1 Title Page (1p)

- Title: Security in automobiles: OBD-II Access Control.

2 Abstract (1/2p)

3 Introduction (3-5 pages)

- **Problem Statement + Motivation**: briefly explain (through examples) the vulnerability of the current modern automobile (attack vectors).
- **Challenges**: basically sufficiently secure + fast.
- **Context**: How does my solution fit into other existing security solutions (e.g. Authentication of nodes, secure key storage, etc).
- **Proposed contribution**: Secure OBD-II authentication.
- **Outline** (basically this text).

4 Literature Review(17-22p)

4.1 Vehicle network Infrastructure (2p)

- ECU's.
- Communication protocols (can etc).
- Gateway.

4.2 OBDII protocol (2-3p)

- The goal of OBDII.
- brief history.
- DLC.
- PID's.
- Scan Tools
- Signalling protocols (can etc).

4.3 CAN Protocol (2-3p)

- brief history.
- Architecture.
- CAN frames.
- CAN priorities.
- CAN security vulnerabilities.

4.4 OBDII Security Threats (4-5p)

- Architectural shortcomings.
- examples of potential attacks.
- examples of impact of attacks.
- e.g. charlie miller and chris valasek.

4.5 Related Work (8-10p)

- Survey of potential attack vectors.
- other proposed OBD security measure (e.g Seed-key).
- Internal vehicle security (e.g. Leia, VatiCAN, VulCAN, CANcrypt).
- External vehicle security (e.g. DoIp, UDS, Connected Repair shop, etc).
- Automobile security requirements/assurance levels: Autosar, ASIL, ASEAL, ENISA.

4.6 Conclusion (1p)

- propose that is is proven that proposed OBD access control solution is a solid addition to the existing automotive security landscape.

5 Preliminaries

5.1 Hardware requirements/limitations (2-4p)

- Typical ECU hardware (e.g 8/16 bit microcontroller).

5.2 Security Primitives (5-6p)

- ECC/ECDSA/ECSS
- Hashing (sha)
- Hmac-Sha
- Secure API for key operations (SGX enclave?)

6 Solution

6.1 Role based Access Control (8-10p)

- types of roles: repairman, dealer, police, etc.
- allocation of public keys to roles.
- Authentication algorithm (both scenarios).
- Key distribution and access.

7 Implementation (8-10p)

- Hardware overview (AT90CAN boards with CAN controller).
- Implementation assumptions: RNG, OBD-Messages, other Gateway functionality, etc.
- implementation specifics (permission table, private key API, etc).
- Demo results (pictures).
- used libraries: AVR-crypto, tinyECC, SANCUS.

8 Evaluation (5p)

8.1 Security Evaluation

- cryptographic strength: ECC, Shared secret, Hmac.
- security against potential attacks: MiM, Side-channel, bruto force, etc.
- importance of secure private key storage.

8.2 Performance Evalution

9 Future Work (3-4p)

- study on which/how many roles are required.
- Private Key infrastructure.
- Raising Automotive industry awareness.

10 Conclusion (1-2 p)

11 References

.