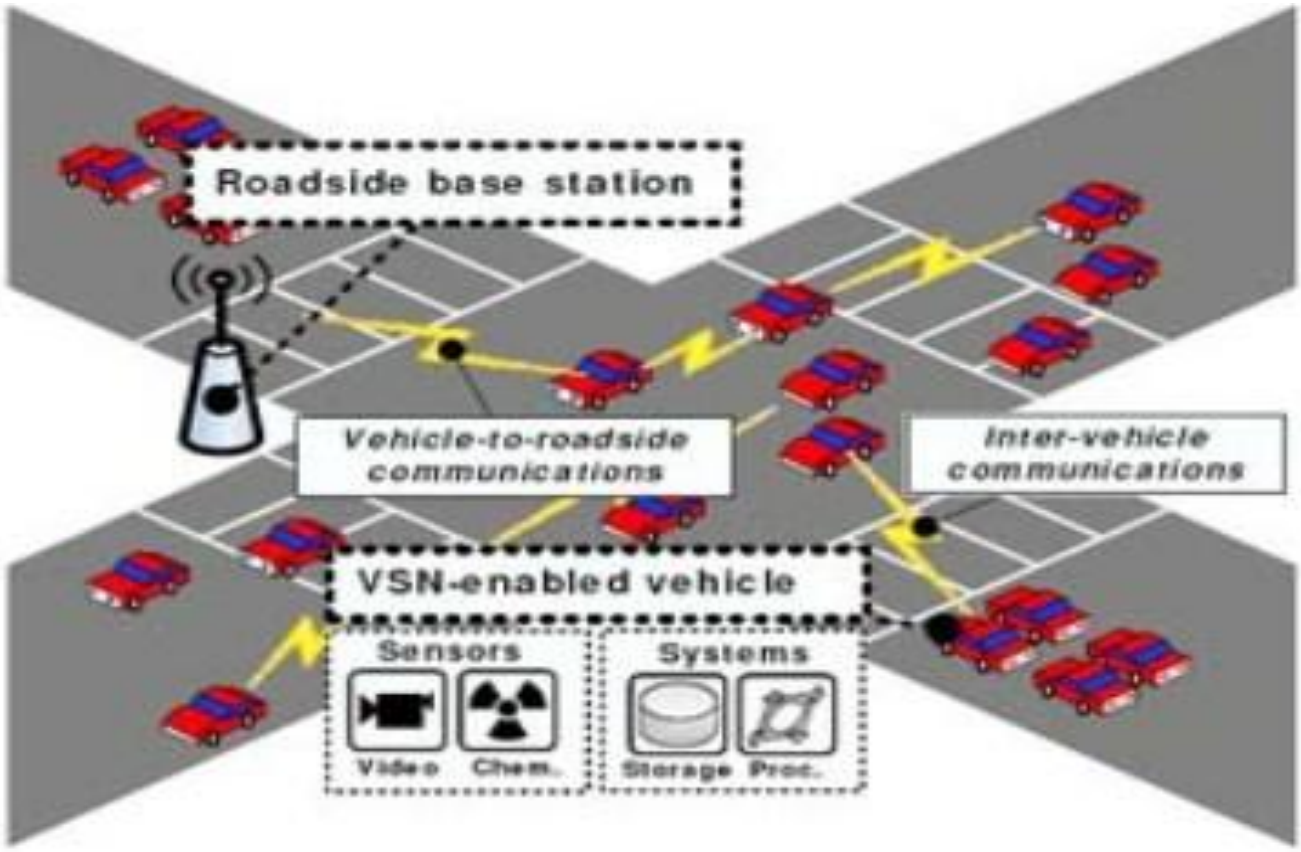
Applied Access Control for Vehicular Networks

Katya Kisyova

IGERT Presentation

4-9-2009

Vehicular Networks



Vehicular Networks

- Intelligent vehicles and surrounding infrastructure (nodes)
  - Vehicles already contain numerous embedded computer systems.
  - Communication enables nodes to share information / provide other nodes access to resources.
  - This information/knowledge can be used to enhance automated systems and as a result improve vehicle driver and passenger experience.

Vehicular Networks

- Sharing information is good, right?
  - Systems can be enhanced by sharing information—improved decision making.

Vehicular Networks

- Sharing information is good, right?
  - Systems can be enhanced by sharing information—improved decision making.
  - However, how much should a user be willing to share? With who? When? Where? Why… for what purpose?

Problem Statement

- Vehicular Networks have a need for an efficient means of enforcing who can access what resources, when, and where.

