TCIPG

Incubator Project

Privacy-Preserving Vehicle-Miles-Traveled Tax Scheme

Chin-Wei Chang, Carl Hauser, and Thoshitha Gamage

GOALS

- Design a vehicle tax scheme based on Vehicle Miles Traveled.
  - Correctness:
    - Tax paid by car owner is proportional to the number of miles driven.
    - Tax revenue is allocated to each state accurately.
  - Security:
    - Users' confidential information is not revealed.
    - System can detect incorrect reporting.
    - System can identify malicious actors.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Current fuel tax may not be suitable for modern vehicles.
  - Some vehicles don't use gasoline (e.g., solar vehicles and battery electric vehicles).
  - Fuel-efficient cars.
- An existing proposal: Vehicle Miles Traveled tax (VMT).
  - Tax based on mileage driven instead of gasoline consumption.
  - The government (or agent) needs mileage data in order to calculate owed taxes and verify correctness.
  - Challenges:
    - Accuracy: Locating cars precisely.
      - Solutions: GPS, toll station, plate recognition, etc.
    - Privacy: confidential information (e.g., location or travel history) could be inferred from mileage data.
      - System entities (on-board devices, government, etc.) should not learn more information than necessary.

RESEARCH PLAN

- Design a vehicle tax scheme that can guarantee accuracy and privacy.
- List possible attack models and investigate their impacts on our scheme.
- Evaluate large-scale performance of our scheme.

Foundation

- Use encryption mechanisms (RSA and AES) to achieve confidentiality (privacy), authentication, and nonrepudiation.
- User identities are concealed by hash chains (SHA1).
- Ring structure network is used during verification process.

Basic Entities

- Car owner: a user who has a registered vehicle and must pay VMT tax.
- Federal government: collects tax from car owners, and then allocates the funding to each state.
- State: each geographical state may have a different tax rate.

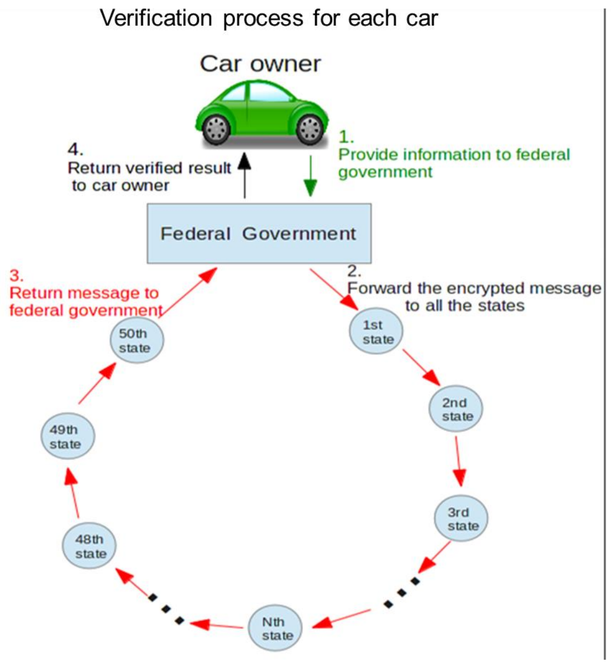
Assumptions

- Users have on-board devices installed on their vehicles.
  - The on-board devices can accumulate mileage in each state.
- Privacy issues related to on-board devices are beyond the scope of our research.

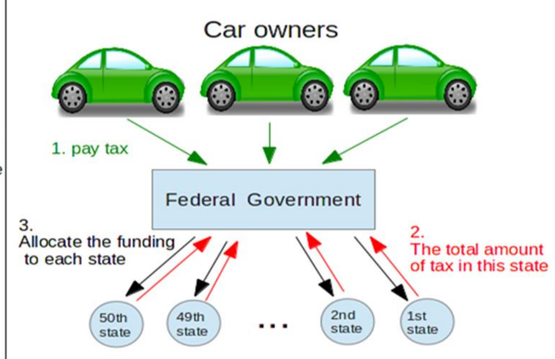
Overview of the Scheme

- Total tax owed by car owner is revealed to federal government.
  - Taxes incurred in each state and mileage remain confidential.
- States cannot link mileage of individual cars to owners' identities.
- Mileage verification data are collected state by state through a ring structure. Each state knows the forwarding information only for its neighbors in the ring.
  - States may be grouped into multiple rings to optimize overhead.

Verification process for each car



Payment structure once the verification process has been completed for all car owners



Details of the Scheme

User:

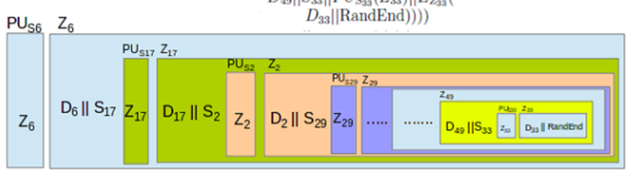
User provides following encrypted data to federal government:
$D_1 = PU_{S_1}(N_1||K_1||\text{Mile}_{S_1})$
$D_2 = PU_{S_2}(N_2||K_2||\text{Mile}_{S_2})$
$D_3 = PU_{S_3}(N_3||K_3||\text{Mile}_{S_3})$
.....
$D_{50} = PU_{S_{50}}(N_{50}||K_{50}||\text{Mile}_{S_{50}})$
and Bias, K_0, amount of Tax.

