IEEE International Conference on Wireless & Mobile Computing, Networking & Communication

Security and Access Control for Vehicular Communications

Saber Zrelli, Atsuko Miyaji and Yoichi Shinoda
Japan Advanced Institute of Science and Technology
School of Information Science
Ishikawa, Japan
zrelli@jaist.ac.jp, miyaji@jaist.ac.jp, shinoda@jaist.ac.jp

Thierry Ernst
The French National Institute for Research
in Computers and Control
Paris, France
thierry.ernst@inria.fr

***Abstract*—In this paper, we present an architecture for security and access control in Intelligent Transportation Systems. The applicability of the proposed architecture is demonstrated by developing a case-study based on CVIS (Collaborative Vehicle Infrastructure system). The proposed framework ensures maximum security for the communication infrastructure by implementing access control at both the data link layer and the network layer. The originality of the proposed framework consists on adoption of a universal security mechanism approach by using the Kerberos protocol for link layer authentication as well as for establishing IPSec security associations, which simplifies credential management and ensures reduced overhead. The operations of the EAP-Kerberos authentication method that we have designed and implemented for the purpose of this project is also presented.**

I. Introduction

With the growing availability of the Internet connectivity and the wider deployment of wireless access networks, we can see a number of new Internet-based applications in domains such as Health-Care, Industrial Automation, Wearable Computing, Disaster Response, etc. In the same fashion, the transportation industry is developing technologies for enabling advanced monitoring, traffic control and multimedia applications for vehicles. Intelligent Transportation Systems or ITS, is the research area that focuses on investigating the use, adaptation and development of telecommunication and Internet technologies for transport infrastructure and Vehicles.

A transportation system is an environment that poses several challenges with regard to technology requirements. Because of the large number and high speed of Vehicles, technologies for ITS must be scalable and robust enough to cope with these characteristics. Architectures and protocols for ITS thus need to be deeply examined and assessed for performance and scalability before their final adoption as part of a standard ITS framework.

Security and protection of business assets within the ITS framework is also a vital part without which the whole system can not be deployed in real life. Security is needed to provide authentication, integrity protection and confidentiality of information within the ITS framework. Without it, malicious entities may alter the normal operations of ITS applications and cause faults that can lead to disasters. On the other hand, a proper management of authorization for services and accounting is necessary in order for service providers to be able to deploy commercial services such as Internet access and multimedia streaming.

In this paper, we propose a security and access control framework for ITS. By following a case-study based on the CVIS (Collaborative Vehicle Infrastructure system) specification, we demonstrate the deployment and operations of our proposal. After a brief overview of the CVIS project, its components and its communication infrastructure, we highlight different network security threats that need to be addressed in order to protect the CVIS project's communication infrastructure. Then, we propose a security and access control framework based on the well known Kerberos authentication protocol, that implements the needed security measures. The proposed solution inherits simplicity and performance of Kerberos authentication which makes it suitable for mobile environments such as vehicular communications.

II. The CVIS Project

A. Overview

CVIS (Collaborative Vehicle Infrastructure system) [1] is an European project aiming at developing an Intelligent Cooperative System based on Vehicle-to-Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The CVIS system has the following objectives:

- To create a unified technical solution allowing all Vehicles and infrastructure elements to communicate with each other in a continuous and transparent way using a variety of media and with enhanced localization;
- To enable a wide range of potential cooperative services to run on an open application framework in the Vehicle and roadside equipment;
- To define and validate an open architecture and system concept for a number of cooperative system applications, and develop common core components to support cooperation models in real-life applications and services for drivers, operators, industry and other key stakeholders;
- To address issues such as user acceptance, data privacy and security, system openness and inter-operability, risk and liability, public policy needs, cost/benefit and business models, and roll-out plans for implementation.

978-0-7695-3393-3/08 $25.00 © 2008 IEEE
DOI 10.1109/WiMob.2008.114

B. CVIS subsystems

The CVIS framework is composed of three types of CVIS subsystems: Vehicle subsystems, Road-Side subsystems and Central subsystems.

