Two Privacy Enhanced Context Transfer Schemes

Giorgos Karopoulos
University of the Aegean
Karlovassi, GR-83200
Samos, Greece
+30-22730-82246
gkar@aegean.gr

Georgios Kambourakis
University of the Aegean
Karlovassi, GR-83200
Samos, Greece
+30-22730-82256
gkamb@aegean.gr

Stefanos Gritzalis
University of the Aegean
Karlovassi, GR-83200
Samos, Greece
+30-22730-82234
sgritz@aegean.gr

ABSTRACT

Foreseeable 4G environments will extensively take advantage of the concept of context transfer to provide seamless secure handovers between different administrative domains. However, the utilization of context transfer comes with a cost in the users' privacy. The purpose of this paper is to elaborate on these privacy issues and propose two privacy enhanced context transfer schemes that alleviate these problems. In the first scheme the Mobile Node (MN) is responsible for the transmission of the context to the new domain. In the second scheme the Home Domain (HD) of the user forwards the context acting as a proxy between the old and the new domain. In addition, assuming that the most appropriate form of user identity for the context is the Network Access Identifier (NAI), we show how the employment of temporary NAIs can further increase the privacy of our schemes.

Categories and Subject Descriptors

C.2.1 [**Computer - Communication Networks**]: Network Architecture and Design – *Wireless Communication*

General Terms

Security

Keywords

Privacy; context transfer; Network Access Identifier; all-IP networks; secure handover.

1. INTRODUCTION

The advances in wireless communication technologies towards 4G networks and the wide use of mobile devices have enabled users to communicate with each other and receive a wide range of mobile wireless services through various types of access networks and systems everywhere, anytime. It is envisioned that in the near future mobile users will be able to use WLAN and UMTS networking in parallel. An open issue towards this direction is the uninterrupted continuation of the received services during handover between networks with different access technologies. In order to have fast, secure handovers new methods were recently proposed like Optimized Integrated Registration Procedure of Mobile IP and SIP with AAA operations (OIRPMSA) [3], Media – independent Pre - Authentication (MPA) [4] and Context Transfer [5]. As discussed in [6], while these methods do succeed in minimizing the disruption caused by security related delays, it seems that they do not take into consideration the protection of the end users' privacy at all.

It is true that a lot of work has been done in privacy and more specifically in location privacy; however, 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) [5] and propose two schemes towards solving these problems. In the first one the MN is responsible for the transmission of its own context, while in the second the HD acts as a proxy between the previous and the new administrative domain. We further extent our schemes based on the observation that the NAI [7] is a suitable type of identity for networks that span across multiple administration domains.

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 first scheme that tackles these privacy issues based on two concepts: Mobile Node (MN) submitted context and frequent NAI change. In Section 4 the second scheme which utilizes the HD as a proxy to perform the context transfer is presented. Section 5 provides a discussion about prerequisites and deployment issues for the proposed privacy preserving mechanisms. Last section offers concluding thoughts and future directions for this work.

2. THE PROBLEM: PRIVACY ISSUES IN CONTEXT TRANSFER PROTOCOL

The first observation has to do with the inner workings of the CTP 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 there are not many things that can be done to prevent the administrative domain from being aware of the movement of a single MN inside its own network. However, when the two ARs belong to different administrative domains there is no reason for

Q2SWinet'07, October 22, 2007, Chania, Crete Island, Greece.
Copyright 2007 ACM 978-1-59593-806-0/07/0010…$5.00.

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. Moreover, the complete movement of the user can be tracked, given that some administrative domains collude.

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 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, in the case that 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. SCHEME I

The first scheme protects the location privacy of users roaming between different administrative domains utilising the CTP. Our solution is twofold and it is proposed that: 1. the context should be submitted by the MN, and 2. there should be a frequent NAI change.

3.1 Mobile Node Submitted Context

One possible solution to protect the user's privacy is to have the MN submitting its own context to the network it is moving to. The complete abstract protocol steps are as follows:

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.
2. The MN sends the context over the previously established protected channel.
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 [8] or an EAP-TTLS [9] authentication and key establishment method using the context as user authentication means. 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.

Figure 1 illustrates both our schemes. In this figure an example of a context transmitted by the MN is shown (Scheme 1 Context transfer). When the MN moves towards P2 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.

