EAP-Kerberos: A Low Latency EAP Authentication Method for Faster Handoffs in Wireless Access Networks

Saber ZRELLI\(^{(a)}\), Nonmember, Nobuo OKABE\(^{(b)}\), Member, and Yoichi SHINODA\(^{(c)}\), Nonmember

SUMMARY
The wireless medium is a key technology for enabling ubiquitous and continuous network connectivity. It is becoming more and more important in our daily life especially with the increasing adoption of networking technologies in many fields such as medical care and transportation systems. Although most wireless technologies nowadays provide satisfying bandwidth and higher speeds, several of these technologies still lack improvements with regard to handoff performance. In this paper, we focus on wireless network technologies that rely on the Extensible Authentication Protocol for mutual authentication between the station and the access network. Such technologies include local area wireless networks (IEEE 802.11) as well as broadband wireless networks (IEEE 802.16). We present a new EAP authentication method based on a three party authentication scheme, namely Kerberos, that considerably shortens handoff delays. Compared to other methods, the proposed method has the advantage of not requiring any changes on the access points, making it readily deployable at reasonable costs.

key words: wireless, authentication, handoff, performance

1. Introduction

Handoff latency can be defined as the period of time starting from the instant when the station last received data packets from its old access point until the instant when it starts receiving data packets from the new access point. Handoff delays are high in actual deployments and seamless handoff is a property that is still missing in most wireless technologies. The motivation behind seamless handoffs is to prevent service disruption when a wireless station changes of access point. The delay introduced by the handoff procedure translates into positive jitters which can impact the quality of service in real time applications such as voice over IP (VoIP) and multimedia streaming.

Handoff latency has long been an acknowledged issue in wireless networks. Some of the experimental studies\(^{[1],[2]}\) have attributed the handoff delay in wireless local area networks (IEEE 802.11\(^{[3]}\)) to the scanning phase during which a wireless station discovers neighboring access points. As we have shown in a previous work\(^{[4]}\), authentication delays during handoff may introduce substantial delays especially when there is a large network latency between authentication servers and access points.

The Extensible Authentication protocol (EAP) is the main component of the standard AAA (Authentication Authorization and Accounting) framework for network access control. In these frameworks, EAP authentication delays become an issue especially in roaming situations. The authentication of a roaming station using EAP requires message exchange between the AAA server of the visited network and the AAA server of the station’s home network. Since these inter-domain exchanges occur over the Internet, they are subject to degradations such as packet loss and network delays thus increasing the overall authentication time. When the station changes of access point, the same authentication procedure takes place again, disrupting user traffic at each handoff.

In this work, we designed and evaluated a wireless authentication method based on the Kerberos authentication protocol\(^{[5]}\) that addresses handoff delay issues in wireless access networks that rely on the EAP authentication framework (such as IEEE 802.11\(^{[3]}\) and IEEE 802.16\(^{[6]}\)). Our approach leverages the highly prized performance and simplicity characteristics of Kerberos to achieve superior performance compared to legacy EAP authentication methods. In the same time, the proposed method has high levels of trustworthiness since it inherits the security strengths of the Kerberos authentication protocol.

There are several aspects in the design of the Kerberos protocol that make it suitable for use as the underlying authentication mechanism in wireless networks where handoff performance is needed. The first aspect is that the Kerberos protocol uses symmetric key cryptography which consumes much less computing resources and hence introduces less delays compared to common methods based on public key cryptography\(^{[7]}\). Second, the use of Tickets\(^{[5]}\) in Kerberos allows the station to perform fast re-authentication with the local authentication server, without the need for contacting any remote entity, even if the station is in a roaming situation.

The approach proposed in this paper has two main advantages when compared to existing works; First, the proposed method is link layer independent and is applicable to more communication technologies since it only extends the EAP authentication layer. Second, the proposed approach does not introduce changes in the role of the access point and does not require upgrades in the wireless infrastructure besides the back-end authentication servers, which makes it readily deployable with minimal costs.
The paper is organized as follows; Sect. 2 provides background information about the handoff procedure in wireless access networks. As a study case, we will provide an overview of the IEEE 802.11 handoff process as specified in the IEEE 802.11i standard [8]. In Sect. 3, we provide an overview of the Kerberos authentication protocol. In Sect. 4, we introduce the EAP-Kerberos authentication method. In Sect. 5, we provide performance evaluation results of the EAP-Kerberos method and compare it with a legacy EAP authentication method (EAP-PEAPv0). In Sect. 6, we discuss related works and compare them to the proposed method. In Sect. 7, we perform security analysis of the EAP Kerberos method and explain how it complies with IETF security requirements for EAP authentication and keying architectures.

2. Handoff Process in Wireless Access Networks: The IEEE 802.11 Case

The IEEE 802.11 specification uses the Extensible Authentication Protocol for performing mutual authentication between wireless stations and the access network [8]. Throughout this research, we used IEEE 802.11 as a study case since it is a good representative of the class of wireless network technologies that can be subjected to handoff latencies caused by EAP authentication delays.

The IEEE 802.11i standard [8] specifies the necessary steps for a wireless station (STA) to associate and start sending and receiving data traffic through a target access point (AP). The handoff process as defined in IEEE 802.11i consists of four logical phases; Scanning, Association, IEEE 802.1X [9] authentication, and Link layer key establishment.

The scanning phase allows the STA to discover neighboring APs in order to select a suitable handoff candidate. During the scanning phase, the STA collects information about the security capabilities of the target AP. The next phase consists of establishing a IEEE 802.11 association. The association procedure starts by an Open Authentication System Exchange based on the null authentication algorithm, followed by an Association Exchange. The Association Exchange allows the target AP to disassociate the STA from the previous AP and the negotiation of authentication and cipher-suite properties between the STA and the target AP. The scanning and association phase are depicted in Fig. 1.