For State i:

(assume that state $i-1$ is the previous state in the sequence, and state $i+1$ is the next state in the sequence)
1. Decrypt message, calculate $A_i = A_{i-1} + \text{Mile}_{S_i} * \text{Tax}_i$
2. Remove $PU_{S_i}(Z_i)$, D_i, and S_{i+1} from the List
3. $\text{Verify}_i = N_i||E_{K_i}(A_{i-1}||\text{Verify}_{i-1})$
4. Send the following message to the next state:
$PU_{S_{i+1}}(K_{temp})||E_{K_{temp}}(R_i||A_i||\text{Verify}_i||\text{List})$
or send to the federal government:
$PU_{S_0}(K_{temp})||E_{K_{temp}}((R_i||A_i||\text{Verify}_i)$

Federal government:

1. Decide a sequence for 50 states.(e.g. $S_6, S_{17}, S_2, S_{28}.....S_{49}, S_{33}$)
2. Generate a sequential encrypted list:
$\text{List} = PU_{S_6}(Z_6)||E_{Z_6}($
$D_6||S_{17}||PU_{S_{17}}(Z_{17})||E_{Z_{17}}($
$D_{17}||S_2||PU_{S_2}(Z_2)||E_{Z_2}($
$D_2||S_{28}.....$
$.....E_{Z_{49}}($
$D_{49}||S_{33}||PU_{S_{33}}(Z_{33})||E_{Z_{33}}($
$D_{33}||\text{RandEnd}))))$



3. Send this message to the first state (e.g. state 6,)
$PU_{S_6}||E_{Z_6}(R_0||A_0||\text{Verify}_0||\text{List})$

The Format of the Table in state i

Reference ID (R_i)	Miles in this state	Next state	Status

The Format of the Table in Federal Government

Car ID	R_0	Amount of Tax	Bias	The First State	Status

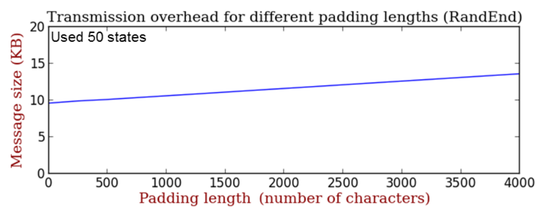
K_{temp}	a one-time symmetric key
R_i	R_i= hash(R_{i-1})

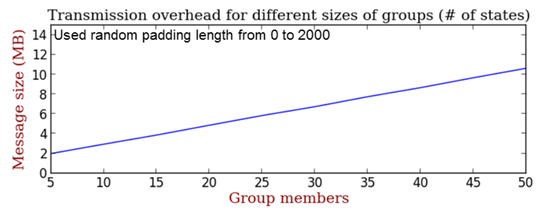
Mile_{S_i}	miles driven in state i
N_i	a (random) number that represents the state i
K_i	symmetric keys
Bias	a random number

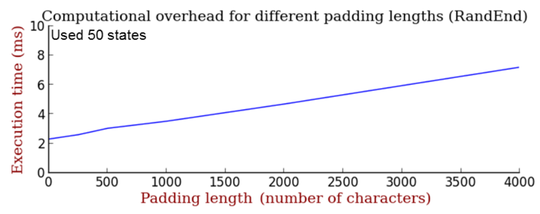
R_0	hash value of user ID
A_0	initial accumulated amount of tax: 0 + Bias
$RandEnd$	A random string with arbitrary length
Verify_0	$N_0||E_{K_0}(RandEnd)$
Z_i	a symmetric key for state i

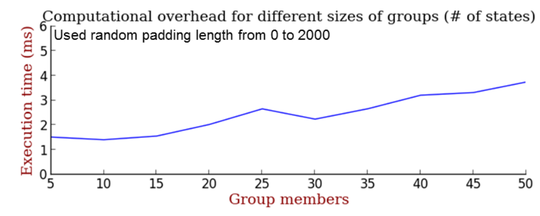
RESEARCH RESULTS

- Performance using 50 states (averaged over 500 trials):
  - Transmission overhead: 10.63 KB for each message sent from the government to the first state.
  - Computational overhead: 3.7 ms for the federal government to generate an encrypted message.
  - Large scale: approximately 257 hrs to generate all the encrypted messages for 250 million car owners.









CPU:3000MHz, Memory:8G, Programing language: Python

BROADER IMPACT

- Provides an infrastructure for implementing vehicle tax schemes.
- Addresses privacy issues associated with VMT tax.

INTERACTION WITH OTHER PROJECTS

- Potential integration with VMT projects (e.g., Oregon VMT tax pilot project).
- Complements projects addressing privacy issues with on-board devices.

FUTURE EFFORTS

- Consider the geographical relation between states. Experiment with group size in order to improve performance without reducing privacy strength.
- Implement reputation-based grouping of users to optimize performance.
- Address the threat of denial of service attacks.

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T