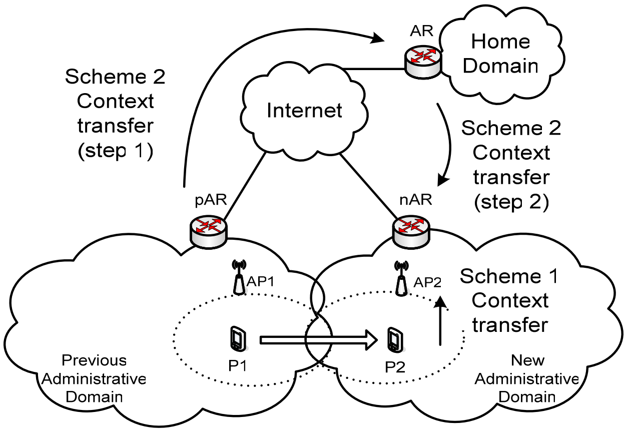
AR
Home Domain
Scheme 2 Context transfer (step 1)
Internet
Scheme 2 Context transfer (step 2)
pAR
nAR
AP1
AP2
Scheme 1 Context transfer
Previous Administrative Domain
P1
P2
New Administrative Domain

Figure 1. Privacy preserving context transfer schemes.

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.

3.2 Frequent NAI Change

As it has already been discussed in Section 2, the use of NAI in conjunction with the CTP is a source of possible privacy threats for the user. The solution is based on the use of temporary NAIs and the frequent change of them:

- The home domain is the only one that has the correspondence between the true identity of the user and the NAI assigned to him.
- 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.
- 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, even if the user returns to a previous visited domain, the domain cannot recognize him.

An advantage of our method is that 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 Figure 2 a message sequence diagram of the first proposed scheme 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 and the new session has been established, 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.

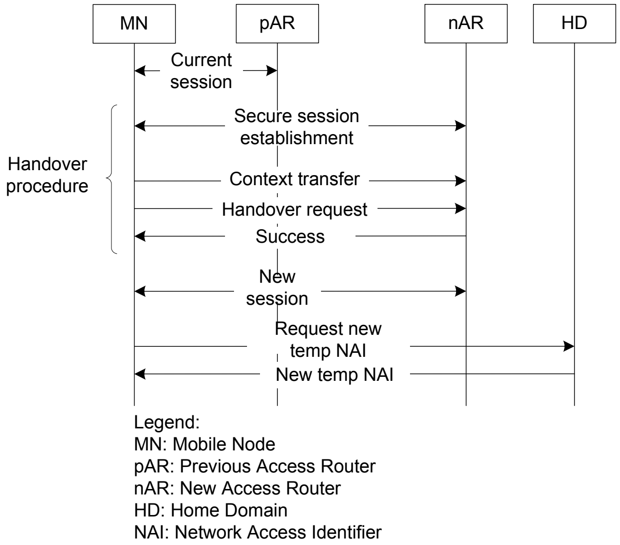

Figure 2. Message sequence of scheme I.

4. SCHEME II

The second proposed scheme protects the location privacy of users who roam between different administrative domains using the CTP for more demanding services than the abovementioned ones. Again, this solution has two main points: 1. the context is transferred through the Home Domain (HD), and 2. there is a frequent NAI change as well.

4.1 Home Domain Submitted Context

In this scheme the HD acts as a proxy between the pAR and the nAR executing the context transfer prior to the MN's movement to the new domain in order to protect the privacy of the MN's user. Here the frequent NAI change is tightly bundled with the context submission procedure. The complete abstract protocol steps are as follows:

1. The MN realizes that it is about to handover to a new AR that belongs to a different administrative domain from the current one. Thereby, it establishes a secure session with its HD and requests from it to execute a context transfer to the new administrative domain on behalf of the MN. This request contains the current temporary NAI of the MN.
2. The HD requests the context of the MN from the pAR using the MN's current temporary NAI.
3. The HD changes the temporary NAI in the context and forwards the context to the nAR.
4. The HD uses the established secure session with the MN and forwards the new temporary NAI to it.
5. The MN handovers to the nAR using its new temporary NAI.
6. The nAR authenticates the MN and re-establishes other services based on the context. It is also assumed that the current domain has established some kind of trust relationships beforehand with the HD. This way the authentication is processed locally based on an authentication token located in the context, which is digitally signed by the HD.

An example of a context transfer based on the second scheme is shown in Figure 1 (Scheme 2 Context transfer). When the MN moves towards P2 the handover procedure starts. The MN establishes a secure channel with the HD and requests from it to transfer the MN's context from the pAR to the nAR. As it is illustrated in Figure 1, the HD first retrieves the context from the pAR (step 1), it makes the necessary modifications to it and then forwards it to the nAR (step 2). When the context transfer is completed, the HD sends the MN its new temporary NAI. The protocol is finished when the MN handovers to the nAR. As in the first scheme, the ARs do not play any role in the context transfer procedure and there is no communication between them; therefore, they are not aware of each other in any way.

Figure 3 illustrates a message sequence diagram of our second scheme. At first the MN has an existing session with the pAR. When the MN decides to handover to the nAR it first establishes a secure session with its HD. Using this secure session, the MN requests from the HD to perform the context transfer acting as a proxy. The HD retrieves the context from the pAR (step 1), replaces the current temporary NAI with the new one and forwards the new context to the nAR (step 2). Through the previously established secure session the HD also forwards the new temporary NAI to the MN. After these steps the MN can handover to the new domain using the current (active) context.