The establishment of an association does not allow the STA to gain network access yet. It only allows the AP to initiate IEEE 802.1X port control. After successful association, the STA will be able to exchange IEEE 802.1X frames with the AP and other elements in the distribution system. However, the STA's regular data frames will be blocked until the STA is authenticated and the data frames are encrypted using a key freshly shared with the AP. For this reason, the STA needs to authenticate and share a key with the AP using the Extensible Authentication Protocol (EAP) [10] and IEEE 802.1X. During EAP authentication, the AP acts as a pass-through between the STA and a back-end authentication server. As shown in Fig. 2, EAP packets are transported over IEEE 802.1X between the AP and the STA on one side, and using a AAA (Authentication Authorization and Accounting) protocol such as RADIUS [11], [12] or Diameter [13], [14] between the AP and the authentication server. After a successful authentication, the STA and the authentication server derive a shared key called Master Session Key (MSK). Finally, the the back-end authentication server sends the MSK to the AP.

The last phase of the handoff process consists of establishing link layer encryption keys called Transient Session Keys (TSKs) between the STA and the AP. These encryption keys will allow the STA to exchange regular data frames with the access network through the controlled IEEE 802.1X port. To derive the TSKs from the MSK, the STA and the AP perform a what is called the four-way handshake [8].

3. The Kerberos Authentication Protocol

Kerberos [5] is a widely deployed authentication system.
The authentication process in Kerberos involves principals and a Key Distribution Center (KDC). The principals represent users and services registered in a Kerberos domain or realm. The KDC maintains a database of principals and shares a secret key with each one of them.

In order to access an actual service, the client must submit valid Kerberos credentials to the service. In the following, we present the Kerberos credentials and explain how they are obtained and used to authenticate users to services.

### 3.1 Kerberos Credentials

In order to be authenticated to access a certain service, the client must submit credentials that consist of two components referred to as Ticket and Authenticator. A Ticket is a message created by the Kerberos key distribution center and encrypted using the secret key of the desired service. It contains information about the client and a secret session key. When a service receives a Ticket, it can decrypt it using its secret key, shared with the KDC, and obtain the secret session key. In order to prove its identity to the service, the client must prove that it knows the session key included in the Ticket. This is done by means of the Authenticator which contains information about the client and must be encrypted using the secret session key. The service authorizes the client after successfully decrypting and validating the authenticator using the secret session key obtained from the Ticket.

In summary, the client must obtain a Ticket and the associated secret session key (needed to build the Authenticator) from the KDC in order to access a certain service.

### 3.2 Kerberos Exchanges

The Kerberos protocol specifies three exchanges, the Authentication Server (AS) exchange, the Ticket Granting Service (TGS) exchange and the Client Server (AP) exchange. The three exchanges are depicted in Fig. 3. The AS exchange allows the client to obtain credentials that it can use to prove its identity to the KDC. These credentials consist of a Ticket referred to as Ticket Granting Ticket (TGT), and the associated session key referred to as TGS session key. The AS exchange is initiated by the client by issuing an AS Request message (AS-REQ), to which the KDC replies with an AS Reply message (AS-REP) containing the TGT and the session key encrypted using the client’s secret key.

The TGS exchange, on the other hand, allows the client to authenticate to the KDC using the TGT and obtain a Ticket for a certain service. For that, the client issues a TGS Request message (TGS-REQ) that contains the TGT and an Authenticator encrypted using the TGS session key. The TGS-REQ also contains the name of the service that the client wants to access. After validating the TGT and the Authenticator, the KDC issues a Ticket for the client and sends it along with the associated session key in a TGS Reply message (TGS-REP). The newly generated session key is protected using the TGT session key shared by the client and the KDC.

Finally, the AP exchange is performed between the client and the service to authenticate the client before granting it access to the resources. The client initiates the authentication by issuing an AP Request message (AP-REQ) that contains a Ticket for the service and an Authenticator. After validating the credentials the service authorizes the client, and optionally sends an AP Reply message (AP-REP) to achieve mutual authentication.

### 4. The EAP Kerberos Authentication Method

#### 4.1 Overview

The network access control architecture proposed in this paper relies on the ticket caching mechanism of the Kerberos authentication protocol to improve handover performance in roaming situations.

The proposed authentication mechanism details how to use a Kerberos Key distribution center in collaboration with existing RADIUS authentication servers to authenticate wireless stations using the Kerberos authentication protocol.

Traditionally in a roaming scenario, each time the station changes of access point, the station’s home RADIUS server is contacted to perform mutual authentication between the station and the new access point. The inter-domain message exchange between the visited network’s RADIUS server and the home network’s RADIUS server results in handover delays that can cause packet loss and degradation in the quality of service [4].

The EAP-Kerberos method mitigates handover delays by eliminating the need for contacting servers in the home network when the roaming station performs a handover.

As illustrated in Fig. 4, in order to authenticate a roaming station using EAP-Kerberos, the station starts by obtaining authentication credentials (TGT) from its home Kerberos key distribution center in the station’s home network. The access point and the RADIUS server of the visited network will relay the Kerberos messages between the station and the home KDC (1). Using the TGT that it ob-
tained from the home KDC, the station performs a TGS ex-
change with the KDC of the visited access network (2) to
obtain a service ticket. This exchange is also relayed by the
access point and the RADIUS server of the visited network.
The station then uses the service ticket in an AP exchange
to perform mutual authentication with the RADIUS server
of the visited network (3).

