed by accident or other reason, the user's past routes cannot be revealed without the help of his home domain. The obvious drawback of this method is the increase in the signaling between the domains. However, this is done after the completion of the handover and therefore has no real effect in the QoS perceived by the user during the handover. In Fig. 2 a message sequence diagram of the overall proposed solution is presented. The MN has an existing session with the pAR; when it wants to handover to the nAR it first establishes (proactively or reactively) a secure session with it. Then, through this secure session, it transfers the

context that will allow the MN to authenticate, establish session keys and re-establish the services it already uses. When the handover procedure is finished, the MN should contact its home domain in order to obtain some new credentials (for example a new temporary NAI) that will be used in its next handover.

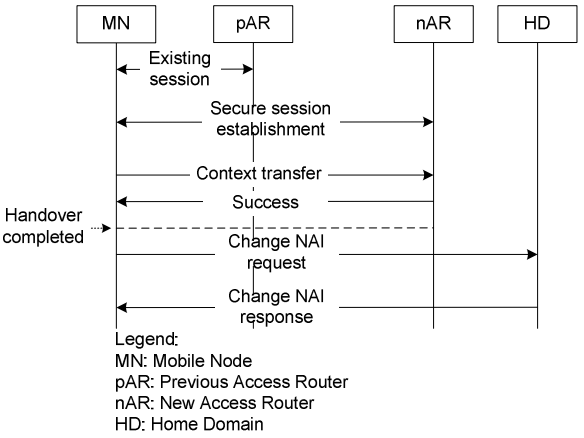

Fig. 2. Message sequence of our solution

4 Discussion

From the trust requirements point of view, the proposed solution has some prerequisites that are analogous to those of CTP. More specifically, CTP requires that trust relationships exist among the ARs and between the MN and each of the ARs (pAR and nAR). In our case, each AR should have trust relationships with the home domain of the roaming MN; since the MN also has trust relationships with its home domain, new trust relationships between the MN and each AR can be established on-the-fly. An important factor concerning the wide deployment of a protocol is the number of changes required in the already installed infrastructure. Taken into account the situation as it is today, our protocol requires a reasonable number of such changes which are comparable to those required for the deployment of the CTP. More specifically, in CTP the ARs should be able to transfer the context among them and interpret the contents of the context; the MN should also implement the CTP in order to be able to request the transfer of the context. In our proposal the ARs should only be able to interpret the contents of the context while the MN should be able to handle the context which it possesses according to the proposed protocol.

Another point of consideration is the protection of the context itself. Since in the proposed protocol the context is carried by the MN, actions must be taken so that the context cannot be altered by the user unnoticed. This implies that there should be a kind of digital signature in place ensuring the integrity of the transmitted context. The encryption of the context while stored in the MN is not a strict requirement since the information contained in it is already known to the user. However, having in mind that the MN is a portable device and thus it is easy to get lost or stolen, some care to

prevent tampering, unauthorized use, or fraud could be taken. One final remark about the context is its expiration. The time interval of expiration should be neither too large, containing expired information, nor too small, causing excessive signaling among the administrative domains. What is obvious for our protocol is that when the MN moves to a new domain the context is renewed since a new temporary NAI is requested. In any case, the expiration interval can be set by the network administrators and the current point of attachment (some AR) of the MN can warn it that its context has expired or is about to expire.

5 Conclusions

We have presented a novel solution that preserves user's location privacy when using the CTP which is currently employed by the state of the art methods for seamless secure handovers between different administrative domains. We showed that the standard way the protocol behaves arises some privacy issues and proposed an alternative protocol that alleviates these problems. Moreover, we have proposed how the use of the context in conjunction with a NAI can further enhance user's privacy. Part of our future work is to measure the delays incurred by our protocol. Preliminary analysis discloses that these times are expected to be tolerable with medium-end devices, achieving seamless handovers even to very demanding applications.

References

1. Xu, P., Liao, J., Wen, X., Zhu, X.: Optimized Integrated Registration Procedure of Mobile IP and SIP with AAA Operations. In: Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA), pp. 926–931 (2006)
2. Dutta, A., Fajardo, V., Ohba, Y., Taniuchi, K., Schulzrinne, H.: A Framework of Media-Independent Pre-Authentication (MPA). IETF Internet Draft, draft-ohba-mobopts-mpa-framework-03, work in progress (2006)
3. Loughney, J., Nahkjiri, M., Perkins, C., Koodli, R.: Context Transfer Protocol. RFC 4067 (2005)
4. Karopoulos, G., Kambourakis, G., Gritzalis, S.: Survey of Secure Handoff Optimization Schemes for Multimedia Services Over All-IP Wireless Heterogeneous Networks. IEEE Communications Surveys and Tutorials (to appear)
5. Aboba, B., Beadles, M., Arkko, J., Eronen, P.: The Network Access Identifier. RFC 4282 (2005)
6. Palekar, A., Simon, D., Salowey, J., Zhou, H., Zorn, G., Josefsson, S.: Protected EAP Protocol (PEAP) Version 2. IETF Internet Draft, draft-josefsson-pppext-eap-tls-eap-10, expired (2004)
7. Funk, P., Blake-Wilson, S.: EAP Tunneled TLS Authentication Protocol (EAP-TTLS). IETF Internet Draft, draft-ietf-pppext-eap-ttls-01, expired (2002)