The Central subsystem is the back-end infrastructure that a service provider uses to serve applications and interact with remote entities in Vehicle and roadside subsystems. Control center, Traffic management center, application management center and content center are examples of CVIS Central subsystems. The Central subsystem consist of the collection of equipment, software and operators that achieves the center's function in the global CVIS system. The computing infrastructure in Central CVIS subsystems is the same and consists of a host computer where the applications are deployed, a GATEWAY that acts as interface between external data resources such as authority databases, sensors, etc, and applications deployed by the Central CVIS subsystem. And a border ROUTER provides Internet connectivity to the whole computing infrastructure in the Central CVIS subsystem's ingress network.

The Vehicle CVIS subsystem is the the networking and computing facilities on-board Vehicles that are part of the CVIS system. It enables Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication and collaborative applications. The Vehicle subsystem allows interaction with on board sensors and actuators through a GATEWAY unit. A HOST unit runs applications and, a ROUTER unit is in charge of assuring network connectivity to the ingress network. The ROUTER may implement the network mobility protocol (NEMO) [2] for providing session continuity to mobile network nodes. For this purpose, the mobile ROUTER uses a Home Agent managed by a Mobility Service Provider (MSP) that can be seen as a Central CVIS subsystem.

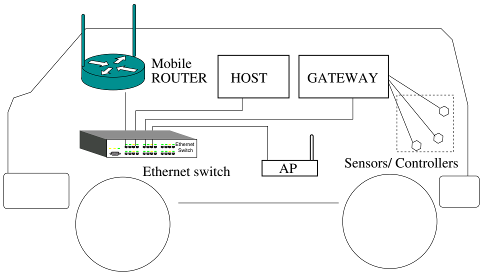


Fig. 1. Vehicle CVIS subsystem

The Road-Side CVIS subsystem, as its name implies, is is the computing and communication facilities that are responsible for road side CVIS services (Traffic Signaling, Alarms, Internet Access, etc.). It comprises a HOST unit where CVIS applications are deployed, a GATEWAY through which the HOST and other entities can access sensors and actuators deployed on the road-side (Traffic lights, Cameras, etc.). The roadside subsystem has permanent Internet connection through a Border ROUTER. An Access ROUTER on the roadside CVIS subsystem allows Vehicle CVIS subsystems and other mobile units to connect to the Internet and reach central CVIS subsystems or other Internet locations.

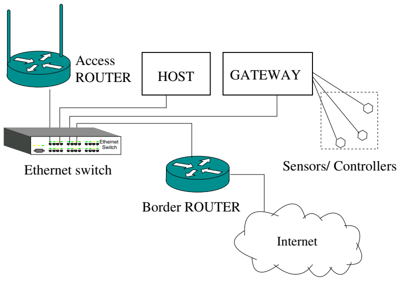
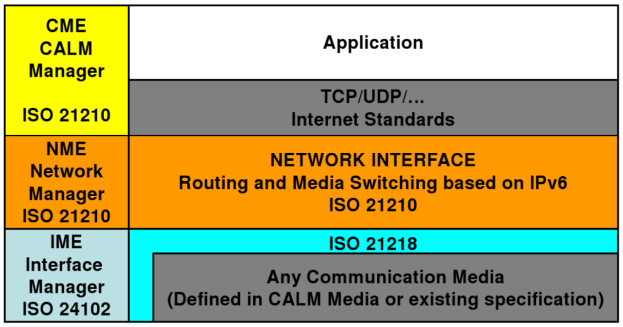


Fig. 2. Road-Side CVIS subsystem

Several communication media may be used in the ingress network. At least wireless 802.11 and wired Ethernet communication should be supported.