When the station changes of access point, the same ser-
vice ticket obtained during the initial authentication phase is
used in an AP exchange to authenticate with the RADIUS
server of the visited access network (4) and gain network
access through the new access point. Since the only entities
involved in re-authenticating the station are located in the
same access network, the re-authentication exchange is far
less exposed to network latency and packet loss compared
to the initial authentication which involves communication
with entities located in the station’s home access network.

The EAP-Kerberos method requires the station to pos-
sess a Kerberos login and password pair delivered by its
home network. Roaming stations may use their Kerberos
login and password pair to perform EAP-Kerberos authen-
tication in a visited network if their home network has an
inter-domain agreement with the visited network. The EAP-
Kerberos method also requires that all entities involved in
the authentication (EAP peer, Server and KDC) to have
loosely synchronized clocks. In most Kerberos implementa-
tions, the clock skew is configurable and is generally
about 5 minutes. This requirement comes from the fact that
Kerberos servers use a technique based on loosely synchro-
nized clocks, replay cache and time-stamps for detecting re-
played messages.

4.2 Network Access Zones

Our approach for using Kerberos for network access con-
control is based on the notion of Network Access Zones that we
define as a collection of access points managed by a single
authentication server. A set of network access zones that
belong to the same provider constitutes an Access Network.
Although an average sized access network may consist of
a single network access zone, the partitioning of the access
network into different zones is important for larger access
networks such as those deployed by commercial wireless ac-
cess providers. Generally, the use of multiple zones in large
access networks makes management easier and ensures a
scalable infrastructure.

To each network access zone corresponds a Kerberos
service registered in a Kerberos key distribution center man-
aged by the access network. An authentication server man-
aging a certain zone is able to authenticate wireless stations
through a Kerberos AP exchange over EAP. During the AP
exchange, the authentication server validates AP-REQ mes-
sages built using Kerberos Tickets for the service principal
that represents the network access zone. For this purpose,
the authentication server uses the zone’s secret key, trans-
ferred from the KDC to the authentication server using an
off-line secure channel to decrypt the Kerberos service tick-
et.

In order to gain network access within a zone, the sta-
tion must obtain a service Ticket for the local zone and
present the Ticket to the zone’s authentication server. The
EAP-Kerberos method described hereafter specifies how the
station perform these two operations.

4.3 EAP-Kerberos Packet Format

As depicted in Fig. 5, EAP-Kerberos packets contain the
standard EAP fields [10]: Code, Identifier, Length and Type,
as well as EAP-Kerberos specific fields. The additional
fields are as follows:

- The Kerb-Type field, which carries an integer value that
  specifies the type of EAP-Kerberos message and the
  Kerberos payload carried in the message if applicable.
- The Reserved field which is left for future use.
- The EAP-Kerberos packet may contain one or more of
  the Type-Length-Value (TLV) fields listed in Table 1.
4.4 EAP-Kerberos Operations

Authentication using Kerberos credentials is implemented as an EAP method. The station (hereafter referred to as ‘STA’) and the authentication server negotiate the EAP-Kerberos method as they would do for any legacy EAP method; After the STA issues an EAP-Identity Response message, the authentication server issues the first message of the EAP-Kerberos method. If the authentication server chooses another method, the client can use an EAP NAK [10] message to explicitly request the use of the EAP-Kerberos method.

The first message in the EAP-Kerberos authentication exchange is issued by the authentication server. This message includes the Kerberos realm name as well as the identification of the local network access zone (REALM and ZONE in Fig. 6). These two information together constitute the local zone’s Kerberos principal name that uniquely identifies it within the global Kerberos name space. This information is carried in a Kerberos-Principal TLV as described in Sect. 4.3.

Upon reception of this first message, the STA checks whether it has a Kerberos service Ticket in its credential cache for the local zone. If such Ticket exists, the STA initiates an AP Exchange over EAP with the authentication server managing the local zone. If the STA does not have a Ticket for the zone, but has a Ticket Granting Ticket for the local zone’s Kerberos realm, then the STA must acquire a Ticket by performing a TGS Exchange with the Key Distribution Center where the zone is registered. The TGS exchange is relayed by the local zone’s authentication server between the STA and the Kerberos KDC. The authentication server extracts the TGS-REQ message from the EAP-Kerberos message issued by the STA and sends it to the Kerberos KDC. The reply message from the KDC is sent back to the STA in an EAP-Kerberos message. After obtaining the service Ticket, the STA can perform an AP Exchange with the authentication server.

If the STA does not have a service Ticket for the zone nor a TGT for the local realm, then it first needs to obtain a TGT. The process of obtaining a TGT for the local realm depends on whether the STA is in its home network or in a visited network. In the former case, the STA uses an AS exchange with the Kerberos KDC of the home network to obtain the TGT. In the latter case, the STA first gets a TGT for its home Kerberos KDC, then performs Kerberos a cross-realm TGS exchanges as specified in [5] to obtain a TGT for the KDC of the visited network.

When a STA performs a handoff from an access point to another, it follows the same procedure described in the previous paragraphs. In the following, we provide more details on how the EAP-Kerberos method is bootstrapped and how it works in different handoff scenarios.

![Diagram showing the EAP-Kerberos authentication process](image-url)

Fig. 6 Full EAP-Kerberos authentication in the home access network.
4.4.1 Full EAP-Kerberos Authentication in the Home Access Network

The first case we consider is when the STA is accessing a network access zone that is in the STA's home network. If the STA does not possess any cached Kerberos credentials for network access, then it needs to perform a full EAP-Kerberos authentication, meaning that it must perform all of the three Kerberos exchanges (AS, TGS and AP) with the Kerberos KDC and the authentication server managing the network access zone.