1. Access Control Model
   - Flexible to changes in user preferences
   - Scalable to large number of users
2. Enforcement
   - Guarantees that user preferences are met
   - Efficient when large amount of data is exchanged

Problem Statement

Challenges:

- User identities are not known in advance – how do we specify who has access if we don't know who they are
- Broadcast means of communication: everybody within communication range will receive the information, but we want only authorized nodes to be able to read it.
- Context Awareness: information and services are only relevant to some location.

Access Control Model

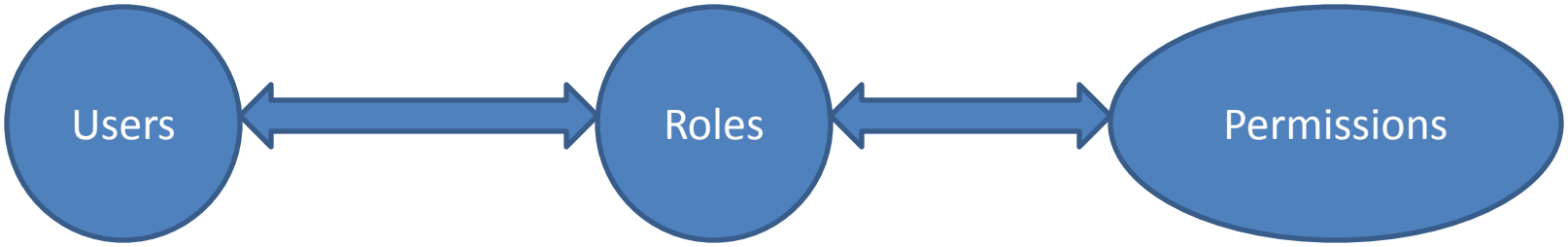
- Categorize users based on some common attributes
- Specify access control policies for each category of users

Example:

Vehicles	Infrastructure
Ambulances	Road Side Units
Police Vehicles	Traffic Lights
Regular Vehicles	Tolls

Role Based Access Control

- First proposed by Ferrairo and Kuhn[92] and later expanded by Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman[96]
- NIST Standard for RBAC [2000] : Sandhu, D.F. Ferraiolo, D, R. Kuhn (2000)



Role Based Access Control

- Why use RBAC?
  - Don’t need to know identities only common properties
  - Scales to large number of users: the policy will only be as large as the number of identified roles **X** number of permissions per role
  - Flexible to changes in user preferences: once a user is mapped into a role, we only need to change the permissions associated with the role, rather then re-categorize the user

How do we enforce RBAC?

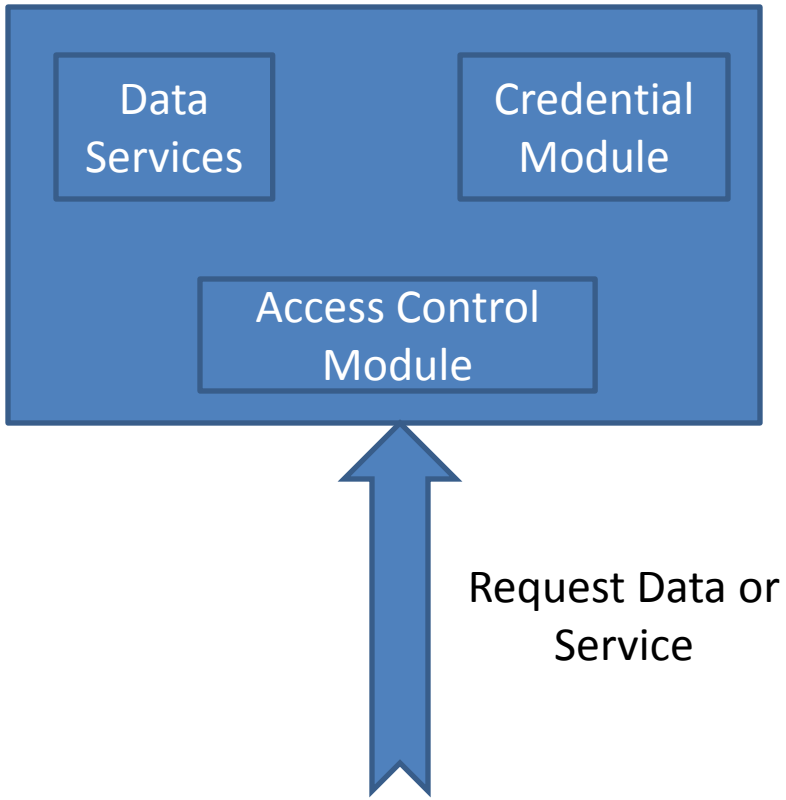
- Remaining challenges:
  - Broadcast means of communication: everybody within communication range will receive the information, but we want only authorized nodes to be able to read it.
  - Context Awareness: information and services are only relevant to some location.

