Fraunhofer Institute for Open Communication Systems

Risk Analysis for Privacy in VANETs

Matthias.Gerlach@fokus.fraunhofer.de

Motivation

We all know intuitively

- "Privacy is Important"
- "We need Changing Pseudonyms"

But we don't know

- What kinds of attacks are probable
- What types of attackers will be there

These are the results of a Risk Analysis

Approach

Attack Trees

- Hierarchical
- Structured
- A common means to write down attacks [Schneier99]

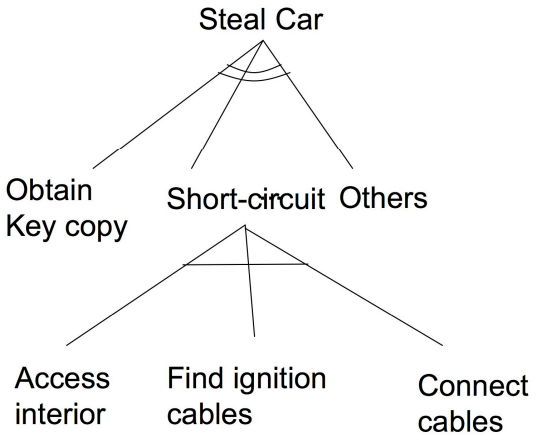
Risk Analysis

- Mark up attacks as attack tree
- Estimate cost and other prerequisites for the attacker
- Find out cheap and probable attacks

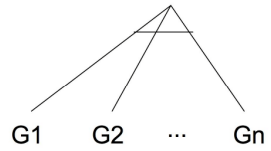
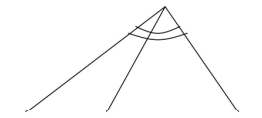
Assumptions

- Permanent pseudonym
- Broadcast of pseudonym, location, time

Example Attack Tree



Goal **Steal Car** (OR)
- Obtain Key copy
- Short circuit (AND)
  - Access Interior
  - Find ignition cables
  - Connect cables
- Others

	graphical	textual
AND		Goal G0 (AND) G1 G2 ... Gn
OR		Goal G0 (OR) G1 G2 ... Gn

AND - all subattacks (cost add)
OR - one subattack (cheapest cost counts)

Top Level View

Violate privacy

- perception different for different people
- „obtain current or past location(s)“ according to Beresford‘s definition

Two subattacks to violate privacy:

- Track location (pseudonym, time, location)
- Link pseudonym to name

Finally: make use of obtained data

- matter of creativity

Location Tracking (1)

Attack Method

- Build a grid of receivers
- Connect these receivers
- Store the data
- Process the data

Coarse Cost Estimation (Examples)

- Road Side Unit (10 .. 30 EUR)
- Surveillance Camera (50 .. 100 EUR)
- DSL Connection (0 .. 15 EUR / Month)
- Storage (3K EUR / Tbyte)
- Access to database of phone provider (Proper Authorization)

Location Tracking (2)

Attack Parameters

- Parameters for the abovementioned attack method
- Number of targets
- Coverage

Attack Dimensions:

- All nodes, everywhere
- Some nodes, everywhere
- All nodes, some place
- Some nodes, some place

All nodes, everywhere

Fraunhofer FOKUS Institute for Open Communication Systems

Assumptions

- City of Berlin
- Permanent pseudonym
- Record a beacon every 3 seconds

Conclusion

- Probably rather expensive for an attacker
- Rather improbable attack

Build a grid of receivers

- Cheap, order of 200 K EUR

Connect these receivers

- Expensive, order of 2 Million EUR per year

Store the data

- 6 TB per day (this can probably be reduced) = 18 K EUR per day

Process the data

- Not taken into account

- Countermeasures:
  - Change the identifier
  - Do not provide more accurate data than necessary
  - Do not provide more data than necessary

Some nodes, everywhere

Possible attacks:

- All nodes, everywhere approach
- Use location requests, router functionality

Attacker would go for second possibility

Cost:

- A NOW Receiver (order of 100 EUR)
- Small database (Up to date PC)
- Dense enough network (Our Goal :-))

I consider this as a probable attack.

