dimecres, 24 de febrer de 2021

Nou sistema de la UdL per pagar parquímetre amb més privacitat per a l'usuari

Publiquen els detalls a la revista 'International Journal of Information Security'

Zona blava / Foto: UdL

Investigadors de la Universitat de Lleida (UdL) han desenvolupat un sistema per pagar l'aparcament en zones públiques regulades mitjançant el telèfon mòbil amb més seguretat i garanties de privacitat pels usuaris. Asseguren que presenta les mateixes funcionalitats que els més complets que existeixen i resulta més àgil en quant a cost computacional [http://diccionario.raing.es/es/lema/coste-computacional], és a dir, hardware, software i manteniment. Els detalls d'aquest sistema, emmarcat dins del projecte de recerca Criptografia i codis per a aplicacions segures i fiables finançat pel ministeri de Ciència i Innovació, els han publicat la revista *International Journal of Information Security* .

Les aplicacions de mòbil actuals permeten el pagament de la zona blava de manera automàtica a través de targeta de crèdit o descomptant l'import d'un saldo previ. Podem ampliar el període d'estacionament sense desplaçar-nos i algunes, fins i tot, ens retornen els diners sobrants en el cas que l'estada duri menys temps de l'indicat a l'inici. "Malauradament, aquesta automatització implica que el proveïdor del servei disposa d'un sistema informàtic que recull tots els nostres estacionaments i que fa possible deduir informació confidencial sobre nosaltres com ara l'horari i lloc de treball, els moments en què ens desplacem a un centre de salut, o si freqüentem una delegació de caire polític o sindical, etc.", explica l'investigador del departament de Matemàtica de la UdL Ricard Borges.

La seua proposta es basa en que la informació gestionada pel sistema no permeti la creació de perfils de conductors."Val la pena destacar que molts cops sembla que la utilització de determinats serveis solament sigui possible després de renunciar a la nostra privadesa. El sistema desenvolupat en aquest treball és un exemple que demostra el contrari", afegeix l'altre autor de l'article, el professor de l'Escola Politècnica Superior de la UdL Francesc Sebé [http://www.eps.udl.cat/ca/info_sobre/pdi/francesc-sebe-feixas/].

Borges i Sebé han dissenyat un sistema que, mitjançant l'ús de la criptografia, garanteix que ni tan sols el proveïdor del servei pot obtenir cap informació personal sobre els seus usuaris, tret del moment de realitzar una inspecció presencial per un controlador de parquímetres. Llavors només pot saber si un client (cotxe) ha pagat per aquell instant de temps. No es pot obtenir cap més informació: ni l'hora d'inici d'estacionament, ni l'hora de fi prevista, ni els anteriors aparcaments.

La seua proposta requereix que els conductors estiguin connectats només al començament d'una transacció d'aparcament o en el moment d'indicar que l'estacionament ha estat més curt del previst. "Els experiments de prototipus han demostrat que aquest sistema és molt més eficient que altres, en termes de cost computacional, alhora que proporciona les mateixes funcionalitats i una major seguretat, assegura Ricard Borges.

En cas de rebre una multa injusta, el conductor podrà demostrar criptogràficament que ha realitzat el pagament de forma correcta per aquell instant de temps sense revelar cap més tipus d'informació addicional. "La utilització d'un sistema com aquest beneficia els ciutadans, ja que obtenen garanties tecnològiques de que ningú podrà esbrinar informació sobre la seua vida privada, i també per al proveïdor del servei, que no s'exposa a cap sanció ja que ningú el podrà acusar d'haver custodiat de manera inadequada una informació que no ha estat mai en el seu poder", destaca Sebé.

Aquest sistema desenvolupat per la UdL requereix l'aplicació de mòbil i un dispositiu d'identificació per radiofreqüència (RFID [https://ca.wikipedia.org/wiki/RFID]) que genera i emmagatzema un parell de claus, una privada i una pública. Només aquesta última s'envia a l'app, que connecta amb el servidor. Cada bitllet sol·licitat es paga a través d'un canal anònim per evitar el seguiment de les adreces IP.

"Els experiments sobre una implementació de prototips mostren que la nova proposta és més eficient, en termes de cost de càlcul", asseguren els investigadors. "Les noves eines sorgides d'aquest article ens permetran dissenyar protocols eficients i simples pel pagament de peatges garantint la màxima privacitat pels conductors", afegeixen.

MÉS INFORMACIÓ:

Article *An efficient privacy-preserving pay-by-phone system for regulated parking areas* [https://link.springer.com/article/10.1007/s10207-020-00527-2]