How do we enforce RBAC?

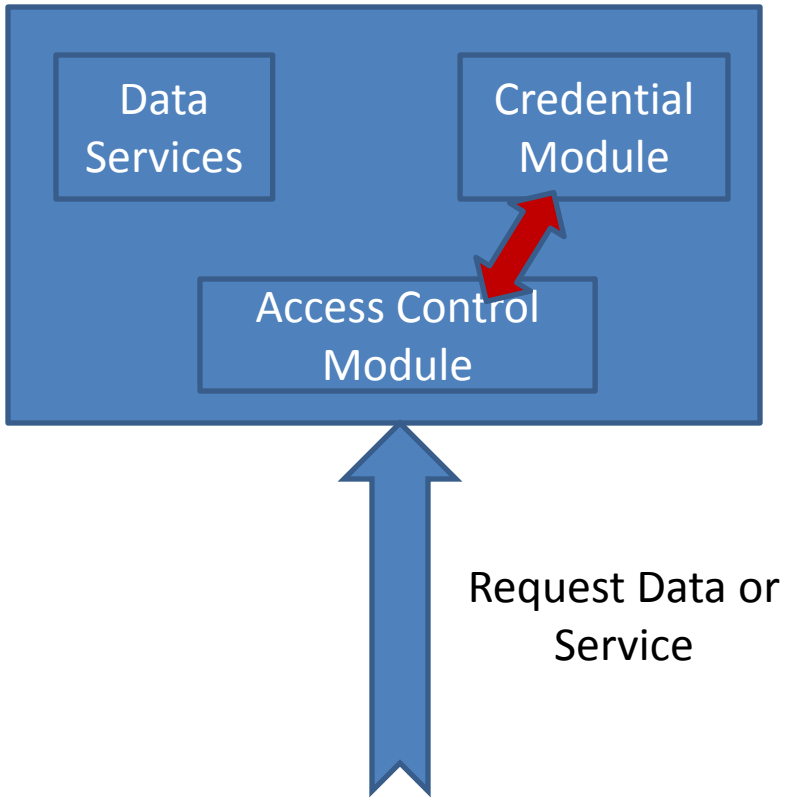
Assumptions:

- Trusted Third Party capable of distributing credentials to all users
- Users have tamper proof devices capable of securely storing credentials and verifying credentials
- Credentials can be used to:
  - Prove someone's identity or ownership of a set of attributes
  - To establish secure communication channels for exchange of information

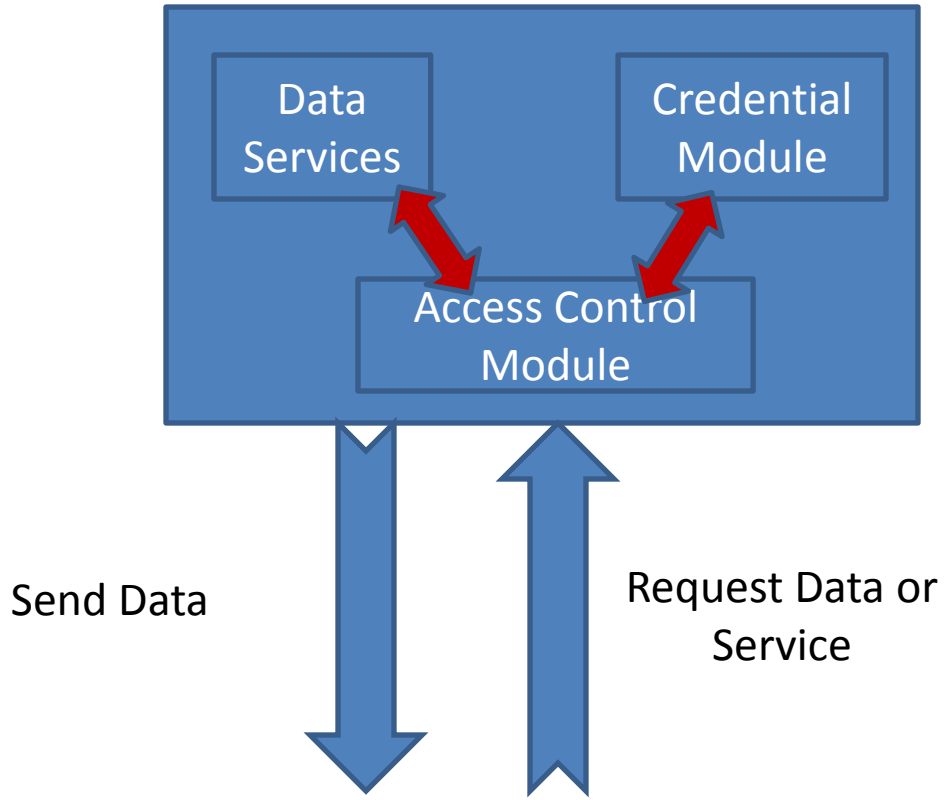
How do we enforce RBAC?