Countermeasures

- Artificially restrict max hops for location query
- Change pseudonym frequently
- Block frequent location queries by the network

All nodes, some place

Install a receiver at a fixed location

Log all beacons nodes at a specific location

Cost

- A NOW Receiver (order of 100 EUR)
- Small database (Up to date PC)
- Dense enough network (Our Goal :-))

I consider this as a probable attack.

Countermeasures

- Do you know any?

Link Pseudonym to User

The last attack yielded only a pseudonym

Useless without a name attached to it

This attack is about getting your name

Candidates:

- Use an existing database
- Restricted space identification
- Inference from external database information
- Ask

Use an Existing Database

We proposed to create such a database to be able to revoke faulty/malicious nodes

This database links pseudonyms to names

Authorized entities may use this database

Cost:

- be authorized to use the database (high)

Not a very probable attack (except for the „authorized party“)

Restricted Space Identification

Use a publicly known one-to-one mapping of location and name (like home address)

Example:

- Obtain home location
- Obtain home address (trivial, using a map software)
- Get name from address (in theory, this data is contained in phonebooks)

Discussion:

- One-to-one mapping not always there
- For particular pseudonym, need full track to find this mapping

Inference from External Database Information

Some also call this *statistical disclosure*

Method:

- Create (external) user profile
- Link the profile to the vehicle

Example:

- Database says user drives blue car
- User just paid
- There is only one blue car on the parking (voilá)

Discussion

- The better the profile or if there are additional tokens (such as parking-ticket, RFID tokens), this attack is easy

Countermeasures

- Reduce accuracy of disclosed data
- Change pseudonyms shortly after/before possibly statistical disclosure

Ask

Use the name when embedded in a packet

Typical applications are

- Credit card payment
- Loyalty cards

Discussion

- The cheapest method to get the pseudonym name mapping
- Very probable
- But: user decides when to provide this (at least once: when installing the application)

Link Changing Pseudonyms

The previous slides suggest that changing pseudonyms is a solution.

What are possible attacks on pseudonym change algorithms?

Assumption:

- Attacker has a set of messages with different pseudonyms (Track location classification applies)
- Objective: link messages coming from the same sender.

Attack Classification

- Based on non volatile data (e.g. vehicle brand)
- Protocol based attacks (e.g. beacon send period)
- Attacks based on physical parameters and constraints

Cost Gain Analysis

- Depends on the quality/quantity of available data
- Measured rather in terms of confidence in resolution (or meters after which a track is lost) than in money

Use Location and Name - Real World Attacks

Now the attacker knows your tracks (or parts thereof) and your name.

What could he do with it (Some ideas):

- Request a fine
- Blackmail
- Personalized advertisements, spamming
- Price discrimination
- Suspicion by location

Price Discrimination

Is current practice in commercial scenarios

Change the price according to a profile of a user.

Example:

- Parking price is higher for cars of certain users
- Get the desired item (parking space, Big Mac, ...) only if you visited a certain location

Attacker:

- Commercial enterprises

Suspicion by location

Firefighter case (Based on a loyalty card profile a firefighter has been put in jail for six months)

Abuse of information

Information collected by commercial enterprises

Misused by authorities

Example

- anyone whose pseudonym has been observed at a crime scene may be guilty.

Conclusion

This is still work in progress

Attacks

- Global attacker is improbable but feasible, in particular if attackers team up (www.payback.com)

Attackers

- Rather not governments (yet - access to the pseudonym - name database should be restricted),
- Rarely individuals
- Pretty surely commercial enterprises

Countermeasures

- Changing pseudonyms are a good choice; make most attacks harder to carry out.

Acknowledgements

This work has been carried out within the Network on Wheels Project.