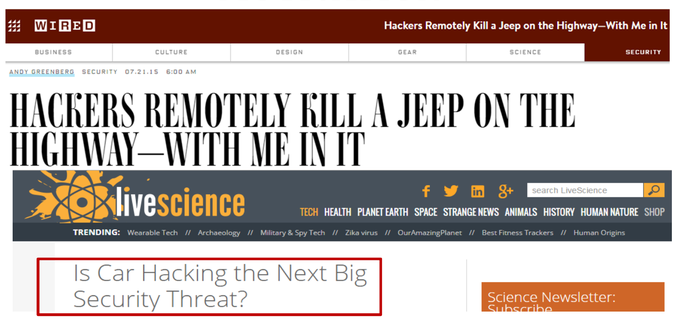
CERIAS

The Center for Education and Research in Information Assurance and Security

Systematic Attack Analysis and Adaptive Security in V2V Networks

Bharat Bhargava, Pelin Angin, Miguel Villarreal-Vasquez, Amber Johnson, Gisele Munyengabe, Denis Ulybyshev
CS and CERIAS, Purdue University, West Lafayette, IN 47907

MOTIVATION


WIRED — Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

livescience — search LiveScience

TECH HEALTH PLANET EARTH SPACE STRANGE NEWS ANIMALS HISTORY HUMAN NATURE SHOP

TRENDING: Wearable Tech // Archaeology // Military & Spy Tech // Zika virus // OurAmazingPlanet // Best Fitness Trackers // Human Origins

Is Car Hacking the Next Big Security Threat?

Science Newsletter: Subscribe

- Security and privacy of communications and data affects vehicle safety.
- **Authenticating source and messages causes overheads and delay for critical actions such as braking, turning and changing lanes.**

PROPOSED SOLUTION: ADAPTIVE SECURITY

❑ Adapt/Change security measures/parameters based on:
- sensitivity/type of messages
- safety level of vehicles
- context
- congestions/accident/mobility of vehicles
- communication parameters: latency, losses

SECURITY METRICS

❑ Secure throughput
❑ Error detection rate / Corrupt data acceptance
❑ Certificate revocation speed
❑ Degree of privacy

SAFETY-RELIABILITY METRICS

❑ Packet reception ratio
❑ Packet delivery ratio
❑ Successful packet delivery probability
❑ Effective range
❑ Connectivity in multi-hop VANETs

ATTACK ANALYSIS APPROACH

Construct anatomy of attack, implementation/ mitigation costs, identifying similar features across attacks

Anatomy of an attack:

❑ Name
❑ Description
❑ Features
❑ Mitigation
❑ Cost
❑ Impact on safety
❑ Impact on security

SECURITY / SAFETY ISSUES

❑ Confidentiality: attackers may have full access to a generic DSRC radio:
- Related attacks: eavesdropping messages, stealing location information, ID disclosure or track location

❑ Authenticity and integrity: vehicles may present erroneous warnings:
- Related attacks: Replay attacks, GPS spoofing, tunneling, sybil attacks, masquerade attacks.

❑ Availability: safety critical messages not to bse transmitted correctly
- Related attacks: DoS attack, black hole attacks

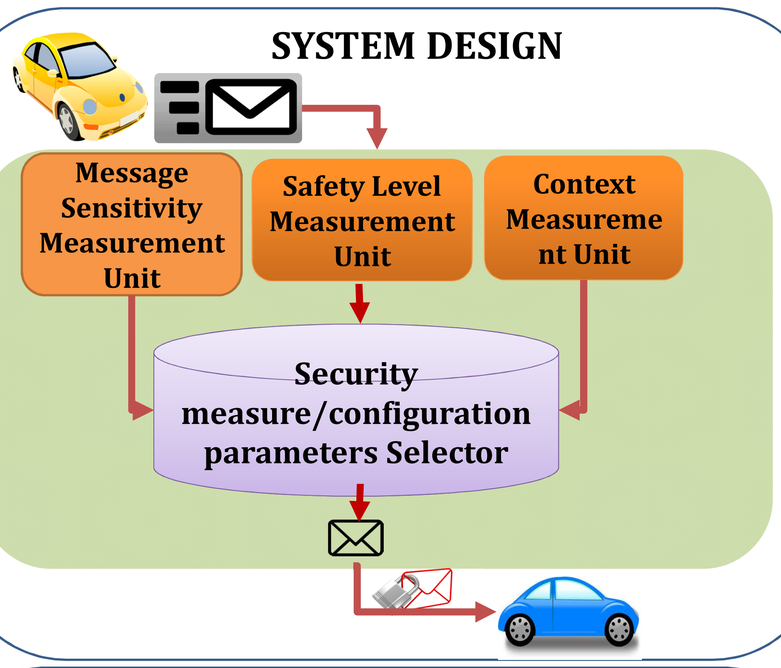
❖ contacting other vehicles through secure channel establishment may result in packet loss*

❑ Hidden terminal problem in broadcast
- Data packet collisions

❑ Radio channel fading
- Mult,iple reflecting objects degrade signal quality

❑ Impact of high mobility
- High mobility may cause adverse effects on performance of sending/receiving

SYSTEM DESIGN



ATTACK ANALYSIS EXAMPLE

GPS Spoofing and Hidden Vehicle Attack

❑ Description: Attacker creates false GPS readings to deceive other vehicles
❑ Mitigation: Digital signatures
❑ Attack cost: C1: No alert issued, C2: Response delay, C3: Entering dangerous road situation
❑ Mitigation cost: C4: Signature verification time, C5: Increased number of broadcasts
❑ Impact on safety: Cryptographic loss
❑ Impact on security: Negative effect on real-time transactions

CHALLENGES

❑ Adding security measures to prevent all possible attacks causes high performance overhead.
❑ High performance overheads affect accuracy and timeliness of message transmissions for safe operation of vehicle.

SAFETY-SECURITY-PERFORMANCE TRADE OFFS

Different security measures of different configuration parameters for a secure channel result in different performance overhead

Complexity of authentication mechanisms

Complexity ↑ → Security ↑ → Performance ↓

Key management:

PKI: Key management time ↓, authentication time ↑

Symmetric: Key management time↑, authentication time↓

Certificate revocation:

Performance ↑ → Safety ↑ , Security ↑

Privacy:

Complexity ↑ → Security ↑ → Performance ↓

IMPLEMENTATION PLATFORMS

❑ SUMO: Simulation of Urban Mobility (sumo.dlr.de)
❑ TraNS: Realistic Joint Traffic and Network Simulator for VANETs
- Open source traffic simulator (trans.epfl.ch)
- Links to SUMO and ns2 network simulator
- Goal is to avoid having simulation results that differ significantly from those obtained by real-world experiments

COST ANALYSIS EXAMPLE

GPS Spoofing and Hidden Vehicle

Code	Transaction	Total cost
T00	Receive message	μ
T01	Get Satellite Signal	100 ms
T02	Compute Position	0.3 ms
T1	Message Authentication	1.48 ms
T2	Collision Distance	0.5 ms
T3	Send Notification	2 ms
	Total overhead	104.28 ms + μ

ACKNOWLEDGEMENT: This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

CERIAS

PURDUE UNIVERSITY