How do we enforce RBAC?



How do we enforce it?



How do we enforce RBAC?

- What will be the user credentials?
- How can we guarantee the person who requested the service/data is the one accessing it?

We can use cryptography to authenticate users and to securely transmit information.

  - Attribute Certificates
  - Attribute Based Encryption

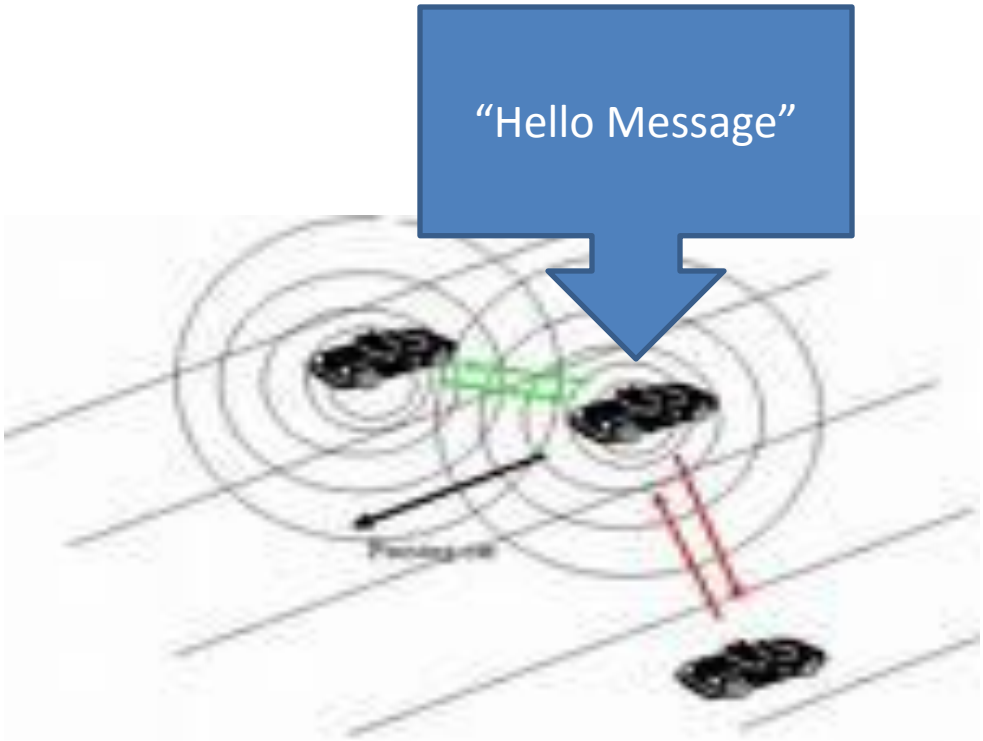
Distribute Credentials

Attribute Certificates

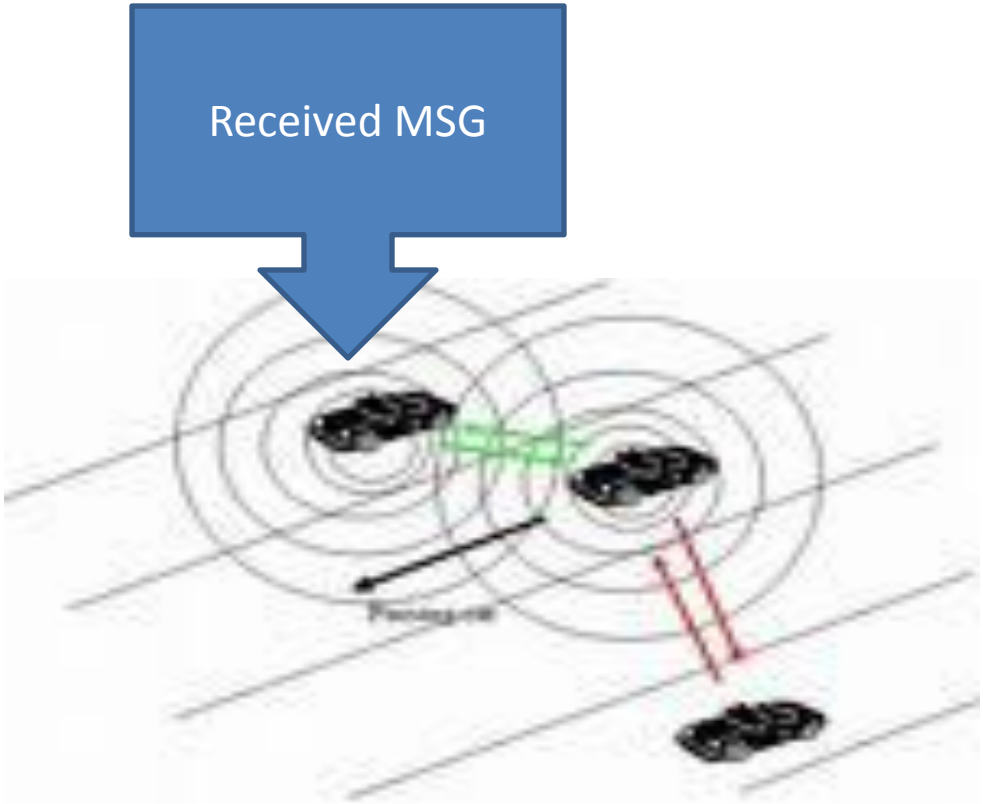
Attribute Certificate: a digital certificate that can be used to prove the right to access some service

- it is provided by the trusted third party
- Includes attributes related to the owner
- A user can have more then one attribute certificate related to different roles, or all attributes could be included into one certificate

Attribute Certificates



Attribute Certificates



Attribute Certificates

Attribute Certificates

- Problems: does not scale up when large number of users are present
  - Each user will need to keep credentials for all users
  - Redundant re-transmission of data: if we are sending information targeted at **N** number of users we can either send it in the clear or encrypt the message with each intended receivers key and send it out N-times

Attribute Based Encryption

- A. Shamir. “Identity-based cryptosystems and signature schemes", in Advances in Cryptology Crypto '84.
- A. Sahai and B. Waters, ”Fuzzy Identity-Based Encryption”, Advances in Cryptology-Eurocrypt’05.
- Proposed initially in e-mail communication: as means to encrypt messages without initial hand-shake and agreement on a secret key
- Trusted Third Party authority still distributes Public/Private keys, however anybody can re-create the public key by using some specific data about the recipient: e.g e-mail address
- Private keys are unique and encode attributes related to the owner

Attribute Based Encryption