C. The CVIS communication services

CVIS subsystems rely on different communication technologies to enable deployment of distributed applications. At the link layer, the CVIS reference architecture specifies different communication media such as 802.11p, Cellular technology, 802.11, 802.16e and 802.20. The communication subsystem in CVIS follows the ISO TC204 WG16 series of draft standards under the acronym CALM (Continuous Communications Air interface for Long and Medium range). The CALM project [3] is chartered to specify the communication and networking infrastructure necessary for enabling continuous and reliable ITS services. The CALM networking stack as is depicted in Fig. 3, features standard networking layers and uses Internet standards such as IPv6 and NEMO. Management entities at three layers (Interface level, Network level and Application/Transport level) provide additional functions such as interface selection, mobility and vertical/horizontal handovers, that are not part of legacy networking stacks.



CME CALM Manager ISO 21210	Application
	TCP/UDP/... Internet Standards
NME Network Manager ISO 21210	NETWORK INTERFACE Routing and Media Switching based on IPv6 ISO 21210
IME Interface Manager ISO 24102	ISO 21218
	Any Communication Media (Defined in CALM Media or existing specification)

Fig. 3. The CALM networking stack

With the support of CALM networking capabilities and functions deployed on CVIS subsystems, Vehicle and Road-Side CVIS units provide high-level networking services for local entities and for other CVIS subsystems.

These communication services can be summarized as follows :

Ad-hoc relay service Ad-hoc communication enables CVIS subsystems to communicate with each other without the need of an infrastructure. This mode of communication is especially useful for V2V applications. The roadside subsystem can be a part of an ad-hoc network, it may act as relay for Vehicle CVIS subsystems that are far from the ad-hoc cloud formed by other Vehicle subsystems in the same road. In order to become member of an ad-hoc cloud, the new CVIS subsystem must support the ad-hoc routing protocol in use.

A CVIS subsystem may act as an ad-hoc relay to another subsystem in an ad-hoc network. The serving subsystem allows the client subsystem to participate in the global ad-hoc routing protocol through exchange of network topology routing information. Most ad-hoc routing protocols such as OLSR [4] or AODV [5] use application layer client/server model for exchanging routing messages over UDP.

Internet gateway service A CVIS subsystem may act as an Internet gateway for another subsystem. In order to provide this service, the serving subsystem must have Internet connectivity itself. The ROUTER unit which is part of any CVIS subsystem is the component that provides the Internet connectivity service for other nodes in the same CVIS subsystem and for other CVIS subsystems. For example, a Vehicle subsystem may use the Internet gateway service offered by the Road-Side subsystem to connect to a remote host in the Internet. A Vehicle CVIS subsystem may also act as an Internet gateway for another Vehicle CVIS subsystem.

III. Threat analysis

Like any other telecommunication and information system, the CVIS infrastructure can be subject to different security threats. If left without protection, attackers and malicious entities may cause several damages in different ways. In the following we analyze different categories of security threats and the impact they can have on the CVIS system.

Service disruption: The attacker causes a service disruption when it succeeds in causing a fault in an application or protocol component of the CVIS framework, leading to failures ranging from degradation of quality of service to complete denial of service. The incapacity of the system to achieve its function properly may lead to catastrophic consequences if human safety relies on it. Therefore, it is critical to guarantee the service dependability by understanding security threats and taking proper measures to avoid failures.

Theft of service: Without access control, services can not be protected or restricted, and business assets can not be protected and exploited as intended. For this reason, without access control, business model can not be implemented for commercial use of the CVIS infrastructure.

Privacy violation: In the CVIS infrastructure, malicious entities may eavesdrop on communications and collect information that would allow them to track activity and location of persons.

In order to achieve its malicious goals, an attacker may use any combination of techniques such as eavesdropping, overflooding, masquerading and information forgery.

IV. Proposed security framework

A. Overview

In order to provide adequate security against network threats, the CVIS subsystem should implement security and access control in three layers of the CALM networking stack. First, security measures implemented at the link layer will prevent malicious entities from interfering with ongoing communications in the CVIS framework by preventing non authorized nodes from processing and issuing link layer frames. At the IP layer, we propose to control message forwarding and restrict it to authorized entities only. Entities that are not supposed to communicate with remote hosts in the Internet will be prevented from doing so. Finally, at the application layer, access control allows fine grained authorization to be implemented and avoid an all or nothing authorization policy.