As shown in Fig. 6, the STA receives the Kerberos realm name as well as the current zone's principal name in the initial EAP-Kerberos message issued by the zone’s authentication server. Since the STA does not have any credentials yet, it first obtains a TGT using an AS Exchange relayed by the access network infrastructure (Access point and authentication server). The EAP-Kerberos message carrying the AS-REQ message also contains the Kerberos realm name of the home KDC. This information, carried in a Kerberos-Realm TLV, will be used by the RADIUS server to locate the Kerberos KDC to which the Kerberos message must be forwarded. In practice, IP addresses of Kerberos Key Distribution Centers are resolved from Kerberos realm names using DNS SRV records [16] or mappings using static configuration files. After obtaining the TGT, the STA requests a service Ticket for the service “knas/zone1.domain.com@DOMAIN.COM”. For this, the STA performs a TGS exchange with the Kerberos KDC of the current zone. As with the AS exchange, the TGS exchange is relayed by the access network. Finally, the STA performs an AP exchange with the RADIUS authentication server in order to be authenticated and authorized for network access. After the AP exchange is completed, the STA issues a FINISH message, which is an acknowledgement message that does not contain any Kerberos payloads, to indicate to the RADIUS authentication server that mutual authentication has been established. The authentication server then sends keying material (EAP Master Session Key) to the AP. Finally, the STA and the AP perform the four-way handshake to derive Transient Session Keys [8] from the MSK.

4.4.2 Intra-Zone Handoff

The first handoff scenario we consider is when the mobile STA performs a handoff within the same network access zone. In this case, the STA does not need to acquire new credentials (unless the Ticket for the current zone has expired). The authentication for network access through a new access point in the same zone only requires an AP exchange with the local authentication server.

As shown in Fig. 7, the authentication, including all EAP messages, uses 3.5 round trips. All messages are exchanged within the zone and do not involve entities in remote locations.

4.4.3 Inter-Zone Handoff

When the STA moves across network access zones, it may need to acquire a new Ticket for the new zone. If the new zone belongs to the same access network (meaning it is registered in the same Kerberos KDC) as the previous zone, the STA can re-use the TGT for the local realm to obtain a service Ticket for the new zone. The STA can then authenticate with the local RADIUS authentication server through an AP exchange. This scenario, as shown in Fig. 8, requires one additional round-trip (for a total of 4.5) in comparison to the intra-zone handoff scenario.

4.4.4 Full EAP-Kerberos Authentication in a Visited Access Network

When the STA moves to an access network that is different from its home access network, the STA may need to perform Kerberos cross-realm operations to obtain a TGT for the Kerberos KDC of the visited network. As shown in Fig. 9, after obtaining the TGT, the STA performs the usual TGS and AP Exchanges with the local KDC to obtain a service Ticket for the new zone and authenticate with the corresponding authentication server.

The Kerberos cross-realm authentication for obtaining the TGT depends on the type of trust relationship between the STA’s home Kerberos realm and the Kerberos realm of the visited access network. Figure 9 illustrates the exchanges when the two Kerberos realms have a direct trust relationship. The procedure for obtaining a TGT for a visited Kerberos realm, known as cross-realm authentication, is specified in [5].

In the case where the visited access network and the home access network have an established cross-realm trust, the STA can obtain a TGT for the visited access network through a single TGS exchange with its home KDC.
In case there is no direct trust relationship between the home network and the visited network, Kerberos cross-realm authentication involving intermediary realms will take place [5]. It should be noted that the cross-realm authentication mode can become unreliable and may introduce delays if the number of intermediary KDCs increases. Currently, the Kerberos cross-realm authentication model is under investigation within the IETF [17] and there exist some
proposals [18], [19] for using public key cryptography to enable dynamically establish direct trust relationships between Kerberos KDCs.

5. Performance Evaluation

In order to assess the performance of the EAP Kerberos authentication method, we have implemented the full specification of our proposal and evaluated the authentication delays in a test-bed. For comparison purpose, we used the EAP-PEAPv0/MSCHAPv2 [20] authentication method in the same test-bed and results from both methods were compared.

5.1 The Experiment Test-Bed

We deployed a test-bed that allowed us to implement network access control in roaming scenarios. The test-bed consisted of two access networks, each representing a different network access zone. A different Kerberos realm and Kerberos Key Distribution Center is associated to each access network. A RADIUS authentication server is also deployed in each access network to handle EAP authentications of wireless stations.

In order to emulate network delays, we used the Linux netem utility. The resulting test-bed was equivalent to the reference architecture depicted in Fig. 10.

We implemented the EAP-Kerberos method by extending the open-source hostapd RADIUS server and the wpa_supplicant EAP supplicant. For the EAP-PEAPv0 authentication method, Microsoft Windows 2003 server’s Internet Authentication Server (IAS) was used. The wireless station is a Pentium 3 computer with 2 GB of RAM and a downscaled frequency of 600 MHz. The authentication servers consisted of Pentium 3 computers at 1 GHz with 520 MB of RAM.

5.2 Experimental Results

For both EAP-Kerberos and EAP-PEAPv0/MSCHAPv2, four experiments were carried out. First, two experiments consisting in full authentication in the home network and in the visited network were carried out (Full EAP-Kerberos authentication in the home network and in visited networks is depicted in Figs. 6 and 9 respectively). Then, experiments consisting in re-authentication in the home network and re-authentication in visited networks were carried out (EAP-Kerberos intra-zone re-authentication is depicted in Fig. 7). The EAP traffic generated by the experiment was captured then processed to produce the following performance results.

