Protecting Sensitive Data in VANETs Using Active Data Bundles

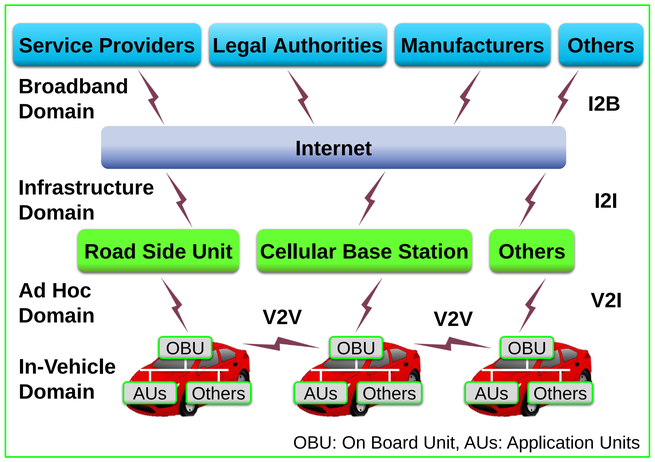
Abduljaleel M. Al Hasnawi (Advisor: Prof. Leszek T. Lilien)
Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

Introduction

Requirements for Vehicular Ad Hoc Networks (VANETs)
- Integrate capabilities of the next generation wireless networks into vehicles
- Share vehicular data over large-scale devices

Typical VANET Applications
- Traffic Safety, Traffic Efficiency, Convenience, Connectivity, Mobility

VANET Communications and Communication Domains
- V2V - Vehicle-to-Vehicle
- V2I - Vehicle-to-Infrastructure
- I2I - Infrastructure-to-Infrastructure
- I2B - Infrastructure-to-Broadband
- Domains: In-Vehicle, Ad Hoc, Infrastructure, Broadband



VANET Communications and Communication Domains

Privacy Challenges in VANETs
- Sharing of sensitive data by a large number of heterogeneous entities
- Revealing identity and location of vehicles, drivers and passengers
- Revealing driving style and habits, points of interests

Two types of Privacy Solutions for VANETs
- Privacy by design
  - Take privacy into account throughout the whole system design process
- Privacy by policy enforcement
  - Centralized policy enforcement
  - Decentralized policy enforcement

Our Focus: Privacy by Decentralized Policy Enforcement
- Avoid relying on centralized trusted third parties, bottleneck, single point of failure

Motivation, Objectives and Research Hypothesis

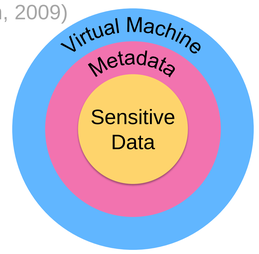
Motivation
- VANETs will not be accepted by the general public if they violate privacy of users
- Privacy of drivers and passengers depends on protecting sensitive VANET data

Objectives
- Protect sensitive data in VANETs throughout their entire lifecycle
- Limit access to sensitive data in VANETs based on the *need to know*

Research Hypothesis
- Sensitive data in VANETs can be protected throughout their *entire lifecycle* by enforcement of data owners' policies *using Active Data Bundles (ADBs)*, where the policies enforce the *need-to-know* principle
  - ADBs described next

Methods

Active Data Bundles (ADBs) (Ben Othmane&Lilien, 2009)
- Sensitive Data: data to be protected
- Metadata: specifies ADB policies
  - *Operational Policies*: control ADB behavior
  - *Access Control Policies*: control data dissemination and disclosure policies
  - *Verification Polices*: evaluate trust, check integrity
- Virtual Machine (VM): executes ADB in order to evaluate and enforce privacy policies
  - Results of policy enforcement:
    - *Full Data Disclosure:* disclosure of all ADB data
    - *Partial Data Disclosure*: disclosure of a part of ADB data due to an insufficient trust level of the visited host, followed by the selective data disclosure
    - *Apoptosis:* complete ADB self-destruction when ADB "feels" threatened with unauthorized disclosure of its data
  - VM is encrypted or obfuscated