Even though security and access control technologies used at each layer are different, they all rely on generic cryptographic algorithms and authentication protocols. It is always a good approach to reduce complexity and administrative burden by reducing the number of cryptographic algorithms and authentication protocols used within a single framework. In accordance to this approach, we propose a security and access control architecture for CVIS based solely on the Kerberos [6] as underlying authentication and key distribution protocol.

The single sign-on feature and the performance of symmetric key cryptography in Kerberos makes it the mechanism of choice for embedded computing and real time systems [7]. Originally, the Kerberos authentication system was intended for application layer authentication and data protection in open networks. Due to the advantages that it offers, in recent years, the use of Kerberos at IP layer for establishing IPSec security associations was specified by the IETF as KINK (Kerberized Internet Negotiation of Keys) [8]. In the proposed security framework, we use IPSec to secure Internet gateway and ad-hoc relay services, and the KINK protocol will be used to establish IPSec association between IP stacks of communicating CVIS subsystems.

In a previous work [9], we investigated the convenience of using Kerberos as authentication mechanism for link layer access control and a reference implementation of the mechanism was made available [10].

Our approach for using Kerberos to perform authentication with EAP [11] (Extensible Authentication Protocol) at link layer is based on the notion of *Network Access Zones* that we define as a collection of lightweight access points managed by a single back-end authentication server. A collection of network zones that belong to the same provider constitutes an Access Network.

In the EAP Kerberos authentication method, each zone constitutes a logical service to which corresponds a Kerberos principal registered in a Kerberos key distribution center managed by the network access zone's owner.

An authentication server managing a certain zone is able to authenticate wireless clients through a Kerberos Client/Server authentication exchange over EAP. The server validates Kerberos AP-REQ messages built using Kerberos Tickets for the zone. For this purpose, the server uses the zone's secret key, transferred from the KDC to the authentication server using an off-line secure channel.

In order to gain network access within a zone, the STA must obtain a service ticket for the local zone and present the ticket to the zone's authentication server. The EAP-Kerberos method specifies how the STA obtains Kerberos credentials and how it uses them to authenticate and gain network access.

B. *EAP-Kerberos operations*

The first message in the EAP-Kerberos authentication exchange is issued by the authentication server. This message includes a Kerberos realm name as well as the identification of the local network access zone (REALM and ZONE in Fig.4). These two information together constitute the local zone's Kerberos principal name that uniquely identifies it within the global Kerberos name space.

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 a Client/Server 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 Kerberos realm where the zone is registered, then the STA must obtain a ticket by performing a TGS (Ticket Granting Service) Exchange with the Key Distribution Center of the Kerberos realm 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 then sent back to the STA in an EAP-Kerberos message. After obtaining the service ticket, the STA can perform a Client/Server Exchange with the authentication server.

If the STA does not have a service ticket for the zone nor a TGT (Ticket Granting Ticket) for the local realm, then it needs to obtain a TGT first. The process of obtaining a TGT for the local realm depends on whether the Kerberos realm where the zone is registered is the same as the STA's Kerberos realm or not. In the former case, the STA uses an AS (Authentication Service) exchange with the local realm's Kerberos KDC. In the latter case, the STA first get a TGT for its home Kerberos realm using an AS Exchange with its home KDC, then performs Kerberos cross-realm TGS exchanges as specified in [6].

Fig. 5 depicts EAP-Kerberos operations for re-authentications within the same network access zone.

