Sumar (limba română)

Teza curentă adresează eforturile noastre de cercetare din perioada 2010-2015 la Universitatea Politehnica Timişoara fiind focalizată pe construcţia de protocoale criptografice pentru securitatea reţelelor din vehicule (e.g., CAN bus) şi a diverselor componente automotive sau funcţionalităţi (e.g., senzori de monitorizare a presiunii în roţi, accesul la vehicule folosind telefoane inteligente). Aceasta constituie doar o parte a cercetărilor noastre în criptografie şi securitatea sistemelor din această perioadă, cercetare care a vizat diverse direcţii de la criptografie teoretică şi metode formale până la zone aplicative precum securitatea reţelelor şi a dispozitivelor mobile (acestea sunt pe scurt prezentate într-o secţiune dedicată unei priviri de ansamblu asupra rezultatelor autorului).

În anii recenţi a devenit din ce în ce mai evident că evoluţia vehiculelor se apropie de cea a calculatoarelor. Cu un secol în urmă, calculatoarele erau dispozitive pur mecanice, apoi ele au devenit dispozitive electronice complexe pentru ca astăzi să fie încărcate cu componente software a căror complexitate (posibil) depăşeşte complexitatea electronicii din fundal. Aceasta în nici un caz nu diminuează importanţa hardware-ului fără de care acestea nu ar putea funcţiona, dar deschide o nouă perspectivă pentru aplicaţii care au îmbunătăţit fabulos calitatea vieţii noastre. Similar, în deceniile anterioare, maşinile au devenit din dispozitive pur mecanice, dispozitive electronice complexe şi sunt încărcate cu sute de funcţionalităţi care rezidă pe duzini (chiar sute) de dispozitive miniaturale, numite ECU (Electronic Control Units), care sunt răspândite prin maşini şi conectate prin reţele interne complexe. Pentru a face lucrurile şi mai interesante din perspectiva securităţii, o parte din aceste reţele sunt expuse în exterior (i.e., către posibili adversari) prin canale cablate (e.g., port OBD) sau canale wireless (e.g., 3G, Bluetooth). Numărul de atacuri raportate a crescut drastic în anii trecuţi, lucrări recente arată cum atacatori pot bloca frânele, roţile sau motorul, asculta conversaţiile pasagerilor, etc., chiar şi de la sute de kilometrii distanţă. Peisajul sterp al securităţii maşinilor din trecut, dominat de infracţiuni minore (modificare kilometraj, furt de maşini, etc.) a început să devină fertil în anii recenţi, de îndată ce a devenit clar că adversarii pot prelua controlul unei maşini şi să o folosească după propria voie - toate acestea prin canale elctronice şi chiar de la distanţă.

Surprinzător, mecanismele de securitate sunt complet absente din magistralele de comunicaţii din vehicule, începând de la cele tradiţionale precum CAN (Controller Area Network) până la cele mai recente dezvoltări precum CAN-FD sau FlexRay. Aceasta se datorează multor provocări tehnice: lăţime de bandă scăzută, putere de procesare scăzută, margini de cost, standardizare lentă, etc. Lucrările noastre sunt focalizate pe construcţia unor protocoale de autentificare broadcast luînd în calcul cele mai promiţătoare trei tehnici: protocoale tip TESLA bazate pe lanţuri one-way şi sincronizare temporală, protocoale bazate pe distribuţia cheilor în sub-grupuri şi semnături one-time. În timp ce protocoalele de tip TESLA s-au dovedit a fi extrem de eficiente în reţele de senzori, acestea nu par să fie o alternativă bună

în automotive: întârzierile de autentificare trebuie păstrate cât mai mici şi aceasta duce la probleme de sincronizare, dacă creştem aceste întârzieri, ajungem la limitări de memorie deoarece cantităţi mari de date trebuie păstrate într-un buffer. Mai mult, încărcarea cu date a magistralei este sporită de eliberarea cheilor de sesiune. Cea mai promiţătoare metodă pare a fi gruparea cheilor pe sub-grupuri, i.e., LiBrA-CAN. Acest protocol este bazat în intregime pe primitive simetrice şi foloseşte două proceduri inovatoare: distributirea cheilor şi amestecarea MAC-urilor. În loc să axăm autentificarea independent pe fiecare nod (ce ar duce la un număr prea mare de chei) vom partaja cheile între grupuri de noduri ceea ce duce la un nivel de securitate mai ridicat în cazul în care nodurile corupte sunt în minoritate. Folosind argumente practice, această presupunere este demonstrabil corectă pentru reţele automotive. Mai departe, codurile standard de autentificare (MAC) sunt amalgamente folosind sisteme de ecuaţii liniare pentru a creşte şansele ca un fals să fie detectat. Prezentăm câteva variante de protocol care sunt flexibile şi deschid posibilitatea unor trade-off-uri între rata de date, încărcarea computaţională şi nivelul de securitate, luînd în calcul cele mai recente magistrale precum standardul CAN-FD sau FlexRay. Pentru a analiza eficienţa protocoalelor propuse acestea au fost testate pe microcontrollere de clasă automotive precum şi prin simulări folosind instrumente standard de simulare folosite în industrie. Prin folosirea CANoe a fost simulată utilizarea ratei de date pe magistrale state-of-the-art precum CAN-FD şi FlexRay. Rezultatele practice arată că intuiţia din comparaţia sintetică este corectă şi că alocarea cheilor pe grupuri este designul preferat de protocol.

Distanţându-ne de reţelele in-vehicle sunt atâtea alte subsisteme din automotive care sunt încă extrem de limitate în ceea ce priveşte funcţionalităţile de securitate, e.g., senzorii din roţi, chei wireless, etc. Mai mult, chiar şi în cazul componentelor care au funcţionalităţi de securitate, ameninţările sunt departe de a fi eliminate, e.g., falsificarea cheilor şi modificarea kilometrajului sunt încă probleme comune. În mod cert, un sistem nu poate fi mai sigur decât cea mai slabă verigă a sa şi trebuie să avem în vedere şi aceste componente. Aici rezultatele noastre sunt distribuite şi adresează câteva subiecte cum ar fi generarea numerelor aleatoare pe microcontrollere de clasă automotive, accesul la maşină folosind telefonul mobil şi securitatea senzorilor wireless. Vom prezenta contribuţiile noastre cele mai recente în securitatea intefeţelor wireless pentru senzori Tire Pressure Monitoring Systems (TPMS). Lucrările noastre au la bază construcţia unor protocoale de autentificare eficiente bazate pe designuri criptografice light-weight şi coduri de autentificare bazate pe coduri bloc simetrice, e.g., CBC-MAC. Rezultatele experimentale demonstrează că soluţiile propuse pot fi integrate în senzori din lumea reală si sunt mai eficiente decât cele propuse în alte lucrări. Lucrările legate de folosirea telefonului mobil pentru accesul maşinii şi generarea de numere aleatoare sunt lucrări rezultate din cooperarea recentă cu industria.