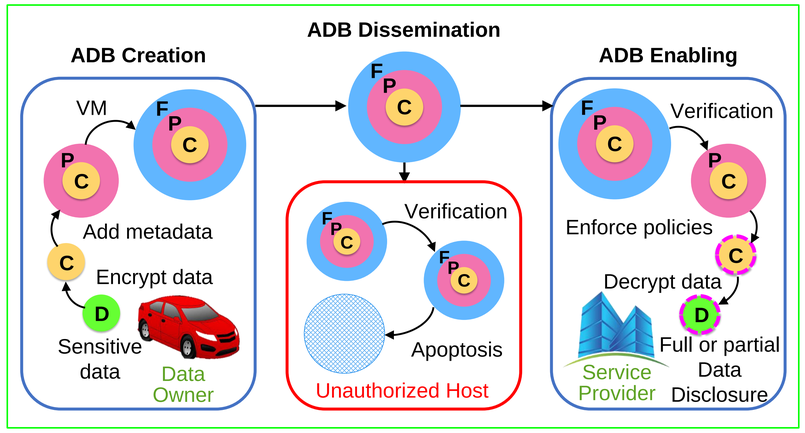


Mobile Agents (MAs)
- Software objects able to:
  - Interact with and use capabilities of visited hosts
  - Transport themselves from one host to another

Java Agent Development (JADE) (http://jade.tilab.com)
- Software framework fully implemented in the Java language
- Simplifies implementation of multi-agent systems

Results: The Proposed Solution

ADB Lifecycle in VANETs



ADB Lifecycle in VANETs

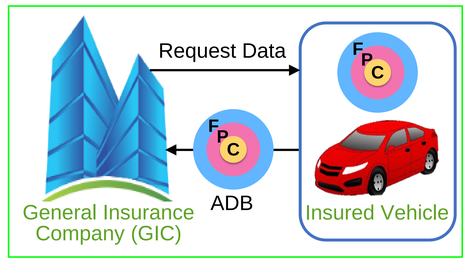
ADB Creation
- Identify data D to be protected by ADB
- Encrypt sensitive data D as cyphertext C
- Create policies P
- Construct virtual machine VM
  - Define policy enforcement functions F(C, P)
    - F(C, P) selectively discloses a subset of data D
  - Determine trust threshold ADB-TT for trust verification
  - Determine hash value ADB-HV for integrity verification

ADB Dissemination
- Plan ADB itinerary
- Get from security server trust values for all hosts in ADB itinerary
- Embed ADB components in an MA structure
- Sign digitally and disseminate ADB according to its itinerary

ADB Enabling
- ADB trust verification for Host H
  - If trust value for H less than ADB-TT, then apoptosis
    Otherwise, full or partial data disclosure
- ADB integrity verification for Host H
  - If hash value for H different than ADB-HV, then apoptosis
- ADB privacy policy enforcement for Host H
  - VM evaluates P for H
  - VM discloses data as indicated by F(C, P)
  - If H is the last host visited by ADB, then VM apoptosizes ADB
    Otherwise, ADB goes to the next host
- ADB decryption

Proof-of-Concept Scenario

Pay As You Drive (PAYD) Insurance Application Scenario
- Insurer requests driving data from an insured vehicle
- Insurance fees calculated based on sensitive data:
  - Distance driven in a period of time
  - Driving style: speed, acceleration, time of day, …



PAYD Scenario using ADB

Virtual Machine
- ADB Verification (TT and HV)
- Enforcement (access control)

Metadata

Operational Policies
Creator ID, owner ID, creation date, itinerary, ADB lifetime, …,

Access Control Policies
ID: Unique ID
Distance: SUM(loc_1, …, loc_n)
Speed: AVG($speed_1$, …, $speed_n$)
Acceleration: AVG(acc_1, …, acc_n)
Time: INTERVAL [x, y]
Data user: General Insurance Co.
Purpose: Billing

Verification Policies
Trust: ADB-TT
Integrity: ADB-HV

Sensitive Data
VID, distance, speed, acc., time

loc—location, acc—acceleration

ADB in PAYD Scenario

Using ADB in PAYD
- Identify driving data in ADB
- Specify ADB operational policies
- Specify ADB access control policies
- Specify ADB verification policies
- Enforce policies specified in metadata
  - Assure policy-based access control
  - Assure data protection by trust verification
  - Assure data integrity by integrity self-checks

Results
- Insurer Perspective
  - Access to data limited by policy enforcement functions and subfunctions
- Adversary Perspective
  - Sensitive data protected by ADB

Conclusions and Future Work

Conclusions
- Integrating ADB with VANETs in an effective and efficient way should solve most of the privacy issues in VANETs
- ADB is extensible - allows adding more security and privacy protection mechanisms
  - According to the sensitivity of the carried data

Future Work
- Evaluate using ADB in VANETs via simulation
- Propose ADB routing protocol for VANETs
- Apply the proposed solution to diverse VANET applications