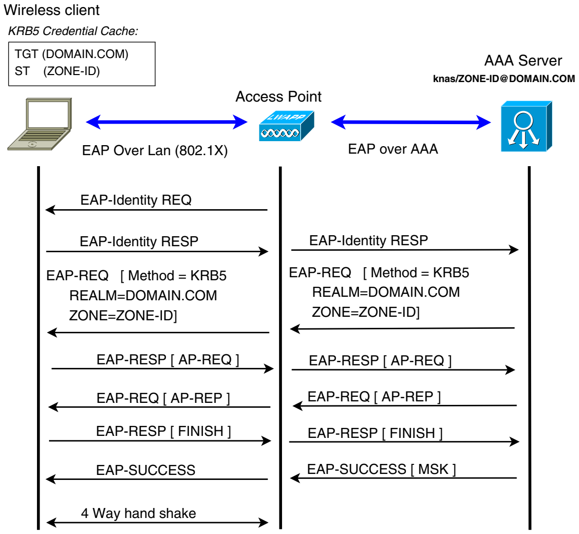


Fig. 5. EAP-Kerberos authentication in an Intra-zone handoff

C. *Kerberos setup for the CVIS framework*

The Kerberos authentication system requires the partitioning of the network infrastructure into Kerberos realms and the deployment of Kerberos Key distribution centers. For the CVIS framework, we propose the following approach; Each CVIS subsystem is a Kerberos realm and has its own Kerberos KDC deployed in the HOST element of the CVIS subsystem. All services offered by a certain CVIS subsystem (Link layer association, Internet gateway, ad-hoc relay, Content servers, etc..) are registered as Kerberos service principals in the Kerberos KDC of the CVIS subsystem where they are deployed. The setup of a service within the CVIS framework would consist on adding an entry in the CVIS subsystem's KDC, and installing a key in the device where the service will be deployed. Any entity acting as a client to any of these services must be registered in a Kerberos KDC and possess Kerberos credentials.

D. *Link layer access control*

Link layer access control is performed between two CVIS subsystems that need to directly communicate with each other (between two Vehicles, or a Vehicle and a Road-Side CVIS subsystem). The link layer access control method proposed in this paper, only applies to link layer technologies that use EAP for authentication and key distribution.

In the proposed framework for network access control, Vehicule and Road-Side CVIS subsystem are considered as independent network access zones as defined in Section IV-B. The EAP-Kerberos method is used between two CIVS subsystems wishing to establish link layer association. As stated previously, each CVIS subsystem, has an 'embedded' AAA server

