IEEE GLOBECOM Design and Developers Forum


Tim Weil – CISSP, CISA
Booz Allen Hamilton
ITS Security Architect

New Orleans
1 December 2008
Table of Contents

- Introduction – WAVE Protocol Stack
  - IdAM Frameworks for ITS
  - ITS Services and OSS Architecture
  - WAVE Service Provisioning, Identity Management and PKI
  - 1609.2 Additional Topics and Recommendations
  - Summary
IEEE 1609.2: WAVE Security Services for Applications and Management Messages
- Defines 5.9 GHz DSRC Security
- **Anonymity, Authenticity and Confidentiality**

IEEE 1609.3: WAVE Networking Services
- Provides description and management of the DSRC Protocol Stack
- Application interfaces, Network configuration management
- WAVE Short Message (WSM) transmission and reception

IEEE 1609.4: WAVE Multi-Channel Operation
- Provides DSRC frequency band coordination and management

IEEE 802.11p: Wireless LAN Medium Access Control (MAC) and physical layer
- Defines the Lower Layers of the communications stack
IEEE Standards Association Publications


DSRC Operations Model

- Dedicated Short Range Communications (DSRC) technology has been chosen to support both Public Safety and Private operations.
- DSRC fact sheet:
  - Based on IEEE 802.11p
  - Range up to 1000m
  - Data rates from 6-27 Mbps
  - 7 licensed channels in 5.9GHz
  - Low latency ~50ms
  - Security using public key infrastructure (PKI)
  - Long term stability (technology evolution is controlled by FCC and standards)
  - Postured for IPv6 at roll-out
System Architecture Overview

- The DSRC portion of the RSE is the Road Side Unit (RSU)
  - Interconnects DSRC Networks with Infrastructure Networks
  - Applications can reside on both the RSU or a Network Host (application server)

- The DSRC portion of the OBE is the On Board Unit (OBU)
  - Interconnects Vehicle Systems with DSRC Networks
  - Applications can reside on both the OBU and a Vehicle Host
The VII System is composed of many Services, Subsystems and interfaces defined in the VII National System Specification.
Table of Contents

- Introduction – WAVE Protocol Stack
- IdAM Framework for ITS
- ITS Services and OSS Architecture
- WAVE Service Provisioning, Identity Management and PKI
- 1609.2 Additional Topics and Recommendations
- Summary
ITS Security and Privacy – Data You Can Trust

Confidentiality

Privacy

Availability

Integrity

- **Attack 1**: Bogus traffic information
  - Traffic jam ahead

- **Attack 2**: Disruption of network operation
  - SLOW DOWN

- **Attack 3**: Cheating with identity, speed, or position
  - Wasn’t me

- **Attack 4**: Jamming
  - The way

- **Attack 6**: Tracking
  - 1. A enters the parking lot at time t1
  - 2. A communicates with B
  - 3. A downloads from server X

Date: 12/22/08
Identity and Access Management for ITS Device and Individual System Access

- **ITS Entity Management**
  - Processes and technologies that manage the lifecycle of the OBE’s and RSE’s credentials as well as system users

- **Credentialing**
  - Creation, revocation, and reconciliation of credentials for OBE’s, RSE’s, as well as individuals

- **Authentication**
  - Verification/validation of OBE’s, RSE’s and system users

- **Authorization**
  - Validation of an OBE’s access rights to network and value added services

- **Storage**
  - Where required, protection of the identifiable information attributes
Table of Contents

- Introduction – Concept, Credits, and IdAM Architectural Models
- IdAM Frameworks for ITS
  - ITS Services and OSS Architecture
- WAVE Service Provisioning, Identity Management and PKI
- 1609.2 IdAM Additional Topics and Recommendations
- Summary
Introduction – ITS Use Cases Services and Applications

- Traveler Information
  - Travel Times, Incident Alerts,
  - Road Closures, Work Zones

- In Vehicle Signage
  - Local Signage (School Zones, Stop Signs)
  - Highway Next Exit Services

- Navigation
  - Off Board Navigation
  - Reroute Information

- Traffic Management
  - Ramp Metering
  - Signal Timing Optimization
  - Corridor Management Planning Assistance
  - Corridor Management Load Balancing
  - Pothole Maintenance

- Weather Information
  - Traveler Notification (Icy Bridge Warning)
  - Improved Weather Observing
  - Winter Maintenance

- Safety
  - Emergency Electronic Brake Light
  - Traffic Signal Violation Warning
  - Stop Sign Violation Warning
  - Curve Speed Warning

- Electronic Payment
  - Parking
  - Toll Roads
  - Gasoline
Advisory Message Distribution Service (AMDS) 
Provides users with the ability to broadcast messages to vehicles.

