УДК 004.773

Ю.А. МОНАСТИРСЬКИЙ, д-р техн. наук, проф., І.В. ГІРІН, ст. викладач
Криворізький національний університет

ОСНОВНІ ВЛАСТИВОСТІ ЄВРОПЕЙСЬКОЇ КООПЕРАТИВНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТРАНСПОРТНОЇ СИСТЕМИ БЕЗПЕКИ

В доповіді хотілося б розповісти про європейську систему безпеки Кооперативної Інтелектуальної Транспортної Системи (C-ITS) - з чого вона складається, як працює, навіщо потрібна та які основні переваги має. Вже понад 10 років у ЄС активно працюють над розробкою європейських стандартів кооперативних інтелектуальних транспортних систем (C-ITS) або, як їх ще називають, V2X у Європейському Інституті Стандартизації Телекомунікацій (ETSI). Тут і ITS G5 – європейська адаптація IEEE 802.11p, і GeoNetworking та різні додатки, типу CAM, DENM та ін, та тестові специфікації. В цій системі цікавість з точки зору безпеки руху викликає один блок, який забезпечує взаємодію всіх інших блоків зверху донизу – система безпеки. Ось про нього то й поговоримо. У звичайному житті в інтернеті ми користуємося системою безпеки, яка базується на сертифікатах X.509, які нам розсилають сайти, щоб підтвердити, що вони ті, за кого себе видають. В архітектурі C-ITS система безпеки робить те саме: дозволяє одержувачу переконатися, що відправник повідомлення мав право його відправляти. Почнемо з того, навіщо це потрібне. Простий приклад: автомобіль розсилає повідомлення, що містять параметри цього автомобіля: тип, положення, швидкість тощо. Без системи безпеки нічого не заважає автомобілю підвищити свій статус на дорозі, наприклад, позначити себе автомобілем спеціальних служб. А що буде, якщо якийсь несвідомий водій почне надсилати повідомлення про фейкові автомобілі на дорозі або про неправильні сигнали світлофора? Отже, система безпеки повинна забороняти користувачеві робити те, що йому не дозволено. Далі - автомобіль спеціальних служб Німеччини не має пріоритету у Франції та навпаки. Отже, система безпеки повинна обмежувати користувача територіально. Більш детально всі ці вимоги викладені та зведені в систему в документі ETSI TR 102893 “Threat, Vulnerability and Risk Analysis (TVRA)”. Як це все реалізувати? Відповідь є: інфраструктура відкритих ключів (Public Key Infrastructure – PKI). Коротко, PKI є ієрархією сертифікатів, кожен з яких має публічний ключ та підписаний вищим сертифікатом. Поля вносять семантичну інформацію, ключ та підпис потрібні для валідації. Будь-хто, хто має доступ до сертифіката, може перевірити цілісність і підтвердити джерело інформації, підписаної цим сертифікатом. Така система верифікації давно винайдена: сертифікати X.509, які широко використовуються всюди у світі, мають широку підтримку, масу центрів, що засвідчують, з відповідним обладнанням і т.п. Але сертифікат X.509 – досить монструозна конструкція. І якщо при інтернет-з'єднаннях зайві 500 байт нас взагалі не хвилюють, то ITS G5 максимальна довжина пакета (MTU) обмежена 1492 байтами і ніякої фрагментації не передбачено. І ось у цей кошик треба покласти і корисну інформацію, і сертифікат із ключами, і підпис. До того ж автомобілі та об'єкти інфраструктури розсилають повідомлення щонайменше раз на секунду, а зазвичай ще частіше. І весь цей потік від усіх навколишніх автомобілів має поміститися в канал завширшки 20 МГц. Загалом, боротьба за розмір в цьому сенсі стає дуже важливою. І саме для мінімізації розміру в IEEE вигадали стандарт IEEE 1609.2. У ньому описані формати захищених повідомлень та сертифікатів, перераховані криптографічні алгоритми, що використовуються для перевірки підпису та кодування інформації. На сьогоднішній момент як алгоритми використовується криптографія на еліптичних кривих (ECDSA та ECIES). Підтримуються американські, європейські та китайські алгоритми. Сертифікати IEEE 1609.2 мають обмеження за часом, місцезнаходженням та дозволеними сервісами. Причому обмеження сертифікатів центрів (CA) повинні включати обмеження сертифікатів кінцевих пристроїв. Отримувати відповідні сертифікати необхідно у засвідчувальних центрів. Процес отримання сертифікатів поділений на 2 стадії – реєстрація та авторизація. І, відповідно, центри, що засвідчують, також розділилися на 2 категорії - Enrolment Authority (EA) і Authorization Authority (AA). Вся ця процедура описана в стандартах ETSI TS 102940 і ETSI TS 102941. Працює це таким чином: при виробництві автомобіль отримує ідентифікатор (canonical ID) та початковий сертифікат (Bootstrap certificate). Ця інформація відома EA. Далі автомобіль запитує і отримує сертифікат тривалої дії (EC), який потім використовується для отримання псевдоніма (AT) у AA. При цьому AA запитує EA дозволу на видачу сертифіката. І ось цей сертифікат AT, вірніше набір таких сертифікатів, які автомобіль постійно змінює, і використовується для підпису повідомлень, що розсилаються.