5.2.1 Analysis of Authentication Delays

- Full authentication delay in the home network and in visited networks: As depicted in Figs. 11 and 12. For the EAP-Kerberos method, the incurred delays for full authentication in the home network and in the visited network are about 220 ms and 300 ms respectively. For the EAP-PEAPv0/MSCHAPv2 authentication method, the figures are 220 ms and 380 ms. The EAP-Kerberos method outperforms the EAP-PEAPv0/MSCHAPv2 when the station is in a visited network. However, since the full authentication does not take place during handovers, the delays incurred from the inter-domain message exchanges are not relevant.

- Re-authentication delay in the home access network: Figure 11 shows authentication delays when using the EAP-Kerberos method. It can be noticed that re-authentication delay with EAP-Kerberos is the same whether the wireless station is at home or in a roaming situation accessing a visited network (about 25 ms). When comparing re-authentication delays of the EAP-PEAPv0 method Fig. 12, with re-authentication delays of the EAP-Kerberos method, we can notice that both methods offer similar performance (25 ms) when the station re-authenticates in the home access network.

- Re-authentication delay in visited access networks: In roaming situations, when the station is in a visited access network, re-authentication delay remains the same at acceptable levels (25 ms) for EAP-Kerberos. However, re-authentication latency increased five times from 25 ms to around 120 ms for EAP-PEAPv0. The poor performance of EAP-PEAPv0 and legacy EAP methods in roaming scenarios compared to EAP-Kerberos is due to the fact that these methods require message exchange with the station’s home RADIUS server for performing re-authorizations in visited access networks while the EAP-Kerberos doesn’t. The reason for this is that, as explained in Sect. 4.1, after obtaining a cross-realm TGT from the home KDC, and a Service Ticket for the visited RADIUS server, the roaming station can use

---

†[http://www.linux-foundation.org/en/Net:Netem](http://www.linux-foundation.org/en/Net:Netem)

††[http://hostap.epitest.fi/hostapd/](http://hostap.epitest.fi/hostapd/)

†††[http://hostap.epitest.fi/wpa_supplicant/](http://hostap.epitest.fi/wpa_supplicant/)
the same Service Ticket for authenticating in the visited access network without involving any entities in the home domain.

5.3 Decomposition of Handoff Delays into Station Side and Infrastructure Side Delays

In the previous paragraphs, we examined total authentication delays when using EAP-Kerberos compared to the EAP-PEAP/MSCHAP method. In this section, we analyze authentication delays in more details by examining the delays caused by station side processing and the delays caused by the infrastructure which include delays introduced by the RADIUS and Kerberos servers as well as delays introduced by network latency.

Figures 13 (a) and (b) show the decomposition of authentication delays during an EAP-Kerberos full authentication in the home network and in visited networks respectively.

Figure 13 (a) shows that station side processing is responsible for about 80% of the full authentication time (175 ms) when the station is in the home network while the infrastructure side delay was about 50 ms. Figure 13 (b) shows that the delay introduced by the infrastructure side processing increased to about 125 ms in roaming situations. This increase is caused by the Kerberos exchanges with the station’s home Kerberos KDC as depicted in Fig. 9.

Figure 13 (c) shows the decomposition of authentication delays when the station performs handovers in the vis-
ited or home networks using the EAP-Kerberos authentication method. It can be seen that during re-authentications, the station side processing is responsible for only 20% of the total authentication delay (2 ms) while the infrastructure side delay is about (22 ms).

These results were obtained using a mobile station with a CPU frequency of 600 MHz, which is equivalent to CPU speeds used in recent mobile devices [21]. According to the performance results, the load on the station side is very reasonable. We can state thus that the EAP-Kerberos method can be deployed on most personal mobile devices such as smart-phones to provide fast-handover capabilities without requiring any extra processing power.

6. Related Work

In the design of cryptographic and security architectures, there is a tradeoff to be made between security, cost, and performance. The main problem addressed in this research topic, which is authentication delay, is related to performance. We have come to the conclusion that most proposals in the literature provide acceptable performance improvements compared to legacy authentication architectures that do not provide fast re-authentication features. However, we also noticed that most existing works have compromised on deployment costs and security, which in certain cases makes these proposals not practical for deployment in real life infrastructures. In the following, we will review major related works and analyze them from security, and deployment cost point of view.

6.1 Approaches Compromising on Deployment Costs

Several fast re-authentication mechanisms proposed by standardization bodies and in the literature, such as IEEE 802.11r [22], the Opportunistic PMK pre-caching [23] and Neighbor Graphs [24], involve distribution of re-authentication keys to access points in a pro-active manner before the mobile stations moves. In order to deploy such fast re-authentication mechanisms, all access points in the infrastructure have to be upgraded. This constitutes a costly operation especially in large scale infrastructures such as those deployed by commercial wireless access providers. The latest standard developed by the IETF for fast re-authentication, called Extensions for EAP Re-authentication Protocol (ERP) [25], also falls in the same category [26].

Among the related works, we found that most re-authentication mechanisms based on the Kerberos protocol [27]–[29] have the same issues regarding the modification of access points. In these approaches, the access points are modified to support processing of Kerberos credentials.

We have also identified works [30], [31] that attempted to address handoff latency while not compromising on costs by seemingly not requiring changing the behavior of access points. However, as we will explain in the next paragraphs, these approaches do not adhere to the requirements of the EAP standard and thus are not guaranteed to work without changing the behavior of access points.