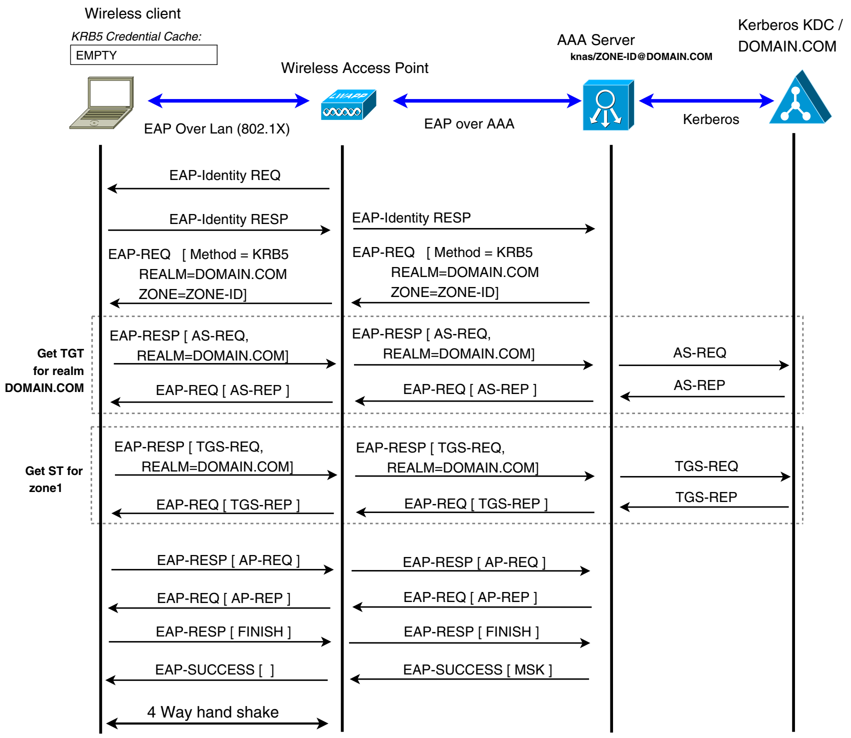


Fig. 4. Initial EAP-Kerberos authentication in home access network

and a Kerberos KDC. The link layer association with a serving CVIS subsystem is a Kerberized service. In order to establish link layer association, the client CVIS subsystem's ROUTER acting as an EAP peer has to obtain Kerberos credentials for the serving CVIS subsystem's network access zone, then authenticate to the serving CVIS subsystem's embedded AAA server. Since the client and the serving CVIS subsystems constitute two distinct Kerberos realms, Kerberos KDCs on both subsystems must have pre-established inter-realm trust relationship. Direct inter-realm trust in Kerberos requires pre-distribution of secret keys to both KDCs. However, this is not a scalable approach when the number of CVIS subsystems is large. The alternative approach that we propose in order to avoid using Kerberos cross-realm operations, consists in using *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*[12], which allows a client CVIS subsystem to obtain a TGT from the serving CVIS subsystem's KDC without the need for pre-shared keys between the two realms.

In case of Vehicle to Vehicle link layer association, the 802.11i standard states that mutual authentication must be performed in both ways. The same procedure described in the previous paragraphs is thus carried by the client CVIS subsystem as well as the serving CVIS subsystem.

E. Securing the Internet gateway

The Internet gateway service is defined as the forwarding of IP packets to destinations not located in the serving CVIS's ingress network. In order to control access for the Internet gateway service and ensure that only authorized nodes can connect to remote hosts through the serving CVIS subsystem, IPSec security policy on the serving CVIS subsystem's border ROUTER are configured such that only authenticated and authorized traffic is forwarded to remote hosts. For this purpose, the IPSec layer on the border ROUTER uses the destination IP address to decide whether the packet must be processed by IPSec.

In the proposed architecture, the *Kerberized Internet Negotiation of Keys (KINK)*[8] is used for establishing IPSec security associations between the client and the serving CVIS subsystems. The KINK protocol requires that the client subsystem be able to communicate with the serving subsystem's KDC. This communication becomes possible after link layer association between the two CVIS subsystems has been established. Kerberos messages from the client CVIS subsystem are forwarded by the serving CVIS subsystem's ROUTER to the embedded KDC located at the HOST element.

During establishment of the IPSec association with KINK, the serving CVIS subsystem's border ROUTER decides whether to authorize the client for the Internet gateway service. For this purpose, authorization data such as in [13] is embedded in the service ticket carried by the AP-REQ message. The KINK's CREATE message, which transports the AP-REQ message to authenticate the client CVIS system thus provides enough information for the serving CVIS subsystem to authorize the client. A separate authorization application may also be used to decide whether to enable the Internet gateway service for the client CVIS subsystem.

F. Securing ad-hoc relay services

The ad-hoc relay service allows a CVIS unit to participate in ad-hoc routing protocols such as OLSR and AODV. In order to control which entities are allowed to participate in the ad-hoc routing protocol, the border ROUTER element of the serving CVIS subsystem uses IPSec to ensure that only authenticated and authorized network nodes may issue ad-hoc routing messages. To implement this, the ROUTER's IPSec policy is configured such as packets in destination to the ROUTER's OLSR or AODV daemon must be processed by IPSec. These packets can be identified using the destination IP address and destination port number.

The client CVIS subsystem and the serving CVIS subsystem use the KINK protocol to establish IPSec security associations. In a way similar to the way Internet forwarding service is protected (Section. IV-E), the serving CVIS subsystem's border ROUTER decides whether to authorize the client for the ad-hoc service. For this purpose, authorization data embedded in the ticket carried by the KINK's CREATE message can be used to authorize the client CVIS subsystem.