- The AMDS provides the following functions:
  - CreateAdvisoryMessage: the ability to create a new message to be broadcasted to the VII System.
  - QueryAdvisoryMessage: the ability to retrieve the parameters of an existing message.
  - Update: the ability to update an existing message.
  - Cancel: the ability to prematurely terminate an existing message.
  - QueryDeliveryStatus: the ability to determine the real-time delivery status of an existing message.
  - Synchronize: the ability to ensure only active, valid messages are being broadcast.

- The AMDS will submit queries to the Information Lookup Service (ILS) as necessary in order to fulfill user requests.

- The AMDS will monitor ILS for changes to the VII System and will dynamically update message broadcast instructions as necessary.

- The AMDS will prioritize the broadcast list based on message parameters.
Introduction – USDOT ITS National Architecture
(http://www.iteris.com/itsarch/index.htm)
WAVE Architecture Integration – Component Services (1609.2/1609.3)

- ITS Service Provisioning
- Network Services
- Configuration Management
- Protocol Enhancements
- WAVE Provisioning (WMIE, WSA)
- Identity Management
- Public Key Infrastructure
- WAVE Monitoring
- Configuration Management
- Network Services
- WAVE Provisioning (WMIE, WSA)
- ITS Service Provisioning
WAVE Architecture Integration – Component Services (1609.2/1609.3)

- ITS Service Provisioning
  - Service Creation
  - PSID Registration
  - PSID Advertisement
  - PSID Security
  - RSE Attributes (MIB)

- Identity Management
  - RSE Naming Convention
  - PSID Format
  - 1609.2 Credentials
  - Anonymous Certificates
  - Directory Services (LDAP)

- Public Key Infrastructure
  - 1609.2 Certificate Authority
  - 1609.2 Certificate Manager (RSE)
  - 1609.2 Certificate Manager (OBE)
  - Identity Based Encryption (IBE)

- Network Services
  - IPv6 Infrastructure (address and routes)
  - Firewall Protection
  - Ports and Services
  - Virtual Private Network Access

- Configuration Management
  - RSE and OBE SW Version Control
  - Software Development Tools
  - 1609.2 Security Libraries

- Protocol Enhancements
  - Vehicular Datagram Transaction Layer Security (VDTLS)
  - Vehicular Host Internet Protocol (VHIP)

- WAVE Monitoring
  - Logging and Fault Tracking
Table of Contents

- Introduction – WAVE Protocol Stack
- IdAM Framework for ITS
- ITS Services and OSS Architecture
- WAVE Service Provisioning, Identity Management and PKI
- 1609.2 Additional Topics and Recommendations
- Summary
The Identity Repository (LDAP) creates and manages the assignment of RSE attributes for certificates (including PSIDs).
ITS Service Provisioning – 2 of 2

Add ITS Application

Application Name: Road Incident  PSID: 33619969

Comment:

Is application cleanup allowed? □
Is this an anonymous application? □

Anonymous Certificate Pool Size: 200
Vehicle Pool Size: 10
Rekey Threshold: 5

Submit  Reset
ITS Identity Management (PSID Creation) – 1 of 2

PSID Definition is WAVE(1609.3)
Configurable data element published in the RSE Identity Certificate
The **RSE Certificate Manager** provides management of the certificates within an RSE required to secure the communications of identifying applications over the WAVE radio access network. The RSE Certificate Manager communicates with the Certificate Authority to acquire and replace certificates and to process certificate revocations.