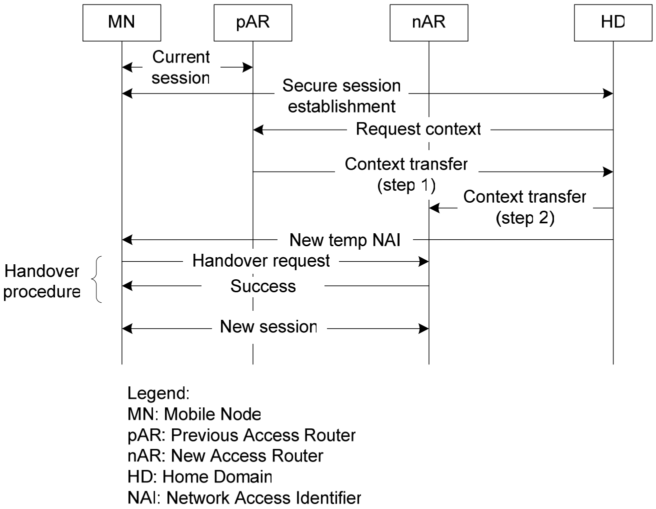

Figure 3. Message sequence of scheme II.

5. DISCUSSION

This section provides some points concerning the deployment of our protocols. From the trust requirements point of view, the proposed solutions have 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 two schemes require 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. Also, in the first scheme the MN should be able to handle the context which it possesses according to the proposed protocol, while in the second scheme the HD should be able to play the role of a proxy between the previous and the new domain.

Another point of consideration that applies only to the first scheme 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. The second scheme does not suffer from such a threat since the HD communicates with other domains through secure channels (e.g. usually IPSec or TLS).

A brief comparison of the two proposed schemes would lead to the conclusion that each one is suitable for different types of applications. The first scheme poses a small amount of load to the HD while at the same time takes longer to handover to a new administrative domain. This makes it more suitable to applications with less strict demands or applications that can tolerate longer delays during the handover procedure. The second scheme requires the exchange of more messages but it is expected to have better performance during the handover. Therefore the second scheme will be more useful towards seamless handovers for demanding applications like multimedia delivery.

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 both schemes 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.

6. CONCLUSIONS

We have presented two novel schemes that preserve 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 two alternative protocols that alleviate these problems. Moreover, we have proposed how the use of the context in conjunction with a NAI can further enhance user's privacy.

Since our schemes involve asymmetric cryptography and increased signaling, part of our future work is to measure the delays incurred by both of these schemes. Preliminary analysis discloses that these times are expected to be tolerable with medium-end devices, thus assisting towards achieving seamless handovers even to very demanding applications like multimedia.

7. REFERENCES

[1] Perkins, C., IP Mobility Support for IPv4, *RFC 3344*, August 2002.

[2] Schulzrinne, H. and Wedlund, E. Application-layer mobility using SIP, *SIGMOBILE Mobile Computing and Communications Review*, Vol. 4, No 3, pp. 47-57, July 2000.

[3] Xu, P., Liao, J., Wen, X. and Zhu, X. Optimized Integrated Registration Procedure of Mobile IP and SIP with AAA Operations, *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*, pp. 926-931, 2006.

[4] Dutta, A., Fajardo, V., Ohba, Y., Taniuchi, K. and Schulzrinne, H. A Framework of Media-Independent Pre-Authentication (MPA), *IETF Internet Draft, draft-ohba-mobopts-mpa-framework-03*, work in progress, October 2006.

[5] Loughney, J., Ed., Nahkjiri, M., Perkins, C., and Koodli, R. Context Transfer Protocol, *RFC 4067*, July 2005.

[6] Karopoulos, G., Kambourakis, G. and Gritzalis, S. Survey of Secure Handoff Optimization Schemes for Multimedia Services Over All-IP Wireless Heterogeneous Networks, To appear in *IEEE Communications Surveys and Tutorials*, 2007.

[7] Aboba, B., Beadles, M., Arkko, J., and Eronen, P. The Network Access Identifier, *RFC 4282*, December 2005.

[8] Palekar, A., Simon, D., Salowey, J., Zhou, H., Zorn, G. and Josefsson, S. Protected EAP Protocol (PEAP) Version 2, *IETF Internet Draft, draft-josefsson-pppext-eap-tls-eap-10*, expired, October 2004.

[9] Funk, P. and Blake-Wilson, S. EAP Tunneled TLS Authentication Protocol (EAP-TTLS), *IETF Internet Draft, draft-ietf-pppext-eap-ttls-01*, expired, February 2002.