Smart-car identity and access management (IAM) system developed

August 12 2021, by John Stevenson

Credit: City University London

A postgraduate student in City's Institute for Cyber Security (ICS) is attempting to plug the vulnerability gaps of smart cars to hacking and security breaches.

Subhajit Bandopadhyay, studying for a Ph.D. under the supervision of Professor Muttukrishnan Rajarajan, director of the ICS, has been involved in [collaborative research](#) to develop the SIUV—a stateful smart car identity and access management (IAM) system, based on usage control (UCON) and verifiable credentials (VCs).

SIUV comes out of Subhajit's research paper, co-authored by Professor Rajarajan, Ali Hariri (Huawei Munich Research Center and the University of Trento), Dr. Athanasios Rizos (Huawei Munich Research Center), Dr. Theo Dimitrakos (Huawei Munich Research Center and the University of Kent) and Professor Bruno Crispo (University of Trento), which was successfully submitted to the 36th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2021) in June 2021.

Over recent decades, several successive innovations have transformed the [motor vehicle](#) into a digital system on wheels. Otherwise known as intelligent cars, smart cars have evolved into safety-critical and cyber-physical systems which are increasingly exposed to cyber vulnerabilities.
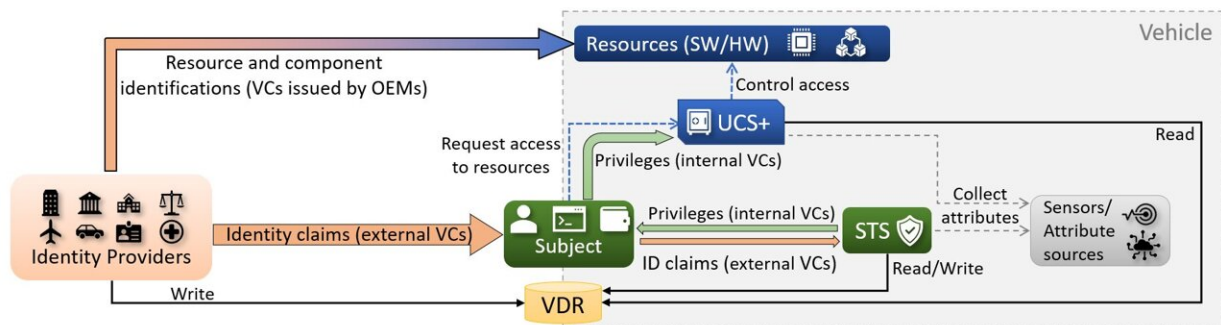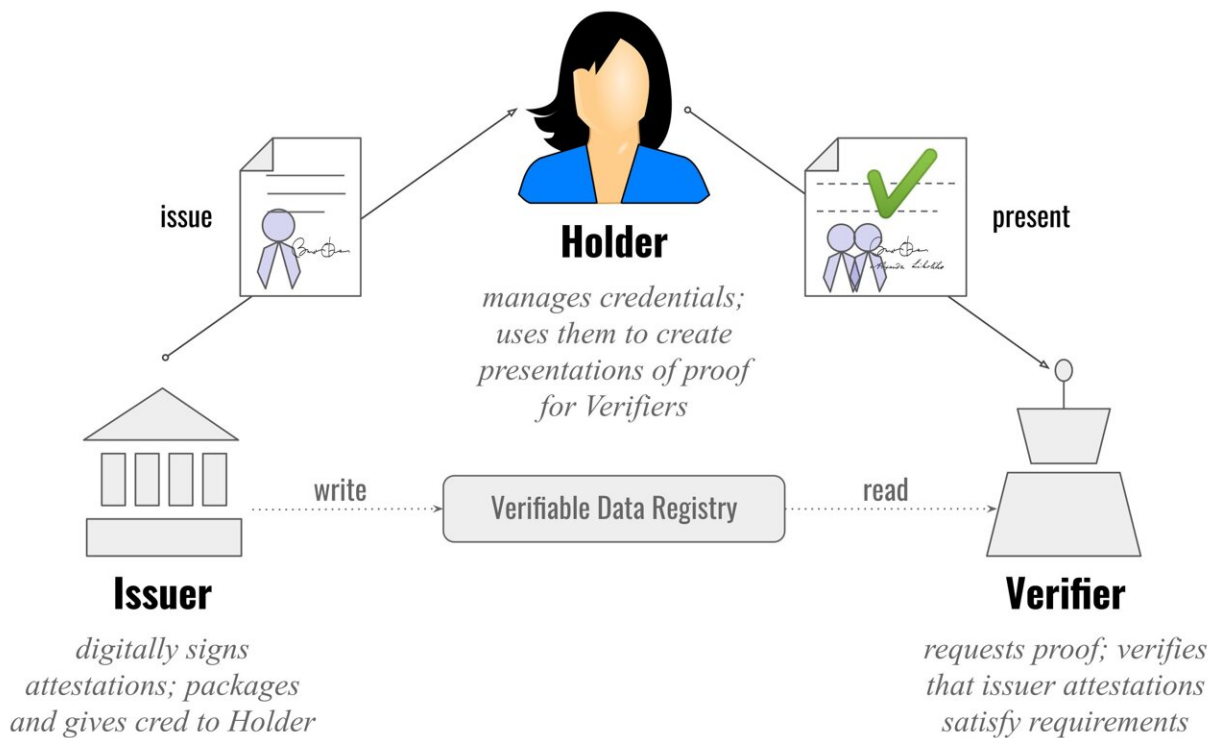
Credit: City University London

SIUV uses usage control policies in order to issue privileges to drivers or applications (such as the deployment of air bags or speed limit control) according to their credentials or claims. The issued privileges are then used to decide whether to grant or deny access to in-car resources.

SIUV also continuously monitors subject claims, resource attributes and environmental conditions such as time or location so that if a change is made, the system can re-evaluate policies, provide updates or revoke issued privileges and usage decisions accordingly.

To understand the work of Subhajit and his colleagues here is a realistic

scenario.

Alice, for example, goes to a car rental company to rent a vehicle for 48 hours to be driven in the London metropolitan area. The car rental company then defines the policies according to their agreement with Alice, and makes this information available for use via SIUV.

Credit: City University London

Alice visits Cambridge briefly and thought the car rental company wouldn't be aware of this. When Alice was about to leave London's city limits, the car displays geographical restriction warnings and suggests

rerouting to stay within the London metropolitan area.

This occurs because of the continuous usage control architecture of SIUV. Verifiable credentials help keep claims secure and verifiable at all times, making them a great alternative to physical cards that are currently issued as driving licenses.

The UK Driver and Vehicle Licensing Agency (DVLA) can be a potential trusted issuer of driving licenses in the form of verifiable credentials that are cryptographically verifiable. The claims within the credential can be continuously validated and access to the in-car components can be allowed or denied based on the usage control policy evaluations by SIUV.

The automotive market is growing rapidly in transforming mechanical car components into digital systems.

From a software perspective, this makes research work on the SIUV vital in comprehensively taking care of the safety and security of the smart cars of the future.

More information: Ali Hariri et al, SIUV: A Smart Car Identity Management and Usage Control System Based on Verifiable Credentials, *ICT Systems Security and Privacy Protection* (2021). DOI: 10.1007/978-3-030-78120-0_3

Provided by City University London