A Certificate Signing Request (CSR) is used to request RSE Identity Certificates.
# Types of Certificates And Certificate Users in ITS

<table>
<thead>
<tr>
<th></th>
<th>Vehicle</th>
<th>RSE</th>
<th>Network</th>
<th>External Providers</th>
</tr>
</thead>
</table>
| 1609.2 Anonymous Certificates | • Has and Uses  
• Processes  
• Processes CRLs | • Processes  
• Processes CRLs | • Not Used | • Has and Uses  
• Processes  
• Processes CRLs |
| 1609.2 Identifying Certificates | • Has and Uses  
• Processes  
• Processes CRLs | • Has and Uses  
• Processes  
• Processes CRLs | • Not Used | • Has and Uses  
• Processes  
• Processes CRLs |
| X.509 Identifying Certificates | • Not Used | • Has and Uses  
• Processes  
• Processes CRLs | • Has and Uses  
• Processes  
• Processes CRLs | • Has and Uses  
• Processes  
• Processes CRLs |
Public Key Infrastructure - Certificate Authority Architecture

Transaction Service Provider - Network Users that send and receive information to or from other Network Users, Vehicles or Public Service Vehicles using facilities provided by the ITS System. Example: State DOT Transportation Traffic Management Center.

Transportation Operations Center (TOC) Network User - Advisory Providers that publish information to the ITS System. Example: a weather alerts provider, that issues warnings regarding weather events.
## AuthN/AuthZ Features addressed in the IEEE 1609 Standards

<table>
<thead>
<tr>
<th>Identity Management Features of 1609.2/1609.3</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes of Digital Certificates</td>
<td>There are classes of certificates identified by the ‘subject_type’ field which describes what kind of entity owns the certificate. It is used to determine the scope of the certificate and the means of identifying the signer.</td>
</tr>
<tr>
<td>Securing Transactions</td>
<td>Transactions are exchanges in which multiple messages are sent by one or both peers. Transactions are initiated when a user receives a Provider Service Table (PST) as advertised by a WSA.</td>
</tr>
<tr>
<td>Securing Messages Structures</td>
<td>A secure message type is a published 1609.2 data structure with these options - unsecured message, signed message or signed WSM.</td>
</tr>
<tr>
<td>Bootstrapping Trust</td>
<td>All WAVE equipment are provisioned with a public key that can be used to validate root certificate updates. OBEs can generate their own key pairs.</td>
</tr>
<tr>
<td>Signed Messages</td>
<td>ECDSA signed messages provides authentication for WAVE multicast messages.</td>
</tr>
<tr>
<td>Encrypting Message Structures</td>
<td>The EncryptedMessage type is a subtype of the SecuredMessage type. A WAVE certificate contains one or two keys for either encryption, verification or both functions.</td>
</tr>
<tr>
<td>Provider Service ID (PSID)</td>
<td>A signed number that identifies a service provided by an application and announced in the WAVE Service Announcement (WSA) PSID.</td>
</tr>
<tr>
<td>Certificate Requests</td>
<td>Device provisioning with certificates use either ‘push’ or ‘pull’ model. ‘Pull Model’ is supported with a CSR message type in 1609.2.</td>
</tr>
<tr>
<td>Certificate Revocation Lists</td>
<td>1609.2 defines a CRL type. The ‘Security Manager’ annex describes the CRL functionality on a 1609 device (i.e. OBE).</td>
</tr>
</tbody>
</table>
Illustrative Mapping of 1609.2 Authorization Scenarios

Certificate Based Authorization

Classes of certificates identified by the 'subject_type'
VII Authentication Scenarios (1609.2 / 1609.3)

- **PKI for VII Devices** – All devices are issued with public-key certificates that grant permissions to take certain actions. *Public key certificates are a well-suited authentication method in the case where entities frequently have to communicate with other entities that they’ve never encountered before.* A device will typically have many different certificates. VII PKI requires a mechanism to remove certificates from the system if their owners misbehave (CRLs).

- **WAVE Short Messages (1609.3)** – A reduced-bandwidth unicast or broadcast message which is *digitally signed by an application per 1609.2* specifications. A WSM is routed to a receiving application using an Application Code Identifier (ACID) and an Application Code Mark (ACM) rather than an IP address and port.

- **Secure MultiCast (Broadcast) Messages** – Asynchronous applications. A secure message type is a published 1609.2 data structure with these options - *unsecured message, signed message* or *signed WSM*. Multicast messages from an OBU need to be authenticated to prove they originated from a legitimate vehicle at the correct time and location.