The mechanisms described in these approaches rely on delivering re-authentication keying material from the EAP server to the mobile station (e.g. a random sequence number in the case of [30]). However, the EAP protocol itself, does not provide any mechanism for carrying such data from the EAP server to the mobile station. For this reason, these approaches [30], [31] explicitly or implicitly rely on the EAP-Success message for carrying the keying material. However, using the EAP-Success message in this manner is prohibited by the EAP specification [10] and does not guarantee that the mechanism would work with existing access points.

In [32], the authors suggest the use of separate access point that were modified to allow the provisioning of keying material to the mobile station. This approach however may become costly for large scale deployments.

In comparison, the EAP-Kerberos method proposed in this paper only extends the EAP layer and does not use the EAP-Success message for carrying bootstrapping material. In this way, EAP-Kerberos ensures that any access point which is compliant with the EAP standard [10] can be used as it is without any necessary changes. As a result, the deployment of the proposed method does not require expensive infrastructure upgrades.

6.2 Approaches Compromising on Security

The security requirements for wireless authentication protocols have been established by the IETF in [33] and [34]. The requirements are separated into mandatory requirements and recommended requirements. Mandatory requirements ensure the safety of the authentication architecture against known network attacks. If a wireless authentication protocol does not obey the mandatory requirements, the protocol can not be considered sound from a security point of view.

In [30] during the bootstrapping phase, the mobile station is provisioned with cryptographic material including a sequence number and information identifying a handover server. However, the proposed architecture does not provide details regarding how the integrity and confidentiality of this cryptographic material are ensured during their transfer from the EAP server to the mobile station. Without such protection, an attacker can perform a denial of service attack by spoofing these parameters and causing the mobile station to derive incorrect keys preventing it from accessing the network. The guarantee of the state equivalence requirement as stated in [33] is thus not satisfied because the state information (a sequence number and the identifier of the handover server) can be modified by an attacker.

In [35], the authors describe a fast re-authentication architecture that relies on Kerberos as underlying authentication mechanism. The proposed re-authentication protocol consists in obtaining then using a Kerberos ticket to authenticate with the EAP server. The authentication exchange however only includes an AP Request message sent by the mobile station to the EAP server to authenticate itself for
network access. By not using the AP Response message \cite{5} which serves to validate the identity of the EAP server to the mobile station, the protocol suffers from lack of mutual authentication at the EAP layer which is a mandatory requirement \cite{33}. This compromise on security for performance makes the protocol vulnerable to a man-in-the-middle attacks associated to the lack of mutual authentication \cite{34}.

In comparison, the EAP-Kerberos method ensures mutual authentication between the mobile station and the EAP server at the EAP layer by performing a full AP exchange and by not relying on the AP Request message alone for authentication as it is the case in \cite{35}. Moreover, in contrast with \cite{30}, the proposed method provides complete specification with regard to the transport of all cryptographic material.

7. Security Analysis

As a security protocol, the EAP method described in this paper has to ensure security goals in order to prevent malicious users from using the infrastructure in any illegal way. The IETF has established security requirements \cite{33} with which any new EAP method, intended for use in wireless LANs, must comply. In the following, we show how the EAP-Kerberos method fulfills these requirements.

Generation of Symmetric Keying material: The EAP-Kerberos method uses an AP exchange between the wireless station and the local zone’s authentication server. The service session key is provided by the KDC to the wireless station during the TGS Exchange. When EAP server receives the AP-REQ message issued by the wireless station, it decrypts the service Ticket and obtains the same service session key. This key is then used by the station and server to derive other keying material.

Key strength: The IETF requirements for EAP methods for wireless networks mandates that the method must derive keying materials with 128 bits of effective key strength. The specification of the Kerberos protocol supports several symmetric-key cryptographic algorithms \cite{36}. Amongst the available algorithms, the Advanced Encryption Standard (AES) \cite{37,38} uses 256-bit length keys. Hence, when using AES, keying material derived by the EAP-Kerberos method meet the 128-bit length requirement.

Mutual authentication: The station and the authentication server perform the AP exchange through which the server can authenticate the station by validating the Authenticator component of the AP-REQ message. The station on the other hand verifies the authentication server’s identity after validating the AP-REP message. The mutual authentication between application client and service is possible but not mandatory in Kerberos. The EAP-Kerberos method however, requires that the client requests mutual authentication in the AP-REQ message by setting the mutual-required option.

Resistance to dictionary attacks: “Dictionary attack” is the name for a category of cryptanalysis techniques for recovering user passwords by actively interacting with other entities in the network or by processing a pre-captured data.

The vulnerability of the Kerberos protocol to dictionary attacks has being initially documented in \cite{39} and experimentally proven in \cite{40}. In short, if an attacker can intercept the AS-REP message from the KDC to the station, he can perform a dictionary attack that eventually yields to the disclosure of the password of the user to whom the AS-REP message was issued.

In order to protect the AS exchange from dictionary attacks against weak passwords, the station can use the PKINIT \cite{41} extension which relies on public key cryptography for mutual authentication and key derivation between the client and the KDC. The use of PKINIT may introduce additional delays during the bootstrapping of EAP-Kerberos. However, the use of PKINIT does not have impact on handoff performance. In deed during a handoff, only the AP Exchange and occasionally the TGS exchange are used.