V. Conclusion

Intelligent transportation systems need to rely on a robust communication infrastructure in order to achieve their functions and provide dependable services. Security and access control has a major role in ensuring safety of the communication infrastructure and its protection against malicious entities. Since the ITS world is a new domain for Inter-networking technologies, it is not clear yet how the existing technologies will fit in the planned usages. Performance and scalability of communication and management protocols is expected to be pushed to the limits. Therefore a design that takes these facts into consideration will likely meet the requirements for the future Intelligent Transportation Systems.

In this paper, we presented a case study of security framework for ITS. The Collaborative Vehicule Infrastructure System is an European project that aims at developing safety and commercial services for transportation systems. We proposed a robust yet simple security and access control framework relying on unified credentials and common authentication mechanism namely Kerberos. The proposed architecture provides security and access control at three layers of the networking stack. At the link layer, the EAP-Kerberos method that we designed and implemented, allows CVIS entities to perform secure associations using Kerberos credentials. The use of the PKINIT extension ensures the scalability of the proposed framework, since even entities without a pre-established mutual trust relationship can authentication each other using public-key cryptography. Once link layer association has been established, CVIS subsystems can obtain more credentials for authentication and authorization of IP layer and application layer services. Apart from its simplicity, the proposed framework has the advantage of scalability and performance since in one hand, Kerberos authentication uses long-lived and reusable credentials (Tickets), and on the other hand, most cryptographic operations rely on symmetric key ciphers that consume less resources that public-key ciphers.

In order to support additional AAA operations such as accounting, each CVIS subsystem acts as a AAA client. The AAA client component can be used by a serving CVIS subsystem to issue accounting records to the appropriate AAA accounting server. Since such operations require AAA routing, the client CVIS subsystem's AAA realm name need to be determined from its Kerberos realm name. The conversion can be performed following a pre-defined rule or static configuration. The details of the Kerberos realm name to AAA realm name conversion and billing operations for the CVIS framework are out of the scope of this document.

The use of Public Key Infrastructure for maintaining mutual trust relationships between CVIS subsystems, considered in our context as autonomous Kerberos realms, requires the resolution of organizational issues such as which authority will be acting as Certification Authority (CA) delivering certificates and issuing revocation lists. We estimate that this decision is not a technical issue and is therefore beyond the context of this paper.

References

[1] "Cooperative Vehicle Infrastructure Systems (CVIS)," Web page, As of June 2008, http://www.cvisproject.org.

[2] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963 (Proposed Standard), Internet Engineering Task Force, Jan. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc3963.txt

[3] "Continuous Communications Air interface for Long and Medium range (CALM)," Web page, As of June 2008, http://www.calm.hu.

[4] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[6] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," RFC 4120 (Proposed Standard), Internet Engineering Task Force, July 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4119.txt

[7] O. Nobuo, S. Shoichi, M. Kazunori, I. Atsuhi, M. Ishiyama, and K. Kamada, "Security Architecture for Control Networks using IPsec and KINK," SAINT, Tech. Rep., Feb 2005.

[8] S. Sakane, K. Kamada, M. Thomas, and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)," RFC 4430 (Proposed Standard), Mar. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4430.txt

[9] S. Zrelli and Y. Shinoda, "Specifying kerberos over EAP: Towards an integrated network access and kerberos single sign-on process," in *AINA*. IEEE Computer Society, 2007, pp. 490–497. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/AINA.2007.130

[10] "The Kerberized Network Access Control project," Web page, As of May 2008, http://www.vornos.com.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), June 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3748.txt

[12] L. Zhu and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)," RFC 4556 (Proposed Standard), June 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4556.txt

[13] K. Jaganathan, L. Zhu, and J. Brezak, "Windows authorization data in kerberos tickets," draft-jaganathan-win-krb-authz, IETF, Internet Draft, July 2005. [Online]. Available: http://tools.ietf.org/html/draft-jaganathan-win-krb-authz-00