- **Setup**: This step is done by a trusted third party called Private Key Generator(PKG). The operation takes a security parameter K and returns the set of *system parameters* and a *master-key*. The system parameters are publicly known, the master key is private and only known by the PKG.

- **Extract**: This step is also done by the PKG in order to create corresponding private keys for all members. Takes as input the *master-key*, system parameters and a set of attributes W (these attributes identify a person). For each attribute create a component *di*, the corresponding private key *d* is a combination of all components.

Attribute Based Encryption

- **Encrypt**: Takes as input the system parameters, any set of parameters A and a message M, and returns a corresponding cyphertext C.

- **Decrypt:** The receiver can read the message with his/her private key only if all attributes used for encryption were used as components *di* for building the private key**.**

Attribute Based Encryption

When a large number of recipients are considered, ABE is more efficient:

- If a user requests some information, the owner will encrypt it based on the access control policy associated with the information item and send it out: if the requestor has the corresponding credentials he/she can read it.
- If we want to broadcast information to a set of users **N** which have common characteristic**,** we only need to encrypt once using the appropriate access key.

Summary

Problem statement:

- ✓ 1. Access Control Model : **RBAC**
  - Flexible to changes in user preference
  - Scalable to large number of users
- ✓ 2. Enforcement : **AC** + **ABE**
  - Guarantees that user preferences are met
  - Efficient when large amount of data is exchanged

Future Work

- Evaluation
  - evaluate performance of AC over ABE: for what number of users should ABE be used over AC?
- Location Constraints?
  - Location information could be included as an attribute into the AC and the users private keys
  - Enforce constraints through the underlying communication protocol