Protection against man-in-the-middle attacks: The Kerberos authentication protocol is designed to provide mutual authentication and establishment of a security association between a client and a server in open networks. The protocol assumes that any entity in the network can capture any message and send any message to the parties involved in the authentication process. In order to detect replayed messages, Kerberos uses a replay cache, where messages are stored for a pre-determined period of time. If a received message is not fresh enough (the included time stamp is too old) or found to be identical to a message from the replay cache, the message is assessed as a replay and rejected. Moreover, sensitive information in Kerberos exchanges are protected using encryption mechanisms that incorporate integrity protection. Message parts that are not encrypted are integrity protected using encrypted checksums. Furthermore, the Kerberos protocol provides cryptographic binding since the identity of the EAP peer is carried in the Ticket, and the identity of the server is carried in the TGS-REP message. The EAP peer and Server’s identities is thus, un-ambiguously known to both parties. Finally, session independence as defined in \cite{10} is ensured since MSKs are derived using a one-way cryptographic hash function with the randomly generated Kerberos session keys as input. The compromise of the MSK thus does not yield any information on how to derive MSK as long as the security of the Kerberos session key is not compromised.

By providing integrity protection, replay protection, cryptographic binding and session independence as defined in \cite{10}, the EAP-Kerberos method implements all the measures for protection against man-in-the-middle attacks.

Protected cipher-suite negotiation: The IETF requirement for EAP methods for wireless access networks mandates that the EAP method must be able to negotiate dif-
different cipher-suites and the negotiation must be integrity protected. The Kerberos authentication protocol supports protected cipher-suite negotiation between the peer and the KDC. When obtaining Tickets (TGT or service Tickets) from the KDC, the client includes a list of preferred cipher-suites in the etype field of the AS-REQ or TGS-REQ message. If the KDC or the target service for which the client requested a Ticket cannot accommodate any of these encryption types, then the KDC issues an error message. If one of the cipher-suites proposed by the client is acceptable, then the KDC will issue an AS-REP or TGS-REP message using the selected cipher-suite. The reply message from the KDC contains a Ticket, a session key and the selected cipher-suite. The key and the cipher-suite are encrypted and integrity protected using the client’s password shared with the KDC in case of an AS exchange, or the TGS session key in case of a TGS exchange. After decrypting the reply message, the client can check whether the KDC has selected an appropriate cipher-suite from the list of proposed cipher-suites sent in the initial request message. During the AP exchange, the peer uses the cipher-suite negotiated with the KDC on behalf of the service during the TGS exchange.

8. Conclusion

In order to achieve true ubiquitous applications, handoff delays in wireless networks must be kept to a minimum. Several steps in the handoff process may be subject to enhancements. In this paper, we consider authentication delays during handoffs which arise when a mobile station is in a visited access network. The inter-domain exchanges necessary for authenticating the roaming station may introduce large delays that would affect quality of service in real-time applications.

We have designed, implemented and evaluated a Kerberos-based EAP authentication method that achieves strong authentication while ensuring acceptable latency during handoffs. In roaming scenarios, experimental results from our test-bed show that EAP-Kerberos re-authentication takes around 25 milliseconds which is five times better than the 120 milliseconds delay introduced by a popular EAP authentication method (EAP-PEAPv0/MSCHAPv2). We have also shown that the EAP-Kerberos method is compliant with security requirements mandated by the IETF.

Furthermore, the EAP-Kerberos method strikes a balanced tradeoff between security, cost and performance making it readily deployable in real life infrastructures to provide enhanced handoff performance while not compromising on security and deployment costs.

In our ongoing investigations, we are designing the integration of the EAP-Kerberos method as a generic re-authentication mechanism for EAP. The extension would allow the station to bootstrap the EAP-Kerberos method after an initial authentication using any legacy EAP method. The EAP-Kerberos method may then be used for subsequent re-authentications to achieve faster handoffs.

References

[1] A. Mishra, M. Shin, and W. Arbaugh, “An empirical analysis of the IEEE 802.11 MAC layer handoff process,” SIGCOMM Comput. Commun. Rev., pp.93–102, 2003.
[2] H. Velayos and G. Karlsson, “Techniques to reduce the IEEE 802.11b handoff time,” International Conference of Communications, pp.3844–3848, 2004.
[3] “IEEE 802.11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications,” IEEE Standards, 2007.
[4] S. Zrelli and Y. Shinoda, “Experimental evaluation of EAP performance in roaming scenarios,” Asian Internet Engineering Conference, 2007.
[5] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, “The Kerberos network authentication service (V5),” RFC 4120 (Proposed Standard), July 2005.
[6] “IEEE 802.16: Air interface for fixed and mobile broadband wireless access systems,” IEEE Standards, 2005.
[7] B. Alrouh and G. Ghinea, “A performance evaluation of security mechanisms for web services,” International Conference on Information Assurance and Security, IEEE, 2009.
[8] “Amendment to IEEE Std 802.11, wireless LAN medium access control (MAC) and physical layer (PHY) specifications — Amendment 6: Medium access control (MAC) security enhancements,” IEEE Standards, 2004.
[9] “IEEE Standard for local and metropolitan networks — Port-based network access control,” IEEE Standards, 2004. Revision of 802.1X-2001.
[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, “Extensible authentication protocol (EAP),” RFC 3748 (Proposed Standard), June 2004.
[11] C. Rigney, S. Willens, A. Rubens, and W. Simpson, “Remote authentication dial in user service (RADIUS),” RFC 2865 (Draft Standard), June 2000.
[12] B. Aboba and P. Calhoun, “RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP),” RFC 3579, Sept. 2003.
[13] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “Diameter base protocol,” RFC 3588 (Proposed Standard), Sept. 2003.
[14] P. Eronen, T. Hiller, and G. Zorn, “Diameter extensible authentication protocol (EAP) application,” RFC 4072 (Proposed Standard), Aug. 2005.
[15] International Telecommunication Union, “Information technology — ASN.1 encoding rules — specification of basic encoding rules (BER), canonical encoding rules (CER), and distinguished encoding rules (DER),” ITU-T Recommendation X.690, July 2002.
[16] A. Gulbrandsen, P. Vixie, and L. Isibov, “A DNS RR for specifying the location of services (DNS SRV),” RFC 2782 (Proposed Standard), Feb. 2000.
[17] S. Sakane, K. Kamada, S. Zrelli, and M. Ishiyama, “Problem statement on the cross-realm operation of Kerberos,” RFC 5868, May 2010.
[18] S. Zrelli, Y. Shinoda, S. Sakane, K. Kamada, and M. Ishiyama, “XTGSP, the inter-TGS protocol for cross-realm operations in Kerberos,” Internet Draft, IETF, 2007.
[19] K. Kamada and S. Sakane, “Client-friendly cross-realm model for Kerberos 5,” Internet Draft, IETF, 2007.
[20] V. Kamath and M. Wodrich, “Microsoft’s peap version 0,” Internet Draft, IETF, Oct. 2002.
[21] “The ARM cortex A8 processor,” http://www.arm.com
[22] “Amendment to IEEE Std 802.11, wireless LAN medium access control (MAC) and physical layer (PHY) specifications — Amendment 2: Fast basic service set (BSS) transition,” IEEE Standards, 2008.
[23] Symbol Technology, “Securing enterprise air: Understanding and achieving next-generation wireless security with symbol technolo-
gies and 802.11i,” White paper, 2005.