- **Secure Transactions (WSAs/PSTs)** – Synchronous applications. Protection of networks services (advertised in the Provider Service Table) is *enabled using signed WAVE Service Advertisement (WSAs)*. WSAs provide assurance that a legitimate service is being announced. Datagram TLS (DTLS) is the candidate security enabler for 1609.2 May require a full WAVE profile.

- **OBU to RSU** – There is currently no specification for OBU to RSU authentication. The *signed and encrypted message type* in 1609.2 encrypts the entire message and *could be used as a single authenticated response from the OBE*. This is the only mechanism used to secure transactions over WSMP.
Illustrative mapping of 1609.2 Authentication Scenarios
Table of Contents

- Introduction – Concept, Credits, and IdAM Architectural Models
- Researching the WAVE Standards and VII Model
- ITS Services and OSS Architecture
- WAVE Service Provisioning, Identity Management and PKI
- 1609.2 Additional Topics and Recommendations
- Summary
Welcome to the IEEE 1609 Working Group Public Site

The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. Together these standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management, and many others. This web site is primarily for the convenience of the members of the IEEE 1609 Working Group who are developing and maintaining these standards, and includes open minutes and public presentations from their meetings.

References to the presentations are given in the minutes. Materials are currently available from the following meetings:

- April 29-May 1, 2008, Los Angeles, California
  - Presentations
  - Minutes
  - Agenda
- August 26-27, 2008, Richmond, California
  - Presentations
  - Minutes
  - Agenda
  - Presentations
  - Minutes
  - Agenda

For more information about these standards and how they may be purchased, see the following reference:

http://vii.path.berkeley.edu/1609_wave/
Table of Contents

- Introduction – Concept, Credits, and IdAM Architectural Models
- Researching the WAVE Standards and VII Model
- Notional PKI Architecture for Authentication
- 1609.2 Capabilities and Features (AuthN, AuthZ, Cryptography)
- 1609.2 Additional Topics and Recommendations
- Summary
1609.2 Security Functions

- IEEE Draft Std 1609.2-2006 was issued July 6, 2006
- It contains formats for secured messages
  - Signed and encrypted
  - Elliptic curve cryptography (bandwidth)
- It contains mechanisms for identified authentication
  - Custom cert format
- It contains certificate issue and expiry mechanisms
- It does not contain:
  - Anonymous authentication mechanisms
  - Secure session protocols optimized for DSRC/WAVE setting (though note that standard internet secure protocols may be appropriate)
  - Any discussion of platform certification
- Note: The 1609 stack mandates 1609.2 security for WSAs. For all other applications, using 1609.2 security is optional.
ITS project: Security

- Implemented:
  - 1609.2 in software security libraries
    - Including some modifications to encrypted messages
  - ECC accelerator (250 verifications / sec with 256-bit keys)
  - Prototype secure session protocols
  - CA and protocol to communicate with it
  - Anonymous authentication mechanism

- Research projects on:
  - Anonymous authentication
    - Detailed analysis of one particular mechanism for over-the-air anonymous authentication
    - Implemented this mechanism in the security libraries
  - Misuse detection
1609.2/ITS Security Overhead

- Increase in bandwidth
  - ~ 200 bytes for a signed message with one certificate
    If cert is known to receiver reduce overhead to ~ 90 bytes.
  - ~ 150 bytes for an encrypted message with one recipient

- Computationally intensive
  - Software: 100 verifications / sec on 400 MHz PC
  - 5-ms latency requirement requires hardware acceleration
    No COTS ECC hardware currently available for this throughput
  - First signed message received from a given cert requires two verifications

- Infrastructure requirements
  - Issue certs and CRLs
    When app is installed / when vehicle is fitted out / when OBE is built
  - Accurate local time and position (also a requirement for the whole ITS project)

- Conclusions:
  - Bandwidth is acceptable
  - ITS infrastructure worked with small POC population
  - Concern about latency requirements
Thank you for joining us!

For Booz Allen Identity and Access Management ITS Engineering Project
WAVE Networking Services – WAVE Service Information Element

Services offered to user (OBU) applications are announced on the air interface via a WSIE inside a WAVE announcement frame.
WAVE Networking Services – WAVE Service Advertisement

- Frame Format with Optional Fields