[24] A. Mishra, M.H. Shin, N.L. Petroni, Jr., T. Clancy, and W. Arbaugh, “Proactive key distribution using neighbor graphs,” IEEE Wireless Communications, IEE, 2004.

[25] V. Narayanan and L. Dondeti, “EAP extensions for EAP re-authentication protocol (ERP),” RFC 5296 (Proposed Standard), Aug. 2008.

[26] R. Marin, P. Garcia, and A. Skarmeta, “Analysis of handover key management schemes under IETF perspective,” Computer Stands and Interfaces, Elsevier Science Publishers, 2010.

[27] Y. Ohba, S. Das, and A. Dutta, “Kerberized handover keying: A media-independent handover key management architecture,” ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture, ACM, 2007.

[28] E. Sung-Hyun and C. Hyoung-Kee, “EAP-Kerberos II: An adaptation of Kerberos to EAP for mutual authentication,” International Conference on ITS Telecommunications, IEE, 2008.

[29] M. Jaatun, I. Tondel, F. Paint, T. Johannessen, J. Francis, and C. Duranton, “Secure fast handover in an open broadband access network using Kerberos-style tickets,” Security and Privacy in Dynamic Environments, Springer, 2006.

[30] R. Marin-Lopez, Y. Ohba, F. Pereniguez, and A.F. Gomez, “Cryptographic identity based solution for fast handover on EAP wireless networks,” IFIP International Conference on Mobile Wireless Communications Networks, IEE, 2007.

[31] H. Almus, E. Brose, and K. Rebensburg, “A Kerberos-based EAP method for re-authentication with integrated support for fast handover and IP mobility in wireless LANs,” ICCE International Conference on Communications and Electronics, IEE, 2008.

[32] R. Marin, P. Garcia, and A. Skarmeta, “A fast and heterogeneous handover architecture based on an extended EAP lower-layer,” IST Mobile and Wireless Communications Summit, IEEE, 2007.

[33] D. Stanley, J. Walker, and B. Aboba, “Extensible authentication protocol (EAP) method requirements for wireless LANs,” RFC 4017, March 2005.

[34] B. Aboba, D. Simon, and P. Eronen, “Extensible authentication protocol (EAP) key management framework,” RFC 5247 (Proposed Standard), Aug. 2008.

[35] R. Marin-Lopez, F. Pereniguez-Garcia, Y. Ohba, F. Bernal-Hidalgo, and A. Gomez, “A Kerberized architecture for fast re-authentication in heterogeneous wireless networks,” Mobile Networks and Applications, Springer, 2010.

[36] K. Raeburn, “Encryption and checksum specifications for Kerberos 5,” RFC 3961 (Proposed Standard), Feb. 2005.

[37] National Institute of Standards and Technology, “Advanced encryption standard (AES) for Kerberos 5,” 2001.

[38] K. Raeburn, “Advanced encryption standard (AES) for Kerberos 5,” RFC 3962 (Proposed Standard), 2005.

[39] S.M. Bellovin and M. Merritt, Limitations of the Kerberos authentication system, ACM Press, 1990.

[40] T.D. Wu, “A real-world analysis of Kerberos password security,” NDSS, The Internet Society, 1999.

[41] L. Zhu and B. Tung, “Public key cryptography for initial authentication in Kerberos (PKINIT),” RFC 4556 (Proposed Standard), June 2006.

Saber Zrelli received a B.E. degree from the Tunisian National School of Computer Science in 2002. He then pursued postgraduate studies in Japan and received an M.E. and a Ph.D. from Japan Advanced Institute of Science and Technology in 2006 and 2009 respectively. His research interests include network security, quality of service and wireless communications.

Nobuo Okabe received a B.E. and an M.E. degrees from Tokyo University of Agriculture and Technology in 1983 and 1985, and then received a Ph.D. in engineering from the University of Tokyo in 2008. His research work has been on information, network and security in the area of industrial automation. His current research interest is to make industrial systems more automated, more efficient, and safer with information technology.

Yoichi Shinoda is a Professor at the Research Center for Advanced Computing Infrastructures, Japan Advanced Institute of Science and Technology since 1991. He obtained his B.E., M.E. and Ph.D. from Tokyo Institute of Technology in 1983, 1985 and 1989 respectively. His research interests include Distributed and Parallel Computing, Networking Systems, Operating Systems, Information Environment.